НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ “ВАСИЛ ЛЕВСКИ”

ФАКУЛТЕТ “АРТИЛЕРИЯ, ПВО И КИС”
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
ДЪРЖАВНА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Катедра “Информационна сигурност”

Н А У Ч Н А К О Н Ф Е Р Е Н Ц И Я 2 0 1 5

НОВИТЕ ПРЕДИЗВИКАТЕЛСТВА ПРЕД СИСТЕМИТЕ ЗА ИНФОРМАЦИОННА СИГУРНОСТ

СБОРНИК НАУЧНИ ТРУДОВЕ

ШУМЕН
2015

КЪМ ЧИТАТЕЛИТЕ ...

Сборникът научни трудове е съставен от докладите, изнесени на научна конференция на тема „Новите предизвикателства пред системите за информационна сигурност", проведена във Факултет "Артилерия, противовъздушна отбрана и комуникационни и информационни системи" към Националния военен университет "Васил Левски" - гр. Шумен, на 4 и 5 юни 2015 г.

Докладите са представени за издаване от авторите без допълнително редактиране от издателите. Отговорността за фактологическите, технически, езикови грешки и произтичащите от това последствия носят изцяло авторите.

Съгласно чл. 31 от Закона за защита на класифицираната информация авторите сами определят грифа за сигурност на докладите си и носят лична отговорност за публикуване на класифицирана информация в тях.

От редакционната колегия

©НВУ "В. Левски" – Факултет "Артилерия, ПВО и КИС"
Шумен, 2015.
c/o Jusautor, Shumen

ISBN 978-954-9681-65-9

СЪДЪРЖАНИЕ

ПЛЕНАРНА СЕСИЯ

М. П. Млеченков,

ОТКРИВАНЕ НА НАУЧНАТА КОНФЕРЕНЦИЯ
„Новите предизвикателства пред системите за информационна сигурност" – 4 юни 2015 г.

Уважаеми госпожи и господа,
Уважаеми господин Полковник,
Уважаеми офицери, курсанти, студенти, докторанти и специализанти,
Скъпи гости,

Добре дошли на деветата ежегодна научна конференция по проблемите на информационната сигурност, организирана от Националния военен университет „Васил Левски", факултет „Артилерия, ПВО и КИС" в Шумен и катедра „Информационна сигурност".

Иска ми се да започна с една мисъл на италианския държавник, историк и философ - Николо Макиавели, изказана в началото на 16 век:

"Не трябва да се забравя, че няма нищо по-трудно и по-съмнително по отношение на успеха от въвеждането на нови уредби. ... Не съществува нищо по-трудно от това да се поеме задължението за ръководство, или по-голяма несигурност в неговия успех, отколкото да се вземе инициатива за запознаване с новия ред на нещата."

Преди много хилядолетия, може би преди зараждането на човешката цивилизация, някакво събитие е програмирало любопитството и амбицията като онтологични свойства на човека. Именно тези свойства го изправиха в края на XX век пред предизвикателствата на вселената и го извадиха от сгушения, закътан свят на ранната индустриална ера. Отрекъл се от много догми, той създаде уникално по своята природа глобално информационно пространство от символи, идеи, концепции и модели и захрани двигателите на Земната цивилизация. Формира се нов ред на нещата.

Днес уникални нови виждания за бъдещото развитие на човешката цивилизация обещават да подобрят средата на нашето съществуване. Тези виждания имат потенциала да предизвикат глобални промени, които трябва да се анализират и прогнозират. Особена актуалност сред тях придобиха проблемите на информационната сигурност, превърнала се в един от основните проблеми на нашето време.

През последните години на XX век и първото десетилетие на XXI век сме сме свидетели на бурно развитие на комуникационните и информационните технологии. Развива се стремежа организации от различен вид да внедряват автоматизирани информационни системи и мрежи и да формират значителни масиви от данни.

Този факт поставя нови предизвикателства пред информационната сигурност, които могат да се обобщят по следния начин:

- Зависимостта от информационните системи и услуги прави организациите уязвими към нарастващите заплахи;
- Свързаността на мрежите и обмена на информационни ресурси затруднява намирането на правилните контроли за повишаване на сигурността;
- Много съществуващи системи не са проектирани да бъдат сигурни;
- Техническите решения за системите за сигурност са ограничени;
- Установяването на необходимите контроли за повишаване на сигурността изисква внимателно планиране и съобразяване с нуждите на бизнеса;
- Информационната сигурност се нуждае от подкрепата на всички служители, както и на клиенти, доставчици и партньори.

Основната цел на системите за информационна сигурност е да осигурят конфеденциалност, цялост и достъпност на информацията.

Основните заплахи за корпоративните инфраструктури са: вирусите; хакерски атаки; (D)DoS атаки; неоторизиран достъп до системите и данните; индустриален шпионаж; кражба на данни и информация и др.

Очертават се нови тенденции в заплахите към информационните системи:

- Заплахи към мобилни устройства – BYOD;
- Заплахи към облачни услуги;
- Целенасочени злонамерени атаки;
- Усъвършенстване на атаките от типа „social engineering";
- Атаки през социални мрежи.

Въпреки, че повече от 15 години с набор от международни стандарти са препоръчани изискванията към системите за управление на информационната сигурност, те слабо се познават и рядко се прилагат. ***Все още битуват погрешни възприятия като:***

- Информацията не е актив на компанията;
- Информацията ни не е подложена на риск;
- Нямаме нищо, което да бъде от полза на хакерите;
- Сигурността е твърде скъпа;
- Сигурността създава неудобства;
- Нямаме стимул за повишаване на сигурността.

Сигурността не е просто продукт, а процес който трябва постоянно да се управлява.

Доброволният сертификационен режим за организациите, предоставящи IT услуги у нас, не съдейства за внедряване и управление на ефективни системи за информационна сигурност. За липсата на фокус върху информационната сигурност се открояват следните симптоми:

- Липса на време за подобрение на сигурността поради пренатоварване с ежедневни операции на администрациите;
- Неточно документиране на процесите по защита на информационните активи;
- Наличие на голямо количество "shelfware" (асортимент от изделия);

- Закупуване на нови инструменти без оглед на изискванията за квалифициран персонал;
- Оплаквания от страна на бизнеса, че сигурността е пречка;
- Липса на фокусиране върху основни практики като защита на системите, управление на „кръпките“, управление на уязвимостите и др.;
- Неточни стратегиите и политиките за управление на сигурността.

Днес, когато информационната сигурност е ключов проблем, всички специалисти, работещи в областта на ***информационното противоборство, считат за тривиален и общоизвестен фактът, че успешните стратегии на поведение в информационните конфликти се градят на базата на информационно превъзходство в областта на знанията и културата***. За съжаление знанието, което специалистите считат за общоизвестно в своите среди и това, което е придобило публичност, са различни неща. Като правило, общественото съзнание изостава от достиженията на научната мисъл от 2 до 5 години. При сегашното състояние на нещата се отчита, че са прекъснати връзките между научните общности и практическите постиженията на отделните науки, с което те не могат да бъдат използвани като универсални инструменти.

Като отчитаме съвременната обстановка в информационната среда за сигурност и необходимостта от интердисциплинарен подход за издигане нивото на сигурност на информацията в корпоративните информационни системи и водени от стремежа да се ангажират широк кръг от експерти на национално и съюзно ниво, обявихме ***темата на конференцията*** за тази година: „НОВИТЕ ПРЕДИЗВИКАТЕЛСТВА ПРЕД СИСТЕМИТЕ ЗА ИНФОРМАЦИОННА СИГУРНОСТ”.

Поставяме си за цел да спомогнем за развитието, обогатяването и споделнето на знания, умения, практики и научни достижения в сектора за сигурност.

Основното предизвикателство пред съвременния дигитален свят е формирането на дигитална култура, базираща се на националните и международните норми, адекватна на постоянно еволюирашата среда за сигурност. Това е и нашия стремеж и в това направление сме насочили своите усилия за провеждане на научни изследвания и подготовката на кадри за сектор сигурност.

НОВИ НАПРАВЛЕНИЯ В РАЗВИТИЕТО НА КРИПТОГРАФИЯТА

Николай Т. Стоянов **Мая Г. Божилова**

ИНСТИТУТ ПО ОТБРАНА "ПРОФЕСОР ЦВЕТАН ЛАЗАРОВ" –
МИНИСТЕРСТВО НА ОТБРАНАТА
СОФИЯ, 1592, БУЛ. „ПРОФЕСОР ЦВЕТАН ЛАЗАРОВ" № 2

NEW DIRECTIONS IN THE CRYPTOGRAPHY DEVELOPMENT

Nikolai T. Stoianov **Maya G. Bozhilova**

DEFENCE INSTITUTE "PROFESSOR CVETAN LAZAROV" –
MINISTRY OF DEFENCE,
SOFIA, 1592, BLVD. "PROFESSOR CVETAN LAZAROV" 2

***ABSTRACT**: Cryptography is one of the most important parts of information security. Most of the asymmetric cryptographic algorithms are based on hard solved mathematical problems. With growing of computer operation speed and with availability of huge amount of computer memory some of these problems look to be solved in near time. In addition exploring physics and in particular developing of quantum computer will dramatically change world of cryptography. So called quantum algorithms of Shor and Grover are facts. These algorithms will break widely used asymmetric algorithms – RSA and Diffie-Hellman key-exchange. Beside this some groups of new algorithms are developed and they seem to be harder to solve with quantum algorithms (quantum computers). This paper presents an overview of four groups of algorithms forming so called post-quantum cryptography. Basic mathematical definition are given, explanation of hard mathematical problems which they are based and related cryptographic issue are shown. The most popular cryptographic scheme from each class is described.*

***KEY WORDS:** Post-quantum cryptography, Lattice-based cryptography, Hash-based cryptography, Code-based cryptography, Multivariate-quadratic-equations cryptography*

1. ВЪВЕДЕНИЕ

Непрекъснатото развитие на технологиите, доведе до пълна зависимост на всички сфери на човешката дейност от компютърни системи и мрежи. Осигуряването на сигурността на информацията в тези системите е решаващ фактор за успешното им приложение. Един от най-сериозните проблеми пред масовото навлизане на концепцията „Internet of things" в бизнеса и бита на съвременното общество е сигурността на комуникациите по Интернет.

Необходимостта дадена информация да е достъпна само за определени хора, датира от древни времена. Но докато дори и преди около 40 години, това е приоритет основно на военни организации и правителствени служби, на настоящия етап от развитието на компютърната техника и технологии, засяга все повече държавни и частни фирми и организации. Неправомерното разкриване, използване модифициране и разрушаване на информация може да се окаже с тежки не само икономически последици, но и със загуба на човешки живот.

Криптографията е основно средство за осигуряване на конфиденциалност, цялостност на данните, автентификация и контрол на участниците във комуникациите. Съвременната криптография включва два основни класа криптографски алгоритми – симетрични криптографски алгоритми и асиметрични криптографски алгоритми. При симетричните алгоритми се използва един и същи ключ за двете основни математически операции – криптиране и декриптиране, или двойка ключове, при които сравнително лесно може да се получи декриптиращият ключ от криптиращия ключ. Този тип алгоритми са известни още като алгоритми със секретен ключ.

При асиметричните криптографски алгоритми за операциите криптиране и декриптиране са необходими двойка ключове – частен и публичен. Изчислително трудно е да се получи частният ключ от публичния. Публичният ключ е общодостъпен и се използва за криптиране, но с него не може да се декриптира. Декриптира се с частния ключ, който е известен само на притежателя му. Този клас от криптографските алгоритми се нарича още криптографски алгоритми (криптография) с публичен ключ.

Едни от най-разпространените симетрични криптографски алгоритми в момента са: Data Encryption Standard (DES) 24, 3DES [24 и Advanced Encryption Standard (AES) 24. Сред най-приложимите асиметрични криптографски алгоритми са Rivest-Shamir-Dleman (RSA) 21, Elliptic curve cryptography (ECC) 13, 17, ElGamal 7.

Алгоритмите с публичен ключ са в основата на цифровия подпис, цифровите сертификати, банкови транзакции, виртуални частни мрежи, обмен на ключове за симетрични криптографски системи. Сигурността на посочените асиметрични криптографски алгоритми се основава на т. нар. трудно решими математически задачи. При RSA сигурността се базира на трудността да се разложи голямо цяло число (между 1024 и 2048 бита) на прости множители, а при ElGamal – на трудността да се изчисли дискретен логаритъм. Понятията „трудно решими“ и „изчислително трудно“ се разглеждат в контекста на теория на сложността на алгоритмите 4 и тук означават (неформално), че не съществува алгоритъм, който да дава решение за време, зависещо полиномиално от параметри на задачата . Когато такъв алгоритъм не съществува се казва, че задачата е в класа *NP*. Класът *NP* – това е класът от езици, разпознаваеми от недетерминирана машина на Тюринг за полиномиално време..

С появата и развитието на идеята за т.нар. квантов компютър се появиха и идеи и предложения (алгоритми) за решаване на някои от т. нар. трудно решими математически задачи, с които се поставят въпроси за бъдещето на криптографията с публичен ключ.

Квантов компютър

Квантовият компютър е машина, основана на квантовата логика, т.е. може да обработва информацията и да извършва логически операции в съответствие със законите на квантовата механика.

Елементарната единица за квантова информация е кубитът (квантовият аналог на бит) и един квантов компютър може да се разглежда като една многобитова система. Физически, един кубит (qubit) е система с две нива, подобно на двете състояния на спина на една частица със спин 1/2, на състоянията на вертикална и хоризонтална поляризация на един фотон или на двете нива на един атом.

Класическият бит е система, която може да съществува в две различни състояния, които се използват за представяне на 0 и 1, т.е. на отделна двоична цифра. Единствените възможни действия в такава система са тъждественост (0→0, 1→1) и *не* (0→1, 1→0). За разлика от това, един квантов бит (кубит) представлява квантова система с две нива, описвана в двумерно комплексно хилбертово пространство. В това пространство може да се избере двойка нормирани и ортогонални помежду си квантови състояния, наречени |0> и |1>, които представят стойностите 0 и 1 на класическия бит. Тези две състояния представляват основата за пресмятанията.

Съгласно принципа на суперпозицията, всяко състояние може да бъде представено във вида: $|\psi> = \alpha|0> + \beta|1>$, където амплитудите α и β са комплексни числа, удовлетворяващи условието за нормираност:

$|\alpha|^2 + |\beta|^2 = 1$.

Набор от n кубита е известен като квантов регистър с размерност n.

Докато състоянието на класическия компютър се определя чрез n бита на всички регистри, състоянието на квантовия компютър е суперпозиция от всички възможни състояния, т.е. 2^n за n кубитов регистър, т.е. за един такт квантовата операция може да изчисли 2^n машинни състояния наведнъж.

Когато се извършват пресмятания с класически компютър, различните входни данни изискват отделни действия. За разлика от това, един квантов компютър може да прави едновременно пресмятания с експоненциално растяща входна информация. Този голям паралелизъм е в основата на мощта на квантовите компютри.

Квантови алгоритми

Квантовият алгоритъм е последователност от действия изпълняващи се на квантов компютър. Всички задачи, които могат да се решат на квантов компютър, могат да бъдат решени и на класически компютър, но на квантовия компютър много от задачите се решават по-бързо. Мощността на квантовите компютри се дължи на квантовия паралелизъм, свързан с принципа на суперпозицията. Това означава, че квантовият компютър може да обработва едновременно голям брой класически входни данни. Същевременно обаче, не е лесно да се получи полезната информация от изходното състояние. Проблемът се дължи на факта, че в известен смисъл тази информация е скрита. Всяко квантово пресмятане приключва с проектиращо измерване в базиса на пресмятането. Резултатът от измерването е по принцип вероятностен и вероятностите за различните резултати се определят от основните принципи на квантовата механика.

Съществуват обаче квантови алгоритми, които ефективно извличат полезната информация. Известни квантови алгоритми, свързани с криптографията са алгоритъмът на Shor [11] за разлагане на големи цели числа на прости множители и алгоритъмът на Grover 8 за търсене в неструктурирани бази данни.

През 1994 г. Shor предлага квантов алгоритъм, който решава ефективно задачата за намиране на простите множители на едно сложно положително нечетно число N. Това е централен проблем в криптографията и се предполага (без да е доказано), че за един класически компютър е изчислително трудно да намери простите множители. Алгоритъмът на Shor решава успешно проблема за разлагане на прости множители с $O(n^2 log n log log n)$ елементарни квантови гейта, където $n = \log N$ е броят битове, необходими за записване на входната информация N. Следователно този алгоритъм осигурява експоненциално подобряване на скоростта за пресмятане, в

сравнение с известните класически алгоритми. Най-добрият класически алгоритъм, филтъра за полето на числа, изисква $\exp(O(n^{1/3}(\log n)^{2/3}))$ операции.

Сигурността на криптографската система RSA се основава на предположението, че не съществуват ефективни алгоритми за решаване на задачата за разлагане на прости множители. Следователно алгоритъма на Shor, ако се реализира от квантов компютър, ще компрометира тази криптографската система.

Grover 8 показва, че квантовите компютри могат да се използват и при решаване на проблема за търсене на един маркиран обект в неструктурирана база данни от $N = 2^n$. Най-доброто, което може да се направи с класически компютър, е да се търси в базата, докато се намери обекта. Това изисква $O(N)$ операции. Същата задача може да бъде решена от квантов компютър с $O(\sqrt{N})$ операции. В този случай подобрението в сравнение с класическите компютри е квадратично.

Квантовите алгоритми поставят важен въпрос пред криптографията и сигурността на информацията: „Сигурни ли са използваните днес криптографски алгоритми и до кога е възможно да бъдат прилагани за защита на информацията?“

2. НАПРАВЛЕНИЯ ЗА РАЗВИТИЕ НА КРИПТОГРАФИЯТА СЛЕД КВАНТОВИЯ КОМПЮТЪР

Въпреки че не е известно кога квантовият компютър ще бъде факт, изследователите в сферата на криптографията са изправени пред проблемите, които той поставя за бъдещето на системите с публичен ключ. Алгоритъмът на Shor ще направи неприложими традиционни криптографски системи като RSA [16], Digital Signature Algorithm (DSA) 7 и Elliptic Curve Digital Signature Algorithm (ECDSA) 12, но свърхбързите изчисления няма да са в състояние напълно да елиминират криптографията, като средство за сигурни комуникации и защита на информацията. Криптографски системи, работещи върху класически компютри, които са устойчиви на атаки с тези компютри и остават сигурни и при атаки с квантови компютри се наричат постквантови криптосистеми.

Съществуват класове криптографски системи, за които се смята, че ще се справят с проблемите, свързани с квантовите атаки 5, т.е. тези системи се класифицират като постквантова криптография:

- Криптография базирана на хеш (Hash-based cryptography) – Класическият пример е системата с публичен ключ за цифрово подписване с хеш-дърво на Merkle (Merkle’s hash-tree public-key signature system), която е изградена на идеята за еднократен подпис на Lamport и Diffie.
- Криптография, базирана на кодове (Code-based cryptography). – Класическият пример е криптографска система с публичен ключ на McEliece, основаваща се на код на Goppa (McEliece’s hidden-Goppa-code public-key encryption system).
- Криптография, базирана на решетки (Lattice-based cryptography) – Пример за криптографска система от този клас е NTRU (N-th degree truncated polynomial ring), разработена от трима математици: J. Hoffstein, J. H. Silverman и J. Pipher. Тя не е първата (исторически) появила се, но е най-известната и практически приложима криптосистема.

- Криптография, базирана на квадратични уравнения на много променливи (Multivariate-quadratic-equations cryptography) – Един от многото интересни примери е системата с публичен ключ за цифрово подписване "HFE^{v-}" (Hidden Field Equation) на Patarin, който обобщава предложението на Matsumoto and Imai (Patarin's "HFE^{v-}" public-key-signature system).

За криптографските системи, базиращите се на посочените подходи, не е известно ефективно приложение на алгоритъма на Shor, а при избора на дължина на ключа, трябва да се има предвид алгоритъма на Grover.

Естествено, предполага се, че симетричните криптографски системи (криптография със секретен ключ), ще продължат да се използват и след появата на квантовия компютър, като отново дължината на ключа трябва да се съобрази с алгоритъма на Grover.

2.1. Криптография базирана на хеш

Цифровото подписване е една от основните причини Internet и други информационни технологии да станат сигурни. С цифровия подпис се осъществява автентификация, интегритет и невъзможност за отказ от авторство при обмен на информация в компютърните системи и мрежи. На настоящия етап най-използваните алгоритми за създаване на цифров подпис са RSA, DSA и ECDSA, но както вече беше отбелязано, тези алгоритми ще станат несигурни в квантовата ера. Хеш-базираната схема за цифров подпис е интересна тяхна алтернатива. Като всяка друга система за цифров подпис и хеш-базираната използва криптографска хеш-функция. Тази схема за цифров подпис е сигурна, тогава и само тогава, когато хеш-функцията, на която се базира е свободна от колизии. Хеш-базираната схема за цифров подпис за първи път е предложена от Ralph Merkle 15. Той стартира с еднократни схеми за цифров подпис, в частност тази на Lamport и Diffie 14. Еднократните подписи са по-фундаментални. Създаването на еднократна схема за цифров подпис изисква само еднопосочна функция. Обаче тези схеми имат недостатъци. Една двойка ключове, състояща се от частен ключ за подпис и публичен ключ за проверка може да се използва за един документ, което е недостатък за много приложения. Идеята на Merkle е да използва хеш-дърво, което редуцира валидността на много еднократни проверяващи ключове (листата на хеш-дървото) към валидността на един публичен ключ (корена на дървото). Началната конструкция на Merkle не е достатъчно ефективна, сравнена например с RSA, но междувременно са направени много подобрения и в момента хеш-базираните подписи са най-конкурентните алтернативи на RSA и схемите за цифров подпис, основаващи се на елиптични криви.

Описание на Схемата за цифров подпис на Merkle (*Merkle Signature Scheme*)

Дефиниция 1: Нека X и Y са произволни множества. *Еднопосочна функция* (*one-way-function*) се нарича функция $f: X \to Y$, такава че е "изчислително лесно" да се пресметне $f(x)$, за всяко $x \in X$, докато за случайно $y \in Im(f)$ е "изчислително невъзможно" да се намери x, такова че $f(x) = y$.

Дефиниция 2: Криптографска хеш-функция (hash function) се нарича еднопосочна функция h, която изобразява редица (от битове) с произволна дължина в редица с фиксирана дължина n и притежава свойствата:

– за дадено съобщение m е „изчислително невъзможно“ да се намери друго съобщение n, такова, че $h(m) = h(n)$;

– „изчислително невъзможно” е да се намерят двойка различни съобщения m и m', такива че $h(m) = h(m')$.

Забележка: “Изчислително лесно” и „изчислително невъзможно” означават, че съществува, съответно не съществува алгоритъм, който решава задачата за време, зависещо полиномиално от нейни параметри.

Схемата за цифров подпис на Merkle (Merkle Signature Scheme – MSS) работи със всяка криптографска хеш-функция и със всяка еднократна схема за цифров

Нека g: $\{0, 1\}^* \rightarrow \{0, 1\}^n$ е криптографска хеш-функция. Предполага се, също, че е избрана еднократна схема за цифров подпис 3.

Генериране на двойка ключове

Подписващата страна избира $H \in N$, $H \geq 2$. Тогава двойката ключове, която ще бъде генерирана ще има възможност да подпише/провери 2^H документа.

Генерират се 2^H еднократни двойки ключове (X_j, Y_j), $0 \leq j < 2^H$. X_j е ключът за подписване, Y_j е ключът за проверка. X_j, Y_j – битови стрингове.

Листата на хеш-дървото на Merkle са хеш-стойностите $g(Y_j)$,), $0 \leq j < 2^H$. Възлите от следващите нива на дървото се изчисляват съгласно следното конструиращо правило: родителският възел е хеш-стойността на конкатенираните ляв и десен наследник.

MSS публичният ключ е коренът на хеш-дървото.

MSS частният ключ е последователността от 2^H еднократни ключове за подпис.

Алгоритъм за създаване на хеш-дърво

Входни данни
Височина H ≥ 2

Изходни данни
Корен на дървото на Merkle

---

1. За $j = 0, \ldots, 2^H$ се изпълняват следните действия:
   a. Пресмята с j-тото листо: $Node_1 \leftarrow Leafcalc(j)$
   b. Докато $Node_1$ има същата височина като най-горното листо на *Stack* се изпълнява следното
      i. Премахва се горното листо от стека:
         $Node_2 \leftarrow Stack.pop()$
      ii. Изчислява се родителския възел:
         $Node_1 \leftarrow g(Node_2||Node_1)$
   c. Поставя се родителския възел в стека: $Stack.push\ (Node_1)$
2. Нека R е единствен възел съхранен в стека: $R \leftarrow Stack.pop()$
3. Връща се като резултат R.

Генериране на подпис в MSS

Първо се изчислява n-битова хеш-стойност $d = g(M)$, на съобщението M. След това се генерира еднократен подпис на σ на d, използвайки s-*тия,* еднократен ключ за подпис X_s, $s \in \{0, \ldots, 2^H - 1\}$. Подписът ще съдържа този еднократен ключ за подпис и съответния му еднократен ключ за проверка Y_s. За доказване на автентичността на Y_s, в подписа се включват и индексът s, както и автентификационния път за ключа за проверка Y_s, който е последователността $A_s=(a_0,\ldots, a_{H-1})$ от възли в хеш-дървото. Това дава възможност на проверяващата страна да конструира път от листото $g(Y_s)$ до корена на хеш-дървото. Възелът h в автентификационния път е братът на възела от височина h, в пътя от листото $g(Y_s)$ до корена на дървото:

$$a_h = \begin{cases} v_h[s/2^h - 1], \text{ако } \lfloor s/2^h \rfloor \equiv 1 \bmod 2 \\ v_h[s/2^h + 1], \text{ако } \lfloor s/2^h \rfloor \equiv 0 \bmod 2, \end{cases}$$

за $h = 0, \ldots, H\text{-}1$. С v_h е означен възел на дървото с височина h.

Проверка на подписа в MSS

Проверката на подписа се състои от две стъпки.

В първата стъпка проверяващата страна използва еднократния ключ Y_s, за да провери еднократния подпис σ на хеш-стойността d, чрез средствата на проверяващия алгоритъм на съответната еднократна схема за подпис.

Във втората стъпка проверяващата страна валидира автентичността на еднократния проверяващ ключ Y_s, чрез построяване на пътя $(p_0, \ldots, p_H)$ от s-тото листо $g(Y_s)$ до корена на дървото. За целта използва индекса s и автентификационния път $(a_0,\ldots, a_{H-1})$ и прилага:

$$p_h = \begin{cases} g(a_{h-1} \parallel p_{h-1}), \text{ако } \lfloor s/2^{h-1} \rfloor \equiv 1 \bmod 2 \\ g(p_{h-1} \parallel a_{h-1}), \text{ако } \lfloor s/2^{h-1} \rfloor \equiv 0 \bmod 2, \end{cases}$$

за $h = 1, \ldots, H$ и $p_0 = g(Y_s)$. Индексът s се използва, за да се реши в какъв ред възлите от автенфикационния път и възлите върху пътя от листото $g(Y_s)$ до корена на хеш-дървото да бъдат конкатенирани. Автентификацията на еднократния проверяващ ключ Y_s е успешна тогава и само тогава, когато p_H е равен на публичния ключ.

2.2. Криптография базирана на кодове

Криптографските схеми базирани на кодове се разглеждат за първи път от Robert McEliece през 1978 г. В основата на този вид криптографски решения е идеята за използването на код, коригиращ грешки. В схемата на McEliece частният ключ е неразложим код на Гопа (Goppa code), а публичният ключ е случайна пораждаща матрица със случайна пермутация на този код. Криптираният текст е кодова дума, в която са добавени грешки и само притежателят на частния ключ (кода на Гопа) може да премахне тези грешки.

***Описание на криптосистемата на McEliece* 3:**

Дефиниция 3: Даден е полином на Goppa g(x) $\in GF(q^m)[x]$,
$\deg(g) = t$ и $L = \{\lambda_1, \ldots, \lambda_n\} \subset GF(q^m)$ с $g(\lambda_i) \neq 0$, за $i = 1, 2, \ldots, n$. Тогава

$\Gamma(L, g) = \{(c_1, \ldots, c_n)\} \in GF_q^n$: $\sum_{=1}^{n} \frac{c_i}{x - \lambda_i} = 0 \bmod g(x)\}$ е (класически) [n, k, d] код на Goppa.

Системни параметри:

$n, t \in N$, където $n \gg t$

Генериране на ключ:

На базата на параметри *n* и *t* се генерират следните матрици:

- *G: k*x*n* пораждаща матрица на код *G* над *F* с размерност *k* и минимално разстояние $d \geq 2t + 1$ (двоичен неразложим код на Гопа);
- *S: k*x*k* случайна, двоична неособена (обратима) матрица;
- *P: n*x*n* случайна пермутационна матрица.

Изчислява се *k*x*n* матрица G^{pub}=*SGP*.

Публичен ключ – (G^{pub}, *t*).

Частен ключ – (*S*, D_G, *P*), където D_G е ефективен декодиращ алгоритъм за *G*.

Криптиране ($E_{(G^{pub},t)}$):

За криптиране на съобщение $m \in F^k$ се избира случаен вектор $z \in F^n$ с тегло *t* и се криптира по следния начин:

$$c = mG^{pub} \oplus z$$

Декриптиране: ($D_{(S, D_G, P)}$)

За декриптиране на криптираното съобщение *c* първо се изчислява

$$cP^{-1} = mS\ G \oplus zP^{-1}$$

и се прилага декодиращ алгоритъм $D_G{}^{pub}$ за *G* към него. Тъй като cP^{-1} има разстояние на Хеминг *t* до *G* се получава кодовата дума:

$$mSG = D_G(cP^{-1}).$$

Нека множеството $J \subseteq \{1, \ldots, n\}$ е такова, че G_J^{pub} е обратимо. Тогава откритият текст *m* се изчислява като:

$$m = (mSG)_j (G_{.J})^{-1} S^{-1}$$

Към настоящия момент не са известни много практически приложения на този вид криптография, което се дължи най-вече на големия публичен ключ – от 100 Kbytes до няколко Mbytes.

2.3 Криптография базирана на решетки

Криптографските алгоритмите, базирани на решетки се основават на съществуващ от дълго време отворен проблем за класически изчисления 3. Прилагайки изчислително трудни задачи върху решетки, могат да се конструират устойчиви криптографски функции, така че криптографията, основаваща се на решетки да бъде сигурна и в квантовата ера.

Основни дефиниции

Дефиниция 4: Нека $n \in N$ и нека $b_1,...,b_n \in R^n$ са n линейно независими вектора, *решетка с размерност n*, генерирана от дадените вектори 16, 11 е множеството от вектори $L(b_1,...,b_n) = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in Z \text{ за } i=1, \ldots, n\}$ (1).

Множеството от вектори $b_1,...,b_n$ се нарича *базис* на решетката. Базисът на решетката може да се представи с матрицата $B = (b_1 \mid b_2 \mid ... \mid b_n) \in R^{n \times n}$, където векторите $b_1,...,b_n$ са колони в *B*. *B* е обратима матрица, т. е. $B \in GL_n(R)$. $GL_n(R)$ е групата от обратими матрици от ред *n,* с коефициенти от *R.*

Неформално, решетката е множество от точки в *n*-мерното пространство с периодична структура.

Дефиниция 5: Нека $q \in Z_+$. Решетка *L*, с размерност *n* се казва, че е *q-арна,* ако $qZ^n \subseteq L$.

Две основни *NP*-трудни задачи са свързани с решетките – за най-късия вектор (Shortest Vector Problem – SVP) 2 и за най-близкия вектор (Closest Vector Problem – CVP) 19:

- Задача за най-късия единствен вектор (SVP): Даден е произволен базис *B* на решетката *L*, да се намери най-късият единствен ненулев вектор в *L*(*B*);
- Задача за най-късите независими вектори (Shortest Independent Vectors Problem – SIVP): Даден е произволен базис *B* на решетката *L*, да се намери множество от най-късите линейно независими вектори в *L*(*B*).
- Задача за най-близкия вектор (CVP): Даден е произволен базис *B* на решетката *L* и целеви вектор t (не е задължително да е от решетката), да се намери точка от решетката $v \in L(B)$ най-близка до *t*.

Предполага се, че тези задачи са *NP*-трудни за решетки с голяма размерност и в квантовия и в класическия изчислителен модел.

Няколко алгоритъма, базиращи се на трудноразрешимите задачи за решетки са предложени за построяване на криптосистема с публичен ключ. Предизвикателството за изследване на тези системи, на първо място е необходимостта от крипто-

система, базираща се на различен тип математически проблем и на второ място – системите базиращи се на решетки са по-бързи от тези, основаващи се на разлагане на големи числа на прости множители или на дискретен логаритъм 10.

Исторически, първата базирана на решетка криптографска конструкция е представена от Ajtai and Dwork 1. Те създават криптосистема с публичен ключ, основаваща се на най-лошия случай на трудноразрешим проблем в решетката. Емпиричните резултати, получени в 18 показват, че криптосистемата на Ajtai-Dwork не е сигурна за $n \leq 32$. Това означава, че тя има само теоретична роля, докато не се открие съществено нейно подобрение.

NTRU (N-th degree truncated polynomial ring) е най-известната и практически приложима криптосистема, базирана на решетки. Алгоритъмът има комерсиално развитие и усилия за изработване на стандартизационни документи в работна група IEEE P1363.

NTRU е криптосистема, разработена от трима математици: J. Hoffstein, J. H. Silverman и J. Pipher, през 1996 г. 9. Тези математици, заедно с D. Lieman основават NTRU Cryptosystems, Inc. и патентоват криптосистемата. Криптосистемата NTRU се описва най-естествено чрез конволюционни пръстени от полиноми, но основният, трудноразрешим математически проблем може да се интерпретира като търсене на най-късия вектор или най-близкия вектор в специален тип решетка. Пръстените са алгебрични обекти, в които са въведени две операции, събиране и умножение, свързани чрез дистрибутивен закон.

Описание на криптосистемата NTRU

Дефиниция 6: Нека да изберем цяло положително число N. Конволюционен пръстен от полиними (от степен N) е пръстенът от частните $R = \frac{Z[x]}{(x^N - 1)}$. Аналогично, конволюционен пръстен от полиноми (по модул q) е пръстенът от частните $R_q = \frac{(Z/qZ)[x]}{(x^N - 1)}$.

Всеки елемент от R или R_q има единствено представяне във вида:

$a_0 + a_1x + a^2x^2 + \cdots + a_{N-1}x^{N-1}$,

с коефициенти от Z или Z/qZ, съответно.

Често е по-удобно полиномът $a_0 + a_1x + a^2x^2 + \cdots + a_{N-1}x^{N-1} \in R$ да се идентифицира с вектора от коефициентите си, т.е. с $(a_0, a_1, a_2, \ldots, a_{N-1}) \in Z^N$

и аналогично за полиномите от R_q. Събирането на полиномите, съответства на обикновено събиране на вектори:

$\boldsymbol{a}(x) + \boldsymbol{b}(x) \longleftrightarrow (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_{N-1} + b_{N-1})$,

Правилото за умножение в R се различава от стандартното умножение на полиноми.

Произведението на два полинома $\boldsymbol{a}(x)$ и $\boldsymbol{b}(x) \in R$ се дава с формулата:

$\boldsymbol{a}(x) * \boldsymbol{b}(x) = \boldsymbol{c}(x)$, където $c_k = \sum_{i+j \equiv k (mod\ N)} a_i b_{k-i}$,

където сумата, дефинираща c_k е за $\forall$ i и j между 0 и N-1, удовлетворяващи условието $i + j \equiv k (mod\ N)$. Произведението на два полинома $\boldsymbol{a}(x)$ и $\boldsymbol{b}(x) \in R_q$ се

получава по същата формула, с изключение на това, че стойностите на c_k се редуцират по модул q.

Дефиниция 7. Нека $a(x) \in R_q$. *Центрирано повдигане* на $a(x)$ към R е полиномът $a'(x) \in R$, удовлетворяващ $a'(x) \bmod q = a(x)$, чийто коефициенти са в интервала $-\frac{q}{2} < a'_i \leq \frac{q}{2}$.

Дефиниция 8. Нека d_1, $d_2 \in Z_+$. С $T(d_1, d_2)$ се означава:

$T(d_1, d_2) = \{a(x) \in R$: $a(x)$ има d_1 коефициенти равни на 1; $a(x)$ има d_2 коефициенти равни на -1; всички останали коефициенти на $a(x)$ равни на $0\}$. Полиномите в $T(d_1, d_2)$ се наричат *тернарни полиноми*. Аналогични са на двоичните полиноми.

Избор на публични параметри

Избират се публични параметри (N, p, q, d) с N и p прости, $gcd(p, q) = gcd(N, q) = 1$ и $q > (6d + 1)p$ 11. С $gcd(a, b)$ се означава най-големият общ делител на a и b.

Алгоритъм за генериране на ключове

1. Избира се случайно полином $f \in T(d + 1, d)$, обратим в R_q и R_p.
2. Избира се полином $g \in T(d, d)$.
3. Изчислява се $F_q(x)=f(x)^{-1}$ в R_q и $F_p(x)=f(x)^{-1}$ в R_p.
4. Ако $F_q(x)$ или $F_p(x)$ не съществува, то $f(x)$ се отхвърля и се преминава към стъпка 1.

Частният ключ се състои от полиномите $f(x)$ и $g(x)$. Частният ключ, който се използва, декриптиране на съобщения е двойката полиноми $(f(x), F_p(x))$.

5. Изчислява се полиномът $h(x)=F_q(x)*g(x)$ in F_q.

Полиномът $h(x)$ е публичният ключ.

Криптиране

1. Откритият текст е полиномът $m \in R_p$.
2. Избира се случаен полином $r \in T(d, d)$ (временен ключ).
3. Изчислява се $c(x) \equiv ph(x)*r(x)+m(x) \pmod q$.

Криптираният текст $c(x) \in R_q$.

Декриптиране

1. Изчислява се $a(x) \equiv f(x)*c(x) \pmod q$
2. Центрирано се транслира полиномът $a(x)$ към R и се изчислява полиномът $b(x) \equiv F_p(x)*a(x) \pmod p$

В 11 е показано, че ако параметрите са избрани подходящо, т.е. ако за публичните параметри е изпълнено $q > (6d + 1)p$, може да се смята, че полиномът $b(x)$ е равен на откритият текст $m(x)$.

Публичният и частният ключ на криптосистемата са полиноми, следователно могат да се представят с вектори, а векторите от своя страна – с вектори от n – мерна числова решетка. Такова представяне на криптосистемата е дадено в 16.

2.4. Криптография, базирана на квадратични уравнения на много променливи

В последните две десетилетия интензивно се изследват и развиват криптосистемите с публичен ключ на много променливи. Криптосистемата с публичен ключ на много променливи има открит ключ – множество от полиноми от втора степен над крайно поле. Основното допускане за сигурността й се основава на *NP*-трудността на задачата за решаване на нелинейни уравнения над крайно поле. Както твърдят Diffie и Hellman, една криптосистема с публичен ключ зависи от съществуването на клас еднопосочни функции със секрет (trapdoor one-way functions). Този клас и математическата структура, на която се основава, определят основните характеристики на криптосистемата. Например в основата на NTRU стои структурата на решетката. Криптографията с много променливи се базира на еднопосочна функция със секрет, която приема формата на система от полиноми от втора степен с много променливи над крайно поле. Публичният ключ, най-общо се задава чрез множество полиноми: $P = (p_1(w_1,..., w_n),..., p_m(w_1,..., w_n))$.

Обикновено, схемата с много променливи се строи от лесна за решаване система $Q(x)=y$, която след това се „скрива“ от две секретни случайни линейни (или афинни) трансформации: S: $w \to x$ и T: $y \to z$. Новата система P се получава композирайки (от ляво и от дясно) Q с S и T. Системата P е публичният ключ, оригиналната система Q и трансформациите S и T формират частния ключ.

По-точно, ако Q е дадена чрез m полинома (q_1,.., q_m) на (x_1,..., x_n), то новата система P се определя чрез полиномите (p_1,.., p_m) на (w_1,..., w_n), като:

(p_1, …, p_m)(w_1, … w_n) = T(q_1(S(w_1, … w_n)), …, q_m(S(w_1, … w_n)), където S и T са тайни случайни линейни (или афинни) биекции на променливите.

Новата система P:=ToQoS е също от втора степен

$$(P)\begin{cases} p_1(w_1,..., w_n) = z_1 \\ ... \\ p_m(w_1,..., w_n) = z_m \end{cases}$$

и намирането на решение за дадена m-орка (z_1, …, z_m) се очаква да бъде трудно без знания за S и T.

Съществуват няколко фамилии от схеми на много променливи, съответстващи на различни избори на системата Q. Някои схеми са били разрушени, а за други са приложени само общи атаки от тип базис на Грьобнер и параметрите им са избрани достатъчно големи, за да останат сигурни.

Описание на HFE схема за цифрово подписване **6**

Нека $F \cong F_q$ е крайно поле от ред q и K е разширение на F от степен n, *с “*каноничен“ изоморфизъм φ, идентифициращ K с векторното пространство F^n, т.е.

$F^n \xrightarrow{\varphi} K,\ K \xrightarrow{\varphi^{-1}} F^n$. Всяка функция или изображение F от K в K може да бъде изразена уникално чрез полином с коефициенти в K и степен $\leq q^n$:

$$F(X) = \sum_{i=0}^{q^n-1} a_i X^i,\ a_i \in K.$$

С $deg_K(F)$ се означава степента на $F(X)$, за кое да е изображение F. Използвайки φ, може да се построи ново изображение $F': F^n \to F^n$

$P(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)) = \varphi^{-1} \circ F \circ \varphi(x_1, \ldots, x_n)$, което е по същество F, но видяно от перспективата F^n. Може да се отъждествят F и F', освен ако съществува възможност за объркване.

Функцията F от втора степен или квадратичната F функция от K в K може в тази конструкция да бъде разгледана като полином, всичките едночлени, на който имат експонента $q^i + q^j$, или q^i и 0, за някои i и j. Общият вид на тази квадратичната F функция е $Q(x) = \sum_{i,j=0}^{n-1} a_{ij} X^{q^i+q^j} + \sum_{i=0}^{n-1} b_i X^{q^i} + c$, разширено полиномиално изображение на Dembowski-Ostrom. Такава $Q(X)$ с фиксирана ниска K-степен е използвана за построяване на криптосистемата с публичен ключ на много променливи:

$$Q(x) = \sum_{i,j=0}^{q^i+q^j \leq D,\ j \leq i} a_{ij} X^{q^i+q^j} + \sum_{i=0}^{q^i \leq D} b_i X^{q^i} + c.$$

Трябва да се отбележи, че коефициентите са стойности от K и всички $a_{ii} = 0$, ако $q = 2$, тъй като са включени в b-частта на коефициентите.

В 3 е направен преглед на съвременните криптосистемите с публичен ключ на много променливи, като са разгледани и общите модификации – „minus“, „internal perturbation“ и „vinegar“.

3. ЗАКЛЮЧЕНИЕ

Постквантовата криптография е перспективна област за изследвания, която се появява след публикуване на алгоритъма на Shor. Широко използвани системи, като RSA и El Gamal ще бъдат изцяло компрометирани в квантовата ера. Съществуват обаче, няколко направления за изследвания и развитие на криптографията, за които се предполага, че няма да бъдат засегнати от квантовите алгоритми: криптография със симетрични ключове (при условие, че дължината на ключовете се увеличи), криптография, основаваща се на решетки, криптография, базирана на кодове, крипрография на основата на хеш-функции и криптография, базирана на квадратични уравнения на много променливи. Прогнозите са, че изследванията в тези направления ще преминат към следващо ниво в следващите десетилетия.

ЛИТЕРАТУРА

1. Ajtai M. and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence, ACM, New York, 1999

2. Ajtai M. The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract). In roceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, 1998

3. Bernstein D., J. Buchmann, E. Dahmen, Post-Quantum Cryptography, Springer 2009, ISBN: 978-3-540-88701-0

4. Cormen, Th. et al., Introduction to Algorithms, MIT Press, 2nd edition, 2001.

5. Daniel J. Bernstein, „Introduction to post-quantum cryptography“, 2009; http://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf

6. Ding J. Bo-Yin Yang, Degree of Regularity for HFEv and HFEv-in P. Gaborit (Ed.): PQCrypto 2013, LNCS 7932, Springer-Verlag Berlin Heidelberg, 2013

7. ElGamal T., A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms; Advances in Cryptology – CRYPTO ’84, LNCS 196, Springer, 1985

8. Grover L.K., A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, 1996

9. Hoffstein J., J. Pipher, and J. H. Silverman. NTRU: a ring-based public key cryptosystem. In Algorithmic Number Theory, volume 1423 of Lecture Notes in Comput. Sci., Springer, Berlin, 1998

10. Hoffstein J., Lieman D., Pipjer J., Silverman J. NTRU: A public key cryptosystem. URL: http://grouper.ieee.org/groups/1363/lattPK/submissions/ntru. pdf.

11. Hoffstein J., Pipher J., Silverman J. An introduction to mathematical cryptography, Springer Science + Business Media, LLC, 2008

12. Johnson, D. and Menezes, A.: The Elliptic Curve Digital Signature Algorithm (ECDSA). Technical Report CORR 99-34, University of Waterloo, 1999

13. Koblitz, N. Elliptic curve cryptosystems, Mathematics of Computation 48, 1987

14. Lamport, L.: Constructing digital signatures from a one way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979.

15. Merkle, R.C.: A certified digital signature. Advances in Cryptology - CRYPTO ’89 Proceedings, LNCS 435, Springer, 1989.

16. Miccianco D., O. Regev, chapter Lattice-based Cryptography in Bernstein D., J. Buchmann, E. Dahmen Post-Quantum Cryptography, Springer 2009

17. Miller, V. Use of elliptic curves in cryptography, CRYPTO Lecture Notes in Computer Science 85, 1985

18. Nguyen P., J. Stern, Cryptanalysis of the Ajtai-Dwork Cryptosystem, vol. 1462 of Lecture Notes in Computer Science, Springer-Verlag, 1998

19. P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice, Technical Report 81-04, University of Amsterdam, Department of Mathematics, Netherlands, 1981

20. Patarin, J., Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In Advances in Cryptology — EUROCRYPT 1996, volume 1070 of Lecture Notes in Computer Science, Ueli Maurer, ed., Springer (1996). Extended Version: http://www.minrank.org/hfe.pdf.

21. Rivest R., A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of the ACM 21, 1978

22. Shor P., Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Symposium on Foundations of Computer Science, 1994.

23. Stoianov N., Bozhilova M., A Study of Lattice-based Cryptography, 5th International Scientific Conference on defensive technologies OTEH 2012, Belgrade, Serbia

24. Wang J. Computer Network Security, Theory and Practice, Higher Education Press, Beijing and Springer-Verlag GmbH Berlin Heidelberg, 2009

МЕТОДИ ЗА ПРЕВЕНЦИЯ И ЗАЩИТА НА АВТОМАТИЗИРАНИ ИНФОРМАЦИОННИ СИСТЕМИ ОТ КИБЕР АТАКИ

Димитрина Л. Полимирова

Национална лаборатория по компютърна вирусология – БАН,
София 1113, ул. „Акад. Георги Бончев“, блок 8, офис 104
dimitrina.polimirova@nlcv.bas.bg

METHODS FOR PREVENTION AND PROTECTION OF AUTOMATED INFORMATION SYSTEMS FROM CYBER ATTACKS

Dimitrina L. Polimirova

ABSTRACT: *In this paper main methods for prevention of AIS are discussed. They are commented in relation to: human factor, media, malware, electromagnetic emissions, network topology, DoS attacks, password and spam. Further, basic functions, tasks, elements and principles of methods for protection of AIS are also discussed. At the end the trends in the methods for prevention and protection are concluded.*

KEY WORDS: *Cyber Security, Information Security, Data Security, Cyber attacks, Methods of Prevention, Methods of Protection*

Еволюцията на компютърните и комуникационните системи, които извършват обработка на информационни потоци при определени изисквания по отношение на сигурността, се характеризира с многогодишна историческа битка между злонамереното и добронамереното мислене.

Престъпленията, извършвани в рамките на съвременната цивилизация по различно историческо време от представители на различни раси, националности, религии, социално положение, образование и др., се характеризират с определени особености, които се повтарят с устойчива последователност през вековете. Тези особености са свързани с няколко най-често срещани мотиви за извършване на престъпленията, между които вероятно най-често срещаният е присвояването с цел лично облагодетелстване.

Постигането на тази цел обикновено е съпроводено с определена подготовка, която включва натрупване на необходимата информация, планиране на определена поредица от действия, извършване на деянието, заличаване на евентуални следи и улики.

Обществото има добре развита система от институции, които извършват процесуално-разследващи и наказателно-репресивни действия като отговор на тези престъпления. Още при възникването и оформянето на информационната индустрия са възникнали и т.нар. информационни престъпления, които, макар и незначителни на пръв поглед, са носители на значителни финансови загуби, а това налага изграждането на система от наказателни мерки.

Киберпространството е възникнало като понятие през последните десетина години и представлява обобщен израз на изградената от съвременното общество информационна инфраструктура, включваща всички йерархични нива на съвременната глобална мрежа [1].

Престъпленията в кибер пространството имат своята сериозна история, която включва стотици разкрити и публично огласени и наказани извършители и, което е много по-важно в случая, десетки милиони неразкрити и ненаказани извършители.

Причините за това съотношение са много и най-различни, но доминиращото е особената невидимост на информационните престъпления, състояща се в това, че престъпление има, но извършител няма, тъй като доказателства за пряката отговорност се намират изключително трудно.

Известните и съответно изучени и класифицирани информационни престъпления са вероятно стотици, но само някои от тях е прието да се наричат кибер атаки.

Съдържанието, което се влага в този термин, не винаги отговаря на поредицата от планирани действия, извършвани от отделни лица или организирани групи, но това, което винаги присъства в подобни действия, е нарушаването на определени забрани, правила и граници със злонамерена цел.

Същността на кибер атаките се заключава в манипулиране на информационната среда, което включва операционната система, приложенията, мрежовите протоколи, транспортните протоколи, протоколите на процедурите за сигурност и др. по такъв начин, че се променя идентичността на отделния потребител, компютър или мрежа, заблуждава се насрещната страна за правомерността на определени действия, извличат се по нерегламентиран начин данни, чието използване носи преки финансови или морални загуби на физически или юридически субекти преодолявайки регионални, национални или глобални граници.

В най-общ план кибер атаките могат да се разделят на активни и пасивни [2].

Активните атаки съдържат в себе си определен сценарий, който предполага планиране и извършване на поредица от действия, свързани с промяна на определена програмна среда и нейните компоненти.

Пасивните атаки също съдържат в себе си определен сценарий, който включва предварително планирана поредица от действия, но този сценарий се отличава с това, че при него не се цели и не се постига промяна в програмната среда, а само се търси достъп до атакуваните ресурси и информационни потоци, като се реализира функцията наблюдение и анализ.

МЕТОДИ ЗА ПРЕВЕНЦИЯ НА АИС

Методите за превенция на автоматизирани информационни системи (АИС) могат да бъдат:

1) приложими към човешкия фактор

Методи за превенция, приложими *срещу нелоялни служители или консултанти.* Примери за такива мерки са ограничаване на достъпа до системата само за определено време и специфична задача, забраняване след края на задачата правата им за достъп и затваряне на временните им акаунти, ограничаване до минимум на отворените комуникационни линии за отдалечена поддръжка, засилване на бдителността и отговорността.

Методи за превенция, приложими *към лоялни служители или консултанти.* Въпреки лоялността на служителите е необходимо да се вземат мерки, свързани с непрекъснато обновяване на операционната система и на използвания софтуер, инсталиране и обновяване на защитни стени, инсталиране и обновяване на антивирусен софтуер, периодично преинсталиране на изпълнимите файлове.

Мерките за превенция трябва да бъдат взети и по отношение на *нелоялните и лоялни потребители.*

Мерките за превенция срещу нелоялни потребители включват:

- ✓ определяне на строги правила за достъп до информацията;
- ✓ инсталиране на система за идентификация и оторизиране;
- ✓ възприемане на правилото "двама души" при разрешаване на критични операции;
- ✓ строги правила по отношение на създаването на пароли;
- ✓ съхраняване на информацията за идентификация и оторизация на сигурно място;
- ✓ редовна проверка на логовете;
- ✓ редовна проверка на правилността на конфигурацията;
- ✓ инсталиране на система за откриване на проникванията (Intrusion Detection System).

Мерките за превенция към лоялни потребители включват:

- ✓ използване на алтернативни браузъри и приложения за електронна поща (e-mail clients) с по-висока сигурност;
- ✓ забрана за използване на програми от тип "peer to peer";
- ✓ забрана за посещаване на неблагонадеждните сайтове;
- ✓ забрана за инсталиране на непроверени и пиратски програми;
- ✓ забрана за кликване върху „изскачащи прозорци“ („pop up boxes“);
- ✓ забрана за инсталиране и използване на „безплатни“ („free“) програми.

И на края, но не на последно място, трябва да се коментират мерките за превенция по отношение *на лоялни и нелоялни системни администратори.*

Срещу нелоялните системни администратори е добре да се изградят отделни системи за развойната и за основната дейности. Освен това трябва да се ограничи достъпа до чувствителното оборудване. Не на последно място е необходимо да се ограничи използването на привилегиите на "super user"/"root".

Мерките за превенция в случаите на лоялни системни администратори включват:

- ✓ създаване на отделни акаунти за всеки потребител, ако един компютър се използва от повече от един човек;

- ✓ забраняване на инсталирането на софтуер от потребителите;
- ✓ забраняване на всички неизползвани услуги;
- ✓ блокиране на "pop ups", филтриране на "web bugs", реклами и бисквитки;
- ✓ блокиране на злонамерени сайтове и/или сървъри чрез използване на т.нар. хост (host) файлове (забраняващи достъпа до цитираните в тях сайтове) или чрез специализирани програми;
- ✓ използване на специализиран софтуер за предотвратяване инсталирането на шпионски софтуер (Spyware) и/или софтуер, свързан с реклата (Adware);
- ✓ намаляване получаването на нежелана поща чрез антиспам програми или чрез алтернативно приложение за електронна поща (Email client);
- ✓ тестване сигурността на системата чрез използване на специални инструменти за проверка на нивото на инсталираните кръпки и откриване на дупки в сигурността, причинени от лошо конфигуриране;
- ✓ отделяне на критичните хостове и поддържаните отдалечено системи в отделни мрежи с много строги ограничения и правила за достъп;
- ✓ насърчаване и изискване (чрез съответни правила и процедури) на сигурно предаване на данни, автентификация и методи за отдалечен достъп до мрежата, като SSH, SSL, VPN;

2) **приложими към носители.** Тук трябва да бъдат предвидени мерките срещу кражба, копиране/прехвърляне на данни от носителите, физически дефект/умишлено разрушаване на носителя и не бива да се забравят случаите на копиране/прехвърляне на данни при сервизно обслужване;

3) приложими към злонамерен софтуер. Включва се освен отделните групи злонамерен софтуер и съответните им разновидности, така и групи злонамерени атаки. Средствата за превенция и процедурите за сигурност трябва да се прилагат и към компютърното оборудване и към софтуера, които са в процес на разработка или тестване [3];

4) **приложими към електромагнитни емисии.** Методите *срещу прихващане на екранна информация* включват използване на защитени (екранирани) помещения, използване на оптични връзки, кодиране на информацията. Методите *срещу прихващане на кабелна информация* включват: кодиране на трафика, сегментиране на трасетата и редовно инспектиране на трасетата в мрежата;

5) приложими към преносими устройства. Тук методите обхващат случаите при непозволено използване на устройствата и случаите на кражба;

6) приложими към мрежова топология. Трябва да се вземат мерки срещу манипулиране на мрежовите компоненти;

7) **приложими към DoS, DDoS атаки.** Превенцията на този тип атака е изключително трудна, тъй като засяга и затворени портове, приема различни форми, насочена е към много услуги и устройства, може да бъде предизвикана и от легитимни пакети, ако те създават рекурсивен ефект, например отваряне на множество едновременни връзки;

8) приложими към пароли. Превенцията е свързана със създаването на строги правила при създаване, съхраняване и споделяне на пароли;

9) приложими съм нежелана поща (Spam). Блокирането на нежеланата поща може да се извършва на пощенския сървър или на компютъра на крайния потребител, като се използват два основни метода: черни списъци и филтриране на съдържанието.

МЕТОДИ ЗА ЗАЩИТА НА АИС

Основни функции

Проблемът за абсолютна защита от злонамерен софтуер и кибер атаки е принципно нерешим, но осигуряването на безопасността на информацията в една компютърна система трябва да:

1) гарантира защита от проникване. Защита, непозволяваща изтичане на информация от корпоративната мрежа по каналните връзки;

2) гарантира недосегаемост на ресурсите и неприкосновеност на информацията. Защита на най-критичните ресурси на мрежата от вмешателство в нормалното й функциониране;

3) гарантира криптографска защита. Защита чрез криптиращи програми на най-важните информационни ресурси.

Основни задачи

Защитата на сигурността на една организация трябва да изпълнява следните задачи:

1) възможност за идентифициране на атаката. Да идентифицира и контролира поведението на злонамерения софтуер;

2) възможност за въздействие на атаката. Да печели време, което да позволи събирането на допълнителна информация за атаката;

3) възможност за откриване на атаката. Да позволява навременно откриване и проследяване на опитите за атака;

4) възможност за отразяване на атаката. Да е насочена както към външните атаки, така и към вътрешните дупки в сигурността;

5) възможност за прозрачна работа. Да допълва конвенционалните системи без да нарушава работата на съществуващите бизнес инфраструктури.

Основни елементи

Методите за защита на една компютърна система включват следните основни елементи:

1) анализ на заплахите. Определя нивото и типовете атаки, които могат да бъдат очаквани, и подходящите средства за защита от такива потенциали атаки;

2) контрол на достъпа. Установява механизмите за гарантиран достъп до мрежата само на упълномощените потребители. Обикновено контролът на достъп се разработва на няколко нива и използва пароли, биометрични методи и др.;

3) автентификация. Верифициране от страна на системата на самоличността на потребителя. Осъществява се чрез прости методи, като обратно повикване, или чрез усъвършенствани - електронен подпис.;

4) конфиденциалност. Тук се определят методите за постигането й по време на комуникацията (обикновено чрез кодиране);

5) интегритет на данните. Постига се чрез валидиране на контролни суми или хеш функции;

6) невъзможност за отричане. Приемащата страна не може да отрече осъществяването на разрешена комуникация;

7) готовност за работа и надеждност на системата. Анализ и избор на филтри и други средства за защита от атаки.

Основни принципи

Основните принципи при планирането на защитата са:

1) най-малки привилегии. Нивото на достъп на потребителите е минималното необходимо за осъществяване на служебните им задължения;

2) изграждане на защита в дълбочина. Едновременно използване на няколко защитни техники;

3) разнообразие на защитата. Използване на различни защитни средства.

4) отказ по подразбиране. Отказване на достъп при възникване на съмнителни ситуации;

5) сигурност чрез неяснота. Използваните средства за защита трябва да са възможно най-незабележими.

ТЕНДЕНЦИИ

Относно методите за превенция и защита

Създаването на високоефективни методи за превенция и защита е съпроводено със значителни трудности, които са породени от силната недетерминираност и хетерогенност на средата, ненадеждни, но исторически обвързани изисквания за съвместимост, участието на човешкия фактор, който внася значителна нестабилност във всяко ново или старо решение, критичната липса на стандартизация в много от управляваните ресурси.

Използването на съществуващите методи е съпроводено с големи пречки, които се дължат на финансови и корпоративни противоречия, сравнително високата нелегитимност на масовите използвани решения и недостатъчната квалификация на участващите в този процес.

Относно средствата за превенция и защита

Разработването на средства за превенция и защита е съпроводено със значителни трудности, които са породени от твърде бързото развитие на технологиите и недостатъчната възможност да се обхванат възможностите за атака, корпоративни интереси, които не допускат пълното публикуване на определени формати и спецификации, необходимостта от финансови разходи, които не винаги са възможни и желани.

Прилагането на съществуващите средства е спъвано от някои пречки, които са породени от необходимостта от допълнителни финансови разходи и от допълнителна квалификация на потребителите, липсата на необходимата дисциплина и загриженост от страна на ръководството както и разпространеното мнение "това няма да се случи точно на мен".

ЛИТЕРАТУРА

1. http://techterms.com/definition/cyberspace, (последно посетен на 27 април 2015)

2. Solange Ghernaouti-Helie, *Cyber Power: Crime, Conflict and Security in Cyberspace*, CRC Press, 2013, ISBN 146657304X, p. 206

3. Gráinne Kirwan, Andrew Power, *Cybercrime: The Psychology of Online Offenders*, Cambridge University Press, 2013, ISBN 1107004446, pp. 96-97

ЧОВЕШКИЯТ ФАКТОР И ИНФОРМАЦИОННАТА СИГУРНОСТ

Васил Ст. Ризов

гр. София 1505, ул. „Черковна“, № 90, Държавна комисия по сигурността на информацията, ел. поща: dksi@government.bg; vsrizov@abv.bg

THE HUMAN FACTOR AND INFORMATION SECURITY

Vasil St. Rizov

ABSTRACT: *The report analyzes the problem with the shortage of qualified specialists for the information security and proposes some possible ways to solve it.*

KEY WORDS: *information security, cybersecurity, human resources, e-Skills*

Целта на информационната сигурност е да защити и гарантира непрекъснатост, цялостност и автентичност на информацията, с която работи една организация и нейните партньори, както и да сведе до минимум щетите от нерегламентиран достъп до системите за обработване, съхранение и пренос на тази информация.

Проблемите пред информационната сигурност най-общо могат да бъдат разделени на такива, отнасящи се до технологиите, организацията или хората. Тези, които са свързани с хората, обикновено се отнасят до недостиг на знания, умения или съзнание за сигурност.

Едно от основните предизвикателства пред системите за информационна сигурност е именно недостигът на знания и умения в хората, които ги експлоатират или погледнато от друга перспектива, недостигът на квалифицирани специалисти за изпълнение на все по-разнообразните задачи в тази област.

В настоящото изложение ще се спра на основните аспекти на този проблем, като опиша основните му характеристики; ще се мотивирам защо считам, че това е проблем пред държавата и бизнеса; ще разгледам какви са предизвикателствата и възможностите пред обучаващите и образователни институции; ще очертая накратко възможни пътища за неговото решаване.

Непрекъснато развиващите се заплахи от инциденти в системите за информационна сигурност не само ни изправят пред нови предизвикателства, но и разкриват нови възможности. Притежаването на умения и способности за успешно противодействие на тези заплахи може, ако не да предотврати, то да намали значително причинените от тях финансовите загуби, а също и да увеличи доверието на потребителите и клиентите, осигурявайки на бизнеса в тази област значително конкурентно предимство.

В началото на 21-ви век способностите на организациите да се конкурират и развиват, зависят все по-силно от иновативния и ефективен начин на използване на новите информационни и комуникационни технологии (ИКТ). В същото време инцидентите в областта на информационната сигурност, причинени от човешки грешки, природни явления, технически повреди или злонамерени атаки стават все по-чести, по-мащабни и по-сложни.

Новостите в областта на информацията и мрежите (включително облачните услуги, голямото количество данни, социалните медии, мобилният интернет и конвергенцията) създават необходимост от нови умения и огромни възможности за тези, които ги овладеят първи.

Тъй като държавата и бизнесът ще продължават да предприемат стъпки, за да повишават своето ниво на защита срещу кибер атаки, нуждата от продукти и услуги в областта на информационната сигурност ще продължава да расте, предоставяйки все по-разнообразни възможности за тези, които могат да ги предоставят. Подготовката и развитието на високо квалифицирани специалисти в тази област ще даде възможност както на публичните, така и на бизнес организациите, предоставящи такива продукти и услуги да извлекат максимални ползи от тези нови възможности.

В контекста на тези нови възможности, през последните години прави впечатление, че въпреки високите равнища на безработица в света като цяло, недостигът на лица, притежаващи електронни умения, продължава да се увеличава във всички сектори. Несъответствието между наличните умения и нуждите на пазара на труда засяга всички държави, макар това да им влияе в различна степен. Тази световна тенденция важи с пълна степен и за европейските държави, въпреки полаганите усилия и иницииране на нови програми в областта на заетостта, както в съюзен, така и в регионален и национален мащаб.

През септември 2007 г., след обширни консултации и дискусии със заинтересованите страни и държавите членки на ЕС в контекста на европейския форум за електронни умения, Европейската комисия прие съобщение относно „Електронните умения за 21-ви век: насърчаване на конкурентоспособността, растежа и заетостта", което включва дългосрочна стратегия за електронните умения в Европа. Тази стратегия беше приветствана от страните членки в заключенията на Съвета по конкурентоспособност от ноември 2007. Заинтересованите страни, също така, приветстваха дългосрочната програма за електронни умения. ИКТ индустрията създаде Ръководен съвет на промишлеността по електронни умения, който да допринесе за изпълнението на стратегията. [1]

Проучване в тази област посочва, че националните политики за развитието на информационните технологии (ИТ) акцентират предимно върху развитието на основни ИТ умения. Развитието на по-напреднали ИТ умения често се смята за част от професионалното образование.

Резултатите от проучването показват, че девет страни имат политики, насочени към развиването на електронни бизнес умения. Двадесет и шест страни имат политики за електронни умения, предназначени за обикновените потребители, докато единадесет държави (Дания, Франция, Германия, Унгария, Ирландия, Малта, Испания, Португалия, Румъния, Великобритания и Турция) имат политики насочени към развитието на електронни умения сред специалистите. Проучването идентифицира общо четиридесет и пет инициативи, специално насочени към развитието на специализирани ИТ умения.

Последните проучвания в областта на пазара на труда в Европа показват, че нуждите от ИКТ специалисти нарастват с много по-високи темпове от възможностите за тяхната подготовка и обучение. Забележителното е, че търсенето на ИКТ специалисти, което нараства с 4% всяка година, в последните десетина години непрекъснато надвишава предлагането. Според прогнозите, до 2015 г. броят на

незаетите работни места ще достигне близо 500 000, като много от тях ще останат трайно незаети, освен ако не бъдат положени повече усилия за привличането на млади хора в компютърни специалности и за преквалифицирането на безработните, и насочването им в тази област. [2]

През 2012 г. Европейската комисия официално прие Програмата в областта на цифровите технологии за Европа („Digital Agenda for Europe“) и очерта седем приоритетни области за действие: изграждане на единен дигитален пазар, по-голяма оперативна съвместимост, увеличаване надеждността и сигурността на интернет, много по-бърз интернет достъп, повече инвестиции в научноизследователската дейност, подобряване на дигиталната грамотност и приобщаването, прилагане на ИКТ за справяне с предизвикателствата, пред които нашето общество е изправено (като климатични промени и застаряващо население). Примери за ползите от това включват по-лесно фактуриране и заплащане по електронен път, по-бързо внедряване на телемедицината и енергийно ефективно осветление.

Програмата предвижда Европейската комисия да:

- насърчи електронното управление и ИКТ професионализма, за да повиши броя на квалифицираните кадри в Европа, както и компетенциите и мобилността на ИКТ специалистите в цяла Европа;
- подкрепи разработването на онлайн инструменти за определяне и разпознаване на компетенциите на ИКТ специалистите и потребителите, съобразно Европейската рамка за електронни компетенции и системата Европа (EUROPASS);
- насърчи по-голямото участие на жените в ИКТ работната сила;
- направи дигиталната грамотност приоритет за Европейския социален фонд (2014-2020);
- предложи показатели за дигиталните компетенции и медийната грамотност в рамките на ЕС. [3]

За постигане на тези цели се очаква държавите членки да реализират дългосрочните политики за електронни умения и дигитална грамотност и да включат електронното обучение в политиките за модернизация на образованието и обучението, включително учебните планове, професионалното развитие на учителите и преподавателите и оценката на резултатите от обучението.

Прегледът на състоянието на ИТ сектора в Европа показва, че ИТ индустрията в ЕС продължава да отбелязва ръст от около 4 – 6% всяка година. Според експертни проучвания големите софтуерни компании в Европа отчитат ръст на приходите между 5% и 15%. Очаква се Европейският софтуерен пазар да продължава да се увеличава. В същото време професиите в сферата на ИКТ - програмисти, проектни мениджъри в ИТ, специалисти по обработка на данни, са на второ място по дефицит на кадри в Европа след медицинските професии – сестри, фармацевти, лекари. След тях са инженерите, търговските представители и счетоводителите.

През миналата година беше публикуван секторен анализ за сектор „Информационни технологии 2013“, подготвен по проект „Разработване и внедряване на информационна система за оценка на компетенциите на работната сила по браншове и региони”, който беше осъществен в периода 2009-2013 г. от Българска стопанска камара - съюз на българския бизнес (БСК).

Целта на секторния анализ за сектор „Информационни технологии 2013“ е да се представи реален и обективен анализ на последните налични данни за развитието на сектор „Информационни технологии“, на текущите тенденции, проблеми и

потребности в този бранш. Акцентира се върху работната сила и тенденциите, свързани с нейното развитите. Представени са данни за развитието на сектора в България и мястото на сектора в икономиката на ЕС. [4]

В ЕС се очертава ясна тенденция за намаляване на броя на завършилите висше образование в областта на компютърните технологии, както като абсолютен брой, така и като относителен дял спрямо всички завършили висше образование. През 2011 г. в сферата на компютърните технологии са завършили около 128 000 студенти, което е съизмеримо с броя на завършилите през 2003 г.

Според ЕК броят на хората, които ще се пенсионират в сектора на ИКТ, ще нарасне от около 90 000 души годишно през 2012 г. до около 120 000 души годишно през 2015 г. – увеличение с около една трета. Според Cedefop (Европейския център за развитие на професионалното обучение) търсенето на специалисти, занимаващи се с компютърни технологии на ниво ЕС, ще расте по-бързо от всички останали професии – очакванията са за ръст на броя на заетите от около 13% през 2020 г. спрямо нивата от 2010 г. (средният очакван ръст за всички други професии за същия период е 3%). Според последните данни на ЕК в сферата на компютърните технологии всяка година се откриват над 100 000 нови работни места.

В резултат на очертаните тенденции и при запазване на настоящите темпове на развитие очакванията на ЕК са за около 900 000 незаети работни места в ИКТ сектора на Европа през 2015 г., като около 300 000 от тях ще бъдат в сферата на компютърните технологии.

Основни изводи и тенденции за сектора в ЕС:

- Дефицитът на кадри в ИТ индустрията е на европейско ниво – недостигът е повсеместен. От тази гледна точка, колкото и кадри да се създадат от българската образователна система, щом са на необходимото ниво, то те лесно ще намерят реализация на отворения европейски пазар на труда.

- Софтуерната индустрия ще продължи сериозния си ръст, като очакванията са темповете на растеж да се запазят в средносрочен план.

- Огромната част от ИТ предприятията са микро предприятия (до 10 заети лица), като значителна част от тях представляват отделни ИТ специалисти.

- Намаляване на завършващите висше образование в сферата на компютърните технологии, природните науки и математиката, съчетано с тенденция за увеличаване на броя на хората, които се пенсионират.

- Младежката заетост в сферата на ИТ намалява за сметка на хората в зряла възраст.

- Фокусът на софтуерната индустрия през следващите години ще бъде върху облачните услуги (Cloud Services), софтуера като услуга (SaaS), мобилните приложения (Mobile), големите данни (Big Data) и социалния елемент (Social).

Ако в други отношения с основание да казваме, че нашата страна все още не е достигнала по-напредналите си партньори в ЕС, то по отношение нуждата от ИКТ специалисти, съвременните европейски тенденции са силно изразени и у нас. И това се отнася не само до все по-острата нужда от такива специалисти, но и до бавното настройване на обучаващите и образователни институции към специфичните нужди на бизнеса. Към широкия кръг от причини за недостиг на такива умения бих добавил бавното развитие на информационната сигурност като специалност и обособяването ѝ като професия, намаляващата степен на застъпеност на

математически и инженерни специалности в образованието и все още слабия интерес на жените към реализация в тази област.

В този смисъл от изключително голямо значение и за държавата, и за частният сектор е да стимулират развитието и инвестициите в информационната сигурност. Ето защо ние трябва да продължаваме да насърчаваме подобни инициативи и да привличаме в тях не само правителствени институции и академичната общност, но и представители на бизнеса в тази област. Само така ще можем да сме сигурни, че уменията и способностите, които развиваме, са насочени към нуждите на реалния живот, ще гарантираме успешна защита от кибер заплахи, намалени загуби на ресурси и не на последно място – успешна реализация на готвените от нас специалисти.

През месец април тази година в София се проведе кръгла маса на тема „Предизвикателства пред пазара на труда в България: ролята на уменията и компетенциите“. Събитието се организира от Българската стопанска камара съвместно с Институт „Отворено общество“ – София и Световната банка. Представители на Световната банка, държавната администрация, изпълнителни директори и секторни асоциации, социални партньори, академична общност, мениджъри „Човешки ресурси“ от водещи компании, както и агенции за подбор на персонал направиха преглед на състоянието и предизвикателствата, пред които е изправен българския трудов пазар и проведоха дискусия за възможностите за преодоляване на съществуващото разминаване между търсене и предлагане на умения на пазара на труда. По време на форума бяха представени данните от национално представително панелно проучване за България - Bulgarian Longitudinal Inclusive Society Survey (BLISS), проведено от Световната банка в партньорство с Институт Отворено Общество – София.

Проучването отчита, че работодателите са загрижени за подготвеността на наличната работна сила в България. Тя е най-сериозна в сектора на информационните технологии и в някои сектори на производството, а образователното равнище на работниците се поставя на 4-то място по важност от работодателите у нас. Изследването на познавателните и социално-емоционални умения показва още, че България е сред страните с най-високо ниво на функционална неграмотност по математика. В същото време едва 7% от българите са участвали в обучение за повишаване на квалификацията.

Изследването отчита и положителни резултати - българите искат обучение и биха се възползвали от него, ако им бъде предоставено. Що се отнася до видовете обучение, младите искат да получат нова квалификация или специализация, а повъзрастните – да усъвършенстват уменията си.

Според данни на НОИ, ИТ секторът осигурява работа на близо 40 000 души, като той е силно концентриран – малко големи компании, в които работят преобладаващата част от заетите лица. Извън тази статистика остават т.нар. фрилансъри или заетите на свободна практика, които най-често намират своите ангажименти в специализирани интернет платформи за посредничество между търсещи и предлагащи работа на свободна практика.

В цитираният по-горе анализ за сектор „Информационни технологии 2013“ , са направени следните основни изводи и тенденции за сектора в България:

- Секторът е един от малкото в индустрията на България, останали почти незасегнати от икономическата криза.

- ИТ секторът в България се представя отлично във всички ключови аспекти и има значителен потенциал за иновации и експортно-ориентиран растеж.

- Общият брой заети в сектора е едва 1% от общия брой заети лица в България. Въпреки това секторът генерира 3% от БВП на страната, което го определя като един от тези с висока добавена стойност.

- Сред значимите компании в бранша започват да се нареждат не само чуждестранни аутсорсинг компании, но и местни представители със своите иновативни продукти и успешни бизнес модели, което говори за изкачване на местния ИТ бизнес по веригата на добавената стойност.

- Въпреки икономическата криза през последните години работодателите в ИТ сектора продължават да наемат персонал, като средното месечно възнаграждение в бранша непрекъснато се повишава.

- Прогнози на БАСКОМ сочат, че при среден растеж от 10% годишно и при запазване на сегашните темпове без съществени реформи след 10 години делът на софтуерната индустрия ще достигне 1700 млн. лв. или 1.8 % от БВП. При образователна реформа и повече софтуерни специалисти софтуерната индустрия може да удвои размера си до около 3700 млн. лв. или 3.8% от БВП. Този ръст би я превърнал в структуроопределяща за българската икономика.

- Намалява делът на младите, които навлизат в ИТ сектора. Причини: демографските процеси; нееднакво добрата информираност на младите относно възможностите, които предлага индустрията; намаляващият интерес към точните науки.

- Процентът на лицата с висше и средно образование в страната нараства. Но завършилите в чужбина младши ИТ специалисти се нуждаят от два пъти по-малко време за първоначално обучение, отколкото тези, които са следвали в България. [4]

Какво предстои, какво може да се направи и къде е нашето място?

Европа трябва да изгради нова работна сила, която притежава цифрови умения, за да използва максимално потенциала на новите технологии и да бъде конкурентна в световен план. Около този извод се обединиха участниците в европейския проект „e-Skills for Jobs 2014", който приключи в края на миналата година. Инициативата се реализира едновременно в 30 страни, като изпълнител за България беше Българската асоциация по информационни технологии (БАИТ).

Проектът завърши с документ – „Манифест на е-уменията", в който се обръща внимание, че Европа е в критичен момент. Причината за това е, че се наблюдава все по-растяща разлика между изискванията за дигитална трансформация на икономиката, от една страна, и уменията, ноу-хау и способността на участниците на пазара на труда, от друга. За целта е необходимо спешно да се създаде eSkilled работна сила в Европа. Това може да стане по пътя на ползотворното сътрудничество между ИКТ индустрията, образованието и правителството за осигуряване на дългосрочно действие и успех, който ще произвежда работни места, конкурентоспособност и растеж, са установили участниците в проекта.

Манифестът на е-уменията представлява план за осъществяването на тази цел. Това е третото издание и се основава на широк обхват от гледни точки. Статиите са подготвени от висши корпоративни мениджъри, вземащите решения, изтъкнати университетски преподаватели, водещи изследователи на пазара и експерти и предвиждат цялостен преглед на състоянието на нещата във всички сектори на обществото.

"Новостите в областта на информацията и мрежите (включително изчисленията в облак, голямото количество данни, социалните медии, мобилният интернет и конвергенцията) създават необходимост от нови умения и огромни възможности за тези, които ги овладеят първи.", пише в документа.[5]

Предлагането на специалисти и услуги в областта на технологиите и стимулирането на иновациите е една област, в която университетите, бизнесът, научните звена и правителството трябва да обединят сили. Университетите трябва да знаят от какво има нужда бизнесът, за да могат да пренастроят своите учебни програми спрямо търсенето. В същото време бизнесът трябва активно да търси университетите и правителството и да им показва от какви умения, от какви специалисти има нужда в момента и ще се нуждае в бъдеще.

Различните институции в този своеобразен триъгълник на знанието могат да увеличат сътрудничеството си, за да създадат среда за раждане на иноватори. Така, сближавайки се с бизнеса в съответната област, университетите да започнат да изграждат у студентите нова бизнес култура, която да ги стимулира в последващата им реализация, включително и като създават свои стартъп компании в областта на информационните технологии и услуги. Това е един модел, който много успешно се реализира в САЩ, особено в Силициевата долина, но много по-слабо е разпространен в страните от ЕС, а в нашата страна почти не се среща. В същото време, много наши млади таланти предпочитат да продължат развитието си в университети, както в ЕС, така и в САЩ и други страни. Една от основните причини е, че образованието, което ще получат там, им предоставя по-добри възможности за реализация след завършването. И тук говорим не толкова за придобитите знания в съответната област, а именно за тази нова бизнес култура, която да ги стимулира в последващата им реализация.

Необходимо е да бъдат създадени по-добри рамкови условия за иновации и растеж и нови работни места в областта на цифровите технологии и да се гарантира, че знанията, уменията, компетенциите и иновативността на работната сила в Европа, включително на ИТ специалистите, отговарят на най-високите световни стандарти и че те се осъвременяват постоянно чрез ефективен процес на учене през целия живот.

ЛИТЕРАТУРА

1. Съобщение на Комисията до Съвета, Европейския Парламент, Европейския Икономически и Социален Комитет и Комитета на Регионите - Електронните умения през 21-ви век: насърчаване конкурентоспособността, растежа и работните места / COM/2007/0496 окончателен /, Брюксел, 7.9.2007

2. Електронни умения: Международното измерение и влиянието на глобализацията. Европейска комисия, ГД „Предприятия и промишленост“, „Главни базови технологии и цифрова икономика“

3. Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите, Програма в областта на цифровите технологии за Европа („Digital Agenda for Europe“) COM(2010)245 окончателен, Брюксел, 19.5.2010

4. Анализ на компетенциите на работната сила в сектор „Информационни технологии“ 2013 г.

5. Манифест на е-уменията, http://www.bait.bg/ BG_Manifesto.pdf

ПРЕДИЗВИКАТЕЛСТВАТА НА СТЕГАНОГРАФИЯТА КЪМ ИНФОРМАЦИОННАТА СИГУРНОСТ И ОБУЧЕНИЕТО НА СПЕЦИАЛИСТИ В УНИВЕРСИТЕТИТЕ[1]

Станимир С. Станев

Шуменски университет „Епископ Константин Преславски”
stan@shu-bg.net

CHALLENGES OF STEGANOGRAPHY TO INFORMATION SECURITY AND TRAINING OF SPECIALISTS IN UNIVERSITIES

Stanimir S. Stanev

Bishop Konstantin Preslavski University of Shumen
stan@shu-bg.net

ABSTRACT: *This work provides an overview of the latest trends in contemporary steganography and their challenges to information security, security services and teaching in universities. An taxonomy of IT- steganography and overview of some bulgarian terms are presented.The possibilities of using online social networks, cloud services and mobile applications for criminal purposes are marked, and some tools for steganological protection are shown. Special attention is paid to the training of specialists in steganography abroad and at Shumen University.*

KEY WORDS: *information hiding, steganology, steganography,information security, cloud computing, training specialists, cloud security, insiders, network steganography, sterilization.*

I. Въведение

Един от най-ефективните подходи за защитата на важна информация е скриването на съществуване на такава информация (information hiding). Това направление включва много техники и методи - криптография, сигнални системи, условни знаци, маскировка и измами и др., сред които е и стеганографията [1,2].Тя има хилядолетна история и предлага много средства за скриване на съобщения (симпатични мастила, микроточки, тайни канали, холография, и др.). Днес техни наследници са методите на компютърната и мрежовата стеганография - самостоятелни научно-приложни направления за информационна сигурност, изучаващи проблемите на създаване на компоненти със скрита информация в явна информационна среда, генерирана от компютърните системи и мрежи.

[1] Разработката е частично финансирана от фонд „Научни изследвания” на Шуменския университет „Епископ К. Преславски” по проект РД 08-316 /2015 г.

Стеготехниките могат да се прилагат както за целите на защитата на данните в областта на военните и правителствени комуникации, защитата на авторското право, и при решаването на други задачи по осигуряване на информационната сигурност, така и за незаконни цели – например за създаване на скрити канали за изтичане на забранени документи и за комуникация на престъпници [3].

През май 2011 год. германската полиция арестува подозреваем член на Ал Кайда в Берлин. В неговият компютър следователите откриват видео, в което са скрити чрез стегопрограми 141 текстови файла- документи с детайлно описание на операции на Ал Кайда и планове за бъдещи операции [4].

През октомври 2011 година ФБР на САЩ публикува на своя сайт документи за арестуваните през 2010 година руски граждани, обвинени в шпионаж. В техните квартири в САЩ са намерени защитени с 27 символни пароли компютърни дискове, съдържащи стеганографски програми за връзка с центъра на службата за външно разузнаване на Русия. Това е първият доказан случай на използване на стеганографията от разузнавателни служби [5].

Стана известно използването на стеганографски методи при вълната от кибератаки Shady RAT срещу правителства и организации като ООН, МОК, антидопинговата агенция WADA и др.

Вътрешните заплахи от т.н. „инсайдери”за чувствителна информация са особено трудно разрешим проблем. Той официално е поставен под номер 2 в списъка на най-трудните проблеми – HPL (Hard Problem List), на Американският съвет за изследване на сигурността на информационните системи – INFOSEC [6]. Традиционните средства за мрежова сигурност и системи за предотвратяването на загуба на данни не откриват употребата на стеганография от вътрешни служители.

В Индия стана известен случай на корпоративен шпионаж за изтичане на поверителна информация към конкурентна фирма с използване на стеганографски средства, скриващи информация в аудио- и графични файлове.

Актуалността на разглеждания в работата проблем е свързана с отговорностите на службите за сигурност за ефективно противодействие на подобни начини на използване на стеганографски методи. Тя изисква запознаването с основите на съвременната стеганология на по-широк кръг от специалисти, чиято задача е не само разработването, анализа или противодействието на стеганосредствата, но и квалифициран избор на съществуващите стеготехнологии и тяхното умело използване за решаване на конкретни приложни задачи в областта на защитата на информацията. Това е особено важно за бъдещите специалисти в областта на информационната сигурност.

II. Таксономия и терминология на стеганографията и стеганологията

Стеганографията (steganography) е интердисциплинарна научно-приложна област, съвкупност от технически умения и изкуство за начините за скриване на факта на предаване (наличие) на информация [7].

От средата на първото десетилетие на XXI век сред специалистите се използва терминът стеганология (steganology), обхващащ два смислово противоположни компонента- стеганография и стеганализ (по аналогия с криптологията, състояща се от криптография и криптоанализ) [1,7,8]. На фиг.1 е показана класификация на стеганологията на съвременния етап на нейното развитие. Тази класификация може да се променя с развитието на новите методи.

Терминът „Класическа стеганография“ се използва само за обобщаване на съвокупността от огромния брой исторически развили се методи, системи, техники, приложения (симпатични мастила, микроточки, тайни канали, и др.). Скритото предаване на информация и данни е „класическата“ цел на стеганографията. Задачата е така да се предават или съхраняват данни, че противника въобще да не се досеща за факта на наличието на скритите съобщения.

Високотехнологична стеганография (high-tech steganography) е термин за обобщаване на направленията за скриване на съобщения с използване на комуникационните и компютърни технологии, нанотехнологиите и съвременните постижения на биологията. От края на осемдесетте години на миналия век с внедряването на първите персонални компютри за решаване на класическите стеганографски проблеми, датира и началото на съвременната IT – стеганография.

В зависимост от използваните методи и контейнери, тя от своя страна се дели на компютърна, мрежова и лингвистична стеганография [7].

Компютърната стеганография има две основни направления за скриване на информация- използването на специалните свойства на компютърните формати, и използване на преобразувани в дискретна форма сигнали, имащи непрекъсната аналогова природа (изображения, видео, звук).

От началото на XXI век се развива и новото направление мрежова стеганография (network steganography), продължение на идеята за скритите мрежови канали (covert chanels) [9]. За разлика от компютърните стеганографски методи, които използват цифрови контейнери (изображения, аудио- и видео файлове), мрежовата стеганография използва управляващите елементи на комуникационните протоколи и тяхната основна присъща функционалност. Скритата по този подход информация е по- трудна за разкриване и елиминиране.

Методите на компютърната стеганография (в някои публикации се обозначава с термина Steganography 1.0), основно вграждат информация в излишъка от битове в служебната и „потребителската” част на файловете. Мрежовата стеганография (Steganography 2.0) вгражда секретни данни в две части на протоколите - контейнери - заглавната част на протоколите или полетата за потребителските данни, или манипулира на времевите интервали между протоколните единици на някои мрежови протоколи.

Днес стеганологията се развива бурно, и това води неизбежно и до изменения и развитие на използваните термини, понятия, походи и методи. Тя е млада наука, и нейната терминология се развива и променя. Началото на съгласуване на терминологията е поставено през 1996 в Кембридж, Великобритания. В [7,10] са дефинирани основните български термини на стеганологията, най-близки по смисъл до съответните английски и руски термини. Изхождайки от смисловата натовареност и за по-кратко изразяване, в тях е прието използването (по аналогия с повечето западни публикации) на представката „стего” вместо „стегано”- например стегосистема, стегопроткол, стегометод, стегоалгоритъм, стегопрограма, стего (стегофайл), стегограма, стегокапацитет, стеганализ и др. Въведен е нов термин – стегоинцидент - криминална дейност по използване на стеганография за посегателства към чувствителна информация чрез секретен канал за изтичане или за несанкциониран достъп до нея [7].

Стеганализът (steganalysis) обединява методи и технологии за откриване на секретни стеганографски комуникации. Стегоатака е всеки опит да се открие, изв-

лече или да се унищожи скрито чрез стеганография съобщение. По аналогия скриптологията, специалистите в областта на стеганализа се наричат стеганалитици. Стеганализът се прилага при компютърни съдебни разследвания, при проследяване на криминални дейности в Интернет и при събиране на доказателства за разследвания, особено на анти-социални елементи. Може да се използва за усъвършенстване на сигурността на стего средствата чрез оценка и идентификация на техните слабости.

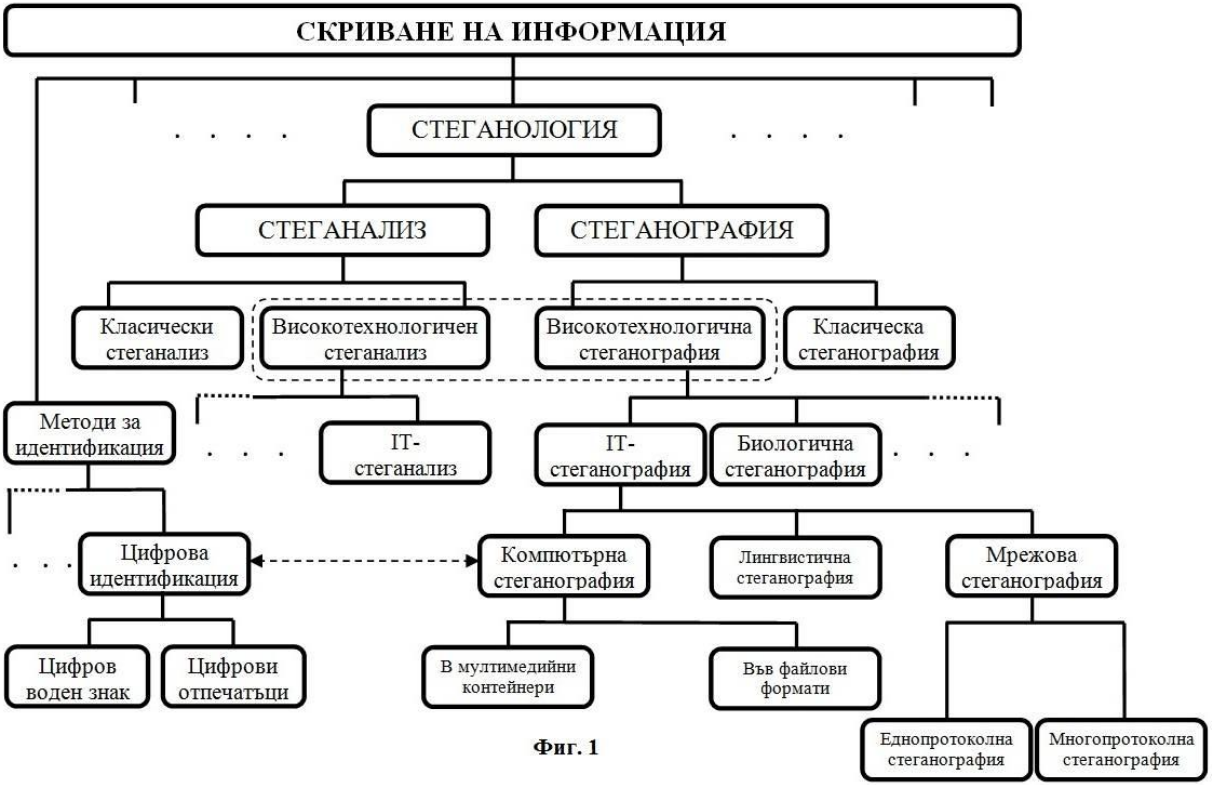
Някои автори използват термина цифрова стеганография (digital steganography) като синоним на компютърната стеганография. В други източници цифровата стеганография се представя като направление за използване на стеганографски методи за създаване на цифрови водни знаци (ЦВЗ) (digital watermarking), сигнатурни отпечатъци (digital finger prints) и надписи (captions) [11]. Методите за създаване на ЦВЗ вграждат информация в цифрови обекти (наричани произведение или творба), с цел защита на тяхното авторско право. Най-съществената разлика между скритото предаване на данни със стегометоди и вграждането на ЦВЗ се състои в това, че в първия случай нарушителите не знаят, но се стремят да открият скритото съобщение, а във втория всички знаят за това, че то съществува. Методите за ЦВЗ и за отпечатъци използват методи, аналогични на стеганографските.

Използването на стегометоди за ЦВЗ не е достатъчно основание те да бъдат разглеждани като цифрова стеганография [11], затова те по-нататък не се разглеждат.

III. Използването на он-лайн глобалните услуги и мобилните комуникции за стеганографска комуникация на злоумишленици

От първите он-лайн социални мрежи (ОСМ), стартирани в Интернет през 1999 г., досега в киберпространството са известни няколко стотин такива мрежи. Според [12], най- популярните 15 мрежи са Facebook, Twitter, Linkedin, Pinterest,Google Plus+, Tumber,Instagram, VK, Flickr, Vine, Meetup, Tagged, Ask.fm, MeetMe и ClassMates. Докато нормалните потребители на ОСМ могат да използват тази технология за комуникация и информационен обмен, същата технология може да се използва като инструмент на тероризма за комуникация, кибератаки, пропаганда, набиране на нови членове, обучение и др.

В доклад на Института за национална сигурност на университета Джорж Вашингтон (Homeland Security Institute, 2009) се отбелязва, че Интернет е станал важен инструмент в ръцете на терористи. Днес 90 % от терористичната дейност в Интернет се осъществява с използване на инструментите на ОСМ.. Прилагането на стегометоди за скриване на съобщения в цифрови изображения е еквивалент на шпионския тайник "dead drop", но в киберпространството. В [13] е посочено, че Al-Qaeda са използвали стеганографията. По време на терористичната атака Westgate в Найроби, Al-Shabaab, терористична група , базирана в Сомалия, използва ОСМ Twitter да разпространява информация и да потвърди отговорността си за атаката [14].


СКРИВАНЕ НА ИНФОРМАЦИЯ
СТЕГАНОЛОГИЯ
СТЕГАНАЛИЗ
СТЕГАНОГРАФИЯ
Класически стеганализ
Високотехнологичен стеганализ
Високотехнологична стеганография
Класическа стеганография
Методи за идентификация
IT-стеганализ
IT-стеганография
Биологична стеганография
Цифрова идентификация
Компютърна стеганография
Лингвистична стеганография
Мрежова стеганография
Цифров воден знак
Цифрови отпечатъци
В мултимедийни контейнери
Във файлови формати
Еднопротоколна стеганография
Многопротоколна стеганография

Фиг. 1

От края на деветдесетте години на XX век досега в Интернет са разпространени над 2000 стеганографски, и стотици стеганалитични програми от 8 поколения с различен лицензионен статут. Съществуват много източници за обзор на тези стеганографски програми (т.н. steganography tools) , данни за най- популярните от тях са обобщени в [7, 15,16]. Според специалистите, полезни за практиката съвременни софтуерни средства от Интернет сега, са OpenPuff и Our secret [16]. Направените сравнения позволяват да се посочи класацията на най-добрите в момента 5 програми - OpenPuff v.4.0, SecretLayer Pro, Our Secret, QuickStego и Ultima Steganography. Желаещите да използват достъпните в Интернет стегопрограми обаче трябва да са наясно, че вероятността за откриване на скрити с тях съобщения от правоохранителните органи е почти 100%. Стегопрограмите, които имат приемлива надеждност в това отношение, са с голяма изчислителна сложност за кодиране на данни в реално време. Такива програми едва ли се предоставят за публично ползване.

Разкриване на скритите канали в ОСМ изисква изучаването и тестването на различни стегано техники и софтуер в условията на платформите, предоставяни от операторите на мрежите. По разбираеми причини почти липсват публикации за проведени конкретни експерименти по слабостите на ОСМ за допускане осъществяването на тайни комуникации. Това не намалява актуалността на провеждането на изследвания в това направление.

През 2011 год. са били направени изследвания в три социални мрежи – Facebook, Badoo и Google+[17]. От трите ОСМ, Facebook е сравнително най- добре защитена срещу използването ѝ за стегокомуникации Установено е, че скриване на съобщения в публикуваните изображения в профилни албуми на ОСМ Facebook не е възможно, защото всички изображения се компресират на входа на тази ОСМ. Потвърдена е възможността за прилагането на компютърната стеганография само за две функции, които биха предали съобщението със 100% успеваемост – „споделяне на файл“ за Facebook и „споделяне на снимка”в Google+. Но през 2013 год. има разработено ново приложение за браузъра Chrome под названието Secretbook [18], което „пробива“ посочената защита. Когато съобщението трябва да се изпрати, разработеното приложение компресира изображението - контейнер по същия начин, по който би го направила мрежата Facebook, след това добавя малко излишни битове към него, и шифрира текста с парола. По този начин се гарантира, че когато Facebook автоматично наново компресира съобщението, промените, които ще бъдат нанесени в него ще бъдат незначителни и съобщението вероятно няма да се повреди . Това приложение работи само с браузър Chrome, и засега скриваните текстови съобщения в JPEG изображения не са по-дълги от 140 сивола [18]. Изследователи от Технологическия институт на Джорджия (САЩ) са разработиали инструмент - Collage, с който пък е възможно да се вграждат скрити съобщения в Twitter „постове“ и Flickr-фотографии.

Съвместни тестове на екипи от лаборатория „Компютърна сигурност“ на Шуменския университет и Дагестанския Унивеситет за народно стопанство, с участието на студенти от Русия и България, се проведоха за ОСМ - Facebook, Google+, Одноклассники, Вконтакте (VK), Мой Мир, Instagram, Tumblr и Linkedin [19, 20]. Тъй като се приема, че стеганографията може да се използва най-често от злоумишленици със средно ниво на компютърни познания, използващи готови програмни продукти, за тестовете бяха използвани програмите OurSecrets, Red JPEG

XT,Masker 7.5 , Free File Camouflage 1.12, MP3Stego 1.1.18, а за сравнение на резултатите – разработеният в ШУ продукт SHide++. Той се състои се от стегопрограма, предназначена за вграждане на скрити съобщения в графични контейнери с разширение .bmp, и програма за стеганализ на подозрителни графични файлове [21]. Като контейнери при тестовете се използваха графични и аудиофайлове. Използвани са различни хардуерни платформи, за взаимодействие със социалните мрежи: персонални компютри, лаптопи, таблети, смартфони, работещи с различни операционни системи. Бяха анализирани услуги на ОСМ, позволяващи да се предават графична или звукова информация.

Проведените експерименти потвърдиха,че не е възможно използването на безпрепятствена стеганография в албуми във Facebook и VK. При споделяне на снимки чрез Google+ е реализиран успешно целият цикъл на стеганографска комуникация от вграждане до извличане на скрити съобщения със формати JPEG, PNG, BMP и GIF [17,20].Чрез широко разпространените платформи за електронна поща – gmail, yahoo, abv и т.п. е възможна безпрепятствена стеганографска комуникация посредством прикачени към писмата мултимедийни обекти с вградени в тях съобщения.

Наред с внедряването на облачните услуги (cloud computing) възникват и редица редица проблеми, един от най-сериозните от които е сигурността и защитата на потребителските и фирмените данни.

Организацията Cloud Security Alliance дефинира седем от най-важните заплахи за изчисленията в облак [22] :

№1. Злоупотреба и престъпно използване на Cloud Computing (различни "дейности" например спам, зловреден код, крекинг на пароли, DDoS атаки,ботнет C & C и т.н.);

№2. Злонамерени вътрешни лица (инсайдери);

№3. Загуба или изтичане на данни ;

№4. Отвличане на акаунт или услуга;

№5 Несигурни интерфейси и API;

№6. Споделени технологични проблеми. Много от основните компоненти на облачните услуги не са проектирани да предлагат силна изолация при многопотребителска работа. Нападателите фокусират операциите си към други облачни клиенти, за получаване на неоторизиран достъп до техните данни,

№7. Неизвестен рисков профил – неясна информация с кого клиентът ще споделя своята инфраструктура, в допълнение към въведените данни, например проникване при въвеждането на акаунти, опити за пренасочване и др.

Стеганографията трябва да се счита за нарастваща заплаха за изчисленията в облак. Основните доставчици на облачни услуги , като Google (Gmail, Google Doc),Microsoft (Azure), Amazon (Amazon Web Services), Cisco(WebEx) използват понякога сложни протоколи и инфраструктури, подходящи и за контейнери - носители на секретни данни.

В зависимост от разположението на приемника на стегограми, може да се посочат три основни типа стегокомуникации в облачните структури (услуги).

(1) Приемникът на стегограми се намира в същия облак, в който и предавателя на стегофайла. В този случай се извършва т.н. мрежова стеганография с използване на мрежови протоколни единици, или междупротоколна мрежова стеганография. Така могат да се реализират заплахи №№1-3.

(2) Приемникът на стегограми се намира извън средата на облачните услуги и способностите на облачните услуги се използват за извършване на мрежови атаки. Този вид комуникация включва също и използване на мрежа стеганография. Това може да доведе до реализирането на заплахите №№ 1-3.

(3) Приемникът на стегограми се намира в друг облак, различен от този на предавателя. Това може да доведе до реализацията на заплахите №№ 1-3 и 7 [22].

Audio steganography е вид атака, сочена като една от най-опасните и сериозни за системите за съхранение в облака. Атакуващите крият своя злонамерен код в аудио потоци и ги изпращат на потребителите чрез сървърите под различна медийна форма – по този начин те осъществяват достъп до желаните точки за атака.

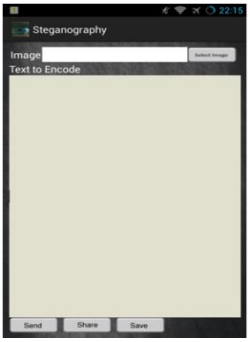
Поради разнообразието и сложността на облачните услуги, специалистите са песимисти относно създаването на универсални и ефективни стеганалитични методи и средства.

Стеганографията чрез мобилните телефони и PDA е по-трудна, защото изисква достъп до операционната система на мобилното устройство, но това се преодолява лесно от ангажираните лица. Една от най-широко използваните ОС – Android, разработена от Google и Open Handset Alliance с отворен код е съвокупност не само от ОС, но съдържа middleware и др. ключови приложения. PDA Siri на Apple може да се използва за скрито предаване на данни от злоумишленик към malware, инсталиран на смартфона, приложението iStegSiri за скриване на данни в звукови файлове, които се генерират от PDA. В процеса на MiTM-атаката, заемайки позиция между PDA на клиент и сървърите на Siri, нарушителят прехваща тези съобщения и ги декодира. По този начин той може да придобие конфиденциална информация от телефона на клиента, съвсем незабелязан от мрежовата защитна стена и антивирусните програми [23].

Вече има разработени програмни продукти за мобилни телефони, много от които са общодостъпни (фиг. 2).

С приложението PixelKnot секретно съобщение може да бъде скрито в графично изображение. Secret Letter е стеганографско приложение за Android, позволяващо да се вграждат и извличат текстови съобщения в изображения или фотографии, направени с камерата на мобилното устройство. Програмата позволява скрито предаване на необходимата информация и да скрие самия факт на това предаване [24]. Разработеното мобилно приложение StegDroid за Android реализира принципа на ехо-стеганографията в звукови файлове, записани от собственика на мобилния телефон. Абонат, на телефона на който е инсталирано същото приложение, може да извлече скритото съобщение от получения аудиостего файл [25]. Популярни стеганографски приложения за ОС Android са Steganography, Steganography Application, Steganography Master, Steganography Image, Stegano Imessage, Stegano Lookup, Photo Hidden Data, Barcode Steganography,

Pocket Stego, Steganographia, MobiStego, Da Vinci Secret Image Pro, Stegais, Crypsis Eye, Stegos. Специалистите предлагат следната експертна класация на първите 5 - Steganography, Photo Hidden Data, Steganografia, Steganography Application и Stegosaurus.



Фиг. 2

IV. Информационната сигурност и стеганологична подсистема за защита на информацията (СПСЗИ)

Основните мерки за защита на конфиденциалната информация в БА и правителствените звена се базират на съответните закони, наредби и правилници [26, 27]. Според редица специалисти засега липсва технология, която да удовлетворява всички концепции за информационна сигурност [28]. Като всяка технология за сигурност, стеганографията не е идеална и не покрива всички изисквания за секретност, но тя удовлетворява много от изискванията за секретна комуникация, понякога в комбинация с други методи като криптографията.

В реалните условия на действие на наши войскови контингенти зад граница, секретната информация е уязвима, както поради случайни, така и поради злонамерени дестабилизиращи фактори (заплахи). Това налага да се вземат мерки за нейната защита, чрез които се постига нужното ниво на информационна сигурност.

Стеганологичната защита (стегозащита) е комплекс от организационни и апаратно-програмни мерки за предотвратяване на стегоинциденти [7]. Може да се определят два основни аспекта на стегозащитата:

1. Защита на секретна информация срещу изтичане с използване на методи на стеганализа.

2. Стегозащита на информацията срещу несанкциониран достъп чрез скриване на malware в безобидни на пръв поглед мултимедийни файлове.

Вторият аспект на стегозащитата не е пряко свързан с контраразузнавателната защита на информацията, и тук само се отбелязва като възможност за използване от службите, осигуряващи предаването на конфиденциалната информация.

Ролята на защитниците и атакуващите, още от публикуваната през 1983 год. статия на Симънс с „проблема на затворниците" Алис и Боб [29], е все още повече обект на теоретични изследвания, отколкото на практическо приложение. Книгата на проф. Джесика Фридрич започва с пример където вече Алис и Боб са шпиони [8]. В [30] на базата на сценария за Алис и Боб, с цел изследване на проблема за възможните стеганографски канали за изтичане на информация, е предложен хипотетичен модел на дейността на разузнавателната служба на престъпна организация срещу военен контингент с използване на стеганографски методи.

Система за защита на информацията (СЗИ) е комплекс от мерки, реализирани от няколко подсистеми за защита – антивирусна, защитна стена, криптозащита и др. Системният подход при разработването на СЗИ изисква стегозащитата да се реализира от стеганологична подсистема за защита на информацията (СПСЗИ) е част от СЗИ. СПСЗИ е съвкупност от апаратни и програмни средства за защита на информацията в компютърните системи и мрежи чрез методите на стеганографията и стеганализа.

От своя страна СПСЗИ се състои от два основни модула [7, 31]:

- модул за стеганографско скриване на информация и защита от несанкциониран достъп (НСД);

- модул за защита от изтичане на информацията чрез скрити канали.

Архитектурата на СПСЗИ и функциите на отделните модули са дадени в [31, 32].

Разкриването на каналите за изтичане на конфиденциална информация и организиране на ефективно противодействие на съществуващите възможности за използване на стеганографските методи е основна задача на контраразузнаването с цел пресичане на престъпната дейност [30]. Детайлното разглеждане на комплекса от мерки за сигурност излиза извън рамките на дадената разработка. Все пак тук могат да се маркират някои от тях:

- забрана на внасянето, качването, тегленето и ползването на криптиращи и стеганографски програми за лични цели ;

- забрана за достъп до Интернет на компютри, в които се обработва конфиденциална информация, и забрана за презапис на данни върху информационни носители;

- забрана на наличието и внасянето в пункта за сигурност на компютри и мобилни апарати с достъп до Интернет, извън компютърната мрежа на контингента;

- организиране на контрол върху изходящия трафик, чрез проксисървър, защитна стена и др.;

- създаване на междинно звено, обслужващо проксисървъра с възможности за заглушаване на всички свободни интернет услуги;

- създаване на сървър за отстраняване на мултимедийни файлове, и ограничаване възможността на служебния канал за прикачване на мултимедийни файлове;

- стеганализ на всички изходящи по официалния мрежов канал на защитавания контингент мултимедийни обекти, предавани в канала или тяхното зашумяване чрез вграждане на специални стеганалитични съобшения, с цел унищожаване на евентуално вградена секретна информация.

За постигане на желаната надеждност и ефективност, задължително условие е съчетанието на горепосочените мерки с класически контраразузнавателни мерки за противодействие [34, 35], със спазване на принципите на контраразузнавателната защита на информацията.

Допълнителен защитен рубеж са и доброволните сътрудници на контраразузнаването [35].

За защита от стегоинциденти трябва да се използват най-съвременни програмни методи и средства. Едно от тези решения са системите DLP (Data Leakage/Lost Prevention). Обаче повечето от разпространените версии на тези системите за защита от изтичане на данни или нямат в състава си модули за стеганализ, или той не е активиран. Едно от изключенията е DLP системата на McFee комбинирана със стеганалитичната програма StegoSuite на WetStone Technologies Inc. Разработват се перспективни системи за стеганализ на данни -SDP (Stegano-graphy Detection Prevention).

По договор с американските ВВС, компанията WetStone Technologies Inc. е разработила една от първите комерсиални стеганалитични програми за правителствени органи - Stego Suite. Освен това Stego Suite позволява да се унищожат данните, скрити по метода LSB, чрез промяна на младшите разряди на всеки байт на мултимедийния стегофайл, в нулева стойност без промяна на качеството на контейнера [36].

Стерилизацията на изображения може да има важно приложение в областта на информационната сигурност и защита. В този сценарий, зашумяването на съобщение, без да променят характеристиките на изображението , е възможна защита от злоупотреби със стеганография.

По аналогия с биологичния смисъл на понятието стерилизация (sterilizing), в [37] за пръв път е въведено понятието „стерилизация на изображение“ в смисъл на премахване на всякаква стеганографска информация, вградена в изображения. Получените експериментални резултати показват е разработеният метод има ефективност средно от 76% до 91% за изтриване на стегопикселите, в които информацията е вградена по метода LSB. Друг метод за стерилизация на изображенията с участие на същите автори е разгледан в [38]. Докато методът от [37], може да стерилизира само един на всеки пиксел от стегофайла, а в по-късната работа [38] - до два бита, в [39] се предлага нов алгоритъм за стерилизация на 4 бита, вградени по метода LSB. Това е „сляпа“ техника за стерилизация чрез намиране на ексцентричност на всеки стего пиксел. Така могат да се унищожат всички четири най-малко значими бита на стего изображения , образувани с помощта на стего алгоритъм, независимо от начина по който алгоритъма вгражда информация в изображенията. Извършената симулация с три вида стего изображения, създадени чрез най-съвременните алгоритми, показва,че метода е успял да стерилизира средно от около 50% до 90% стего бита (в зависимост от конкретния алгоритъм). Проблемите на стерилизацията се разглеждат и в [40].

Стеганологията широко се коментира в Интернет, най-новите са на Steganology.com и хеш-тага #steganology от https://twitter.com/hashtag/steganology.

Американската фирма Backbone Security е световен лидер в продажбите на стеганалитичен софтуер. Тя доставя продукти на правителства и специални служби в много държави. Постоянно се актуализира и разширява най- голямата в света достъпна комерсиална база от данни за стеганографски сигнатурни отпечатъци

Steganography Application Fingerprint Database (SAFDB) [41], създадена от изследователския център на фирмата - Steganography Analysis and Research Center (SARC). Сега Backbone Security доставя четири продукта- StegAlyzerAS, StegAlyzerSS, StegAlyzerRTS и StegAlyzerFS, разработени на базата на хибриден подход за откриване използването на стегоприложения. Според фирмата те могат да открият използването на стеганография от „инсайдери".

Според много специалисти, StegAlyzerRTS (Steganography Analyzer Real-Time Scanner) е най-добрият в момента в света достъпен на пазара стеганалитичен програмно-апаратен комплекс за мрежова сигурност. Той открива в режим на реално време стеганографски приложения и техните сигнатури, скрити в безобидни на пръв поглед файлове, които се изпращат на външни получатели по електронна поща или към общо достъпни сайтове [42].

Постоянно развиващите се стегометоди отправят нови предизвикателства към стеганалитиците и компютърните следователи. Универсалните инструменти, които могат да открият и класифицират стеганографска активност все още се намират в стадий на начално разработване. И се реализира следващ цикъл както при криптографията - стеганализът помага да се открият скрити съобщения, но също така показва на създателите на нови алгоритми за стеганография как да избегнат откриването на такива съобщения.

Допълнително към посочените мерки за стегозащита мерки трябва да се отбележи и възможността за стеганографска защита на информацията, противоположна на разгледаната в [30] стегоатака. Чрез използването на възможностите на стеганографията за контрамярка може да се въведе скрит от всички служители стегомаркер с информация за произхода, собственика, разпределението и предоставянето на секретни документи. След изготвяне от оторизирано лице на важен документ, той се изпраща към сървър на организацията, наречен „стегосървър", който служи за вграждане на такъв стего маркер (сигнатура). Маркерите са вградени по такъв начин, че дори когато обектът е променен или преправен, те остават.

Предложените мерки за стеганалогична защита са само началото на конкретни разработки в тази област.

V. Обучението на специалисти по стеганология в чужбина и у нас

Несъмнено една от основните мерки за стеганологична защита е създаването на добре подготвени специалисти в тази област. За целта фирми-производители на апаратни и програмни ссредства за защита, като MacFee, Wetstone, Backbone Security и др. провеждат краткосрочни и дългосрочни курсове за обучение. С това се занимават и редица академии, фондации и организации.

В много висши учебни заведения по света се работи активно по обучението на специалисти по защита на информацията, и се провежда сериозна изследователска работа по създаване на програмни и технически средства за защита. Научните изследвания като правило се финансират от мощни корпорации и заинтересовани държавни агенции. В редица учебните курсове по информационна сигурност, а даже и като отделни дисциплини се преподават въпросите на стеганологията. Най-известни и престижни при обучението на специалисти са университети в САЩ, Великобритания, Русия и др. страни. В табл. 1 са дадени частични данни за такова обучение. Всички маркирани със (@) в таблицата университети дават в своите официални сайове информация, че извършват изследователска работа в областа на

стеганографията и стеганализа, но не посочват дали имат отделни учебни дисциплини по стеганография, или в кои дисциплини точно включват такива модули и теми. За отбелязаните с * има неофициални данни, че работят в тази област.

Таблица 1

Държава	Университет	Дисциплина
България	Шуменски Университет	Компютърна стеганография
	ИИТ – БАН, ТУ- Варна, ТУ- София, ФАПВОКИС	*
Румъния	University Politehnica of Bucharest	*
Турция	Sakarya University, Yaşar University	@
САЩ	Binghamton University- New York	Fundamentals of steganography (Jessica Fridrich- EECE 562)
	University of Cincinnati, University of Nebraska, George Mason University, Howard University, University of Rhode Island, University of Alabama	@
Белгия	XIOS Hogeschool Katholieke Hogeschool	@
Испания	Universidadad Del Pais Vasco	@
Португалия	The Polytechnic Institute of Setubal	@
Германия	Technische Universität München	Steganography and Steganalysis
Русия	ПГУТИ – Самара, СПБГЭТУ(ЛЭТИ)- С.Петербург, Академия МВД, ДГУНИ-Махачкала	*
	МГТУ им. Н.Э. Баумана	@
	ВолГУ- Волгоград	Стеганография
Русия	ОГУ- Оренбург, ГУТ им. М.А.Бонч-Бруевича- С. Петербург, Казанский (Приволжский) федеральный университет	Основы стеганографии
	СбГУТИ – Новосибирск	@
New Zealand	Auckland Universty of Technology	*
Финландия	Rovaniemi University of Applied Sciences	@

Държава	Университет	Дисциплина
Литва	Vilnius University	**@**
Великобритания	University of Surrey, University of Oxford, University of Kent, Bournemouth University, University of Birmingham	**@**
Чехия	Czech Technical University	**@**
Полша	Warsaw University of Technology, Bialystok University of Technology	**@**
Индия	Sree Vidyanikethan Engineering	*****
Ирак	Nawroz University	**@**

Една от от най-известните в света специалисти по стеганология проф. Jesica Fridrich от SUNY Bingham University, NY, САЩ, преподава от 2006 год. дицсиплината „Fundamentals of steganography“ и развива научно-изследователска дейност в областта на стеганографията и стеганализа, основно със студенти. Нейният екип работи по няколко проекта, финансирани и от правителствени американски агенции и лаборатории [43]. В Полша екипите на Wojciech Mazurczyk и Krzysztof Szczypiorski във Варшавската политехника работят по авангрални проекти по мрежова стеганография със студенти. В Русия въпроси на стеганографията се преподават в над 110 висши учебни заведения [44].

Интересна форма за развитие на методите за стеганализ от млади изследователи е периодично провежданото международно състезание по стеганализ BOSS (Break our steganography system). Целта на състезанието е разби-ването на специално разработения за целта стегометод HUGO [45]. Този метод е най- устойчив срещу стегоатаки чрез най- добрия в момента стеганалитичен метод SPAM, разработен от екипа на една от най-известните специалисти по стеганоло-гия проф. Jesica Fridrich от SUNNY Bingham University, NY. Този екип е световен университетски лидер в областта на стеганалитичните изследвания. Един от резул-татите е разкриването на слабостта на HUGO по отношение на метода 1D за пре-дотвратяване на стеганализа. През през юни 2011 г. състезанието е спечелено от студентския отбор на проф. Fridrich с коефицент на откриваемост Ksa=0,82, а на второ място с Ksa=0,73 е британския отбор Queen с водачи Dr. Fatih Kurugollu и Gokhan Gul [46].

Получените резултати от научно-изследователската работа на водещите университети имат такава практическа ценност, че много от техните автори доброволно спират да ги публикуват в научния печат за да предотвратят тяхното използване от престъпни елементи и групировки.

В Шуменския университет „Епископ Константин Преславски“ проблемите на компютърната и мрежова стеганография се разглеждат като компонент на професионална подготовка студентите от специалност „Информатика” по информационна сигурност. За пръв път във висше учебно заведение у нас от 2010 год. в Шуменския Университет бе въведена учебната дисциплина „Компютърна стеганография”. Изградена е цялостна система за обучение по дисциплината. За подпомагане на обучението на студентите, от преподавателите от катедра КСТ на ФМИ са издадени монографията „Стеганологична защита на информацията“, учебното пособие

„Компютърна и мрежова сигурност“ и методическо ръководство за практически занятия по ствганография [47,48]. Под печат е ново ръководство за практически упражнения по стеганография. В рамките на научно-техническия обмен с ПГУТИ-Самара са обменени 2 учебни пособия и софтуер за мрежова стеганография.

Повишава се научната квалификация на преподавателите- през 2014 г. са защитени 2 докторски дисертации в тази област и е избран един професор. Учебната дисциплина „Компютърна стеганография“ досега е изучавана от над 100 студенти от специалността „Компютърна информатика“ (редовно и задочно обучение) и „Компютърни информационни технологии“. Тя има силно изразен учебно - изследователски характер. Следвайки бързото развитие на научното направление и постоянното внедряване на нови методи и програми, заедно с натрупвания опит в преподаването всяка година се променя и учебното съдържание на дисциплината. Последната промяна бе въвеждане на тема по мрежовата стеганография. Текущият вариант на програмата по учебната дисциплина „ Компютърна стеганография” е с хорариум 50 часа аудиторна заетост, от които 25 часа лекции и 25 часа семинарни занятия, провеждани в учебни зали и лаборатория „Компютърна сигурност”. Лекционният материал включва темите „Проблеми на компютърната и мрежовата сигурност” (в нея са включени общи въпроси на компютърната сигурност, заплахи и атаки и походи за защита на компютърните системи и мрежи), „Криптографски алгоритми в стеганографията”, „Основи на компютърната стеганография”, „Избор на стеганографски контейнери”, „Мрежова стеганография”, „Системи за скрита идентификация (Цифрови водни знаци)”, „Стеганализ и ефективност на стеганографските алгоритми и програми”, „Разработване на системи за защита”.

Разработени са над 20 бакалавърски и магистърски дипломни работи (първите – през 2004 год.), над 30 съвместни научни публикации на преподаватели и студенти. Проф. Станев е ръководил и 3 дипломни работи по стеганография на студенти от Факултет АПВОКИС на НВУ.

Сключени са договори за научно-техническо сътрудничество с Института по отбраната, университети в Самара и Махачкала – Русия, организирано е сътрудничеството с ИИТ на БАН, УНИБИТ и НВУ, Политехника- Букурещ и др. През 2012 в лаборатория „Компютърна сигурност” бе монтирана 32 ядрена клъстерна компютърна система „Радиан-М”, разработена от колектив от ФМИ и ФТН на ШУ. В учебно- изследователската лаборатория се работи по стеганография и стеганализ в паралелна компютърна среда, реализирани са 6 проекта по стеганология, финансирани от фонд „Научни изследвания” на ШУ с участие на преподаватели, студенти и докторанти. Освен разработените стегопрограми и научни публикации, важен резултат е че постепенно се формира ново направление не само за ШУ – компютърна стеганология в паралелни компютърни среди.

През октомври 2014 год. в Шуменския Университет, който се очерта като водещо у нас научно заведение в тази област на защитата на информацията, бе организиран и проведен международен научен семинар по стеганография - ШУСТЕГ14. За пръв път у нас се срещнаха специалисти в областта на стеганографията и стеганализа от нашата страна и чуждестранни университети. Бяха обсъдени направления за практически изследвания в областта на стеганографията и стеганализа във ВУЗ, и се обсъждаха научни публикации по тематиката на семинара. В рамките на семинара бяха представени две нови книги в областта на стеганологията на доц. Илчева и д-р Илчев, и на проф. Ст. Станев.

Опитът от проведеното обучение води до няколко важни заключения, свързани с подготовката на учебни материали за студентите [49]. Методите на стеганографията не трябва да се разглеждат изолирано от криптографията. Независимо от факта, че исторически погледнато, стеганографията се е появила преди криптография, представянето на материала в учебниците е препоръчително да започне с методите за криптозащита, тъй като теоретично криптографията е разработена много по-задълбочено в сравнение със стеганографията. В учебните пособия трябва да има информация за предимствата и недостатъците на различни алгоритми за формиране на псевдослучайни числа и да се разглеждат форматите на контейнерите- графични, звукови, текстови, архивни, видео, Web – приложения. На студентите трябва да се разяснява, че разглежданите класически методи за информационн а защита не са догма и че е възможна тяхната съществена модернизация.

Според специалистите най-добрия начин за усвояване на стеганографията от студентите е изпълнението на лабораторни работи, курсови работи, дипломни проекти и решаване на практически задачи по извличане на информация, скрита в контейнери. За целта студентите трябва да усвоят редактори за дъмп на паметта и мрежови анализатори.

Най-добрите засега учебници за студенти в областта на стеганографията са - на английски език е книгата на проф. Jessica Fridrich ”Steganography in digital media”(2010 год.) и на руски език ”Стеганография, цифровые водяные знаки и стеганоанализ” (2009 год.) с автори А. Агрpreновский, А. Балакин , В. Грибунин и С. Сапожников [50].

Развитието на компютърните технологии и мобилните комуникации неминуемо ще отправят нови предизвикателства към обучението на специалисти по високотехнологична стеганография, и те трябва да има готовност за тяхното посрещане. Ролята на висшите учебни заведения трябва да остане водеща в процеса на обучението им.

VI. Заключение

В момента светът е готов технически за стеганографията, но в културен план съвременното информационно общество още не е дорасло до нея. В най-близко време (2015-2025 год.) ще стане това, което може би в бъдеще ще наричат „стеганографска революция“ поради няколко причини [51].

1. Понастоящем няма единна стеганографска теория. Това е сериозна пречка. Докато в криптографията има теория, създаваща и изучаваща абстрактни математически криптографски обекти, то в стеганографията не е така. И все пак през последните 15 години (2000-2015) има голям прогрес в разработване на математическата теория на стеганографията.

2. Стеганография е интердисциплинарна наука. Това е първото, което трябва да помни всеки начинаещ „стеганограф“. Докато криптографията може да се абстрахира от апаратурата и да решава задачи изключително в света на дискретната математика, то специалистите по стеганография трябва да изучават средата. Стеганографията ще се развива в съответствие със степента на изучаването на средата, в която се предават секретните съобщения. За предаване и скриване на ценни данни ще се използват фантастични от днешна гледна точка методи и контейнери. Заедно с такива, които използват зрителни и акустични образи, най- вероятно ще се използват и контейнери, свързани с други човешки чувства - осезание , обоняние, вести-

буларен апарат. Не е изключено един от контейнерите да стане и Човека [52]. Тогава проблема за неговата идентификация ще се решава с помощта на ефективни средства на криптографията и стеганографията.

3. Съвременният виртуален свят е пренаситен с изображения,, видеоклипове и др. Само в YouTube за една минута се „качват“ над 100 часа видео. В най-бизко време стеганографията и противодействието на стеганографията ще имат същата актуалност , както проблемите с новите концепции BigData или Internet of Things (IoT).

4. Историческите примери с изобретенията в областта на криптографията са показателни с повторенията - първият път „секретно“, вторият път „явно“. Това може би ще стане и със стеганографията. В съвременната западна научна литература вече не публикуват някои учени с интересни идеи в стеганографията през периода 1998-2008. Подобна ситуация е имало в края на тридесетте години на 20 век, преди създаването на атомното оръжие. Може би вече са изобретени съвършенни стегосистеми и те успешно се използват от СРВ, CIA или NSA?

Методите на стеганографията се развиват с времето, могат да се очакват нови заплахи за информационната сигурност. При възникване на необходимост създателите на зловреден софтуер, престъпните организации, терористите и държавните организации да прикрият своите криминални дейности, то е не само вероятно, но и сигурно, че те ще развият и използват нови методи на стеганографията и други авангардни технологии.

Службите за сигурност трябва да са готови да посрещнат тези предизвикателства.

ЛИТЕРАТУРА:

1. Cox,I., Miller, M., Bloom, J. Fridrich, J. and T. Kalker. Digital Watermarking and Steganography, Second Edition. Elsewier, Morgan Kaufmann Publishers, 2008.

2. Аграновский, А., А. Балакин , В. Грибунин и С. Сапожников. Стеганография, цифровые водяные знаки и стеганоанализ. Москва, Вузовская книга ,2009. ISBN 978-5-9502-0401-2.

3. Conway, M. Code Wars: Steganography, Signals Intelligence, and Terrorism. Knowledge, Technology and Policy (Special issue entitled ‘Technology and Terrorism’) Vol. 16, No. 2 (Summer 2003): [онлайн]. [прегледан 28.05.2012]. http://doras.dcu.ie/494/1/know_tech_pol_16 _2_ 2003.pdf.

4. Zielinska,E., W. Mazurczyk и K. Szczypiorski. The Advent of Steganography in Computing Environments.[онлайн].[прегледано 20 май 2013]. http://arxiv.org/ftp/arxiv/papers/1202/1202.5289.pdf.

5. US arrest of Russian agents 'reads like spy thriller.The Telegraph, June 29,2010. [онлайн]. [прегледан 30.05.2012]. http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7860022/US-arrest-of-Russian-agents-reads-like-spy-thriller.html.

6. Steganography and the Insider Threat: Backbone Security Explains Why the IT Security Community Should Take Notice. [онлайн]. [прегледано 20.04.2013].http://www.sarc-wv.com/news/press_releases/2013/steganography _insider_threat.aspx.

7. Станев, С. Стеганологична защита на информацията. Университетско издателство „Епископ Константин Преславски”. Шумен, 2013. ISBN 978-954-577-825-4. 320 стр.

8. Fridrich, J. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2010.437 p. ISBN 978-0521190190.

9. Network Steganography Principles. [онлайн]. [прегледан 20 февруари 2013] http://www.stegano.net/tutorial/net-steg.html.

10. Станев, С. и В. Галяев. Семантична еквивалентност на основните термини на компютърната стеганология в българските, английските и руските научни публикации.В: Сборник научни трудове на международна конференция МАТТЕХ2012, Том 1.Шумен:Университетско издателство „Еп.К.Преславски", 2012, стр.119-126.

11. Грибунин В., И.Оков и И.Туринцев. Цифровая стеганография. Москва: Солон-Пресс, 2002.

12. Top 15 Most Popular Social Networking Sites.[онлайн]. [прегледан 5.08.2014]. http://www.ebizmba.com/ articles/social-networking-websites.]

13.Террористы и стенография. [онлайн].[прегледан 11 ноември 2014]. http://anmal.narod.ru/crypto-gram/steganography.html]

14.Fredrick Romanus Ishengoma, A. Online Social Networks and Terrorism 2.0 in Developing Countries. International journal of Computer Science & Network Solutions December.2013-Volume1.No 4. ISSN 2345-3397. [онлайн].[прегледан 11 юни 2014]. http://arxiv.org/ftp/arxiv/papers/1410/1410.0531.pdf.

15. Станев, С. Софтуерни продукти за стеганализ. В: Сборник научни трудове на Научна конференция 2013 "Защита на личните данни в контекста на информационната сигурност. Факултет АПВОКИС на НВУ"В.Левски". Шумен,2013.Стр.157-164.

16. Алиев, С. и Д. Тончев. Нови стеганографски програми в Интернет. В: Сборник научни трудове на международната научна конференция МАТТЕХ14, Том 1, ISBN 1314-3921. Шумен, 2014. стр.167-172.

17. Chee, A. Steganographic Techniques on Social Media: Investigation Guideline. [онлайн]. [прегледан 20.10.2013]. http://aut.researchgateway.ac.nz/bitstream/handle/ 10292/ 5577/CheeA.pdf?sequence=3.

18. Steganography Now On Facebook. [онлайн]. [прегледан 20.11.2013]. http://www. pentagonpost.com/steganography-now-on-facebook/8346042.

19. Галяев, В. О некоторых экспериментах по передаче стегосообщений через социальные сети. В: Сборник научни трудове на международната научна конференция МАТТЕХ14, Том 1, ISBN 1314-3921. Шумен, 2014. стр.119-122.

20. Еминов, Д., С. Хасанова и Д. Тончев. Стеганография в он-лайн социални мрежи. В: Сборник научни трудове на международната научна конференция МАТТЕХ14, Том 1, ISBN 1314-3921. Шумен, 2014. стр. 173-178.

21. Станев, С., С. Ниязиев, С.Железов, Х. Параскевов. Стеганологичен софтуерен пакет. В: Сборник научни трудове на Научна сесия на НВУ-факултет АПВОиКИС, Шумен, 2013. (под печат).

22.Mazurczyk,W., K. Szczypiorski. Is Cloud Computing Steganography-proof? [онлайн].[прегледан 20.10.2014] http:// arxiv. org/ftp/arxiv/papers/1107/1107.4077.pdf.

23.Siri [онлайн].[прегледан 20.02.2015]. https://www.apple.com/ios/siri/.

24.Secret Letter. [онлайн].[прегледан 21.03.2015]. http://www. securitylab.ru/ software/443202.php

25. White, T., J.Martina Mobile Steganography Embedder. Thomas F. M., [онлайн].[прегледан 21.03.2015]. http://www.peotta.com/sbseg2011/resources/downloads/wticg/91964.pdf.

26. Семерджиев, Ц. Сигурност и защита на информацията. София: Класика и стил. 2007. ISBN 978-954-327-034-7.

27. Наредба за задължителните общи условия за сигурност на АИС или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация. [онлайн]. [прегледан 20.04.2013]. http://www.dans.bg/images/stories/promzak/naredba_ais_mrezhi-06122012.pdf.

28. Гайкович, В. и Д. Ершов. Основы безопасности информационных технологий. Москва,МИФИ.1995.[онлайн].[прегледан 1.06.2013]. http://www. / downloads/wticg/91964.pdf.

29. Simmons, G. The Prisoners' Problem and the Subliminal Channel. Advances in Cryptology: Proceeding in Crypto. CRYPTO'83,1983, pp. 51-67.

30. Кръстев, К. и С. Станев. Стеганологична защита на информацията в контекста на контраразузнавателното осигуряване на сигурността на войскови контингент зад граница В: Сборник трудове на научна конференция „Новата парадигма за сигурност в киберпространството". ФАПВОКИС на НВУ, Шумен, 2014.

31. Stanev,S., H.Hristov and D. Dimanova. Aproaches for stegodefense of sensitive information. Proceedings of ICBBM 2014, Volume 10, RTU Press, Riga, 2014. ISBN 978-9934-10-573-9. pp.117-122.

32. Zhelezov,S., H. Paraskevov, H. Hristov , P. Boyanov and B. Uzunova-Dimitrova. An architecture of staganological subsystem for information protection. Proceedings of ICBBM 2014, Volume 10, RTU Press, Riga, 2014. ISBN 978-9934-10-573-9. pp.123-128.

33. Христов, Х. Особености на организацията и управлението на оперативното противодействие на посегателства срещу фирмената сигурност. В: Сборник трудове на юбилейна научна конференция „10 години от създаването на НВУ „В.Левски", 2012, Том 4 (под печат).

34. Асенов, Кипров. Теория на контраразузнаването. София : Труд, 2002.

35. Землянов, В. Своя контрразведка. Практическое пособие. [онлайн]. [прегледано 20.03.2014].http://coollib.net/b/248996.

36.Wetstone Technologies inc.[онлайн].[прегледан 20.04.2013].http://www. Wetstonetech. com/product/stego-suite/. http://www.htt.co.in/wetstone/Stego-Suite.htm.

37. Paul, G., Mukherjee, I.. Image Sterilization to Prevent LSB-based Steganographic Transmission., CoRR abs/1012.5573(2010). Later appeared in Proceedings of the 11-th International Conference on Security and Management (SAM), July 16-19, 2012, Las Vegas, U.S.A., pp. 448-454 under the title ``Sterilization of Stego-images through Histogram Normalization". [онлайн]. [прегледан 20.03.2015].http://arxiv.org/ftp/arxiv/papers/1012/1012.5573.pdf.

38. Goutam,P., I. Mukherjee. Sterilization of Stego-images through Histogram Normalizationhttp://worldcomp-proceedings.com/proc/p2012/ SAM9764.pdf. [онлайн]. [прегледан 20.03.2015] http:// worldcomp-proceedings.com/proc/p2012/SAM9764.pdf.

39. Mukherjee,I., P. Goutam, A. Jawahar. Defeating Steganography with Multibit Sterilization using Pixel Eccentricity. [онлайн]. [прегледан 20.03.2015]. http:// worldcomp-proceedings.com/proc/

40. Payra, A.K. Steganology for the Computer Forensics Examiners: Steganography,Steganalysis,Sterilization techniques for security issues. LAP LAMBERT Academic Publishing, 2013. ISBN 978-3659403361.

41. Backbone Security Expands World's Largest Digital Steganography Database. [онлайн] . [прегледан 20.05.2013] . http://www. backbonesecurity.com/ SteganographyDatabase1175Applications.aspx.

42. Steganography Analyzer Real-Time Scanner (StegAlyzerRTS).[онлайн].[прегледан 5.05.2013].http://www.sarc-wv.com/products /stegalyzerrts/learn_more.aspx.

43. Jessika Fridrich. [онлайн] . [прегледан 20.05.2013] http://www.ws.binghamton. edu/fridrich.

44. Галяев, В. Современный уровень преподавания стеганографии в России. В: Сборник научни трудове на международната научна конференция MATTEX14, Том 1, Шумен, 2014. стр.115-119. ISBN 1314-3921.

45. HUGO.[онлайн].[прегледан 21.05.2013]. http://www.agents.cz/boss/.

46. BOSS. [онлайн].[прегледан 21.05.2013]. http://www.csit.qub.ac.uk.

47. Станев,С., С. Железов и Х. Параскевов. Обучението по компютърна стеганография в Шуменския университет „Епископ Константин Преславски". Наука, образование, сигурност. София: Издателство на НБУ, 2013. стр.445-451. ISBN:978-954-535-796-1.

48. Станев, С. и С. Железов. Первые результаты внедрения курса „Компютерная стеганография" в Шуменском университете. В: Трудове на международната научно-практическа конференция на ВДПУ „Коцюбински", Винница,Украйна, 2012.стр.205-207.

49. Алексеев, А., М. Макаров и В. Орлов. Криптография и стеганография в учебном процессе. Трудове на научната конференция „ Новите предизвикателства пред системите за информационна сигурност", Шумен, 2015 (под печат).

50. Аграновский, А., А. Балакин , В. Грибунин и С. Сапожников. Стеганография, цифровые водяные знаки и стеганоанализ. Москва, Вузовская книга, 2009. ISBN 978-5-9502-0401-2.

51. Павел МСТУ. Стеганография в XXI веке. Цели. Практическое применение. Актуальность. [онлайн].[прегледан 21.03.2015]. http://habrahabr.ru/post/253045/.

52. Алексеев, А и В. Орлов. Стеганографические и криптографические методы защиты информации (Учебное пособие). Самара, ИУНЛ ПГУТИ , 2010 . 330 с. ISBN 978-5-904029-12-8.

ОБОБЩЕН САМОСВИВАЩ ГЕНЕРАТОР НА ПСЕВДОСЛУЧАЙНИ ПОСЛЕДОВАТЕЛНОСТИ

Жанета Н. Савова-Ташева

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС”, гр. Шумен

GENERALIZED SELF SHRINKING GENERATOR OF PSEUDO-RANDOM SEQUENCES

Zhaneta N. Savova-Tasheva

ABSTRACT: *Nowadays with the introduction of many new communication technologies, new problems related to the provision of reliable and efficient communications via Internet, telephone, wireless, satellite and other channels, are aroused. A method for generating a non-binary pseudo-random sequence, which increases its period and linear complexity and remains their balance property, is proposed in the paper. The proposed p-ay Generalized Self-Shrinking Generator is useful in stream ciphers.*

KEY WORDS: *PRS, p-ary LFSR, SSG, GSSG, Stream Ciphers*

1. Въведение

В днешно време псевдослучайните последователности *PRSs* (Pseudo-Random Sequences) са широко използвани в много приложения, като компютърни симулации и моделиране, статистика, експериментален дизайн, цифрови комуникации, криптография и генератори на случайни числа. От особена важност е тяхното приложение в области като синхронизация на предаваните сигнали, навигация, радарни системи, комуникационни системи с разширен спектър, подобряване на многолъчевата разделителна способност и идентификацията на сигналите в комуникационните системи с множествен достъп [4], [5], [8], [13], [19], [20]. *PRSs* се прилагат в комуникациите и криптографията още от създаването на теорията на информацията през 1948 г. от Клод Шенон. Интересът към *PRSs* се определя от техните свойства, като добра корелация, балансираност и голяма линейна сложност.

В последните десетилетия се забелязва тенденция на увеличаване на научните изследвания не само в областта на двоичните *PRSs* с период $T = 2^n - 1$, но и в тази на троичните и *p*-ични *PRSs*. Повишеният интерес към тях се определя от тяхната близка функционална връзка с функцията следа и разликовите множества и възможността тяхното поведение и характеристики да бъдат математически описани със средствата на съвременната алгебра.

Актуалността на проблема за повишаване на скоростта и сигурността на предаваните данни в съвременните комуникационни и компютърни мрежи и системи произтича от важността на изискванията за получаване на бърза, надеждна и точна информация за изпратеното съобщение, неговия изпращач и получател, както в комуникационни канали с шумове, така и в такива с възможност за подслушване и

умишлени шумове, организирани от престъпни и терористични групи. Наличието на конкурентна среда, използваща прихващане и подслушване на фирмена и секретна информация за извършване на измами, терористични и други престъпни актове е двигател на развитието на нови методи и средства за дешифриране на скрита информация, които нарушават правото на неприкосновеност на нейния собственик. В случаите на невъзможност за придобиване на ценна информация, често се прибягва до умишлено внасяне на шумове в канала за връзка с цел да се осуети възможността за комуникация между двете страни. За решаване на тези проблеми, е необходимо разработването на нови методи за защита на информационния поток в комуникационните и компютърни мрежи и системи.

В статията се представя нов метод за генериране на *p*-ични *PRSs* с повишена нелинейност и сигурност, който може да се използва като генератор на ключов поток в поточните шифри. Статията е организиране по следния начин

2. Приложение на псевдослучайните последователности в поточните шифри

Безспорна е необходимостта от „случайни“ последователности, но същевременно с това е напълно необходимо и да е ясно, какво се има предвид под понятието „случайна“ последователност. Ако съществува начин да се генерира повторно дадена последователност, то тогава тя не е случайна. Само напълно случайни последователности, получени чрез множество природни явления като бял шум, шум в полупроводниците, предизвикан от топлинното движение на неосновните токоносители, радиоактивно разпадане и др., не могат да бъдат повторно възпроизведени, но те не са приложими в гореизброените приложения. Вместо това, когато се казва, че случайната последователност има определено статистическо свойство, се прави изявление за очакваната стойност на съответния статистически критерий. Това означава, че определена последователност преминава даден статистически тест, ако нейното поведение по отношение на този критерий напълно отговаря на осредненото поведение от всички тествани последователности.

Преди да бъде приведени критериите за измерване на случайността на една *PRS* ще бъде дефинирана тяхната същност [5].

Определение 1. Псевдослучайните последователности *PRSs*, наричани също псевдошумови последователности *PNSs* (Pseudo Noise Sequences), са детерминирано генерирани последователности, които притежават някои характеристики на случайно генерираните последователности.

Съществуват множество критерии за измерване на случайността на една псевдослучайна последователност [4], [8]. Те могат да се разделят на две основни групи. Първата група включва *статистически критерии*, които определят характеристики като голям период на повторение, балансираност на елементите, равномерно разпределение на блоковете, автокорелационна функция и χ^2 разпределение. Втората група включва *други мерки, определящи сигурността*, като например, линейна сложност, нелинейност, *N*-адична сложност, устойчивост, корелационен и алгебричен имунитет.

Наличието на множество критерии към случайността често изисква въвеждането на компромиси в процеса на проектиране и изследване на псевдослучайните последователности. От една страна, за да преминат успешно множеството изследвания се налага генераторите на псевдослучайни последователности да се проекти-

рат като твърде сложни устройства, което от друга страна прави процесът на техния анализ доста по-труден по отношение на критериите на случайността. Затова, в зависимост от конкретното приложение, е необходимо да се определят кои критерии са от особено значение и кои са второстепенни.

За приложения с разширен спектър от особена важност са корелационните свойства на две последователности. За криптографските приложения, критериите за линейна сложност и нелинейност предоставят оценка по отношение на трудността на разбиване на даден шифър. При конструирането на генератори на ключови потоци съществуват много практически съображения, които трябва да се вземат предвид. Те могат да варират в зависимост от реалната комуникационна среда, в която ще работи генератора. В общия случай се търси баланс между сигурност и ефективност. Целта при разработката на поточен шифър е дължината на използвания реален ключ да е пряка мярка за сигурността на неговия алгоритъм.

Съществуват няколко фактори определящи ефективността, които е необходимо да се разглеждат при проектиране на един поточен шифър. Едно важно съображение е да се разработи алгоритъм, който да е ефективен, както при софтуерна, така и при хардуерна реализация. Възможно е да се налага периодична смяна на ключа на поточния шифър с цел да се запази синхронизацията. В някои комуникационни мрежи, като например базираните на пакети системи, честата ресинхронизация може да се окаже необходима. Целта е да се проектира ефективна процедура, която не допуска компромис със сигурността.

Основно изискване към трансформациите, използвани в криптографските алгоритми, е те да бъдат нелинейни, за да се осигури максимална защитеност срещу множеството съвременни атаки [18]. Един от възможните методи за постигане на нелинейност е неравномерното тактуване на градивните елементи на генератора.

2.1. Неравномерно тактувани генератори на ключов поток

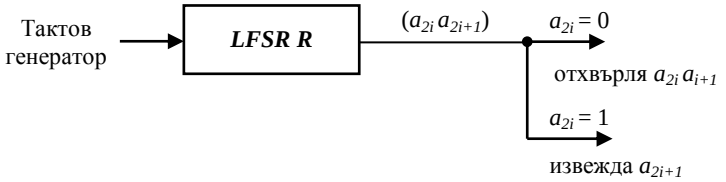
При неравномерно тактуваните генератори на ключов поток, битовете на изхода не се получават при всеки такт на вътрешните преместващи регистри с линейни обратни връзки *LFSR* (Linear Feedback Shift Register), а през неравномерни интервали. Много съвременни предложения за поточни шифри използват неравномерно тактувани генератори на ключов поток, защото е доказано, че те не са податливи на корелационни атаки [21] и бързи корелационни атаки [10], [17], които използват корелационната мярка, основаваща се на разстоянието на Хеминг. За неравномерно тактуваните генератори на ключов поток, тази корелационна мярка не може да бъде приложена. Въпреки това тези генератори може да са податливи на атаки от типа „разделяй и владей“, включително и корелационни атаки от този тип.

Пример за тактово управляван генератор на ключов поток, за който тактуването е ограничено, е генераторът „стъпка 1 – стъпка 2“, При него $LFSR_C$ е с равномерно тактуване и контролира изхода на $LFSR_D$ по следния начин. В момента t се подава такт към $LFSR_C$. Ако изходът $c(t)$ в момента t е 0, към $LFSR_D$ се подава един такт. Ако $c(t)$ е 1 към $LFSR_D$ се подават два такта. Изходът на $LFSR_D$ формира бита $z(t)$ на ключовия поток. Този генератор е податлив на корелационна атака. В [25] е предложена ограничена вградена атака на $LFSR_D$, която може да се използва като първи етап от атака „разделяй и владей“ върху генератора. По-обща атака, която може да бъде приложена към други ограничени тактово управлявани генератори, е предложена в [3].

Свиващият генератор *SG* (Shrinking Generator) [1] е друг пример за генератор на ключов поток с неравномерен изход. Свиващият генератор се състои от два равномерно тактувани двоични *LFSR* регистъра $LFSR_A$ и $LFSR_S$ с дължини съответно L_A and L_S. Изходът на свиващия генератор представлява „свита“ версия на подпоследователността на изхода на $LFSR_A$, като наличието на даден бит в изхода се избира в зависимост от позициите на единиците в изходната последователност на $LFSR_S$. По-точно, последователността на ключовия поток z се състои от онези битове в последователността a, за които съответстващите битове в s са 1. Другите битове на a, за които съответстващите битове в s са 0, се изтриват. Ако полиномите за обратна връзка на *LFSR*s са примитивни, тогава a и s са последователности с максимални периоди съответно $2^{L_A}-1$ и $2^{L_S}-1$. Ако, освен това, L_A и L_S са взаимно прости, тогава, както е показано в [1], периодът на z е $2^{L_A}-1\ 2^{L_S-1}$, а линейната сложност L на z удовлетворява неравенството $L_A 2^{L_S-2} < L \le L_A 2^{L_S-1}$. Свиващият генератор е податлив на корелационна атака.

Принципите на свиване, за пръв път предложени от Коперсмит, Кравчук и Мансур в свиващия генератор *SG* [1] през 1993 г., са обект на изследване и модифициране от много учени и те са в основата на няколко други псевдослучайни генератора. Една година по-късно, на EUROCRYPT ’94, Майер и Стефалбах предлагат самосвиващ генератор *SSG* (Self-Shrinking Generator), който е изграден само от един *LFSR* и днес все още е устойчив на известните до сега криптоатаки [8], [11].

Той има много проста схема, като се състои само от един градивен *LFSR* регистър A, който генерира m-последователност $(a_i)_{i\ge 0}$. Правилото за свиване разглежда изходната последователност на регистъра по двойки (a_{2i}, a_{2i+1}) и извежда a_{2i+1}, само ако $a_{2i}=1$. *SSG* има период $T = 2^{L-1}$, където L е дължината на *LFSR* A. В един период броят на поява на нулите и единиците е равен.



Фиг. 1. *Самосвиващ генератор SSG*

Пример 1. Нека *LFSR* има полином на обратните връзки $q(x) = x^5 + x^3 + 1$ и първоначалното състояния на регистъра е [0 0 1 0 1]. Тогава R произвежда m-последователност A с период $T = 2^5 - 1 = 31$.

A = 1; **0**; 1; **0**; 0; 0; 0; 1; 0; 0; 1; **0**; 1; **1**; 0; 0; 1; **1**; 1; **1**; 1; **0**; 0; 0; 1; **1**; 0; 1; 1; **1**; 0; 1; 0; 1; 0; 0; 0; 0; 1; **0**; 0; 1; 0; 1; 1; **0**; 0; 1; 1; **1**; 1; **1**; 0; 0; 0; 1; 1; **0**; 1; **1**; 1; **0**

Кодовата последователност x, генерирана от самосвиващия генератор, се получава от 2 периода на последователността a и е съответно:

x = 0; 0; 0; 1; 1; 1; 0; 1; 1; 0; 0; 1; 1; 0; 1; 0

Периодът на изходната последователност x е T = 16, а броят на нулите и единиците в периода е N_0 = 8 и N_1 = 8.

В [19] е предложен алгоритъм за преобразуване на L-битов *SSG* в $2L$-битов *SG*. Показано е, че *SG* с регистри с дължини A и B е еквивалентен на *SSG* с дължина $L = 2(A + B)$. Въпреки тези прилики е доказано, че *SSG* е по-устойчив на известните криптоатаки от *SG* [8].

В [12] Михалевич предлага криптоанализ на *SG* с минимална сложност по време $O(2^{0.5n})$ и сложността на необходимите данни е също $O(2^{0.5n})$. При това количеството необходим ключов поток е нереалистичен при големи стойности на дължината на ключа n. Атака, изискваща малко количество ключов поток, само $(2.41n)$, е така наречената диаграма на двоично решение *BDD* (Binary Decision Diagram), предложена в [9]. Тя има сложност по време и памет равни на $O(2^{0.656n})$. Най-добър компромис между време, памет и данни в криптоанализа днес дава атаката "предположи и определи" (guess-and-determine) [12], [24]. Сложността по време варира от $O(2^{0.5n})$ до $O(2^{0.656n})$, а съответно необходимите данни – от $O(2^{0.5n})$ до $O(n)$. Например, при приемлив размер на прихванатия ключов поток от $O(2^{0.161n})$, е възможно с тази атака да се възстанови ключа за време $O(2^{0.556n})$.

В 2004 г. Хю и Ксио предлагат друг прост генератор, който наричат обобщен самосвиващ генератор *GSSG* (Generalized Self-Shrinking Generator) [6]. Той дава възможност да се генерират семейство балансирани обобщени свиващи последователности с добри взаимно корелационни свойства. Между тези последователности не повече от $1/2^{L-k}$ имат период не по-малък от 2^k, $0 < k < L$. Не повече от 1/4 от последователностите имат период не по-малък от 2^{L-1}, $0 < k < L$. Съществуват 2 последователности с най-малък период 2 и няма последователности с период T, такъв че $2 < T < L/2$. По-късно анализът на *GSSG* [2] доказва, че той не е по-сигурен от оригиналния *SSG*.

През 2007 г. Сидек и Шамери извършват сравнителен анализ на поточните шифри използвани в цифровите комуникационни системи [20]. Сравнението е между 7 типа генератори: линеен, подобрен генератор на Гефи, сумиращ, мултиплексиращ, самосвиващ и генератор с памет посредством статистически тестове, линейна сложност, корелационна и предположи и определи атаки. След направените анализи е показано, че само *SSG* генераторът преминава успешно всички тестове.

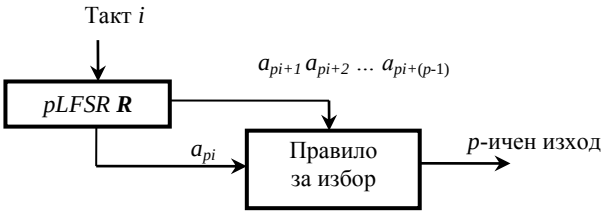
В 2010 г. Кансо предлага нов вариант на *SSG*, наречен модифициран самосвиващ генератор *MSSG* (Modified Self-Shrinking Generator) [7]. Генераторът използва примитивен *LFSR* с дължина L и разширено правило за извеждане на изходния бит, основано на операцията сума по модул 2 от двойка последователни битове. Доказано е, че генерираната последователност е балансирана и има период по-голям или равен на $2^{\frac{L}{3}}$, линейна сложност по-голяма от половината период и има добри статистически свойства. Авторът е доказал по-голямата сигурност на *MSSG* спрямо оригиналния *SSG*.

3. P-ичен обобщен самосвиващ генератор

В този параграф се обобщава самосвиващия генератор *SSG* за произволно просто число p и теоретично се изследват неговите свойства.

3.1. Архитектура на p-ичен обобщен самосвиващ генератор

Архитектурата на *p*-ичния обобщен самосвиващ генератор *pGSSG* (*p*-ary Generalized Self-Shrinking Generator) се състои от един *p*-ичен *LFSR* (*pLFSR*) регистър *R* с дължина *L* (фиг. 2). Той генерира *m*-последователност $A = (a_i)_{i\geq 0}$ от *p*-ични цифри (т.е. $(a_i)_{i\geq 0}, 0 \leq a_i \leq p-1$) и $0 \leq i \leq L-1$. Множителите на обратните връзки в *pLFSR* се определят от коефициентите на примитивен полином в разширението на полето на Галоа GF(p^L). Всеки градивен елемент на *pLFSR* може да съхранява една *p*-ична цифра. Регистърът се инициализира с *p*-ичната последователност (a_0, a_1, …, a_{L-1}).



Фиг. 2. *P-ичен обобщен самосвиващ генератор pGSSG*

P-ичният *GSSG* избира част от изходната *pLFSR* последователност посредством следния алгоритъм:

Определение 2. Алгоритъмът на *p*-ичния обобщен самосвиващ генератор се състои от следните стъпки:

1. *P*-ичният *LFSR* се тактува с тактова последователност с период *T*.
2. Изходната *pLFSR* последователност се разделя на *p*-торки
   $(a_{pi}, a_{pi+1}, a_{pi+2}, \ldots, a_{pi+\ p-1}\ )$, *i* =0, 1, …
3. Ако $a_{pi} = 0$, то цялата *p*-торка се отхвърля, т.е. изходната *pGSSG* последователност е свита.
4. Когато $a_{pi} \neq 0$, съответната цифра $a_{pi+a_{pi}}$ от *p*-торката формира част от изхода на *pGSSG*. Например, ако $a_{pi} = 1$, то a_{pi+1} се извежда на изхода и останалите цифри $(a_{pi}, a_{pi+2}, \ldots, a_{pi+\ p-1}\ )$ се отхвърлят. Ако $a_{pi} = 2$, то a_{pi+2} се извежда и другите цифри $(a_{pi}, a_{pi+1}, a_{pi+3}, \ldots, a_{pi+\ p-1}\ )$ се отхвърлят и т.н. Ако $a_{pi} = p-1$, то на изхода се извежда $a_{pi+(p-1)}$ и останалите цифри от *p*-торката $(a_{pi}, a_{pi+1}, \ldots, a_{pi+\ p-2}\ )$ се отхвърлят.

Самосвитата *p*-ична *GSSG* изходна последователност може да се преобразува в двоична като се приложи предложения метод за преобразуване на всяко *p*–ично число в двоична последователност, при който разпределението на единиците и нулите е равномерно [22].

От алгоритъма на работа на *pGSSG* генератора следва, че генерираната *p*–ична псевдослучайна последователност е *свита, смалена* версия на *pLFSR* последователността когато стойността на първата цифра в *p*-торката е нулева. В противен

случай, когато стойността на първата цифра в *p*-торката е различна от нула, в генерираната последователност се извежда съответната цифра в *p*-торката.

Основен елемент в архитектурата на *pGSSG* генератора е недвоичният *pLFSR* регистър [22]. За сега той се използва по-рядко в сравнение с двоичните *LFSR* регистри, но както ще бъде показано по-нататък приложението му може да подобри характеристиките на получената от *pGSSG* нелинейна *pPRS* в сравнение с тази от *SSG*.

3.2. Примери

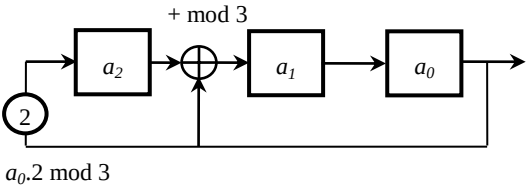
Преди да се премине към анализиране на свойствата на *pGSSG* генератора ще бъдат приведени два примера за поясняване на неговата работа.

Пример 2. *3GSSG*

Нека е избрано разширение на поле на Галоа GF(3^3) и примитивният полином, който генерира GF(3^3) е $p(a) = a^3 + 2a^2 + 1$. Тогава архитектурата на Галоа на съответния *pLFSR* (т.е *3LFSR*) е показаната на фиг. 3.

Полиномът на обратните връзки, прилагайки теорема 3.1, е $q(x) = 2x^3 + x^2 - 1$ и всички алгебрични операции се извършват по модул $p = 3$.

Нека началното състояние на *3LFSR* е $[a_2, a_1, a_0] = [0, 0, 1]$.



Фиг. 3. *Архитектура на Галоа на 3LFSR за GF(3^3) и примитивен полином $a^3 + 2a^2 + 1$*

За всички възможни тройки, генерирани от *3LFSR*, един период от изходната *3GSSG* последователност е [011120210220022110] и начинът, по който тя се получава според определение 4.6, както и преобразуването на *p*-ичната последователност в двоична според таблица 4.2, е показан в таблица 1.

Таблица 1. *Изходна 3GSSG последователност от пример 2*

Тройка	Изход (двоичен)	Тройка	Изход (двоичен)	Тройка	Изход (двоичен)
101	0 (0)	211	1 (0)	201	1 (0)
110	1 (0)	020		212	2 (1)
210	0 (1)	222	2 (1)	001	
012		112	1 (0)	011	
100	0 (0)	202	2 (1)	122	2 (1)
102	0 (1)	220	0 (0)	010	
121	2 (1)	120	2 (1)	111	1 (0)
002		021		221	1 (0)
022		200	0 (1)		

Периодът на *3GSSG* последователността е $T = 18$. Съответният изход се определя от стойността на първата цифра в тройката, която определя кой символ ще формира изхода на *3GSSG*. В таблица 4.6 тази цифра е показана в червено. След това троичната изходна последователност се преобразува в двоична според таблица 4.2 при $p = 3$. Двоичният изход е даден в скоби в таблица 4.6.

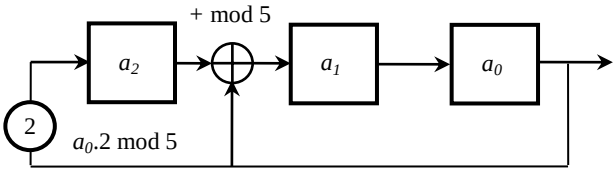
Пример 3. 5GSSG

Архитектурата на Галоа на *5LFSR*, съответстваща на разширение на поле на Галоа GF(5^3) и примитивен полином е $p(a) = a^3 + 3a^2 + 2$, е показана на фиг. 4. Полиномът на обратните връзки е $q(x) = 2x^3 + x^2 - 1$ и всички алгебрични функции се извършват по модул $p = 5$.

Нека началното състояние на *5LFSR* е $[a_2, a_1, a_0] = [1, 1, 0]$.

За всички възможни петорки, генерирани от *5LFSR*, част от периода от изходната *5GSSG* последователност е [0142221310034220123010340401200 0…] и начинът, по който се получава, е показан в таблица 2.

Периодът на изходната *5GSSG* последователност е $T = 100$. Изходът се избира от първата цифра на петорката, която определя позицията на символа, който ще се изведе на изхода. Накрая 5-ичната изходна последователност се преобразува в двоична според таблица 4.2 за $p = 5$. Двоичният изход отново е даден в скопи в таблица 2.



Фиг. 4. *Архитектура на Галоа на 5LFSR за GF(5^3) и примитивен полином $a^3 + 3a^2 + 2$*

Таблица 2. *Изходна 5GSSG последователност от пример 3*

Петорка	**Изход (двоичен)**	**Петорка**	**Изход двоичен)**	**Петорка**	**Изход (двоичен)**
10222	**0**(00)	11032	1(00)	33243	4(11)
31421	2(01)	00202		42302	2(01)
12044	2(01)	42201	1(00)	41143	3(10)
11234	1(00)	20040	**0**(01)	43410	**0**(10)
42403	3(10)	33440	4(11)	23223	2(01)
12241	2(01)	34003	**0**(11)	03132	
03430		11133	1(00)	04144	
12443	2(01)	21300	3(10)	10121	**0**(00)
40131	1(00)	02221		10323	**0**(01)
32433	3(10)	14210	4(11)	02024	
23021	**0**(10)	20444	4(11)	22014	**0**(11)
11431	1(00)	12342	2(01)	00404	
34104	**0**(00)	24033	**0**(01)	34402	**0**(10)

4. Изследване на *p*-ичен обобщен самосвиващ генератор

В параграфа ще бъдат изследвани периода и линейната сложност на последователностите, генерирани от *pGSSG* генератора, както и техните статистически, спектрални свойства и ентропия.

За целта алгоритъмът на *pGSSG* генератора при произволно просто число p е реализиран в среда на Visual C#.

4.1. Период и линейна сложност

Теоретично са доказани минималната и максимална граници на периода на изходната *pGSSG* последователност. Доказателството на теоремите може да се намери в [22], а тук ще бъде приведено само крайното твърдение.

Твърдение 1. Периодът на самосвитата *pGSSG* изходна последователност S удовлетворява неравенството

$$p^{\frac{L}{p}} \leq T \leq (p-1)p^{L-1}. \quad (1)$$

При $p = 2$ *pGSSG* се трансформира в класическия *SSG*. Така, резултатът, доказан от Маер и Стефълбах в [11], следва директно от твърдение 1 при $p = 2$.

Следствие 1. Периодът на самосвитата *SSG* изходна последователност удовлетворява неравенството

$$2^{\frac{L}{2}} \leq T \leq 2^{L-1}. \quad (2)$$

За изследване на линейната сложност на изходната *pGSSG* последователност е използван алгоритъм използващ разширения алгоритъм на Евклид. С алгоритъма са направени над 360 изследвания на изходните последователности от *pGSSG* в полета GF(p^n). Обобщените резултати от изследванията са показани в таблица 3, като освен полето GF(p^n) са представени броят на възможните изходни *pGSSG* последователности, техният период T, получените минимална и максимална линейна сложност. В колоната „Забележка“ е показано разпределението на реалната линейна сложност по брой последователности.

Таблица 3. *Резултати от определяне на линейната сложност на изходни pGSSG последователности*

GF(p^n)	Брой	Период	Линейна сложност		Забележка
			Мин.	Макс.	
GF(3^2)	2	6	4	5	4 – 1бр. 5 – 1 бр
GF(3^3)	4	18	15	16	15 – 1бр. 16 – 3бр.
GF(3^4)	8	54	48	51	48 – 1, 49 – 2, 50 – 2, 51 – 3
GF(3^5)	22	162	152	158	152 – 1, 156 – 6, 157 – 7, 158 – 8
GF(3^6)	48	486	478	481	478 – 1, 479 – 6, 478 – 2, 479 – 2, 480 – 14, 481 – 23
GF(5^2)	4	20	18	19	18 – 1 бр., 19 – 3 бр.
GF(5^3)	20	100	76	98	76 – 1, 96 – 6, 97 – 7, 98 – 6
GF(5^4)	48	500	492	497	492 – 1, 493 – 1, 494 – 3, 495 – 8, 496 – 16, 497 - 19
GF(7^2)	8	42	35	41	35 – 1, 39 – 1, 40 – 3, 41 – 3
GF(7^3)	36	294	288	292	288 – 1, 289 – 3, 290 – 3, 291 – 20, 292 – 9
GF(7^4)	160	2058	2050	2055	2050 – 2, 2051 – 2, 2052 – 9, 2053 – 23, 2054 – 58, 2055 – 66

От анализа на резултатите на линейната сложност в таблица 3 може да се направи изводът, че предложеният обобщен самосвиващ метод за внасяне на нелинейност позволява повишаване на еквивалентната линейност от стойност L до стойност

$$\lambda_{\max} = T - (L-1) = (p-1)p^{L-1} - (L-1). \quad (3)$$

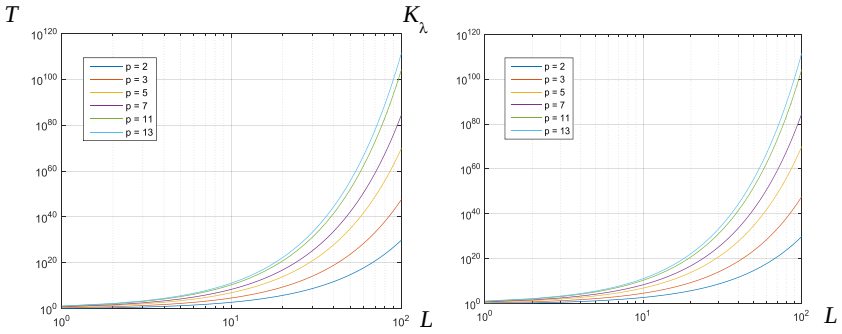
Следователно коефициентът на увеличаване на линейната сложност е

$$K_\lambda = \frac{(p-1)p^{L-1} - (L-1)}{L}. \quad (4)$$

Зависимостите на периода T и коефициента K_λ от дължината L на използвания *pLFSR* като градивен елемент на *GSSG* за различни стойности на простото число p от 2 до 13 са представени на фиг. 5.

4.2. Статистически свойства

За тестване на статистическите свойства на последователностите, генерирани от *pGSSG*, са анализирани резултатите от три различни генератора с обратни връзки. За всеки генератор са тествани по 100 различни последователности с дължина от по 1 000 000 бита всяка, генерирани при различни ядра на генератора (различни начални състояния на регистрите). В резултат са получени общо 300 x 209 = 62 700 *P–стойности*. Средните стойности от анализираните 100 *P–стойности* и 100 пропорции за всеки *NIST* статистически тест [16] са показани в таблица 4. Тъй като всички *P-стойности* ≥ 0.0001, последователността генерирана от *pGSSG* може да се смята за *непериодична с доверителна вероятност 99%.*



Фиг. 5. **Период T и коефициент на увеличаване на линейната сложност K_λ на pGSSG**

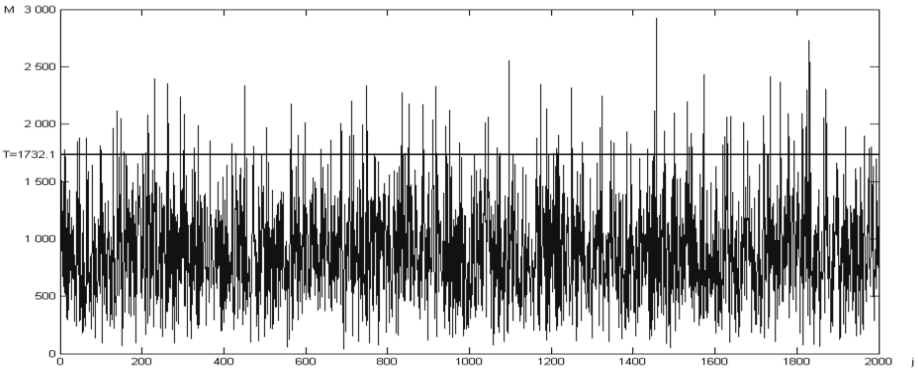
Таблица 4. *Резултати от NIST статистическите тестове на pGSSG*

№	Средно от 100 теста на 1ви *pGSSG*		Средно от 100 теста на 2ри *pGSSG*		Средно от 100 теста на 3ти *pGSSG*		Средно от всички 300 теста	
	P-стойност	Пропорция	*P*-стойност	Пропорция	*P*-стойност	Пропорция	*P*-стойност	Пропорция в %
1.	0,030806	100/100	0,657933	100/100	0,145326	100/100	0,278022	100,00
2.	0,883171	99/100	0,924076	100/100	0,474986	100/100	0,760744	99,67
3.C	0,509199	99/100	0,595769	100/100	0,463985	100/100	0,522985	99,67
4.	0,23681	98/100	0,383827	100/100	0,162606	100/100	0,261081	99,33
5.	0,23681	99/100	0,637119	98/100	0,419021	99/100	0,430983	98,67
6.	0,366918	99/100	0,816537	97/100	0,595549	100/100	0,593001	98,67
7.	0,008266	97/100	0,739918	99/100	0,334538	97/100	0,360907	97,67
8.C	0,496249	99/100	0,525565	99/100	0,496925	99/100	0,506246	99,00
9.	0,304126	99/100	0,759756	99/100	0,334538	98/100	0,46614	98,67
10.	0,55442	98/100	0,075719	97/100	0,013569	100/100	0,214569	98,33
11.	0,897763	100/100	0,851383	100/100	0,911413	97/100	0,886853	99,00
12.C	0,473029	52,5/53	0,603401	63/63	0,379424	58/59	0,485285	99,10
13.C	0,545429	53/53	0,522814	62/63	0,423782	58/59	0,497342	98,90
14.C	0,442316	99/100	0,263238	97/100	0,911102	100/100	0,538886	98,67
15.	0,28966	99/100	0,91141	100/100	0,75975	100/100	0,65361	99,67

4.3. Спектрални свойства

При извършване на статистическия Фурие анализ е избрано ниво на значимост $\alpha = 0.01$. Средните стойности на резултатите от Фурие анализа на изследваните 300 изходни последователности са представени в таблица 5, а модулите на честотните компоненти от *DFT* на *pGSSG* последователност на фиг. 6.

Тъй като *P-стойност* $\geq$ *0.0001*, последователността генерирана от *pGSSG* може да се смята за *непериодична с доверителна вероятност 99%.*



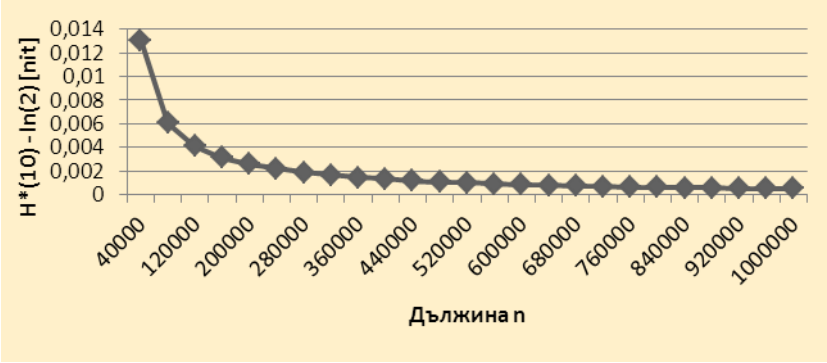
Фиг. 6. *Модули на честотните компоненти от DFT на pGSSG последователност*

Таблица 5. *Резултати от Фурие анализа на pGSSG*

Средна стойност	***P*-стойност**	**Пропорция**
от 100 теста на 1ви *pGSSG*	0,008266	97%
от 100 теста на 2ри *pGSSG*	0,739918	99%
от 100 теста на 3ти *pGSSG*	0,334538	97%
Обща средна стойност	**0,360907**	**97,67%**

4.4. Анализ на приблизителната ентропия

Целта на извършения тест е да сравни честотата на поява на застъпващи се блокове с две последователни дължини m и $m + 1$ в сравнение с очаквания резултат за случайна последователност [14], [15]. Тествани са същите 300 последователности с дължина 1 000 000 bits, като за изследването е използвано $m = 10$ и ниво на значимост $\alpha = 0{,}01$.



Фиг. 7. *Отклонение на приблизителната ентропия от идеалната в зависимост от дължината на генерираната pGSSG последователност*

За да се намери минималната дължина на *pGSSG* изходната последователност, над която последователността може да се счита за наистина случайна, се използва фактът, че приблизителната ентропия $H^*(m)$ клони към $\ln 2 = 0{,}693147$ при дълга случайна последователност [16].

Резултатите от изследването (фиг. 7) показват, че *pGSSG* генерира псевдослучайна последователност с идеални приблизителни ентропийни свойства при дължина на последователността, по-голяма от 5.10^5 бита. Следователно, препоръчително е *pGSSG* да се използва за криптиране на файлове с дължина по-голяма от 48 KB.

4.5. Криптоанализ на pGSSG

Целта на атаките към поточните шифри, използващи тактово управлявани генератори, е да се възстанови секретния ключ, който включва началните състояния на използваните *LFSRs*. За по-добра сигурност, секретният ключа може да съдържа и полиномът на обратните връзки. В този параграф теоретично се анализира сигурността на *pGSSG* чрез атаката на пълно претърсване и атака чрез ентропия [22, 23].

Тези атаки възстановяват началното състояние на предложения от Маер и Стефалбах *SSG* при известен малък сегмент от генерирания ключов поток съответно за $O(2^{0.79n})$ и $O(2^{0.75n})$ стъпки. При разглеждането на тези атаки се приема, че секретният ключ се състои само от началното състояние на *pGSSG*.

Сложността на атаката чрез пълно претърсване и тази чрез ентропия на *pGSSG* за просто *p* до 17 е сравнена с *SSG* и *MSSG* [7] в таблица 6. Резултатите показват, че *pGSSG* е по-сигурен от *SSG* и *MSSG* при тези атаки. Сложността на атаките се увеличава с увеличаване на простото число *p*.

Таблица 6. *Сравнение на сложността на атаката на пълно претърсване и тази чрез ентропия за SSG, MSSG и pGSSG*

Атаки	***SSG***	***MSSG***	***pGSSG***					
			***p* = 3**	***p* = 5**	***p* = 7**	***p* = 11**	***p* =13**	***p* = 17**
Пълно претърсване	$O(2^{0.79n})$	$O(2^{0.862n})$	$O(2^{1.464n})$	$O(2^{2.133n})$	$O(2^{2.612n})$	$O(2^{3.281n})$	$O(2^{3.532n})$	$O(2^{3.937n})$
Чрез ентропия	$O(2^{0.75n})$	$O(2^{0.833n})$	$O(2^{1.437n})$	$O(2^{2.066n})$	$O(2^{2.536n})$	$O(2^{3.210n})$	$O(2^{3.465n})$	$O(2^{3.879n})$

5. Заключение

Предложеният *p*-ичен обобщен самосвиващ генератор *pGSSG* позволява лесно и ефективно генериране на *p*–ична псевдослучайна последователност с повишена нелинейност. Доказаната експоненциална зависимост на периода *T и* линейната сложност λ на генерираната от *pGSSG* последователност от дължината на градивния *pLFSR* регистър позволява предложената архитектура да генерира нелинейни псевдослучайни последователности с много големи периоди на повторение при сравнително проста схема на управление.

Анализът на опитните резултати от *NIST* статистическите и спектрални тестове доказва, че *pGSSG* последователностите притежават характеристиките на псевдслучайни последователности с доверителна вероятност 99%. Посредством анализа на приблизителната ентропия е определена минималната дължина от 500 000 bits на *pGSSG* последователностите, след която те могат да се считат за случайни.

Направеният теоретичен криптоанализ на *pGSSG* посредством атака чрез пълно претърсване и ентропия доказва че *pGSSG* е по-сигурен от *SSG* и *MSSG* при тези атаки. Теоретичният анализ показва, че сложността на атаките се увеличава с увеличаване на простото число *p*.

Гореизброените свойства на предложения *pGSSG* генератор потвърждават факта, че той работи като напълно случаен генератор и неговият изход не може да се предскаже. Следователно, той постига основните цели на псевдослучайните генератори и може да се използва в криптографските системи.

ЛИТЕРАТУРА:

1. Coppersmith, D. H. Krawczyk, Y. Mansour, The shrinking generator, Advances in Cryptology – EUROCRYPT'93, vol.773 of LNCS, Berlin, Springer-Verlag, 1993, pp. 22-39.

2. Fúster-Sabatera A., Caballero-Gil P., Analysis of the generalized self-shrinking generator, Computers & Mathematics with Applications, Volume 61, Issue 4, February 2011, Elsevier Ltd, pp. 871-880.

3. Golic, J. Dj. M. J. Mihaljevic, A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance, Journal of Cryptology 3(3), 1991, pp. 201-212.

4. Goresky, Mark, and Andrew Klapper. *Algebraic Shift Register Sequences*. Cambridge University Press. 2012, ps. 514.

5. Helleseth, Tor, and P. Vijay Kumar. "Pseudonoise sequences." *The Mobile Communications Handbook* 257, 1999.

6. Hu, Y., Xiao, G. Generalized self-shrinking generator. Information Theory, *IEEE Transactions on*, 50(4), 2004, pp. 714-719.

7. Kanso, Ali. "Modified self-shrinking generator." *Computers & Electrical Engineering* 36.5, 2010, pp. 993-1001.

8. Klein, Andreas. *Stream Ciphers*. Springer-Verlag London. 2013, ps. 399.

9. Krause, M. BDD-Based Cryptanalysis of Keystream Generators, Advances in Cryptology — EUROCRYPT 2002, Lecture Notes in Computer Science, 2002, Volume 2332/2002, Berlin, Germany: Springer-Verlag, pp. 222-237.

10. Meier W., O. Staffelbach, Fast correlation attacks on certain stream ciphers, Journal of Cryptology 1(3), 1989, pp. 159-167.

11. Meier, W. O. Staffelbach, The self-shrinking generator. In A.De Santis, editor, Advances in Cryptology – EUROCRYPT '94, vol.950 of LNCS, Berlin, Springer-Verlag, 1995, pp. 205-214.

12. Mihaljevic, M.J. A faster cryptanalysis of self-shrinking generator, In J.Pieprzyk and J.Seberry, editors, Advances in Cryptology – ACISP '96, vol.1172 of LNCS, Berlin,1996, Springer-Verlag, pp.182-189.

13. Nenkov, N. V, Czvetkov K. S., On-Line Consultation Expert System in Insurance. Proceedings of E-learning Conference'07, IEEE, Computer science education, Turkey, Istanbul, 2007, p. 48 – 51.

14. Pincus, St., and R.E. Kalman. "Not all (possibly) "random" sequences are created equal." In *Proceedings of the National Academy of Sciences* 94(8), pp. 3513-3518, 1997.

15. Rukhin, A. "Approximate entropy for testing randomness." *Journal of Applied Probability*, vol. 37(1), pp. 88-100, 2000.

16. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., and Vo, S., NIST Special Publication 800-22rev1a: A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, April 2010.

17. Salmasizadeh, M. L. Simpson, J. Dj. Golic, E. Dawson, Fast correlation attacks and multiple linear approximations, Information Security and Privacy, ACISP'97, Lecture Notes in Computer Science 1270, 1997, pp. 228-239.

18. Sarkar, P., and S. Maitra. "Construction of nonlinear Boolean functions with important cryptographic properties." *Advances in Cryptology—EUROCRYPT 2000*. Springer Berlin Heidelberg, 2000.

19. Schneier, B. Applied Cryptography, Jhon Wiley & Sous Inc., 1998, ps. 758.

20. Sidek, M., Rahim, A., and Sha'ameri, A. Z. Comparison analysis of stream cipher algorithms for digital communication. Jurnal Teknologi, (46D), 2007, pp. 1-16.

21. Siegenthaler, T. Decrypting a class of stream ciphers using ciphertext only, *IEEE Transactions on Computers*, 34(1), 1985, pp. 81-85.

22. Tasheva, A. T, **Tasheva, Z. N.**, Milev, A. P. Generalization of the Self-Shrinking Generator in the Galois Field GF(p^n). Advances in Artificial Intelligence, Hindawi Publishing Corporation, Volume 2011:2, Article ID 464971, 10 pages.

23. Tasheva, A. Some cryptanalysis of ap-ary generalized self-shrinking generator. In: *Proceedings of the 13th International Conference on Computer Systems and Technologies*. ACM, 2012. pp. 126-133.

24. Zhang, B. Feng D., New Guess-and-Determine Attack on the Self-Shrinking Generator, Advances in Cryptology – ASIACRYPT 2006, Lecture Notes in Computer Science, 2006, Volume 4284/2006, Berlin, Germany: Springer-Verlag, pp. 54-68.

25. Zivkovic, M. An algorithm for the initial state reconstruction of the clockcontrolled shift register, *IEEE Transactions on Information Theory 37*, 1991, pp. 1488-1490.

АНОНИМИЗИРАЩИТЕ МРЕЖИ И НАЦИОНАЛНАТА СИГУРНОСТ: КЪДЕ Е ГРАНИЦАТА НА ЛИЧНОТО ПРОСТРАНСТВО?

Иво Е. Емануилов

Фондация „Право и Интернет“
гр. София, 1303, район „Възраждане“, ул. „Българска морава“ № 54, етаж 7

ANONYMISING NETWORKS AND NATIONAL SECURITY: WHERE ARE THE BOUNDARIES OF PRIVACY?

Ivo E. Emanuilov

Law and Internet Foundation, Sofia, 1303, Vazrazhdane District, 54 Balgarska Morava, floor 7

ABSTRACT: *Anonymising technologies have gradually become an important tool in the protection of citizens' and human rights activists' privacy. Many of these technologies are also used for illegal purposes by terrorists and organised crimes groups that aim to remain anonymous in order to escape criminal prosecution. Privacy has never been a subject of so much debate, yet it has also never been as jeopardised by mass surveillance as it is now. The present article has two parts. The first analyses the technical background of anonymising technologies and the second focuses on the legal issues emerging from their pervasive use.*

KEY WORDS: *anonymity, privacy, security, surveillance, Tor*

1. Въведение

Думата „анонимност“ произхожда от старогръцки и в буквалния си превод означава „*да бъдеш без име*“, безименен. „*Псевдонимност*“ е друго, близко по смисъл понятие, което се свързва с идеята даден човек да използва друго име или самоличност вместо своите собствени. [1]

Различни причини мотивират хората да искат да останат анонимни или да се представят с псевдоним. Те се простират от проява на артистичност до желание за прикриване на извършено престъпление. В исторически план развитието на Интернет премахва редица пречки, които не позволяват на хората да останат анонимни. И въпреки тази констатация, все още остава изключително трудно за обикновения гражданин да запази ненакърнена своята анонимност в световната мрежа. Както протоколът IPv4, така и протоколът IPv6 притежават като присъща

своя характеристика направление на съответния IP[2] адрес, който може да бъде проследен до крайно физическо устройство, а следователно – и до неговия притежател. Оказва се, че е изключително лесно нечия самоличност да бъде разкрита чрез доставчика на интернет услуги. Поради технологичната необходимост IP адресът да бъде уникален не е възможно постигането на пълна анонимност. Това от своя страна налага използването на алтернативни способи, които се основават на концепцията за „правдоподобното опровержение“.[3] Пренесена в интернет пространството, тази концепция днес се свежда най-общо до използването на проксита и тунелиране, които скриват самоличността на автора на дадено съобщение.

2. Анонимизиращи мрежи и методи за анонимизиране

За целите на настоящото изследване понятието „анонимизираща мрежа“ следва да се разбира най-общо като мрежа от сървъри, чиято цел е да гарантира на потребителите си високо ниво на анонимност и опазване на личното им пространство. Анонимизиращите мрежи не са алтернативни на световната мрежа инфраструктури, доколкото те позволяват на потребителите си да споделят информация през публични мрежи, без това да нарушава личното им пространство.[4]

Наред с понятието „анонимизираща мрежа“ в изследването се използва и понятието „анонимизиращи методи“, което е по-широко по обхват. Под „анонимизиращ метод“ следва да се разбира метод, който има за цел да затрудни разкриването на част или на целия трафик в дадена мрежа, както и източниците на съдържание както спрямо субектите с достъп, така и по отношение на тези без достъп до инструментите на съответния метод.[3] Най-често подобно „скриване“ на трафика се осъществява посредством маршрутизиране на съобщенията през мрежа от устройства, които изпълняват функции за постигането на тази цел. Скриването на самото съдържание на съобщенията пък включва използването на различни криптографски методи.

Съществува и една специална форма на анонимизиране, която се свързва с използването на псевдоними. При този метод съобщенията могат да се свържат с конкретен псевдоним, но псевдонимът не може да бъде свързан с конкретно лице или компютър.

Два са начините, по които може да се установи връзка между изпращащ или получател и дадено съобщение – чрез анализ на трафика или чрез анализ на съдържанието. Според van Deen [3] анализът на трафика включва установяване и анализ на четири типа информация:

---

[2] Internet Protocol

[3] Правдоподобното опровержение е понятие от американското право и политика, в основата на което стои екскулпирането посредством неразкриване на връзката между причинителя и настъпилия резултат. В политически смисъл това е основната отлика между тайните и открити политически действия, доколкото за тайните винаги съществува подобно „правдоподобно опровержение“. Понятието има и второ значение в областта на криптографията и то се свързва с различни стеганографски техники, чрез които се отрича самото съществуване на криптиран файл или съобщение, тъй като насрещната страна не може да докаже дали такова криптирано съобщение действително съществува. [1]

[4] Вж. напр. https://www.torproject.org/about/overview.html.en

- кои компютри изпращат съобщения в даден момент;
- кои компютри получават съобщения в даден момент;
- какви или колко данни са изпратени;
- какви или колко данни са получени.

Анализът на съдържанието включва анализ на хедърите на съобщението[5] и на неговото съдържание чрез декриптиране и разтълкуване на съдържанието на полученото съобщение.

В литературата се предлагат различни класификации на анонимизиращите методи. Съществува класификация [6], която обединява всички анонимизиращи методи под общото наименование технологии за опазване на личното пространство (privacy enhancing technologies, PET). Според тази класификация основните анонимизиращи способи са: проксита; тунелиране и виртуални частни мрежи; методи, използващи системата за имена на домейни (DNS), както и т. нар. „луково маршрутизиране“ (onion routing). Други автори [3] възприемат по-обща класификация, като разделят технологиите, които осигуряват анонимност, на Mix и Peer-to-Peer базирани. Тази класификация почива на протоколите, които стоят в тяхната основа.

В основата на идеята за анонимизиращите мрежи стои понятието *Mix* Концепцията е разработена от Дейвид Чом[6] през 1981 г., като основната идея е създаването на трудни за проследяване маршрутизиращи протоколи, които използват верига от прокси сървъри, известни като *mixes*. Т. нар. *Mix* представлява маршрутизатор, който скрива комуникацията между входящи и изходящи съобщения. В този случай с понятието „комуникация“ се означава възможността да се направи връзка между входящи и изходящи съобщения и по този начин да се направят изводи за данните, които се обменят. Тази връзка се премахва в две стъпки.

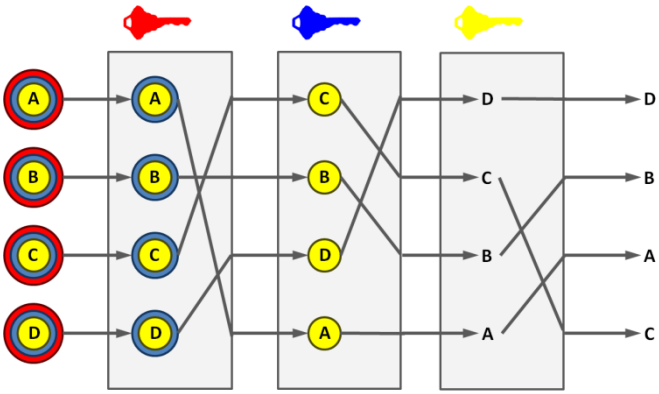
На първо място следва да се промени начинът, по който изглежда съобщението за външния свят (т. е. за публичните мрежи) – напр. чрез добавяне на случайно генериран символен низ към оригиналното съобщение и последващо криптиране.

Втората стъпка включва промяна на потока на съобщенията – или иначе казано на реда, по който съобщенията влизат и излизат от маршрутизатора. Това може да се постигне посредством задържане на входящите съобщения за определен период от време, смесването им (*mixing* – от тук и наименованието на протокола) с други входящи съобщения и изпращането им в този случайно разбъркан ред. *Mix* осигурява анонимизиране и по този начин възпрепятства анализа на трафика. Начинът, по който съобщението „изглежда“, се променя от един *Mix* до следващия и съобщенията не могат да бъдат проследени по размер или по битове, нито пък могат да бъдат проследени от реда на съобщенията, доколкото последният е напълно случаен. Криптирането в този случай може да се прилага по някой от следните начини: от точка до точка, от край до край или като комбинация от двете. Начинът на действие може да бъде илюстриран по следния начин (фиг. 1)[7]:

[5] Вж. повече за хедърите в стандарта за формата на ARPA интернет текстови съобщения, достъпен на адрес: https://tools.ietf.org/html/rfc822

[6] https://en.wikipedia.org/wiki/David_Chaum

[7] Изображението е взето от https://en.wikipedia.org/wiki/File:Decryption_mix_net.png и се разпространява под лиценз Creative Commons Attribution-ShareAlike 3.0



Фиг. 1. Криптиране и декриптиране в Mix мрежа

Най-общо съответният *Mix* приема съобщения от множество изпращачи, разбърква ги и ги изпраща обратно в случаен ред на следващото звено във веригата (най-често – друг *mix*). Именно по този начин се постига прекъсването на връзката между изпращача и получателя. Всяко съобщение се криптира в отделния маршрутизатор посредством криптография с използване на публични ключове. По този начин се създава модел на криптиране, подобен на руските кукли матрьошки, в който последната кукла, образно казано, всъщност е самото съобщение. Анонимността на изпращача не е гарантирана спрямо входната точка, а на получателя – спрямо изходната точка, без значение от наличието на криптиране [1].

Вторият основен модел на анонимизиране е този на *peer-to-peer* (P2P), който представлява мрежова архитектура, която не се основава на традиционния модел клиент-сървър. При този модел съществуват равнопоставени точки, всяка от които осигурява едновременно функционалността както на сървър, така и на клиент. Различните участници предоставят своите ресурси директно на разположение на другите мрежови участници без необходимост от централизирана мрежова инсталация. В този случай съобщенията се маршрутизират през т.нар. *пиъри* (участници), докато съобщението достигне крайната си точка. Съществуват два основни вида P2P мрежи: публични и частни. Публичните мрежи дават възможност на всеки да се присъедини към мрежата като участник, докато частните се основават на кръг от потребители, които се ползват с определен кредит на доверие. Тъй като тези мрежи са по-уязвими на атаки в сравнение с мрежите, основани на *mix* протоколите, се е наложило разработването на методи, които да позволят установяването на комуникационен канал между изпращач и получател, който да не разкрива тяхната самоличност пред останалите участници. За целта са разработени и съществуват два основни метода, а именно – осъществяване на връзка, основана на псевдоними (*Ants*), или на файлови дескриптори (*Freenet*)[8].

[8]Файловите дескриптори (също файлови манипулатори в българската литература) следва да се разбират като абстрактен индикатор, който се използва за достъп до файлове или други входно-изходни ресурси. Дескрипторите обикновено се съхраняват като неотрицателни цели числа от тип integer, които в програмния език C са представени като тип int. Те са част от

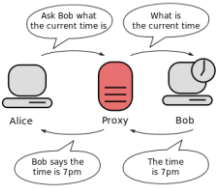
В следващата точка са представени такива конкретни имплементации, които са относими в съвременния свят и които се използват за постигане на анонимизация.

3. Анонимизиращи технологии

Различните технологии за опазване на личното пространство (PET), представляват различни имплементации на описаните в предходната точка протоколи. Тук те са накратко представени, доколкото тяхното използване поставя редица проблеми от гледна точка на информационната сигурност, а следователно – и от правна гледна точка.

3.1. Прокси

Прокси представлява компютърна услуга, която събира заявките от клиенти и ги препраща към местоназначението им от тяхно име. След получаване на отговор, проксито връща информацията на заявителя. В този смисъл проксито се явява посредническа услуга между началната и крайната точка. Тя може да бъде илюстрирана със следното изображение (фиг. 2):



Фиг. 2. Прокси

Въпреки че проксито възниква преди десетилетия като идея за създаването на мощна рамка за системите за разпределени изчисления, понастоящем проксита се използват за наблюдаване и филтриране на интернет съобщения. Съществуват различни видове прокси услуги, сред които уеб проксита, проксита по Hyper Text Transfer Protocol, както и Secure Socks (SOCKS) проксита [6]

3.2. Виртуална частна мрежа

Виртуална частна мрежа (Virtual Private Network, VPN) е най-разпространеното решение за мрежово тунелиране. В основата на тунелирането стои създаването на връзка за предаване на данни между две точки, които са краищата на тунела. Така създадената връзка позволява предаването на данни по начин, че за източника и получателя цялата мрежова инфраструктура, която се намира между тези две точки, остава скрита. То служи за пренасочване на целия или част от мрежовия трафик през различен междинен възел. От техническа гледна точка виртуалната частна мрежа е частна мрежа и представлява взаимна свързаност за информационен обмен между различни субекти, които са част от тази мрежа. Този тип мрежи се използват за достъп до вътрешни мрежи, напр. интранет ресурси. Тъй като трафикът през виртуалната частна мрежа е криптиран и същата може да се използва като прокси,

---

POSIX модела на операционната система UNIX и служат като индекс в таблица, поддържана от ядрото на операционната система, която следи за това кои файлове са отворени за четене или запис от даден процес.

този тип технология може да служи за преодоляване на технически мерки, които имат за цел цензуриране и контролиране на достъпа до Интернет. Посредством виртуална частна мрежа дадено лице може да се свърже с компютър, който не се намира в тази затворена среда, а осъществяването на достъп до търсения ресурс в Интернет всъщност заобикаля цензурата.

Виртуалната частна мрежа има редица предимства пред прокситата. Така например VPN използва Internet Protocol Security (IPSec) или SSL протоколи, които криптират връзката. Предимства като поверителност, интегритет и автентикация са присъщи на виртуалните частни мрежи, така че дори в случай че мрежовият трафик се следи, онова, което е видимо за едно трето лице, ще бъде криптирано, а няма да бъде представено като обикновен текст (plain text).

Виртуалните частни мрежи имат един недостатък и той се свързва с обстоятелството, че IP адресът на VPN сървъра може да бъде открит, а обикновеното му блокиране би било достатъчно, за да се осуети опитът за заобикаляне на наложени технически ограничения.

3.3. Заобикаляне, основано на системата за домейн имена (DNS)

Системата за домейн имена представлява механизъм за транслиране, който преобразува имената на домейни в IP адреси. Тъй като запаметяването на дадено име или друг идентификатор е значително по-лесно от помненето на IP адреси, които са дълги поредици от цифри, осигуряването на достъп до Интернет посредством DNS е значително по-лесно. Така, за да посети даден уебсайт, за потребителя е достатъчно да въведе адреса на уебсайта, а не неговия IP адрес. Останалата част от процеса се осъществява от DNS, който преобразува словесното наименование в IP адреса за съответното име на домейн и препраща заявката към сървъра.

Доколкото първоначалната стъпка в така описания процес включва идентифициране на IP адреса на дадена услуга, DNS сървърът може да се конфигурира по начин, че да блокира тази услуга. Ако дадено име на домейн е включено в т.нар. „черен списък“, DNS просто ще блокира достъпа до този уеб сайт, като не отговаря на заявката. Възможно е DNS да бъде конфигуриран да връща различен IP адрес за конкретна заявка, в който случай на заявката ще бъде отговорено с напълно различен адрес, който ще води до друг уебсайт.

Преодоляването на такива DNS филтри не е сложно. Ако търсеният ресурс или уебсайт не е блокиран, достатъчно е пренасочване на заявката към друг DNS сървър, на който няма активни филтри. В другия случай, ако IP адресът на сървъра е известен, може да е възможно да се получи директен достъп по IP адрес. Тъй като обаче много уебсайтове се обслужват от виртуални хостинг сървъри със споделени IP адреси, този метод много често няма да бъде ефективен. Типичен пример за опит за налагане на цензура посредством DNS филтриране е случаят с Twitter от март 2014 г., когато турското правителство, твърдейки, че Twitter отказва да се съобрази със съдебни разпореждания в Турция, блокира достъпа до услугата. По данни от информационни агенции и изследователи в областта на информационната сигурност мнозина граждани просто са конфигурирали системите си с различни DNS настройки и са използвали отворената услуга на Google - Open DNS, преодолявайки по този начин наложените ограничения.

3.4. „Луково маршрутизиране“ (Onion Routing)

Луковото маршрутизиране е свободен *Mix* протокол, който използва криптографската система Onion, за да гарантира, че между изпращач и получател на едно съобщение не може да бъде установена връзка. При луковото маршрутизиране изпращачът изпраща съобщение на получателя посредством определен от изпращача набор от *Mix* възли, познати още като *Core Onion Routers* (COR). Всеки от тези маршрутизатори има собствен публичен криптографски ключ.

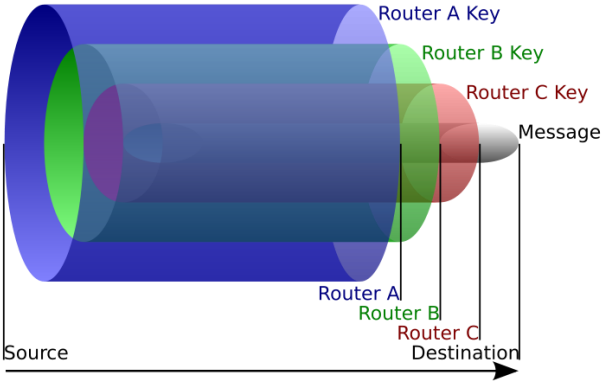
Съобщенията се изпращат като *Onions*. Това са криптирани съобщения, които, когато бъдат декриптирани, се състоят от три части. Първата част съдържа адреса на следващия възел по пътя (следващият COR или пък крайната точка). Втората част съдържа набор от симетрични ключове. Последната част е самото съобщение, което трябва да се предаде на следващия възел по пътя. Когато следващият възел е крайната точка, това съобщение ще бъде оригиналното съобщение, предназначено за получателя. Когато следващият възел е друг COR, съобщението ще бъде друг *Onion*, криптиран с публичния ключ на този конкретен COR. Тази слоеста структура на криптиране гарантира, че всеки COR знае само предходната и следващата точка от пътя, както и че нито един COR не вижда едно и също съобщение и че съобщението не може да бъде декриптирано, преди да достигне получателя си.

Описаният набор от симетрични ключове, които съставляват втората част на т.нар. *Onion*, са ключовете, които COR използва при свързването си с предходната и със следващата точка. Промяната в криптирането се налага заради факта, че публичният ключ е неефективен метод, когато се използва в продължителна комуникация. Криптирането със симетрични ключове е значително по-лесно и бързо и позволява за осъществяването на елегантно двупосочно свързване. По тази причина след изпращането на първия *Onion* и получаването на съответните симетрични ключове от COR, изпращачът криптира по-нататъшните съобщения с всички симетрични ключове в обратен ред. По този начин се създава луковата структура на криптирането, без да се налага преодоляване на трудностите, създавани от публичните ключове. Тази структура е илюстрирана от изображението по-долу[9]:

Даден потребител може да се свърже с COR по два начина: чрез свързване с отдалечен COR или чрез създаване и поддържане на собствен COR, използвайки го като входна точка на пътя. Първият метод е щадящ от гледна точка на ресурси и позволява на клиента да използва мрежа с луково маршрутизиране, без самият той да става маршрутизатор. Вторият метод е с по-голяма сигурност, тъй като съобщенията до собствения COR минават през приложния слой и няма начин други възли по пътя да знаят дали съобщението, изпратено от COR, е създадено от даден потребител или просто е било предадено от него.

---

9 Изображението е взето от http://commons.wikimedia.org/wiki/File:Onion_diagram.svg и се разпространява от Harrison Neal под лиценз Creative Commons Attribution-Share Alike 3.0 Unported



Фиг. 3. Луково маршрутизиране

В този пример (фиг. 3) източникът на данните (Source) изпраща *Onion* на Маршрутизатор A, който декриптира криптиращия слой, за да разбере до кой следващ възел да го изпрати. Маршрутизатор A го изпраща до Маршрутизатор B, който декриптира друг слой, за да разбере следващата точка от пътя. Маршрутизатор B изпраща на Маршрутизатор C, който декриптира последния слой на криптирането и предава оригиналното съобщение на получателя му.

3.5. Ants

Ants е P2P протокол за осъществяване на анонимна комуникационна връзка между два псевдонима. Всеки възел в Ants мрежата съхранява маршрутизираща таблица, в която записва три стойности, както следва: адрес на местоназначението (Destination Address), следващата точка от пътя (Next Hop) и т.нар. *феромонна стойност* (Pheromone Value), която означава вероятността следващата точка от пътя да е налична.

При получаване на заявка от изпращача мрежата записва изпращача като адрес на местоназначението, предходния възел като следващ възел за достигане на изпращача и същевременно увеличава феромонната стойност. Същата операция се повтаря в обратен ред, когато получателят изпраща своя отговор. Последващата комуникация между изпращач и получател се осъществява през точките с най-висока феромонна стойност. Комбинацията от феромонната стойност за местоназначението и следващата точка от пътя се увеличава всеки път, когато съобщение от местоназначението достигне възела през следващата точка от пътя. В противен случай тази стойност намалява с времето. Ants съобщенията носят единствено IP адреса на последната точка (broadcaster) и съобщението на получателя. Както изпращачът, така и получателят получават псевдоними, така че съобщението не носи никакви идентифициращи информация.

3.6. Freenet

Freenet е P2P протокол, който свързва потребителите не с конкретни компютри или потребители, а с конкретни файлове. Всеки файл, съхраняван във Freenet, има определен хеш код и е криптиран със специфичен ключ в зависимост от метода на хеширане. Всеки участник в мрежата съхранява таблица, която съдържа хеш стойностите, които са преминали през него заедно с адреса на съответния участник. Когато потребителят иска да намери даден файл, той генерира заявка за хеш стойността на файла заедно с брояч за *Hops-To-Live* (HTL) и го изпраща на софтуера, който проверява дисковото съдържание на потребителя за съответната хеш стойност. В случай че е открита такава, съответният файл се доставя на потребителя. В случай че не е открит, броячът се намалява с единица и се претърсва базата данни с хеш стойности за участник, който съхранява хеш стойността и заявката се препраща към него. В случай че няма съвпадение, заявката се предава на участика с лексикографски най-близка хеш стойност, който повтаря същата процедура, докато броячът HTL не достигне нула.

При откриване на файла той се предава по веригата от участници, като всеки участник съхранява файла локално. Това копиране на исканите файлове стои в основата на разпределеното споделяне на файлове и по този начин гарантира дълготрайното съхранение на даден файл.

По подразбиране Freenet не включва никакво криптиране от точка до точка, което означава, че технологията е уязвима на методи за анализ на трафика въз основа на размерите на отделните пакети. Това означава, че едно съобщение може да бъде проследено изключително лесно през отделните възли. От гледна точка на съдържанието Freenet отново не осигурява анонимност, тъй като всеки възел съхранява търсените данни и в случай че са намерени файлове, всички участници по веригата придобиват качеството получатели. Анонимността на изпращача е в известна степен в по-добра степен защитена, доколкото отделните възли не знаят своята позиция във веригата, т.е. не могат да знаят дали заявката е оригинална, или е предадена.

Всички представени технологии имат своите предимства и недостатъци по отношение на осигуряването на анонимността на своите потребители. Една от тях обаче предизвиква по-сериозен научен и практически интерес, доколкото стои в основата на най-популярната услуга за анонимизиране – Tor, а именно – луковото маршрутизиране.

4. Мрежата Tor

Според официалното определение на уебсайта на проекта Tor мрежата Tor представлява група от доброволно създадени и поддържани сървъри, които позволяват на хората да повишат нивото на защита на личното си пространство и сигурността си в Интернет. Потребителите на мрежата се свързват помежду си посредством набор от виртуални тунели вместо директно, което им позволява да споделят информация в публични мрежи, без това да нарушава тяхното лично пространство.

Tor позволява на своите потребители да изпращат анонимно данни по Интернет, защитавайки местонахождението на източника. Това се постига чрез сложна криптираща мрежа, която отклонява интернет съобщенията от IP адреса на техния източник. Основната технология, която стои зад Tor мрежата, е разгледаното по-

горе луково маршрутизиране. Различните възли в мрежата са прокси сървъри, които се намират по целия свят. Потребителите на мрежата се свързват с нея, като първо се включват в списък от възли, поддържан от сървър с директорийни услуги. Компютърът на потребителя се свързва с мрежата през произволен такъв възел. Информацията за потребителя се маршрутизира през произволен набор от възли, преди да достигне крайната точка, която изпраща информацията в Интернет. Както вече се отбеляза, най-характерната особеност на тази технология е, че всеки възел комуникира единствено с възела, който непосредствено го предхожда, и с възела, който непосредствено го следва по пътя. По този начин компютърът на потребителя има връзка единствено с първия възел по пътя, а Интернет комуникира единствено с изходния възел. Входният възел не знае крайното местоназначение на данните, а изходният възел не знае произхода на данните. Доколкото единствено изходните възли комуникират директно с публичния Интернет, само маршрутизираният през тях трафик може да бъде проследен. Всяко съобщение се криптира с нов слой криптиране, преди да премине към следващия възел. Слой по слой криптирането се премахва с наближаването на изходния възел, откъдето всъщност произхожда и метафората с лука.

Tor е определян от технологична гледна точка като комуникационна услуга с ниска латентност, т.е. забавянето в отделните сесии е изключително малко за повечето потребители. Забавянето се проявява вследствие на режима на действие. Обикновените Интернет връзки винаги търсят най-краткия, най-бързия и най-ефективния маршрут в зависимост от избрания алгоритъм, а доставчиците на интернет услуги винаги доставят пакетите по най-ефективния начин. При Tor механизмът на действие е съвсем различен, тъй като се създава самостоятелен маршрут (circuit). Започвайки с крайния потребител, мрежовите пакети следват различни точки (relays) до последната точка от маршрута – изходната точка (exit relay). Изходната точка след това предава заявката на местоназначението. Всички връзки между първата точка и изходната точка са криптирани и никой не знае пълния маршрут.

Създаването и поддържането на изходна точка от потребител е противоречив въпрос, който поражда редица правни въпроси. Въпросът е съществен, защото изходните точки са интерфейса на мрежата Tor с Интернет. Една от основните цели на мрежата Tor е защитата на самоличността на нейните потребители. Същевременно обаче в рамките на тази мрежа могат да бъдат защитени и различни ресурси като напр. уеб услуги. Тази възможност на мрежата се нарича „скрити услуги“ (Hidden Services). Тя почива върху концепцията за т.нар. *rendezvous* точки в мрежата. Вместо да се използва адрес за назначение на сървър и да се осъществява директно свързване със сървър, клиентът използва идентификатор, за да намери сървъра. Идентификаторът се състои от наименование от 16 символа, което следва от публичния ключ на услугата (напр. *xyz.onion*). След като е открита такава точка, клиентът и сървърът се „срещат“ на тази точка, без нито една от страните да знае действителното местонахождение на другата. Основната цел на скритите услуги е да осигурят контролиран достъп и скриване на действителната самоличност на администраторите на скрити услуги. В рамките на скритите услуги трафикът никога не напуска мрежата Tor.

Така описаната архитектура на Tor мрежата поставя редица въпроси от обществено и правно значение. Макар и първоначалният замисъл на мрежата Tor да

е тя да служи в името на опазването на самоличността на гражданите в рамките на публичните мрежи като проявление на упражняване на тяхното право на лично пространство, неприкосновеност на кореспонденцията, свободата на изразяване и др. Същевременно обаче с популяризирането на мрежата нараства и броят на случаите на използването ѝ за незаконосъобразни цели. Тези въпроси са предмет на анализ в следващата точка.

5. Правни проблеми на анонимизиращите мрежи – между националната сигурност и личното пространство

Правните проблеми, свързани с използването на анонимизиращи мрежи като Tor и други услуги, обхващат няколко категории проблеми, както следва:

- дейностите на правителствата, свързани с Tor, и опазването на националната сигурност;
- използването на анонимизиращи мрежи за защита на основните човешки права;
- отговорност на операторите за съдържанието, което преминава през изходните точки в Tor мрежата;
- наблюдаване и следене на изходните точки в Tor мрежата.

5.1. Опазването на националната сигурност

Анонимизиращите технологии се използват от гражданите за ефективно упражняване на правото им на лично пространство при използване на публични мрежи като Интернет. Подобни технологии обаче представляват интерес и за други субекти – от държави до организирани престъпни групи.

ЕВРОПОЛ посочва, че през 2014 г. около 27 уебсайта са свалени от мрежата Tor.[10] Не е известна публично достъпна информация относно това по какъв начин разследващите органи са успели да „пробият“ Tor и да разкрият самоличността на потребителите зад тези скрити услуги. Посочва се, че методите не се разкриват поради тяхната „чувствителност“ и поради обстоятелството, че сървърите се намират в чужди държави, което очевидно е наложило достъп до тях, който може и да не е бил законосъобразен.

Така се поставя въпросът къде националната сигурност оправдава използването на средства за разследване по незаконосъобразен начин. В контекста на международното право, ако една държава получи достъп до сървъри, които се намират на територията на друга държава, и ги премахне, подобно действие би трябвало да се основава най-малкото на съгласието на тази чужда държава, дадено съгласно правилата на международното право, било конвенционно, било по силата на международен обичай. Във всеки друг случай подобно действие би следвало да се окачестви като нарушаване на суверенитета на една чужда държава.

Все по-често националните правоохранителни и разследващи органи и агенциите за национална сигурност използват Tor като инструмент за разследване и разузнаване. Проектът Tor изброява на официалната си уеб страница най-честото срещаните случаи на използване на Tor от подобни органи.[11] В обобщен вид това са дейности по:

[10] https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network

[11] https://www.torproject.org/about/torusers.html.en#lawenforcement

- **наблюдение и следене на електронните съобщения**, което включва проследяване на подозрителни уебсайтове и услуги, което се осъществява при пълна анонимност без оставяне на следи. Напр., ако администраторът на нелегален сайт за онлайн залагания засече заявки от правителствени IP адреси в лог файловете[12] на сървърите, от които се предоставя достъп до този сайт, дейностите по разследване биха могли да бъдат възпрепятствани;
- **тайни операции**, които включват разследване в Интернет, доколкото появата на съобщения от IP адрес на полицейско управление компрометира сериозно всяко прикритие;
- **напълно анонимни „горещи линии“ за подаване на сигнали**, които, макар и популярни, са значително по-малко полезни без използването на анонимизиращи технологии. Източниците на такива сигнали си дават сметка, че макар към техния сигнал да не се прикрепя идентифициращa ги информация, лог файловете от сървъра могат да ги идентифицират много лесно.

Tor се използва от държавите като средство за провеждане на разследвания, разузнавателни дейности и инфилтриране. Това е видно и от скорошното премахване на Silk Road 2.0 (нелегален онлайн пазар за наркотични вещества), който съществуваше в мрежата Tor.

Правните въпроси, които подобно използване на анонимизиращи технологии поражда, могат да се формулират по следния начин: дали съществуват ограничения в използването на подобни средства от разследващи и разузнавателни органи за събиране на доказателства и ако данните, достъпни чрез Tor или в самата Tor мрежа, се смятат за публично достъпни, дали има ограничения при тяхната обработка.

Рамката за дейностите на правоохранителните и разузнавателните органи се урежда в националното право на отделните държави и режимът може да разкрива големи разлики между тях. Този извод се отнася с пълна сила до събирането на електронни доказателствени средства, които пораждат трудни въпроси пред националното процесуално право. Използването на Tor за събиране на доказателствени средства от страна на разследващите органи в редица държави би представлявало нарушаване на действащия наказателно-процесуален ред.

В България според Наказателно-процесуалния кодекс (НПК) доказване може да се осъществява само чрез изрично изброените в чл. 136, ал. 1 от НПК способи на доказване, сред които попадат разпит, експертиза, оглед, претърсване, изземване, следствен експеримент, разпознаване на лица и предмети и специални разузнавателни средства. Един от проблемите при всеки един от изброените способи за доказване, с изключение на разпита, експертизата и специалните разузнавателни средства, е изискването за осигуряване на поемни лица съгласно чл. 137 от НПК. При използването на анонимизиращи способи разследващият орган извършва дейност, при която той не идентифицира себе си като орган на досъдебното производство, а и няма как да бъдат осигурени поемни лица при дейност, която предполага по дефиниция анонимността на разследващия орган и се осъществява онлайн. В този смисъл, ако се приеме, че разследващата дейност посредством Tor мрежата има характера на претърсване и изземване а компютърни

[12] Лог файловете са файлове, в които се отбелязват различни събития, които се случват в една система в хронологичен ред.

информационни данни, то същата следва да се извършва в присъствието на лицето, което използва помещението, или на пълнолетен член на семейството, на поемни лица и на технически помощник (арг. от чл. 162, ал. 1 вр. с чл. 162, ал. 6, вр. с чл. 163, ал. 6). Очевидна е празнотата в уредбата по отношение на събирането на електронни доказателствени средства и тя не може и не следва да бъде запълнена по тълкувателен път.

По-различно стои въпросът със специалните разузнавателни средства като способ на доказване в наказателния процес. Бидейки извънредна мярка, при която се ограничават неприкосновеността на личността и жилището и тайната на кореспонденцията и на другите съобщения, използването на специални разузнавателни средства би могло да се разгледа във връзка с дейности на компетентните органи по разследване в мрежата Tor.

Съгласно разпоредбата на чл. 2, ал. 2 във връзка с чл. 2, ал. 1 от Закона за специалните разузнавателни средства (ЗСРС) специалните разузнавателни средства могат да са технически средства и оперативни способи за прилагането им. Техническите средства са определени като електронни и механични съоръжения, както и вещества, които служат за документиране на дейността на контролирани лица и обекти. Оперативните способи пък са наблюдение, подслушване, проследяване, проникване, белязване и проверка на кореспонденцията и компютризираната информация, контролираната доставка, доверителната сделка и разследването чрез служител под прикритие. Разпоредбата на чл. 4 от ЗСРС пък предвижда, че специални разузнавателни средства по реда на този закон могат да се прилагат и за дейности, свързани със защитата на националната сигурност. Осъществяването на наблюдение, подслушване, проверка на кореспонденция и компютризирана информация са все способи, които могат да бъдат приложени посредством използване на мрежата Tor. Доколкото законът запазва технологична неутралност и не определя изрично техническите средства, които могат да се използват, мислима е хипотезата, в която се прилагат подобни разузнавателни средства. Въпреки това, следва да се държи сметка на обстоятелството, че поради анонимния характер на мрежата затрудненията при доказването ще дойдат както от посока на това, че обвиняемият или подсъдимият ще оспорва достоверността на събраните доказателства и факта, че те действително са свързани с осъществявана от него дейност, но също и от посока на това, че компетентният орган ще срещне затруднения да удостовери, че събраните доказателства действително се отнасят до лицето, за което се подозират обстоятелствата по чл. 12 от ЗСРС.

Налага се изводът, че при хипотезите на специални разузнавателни средства е мислимо използването на анонимизиращи технологии от страна на разследващите и разузнавателните органи с цел постигане на целите на разследването – пресичане, предотвратяване и разкриване на престъпления. В този смисъл ограничаването на личното пространство и на някои основни човешки права е допустимо, но само и единствено доколкото е съобразено с рамката, предоставена от действащото законодателство.

Доколкото мрежата Tor се разглежда в контекста на наказателния процес като източник на разузнаване с отворен код (Open Source Intelligence, OSINT), би трябвало да се вземат предвид и някои съображения от гледна точка на обработването на лични данни. Макар и Tor да се използва за анонимизиране на потребители, а техните IP адреси да са скрити зад видимите адреси на изходните

точки и следователно техните личните данни да не са публично достъпни до всички, това не изключва съхраняването на лични данни в бази данни, които се използват от скритите услуги на Tor. Тези данни могат да включват имена, адреси, телефонни номера, данни за кредитни карти, лични осигурителни номера. Типичен пример за това е скритата услуга Doxbin. [6]

Разпоредбата на чл. 32, б. „а“ от Конвенцията за престъпления в кибернетичното пространство на Съвета на Европа предвижда, че една страна може, без да има разрешение от друга страна, да има достъп до съхранявани общодостъпни компютърни данни (отворен код) независимо от географското местонахождение на тези данни. Освен ако в националното право не е предвидено друго, правоохранителните и разследващите органи могат да получат достъп до същите данни, които са публично достъпни и, в случай че е необходимо за дадената цел, да се впишат или регистрират за публично достъпни услуги. Според някои анализатори [6] достъпът до материали с отворен код за целите на наказателното разследване се установява като общоприета практика. Доколкото Tor представлява свободно предоставяна услуга с отворен код и е публично достъпна, тази разпоредба би следвало да намери приложение и по отношение на дейностите по разследване, които включват използването на Tor за събиране на доказателствени средства.

По този въпрос съществува и друго гледище [6], според което фактът, че определена информация е публично достъпна, не означава липса на ограничения при обработването на такива данни. Такива ограничения могат да произтичат от средствата и обема на събраните данни. Автоматизирането на разузнаването с отворен код създава заплахи за правото на лично пространство и по тази причина се налага и препоръчва законодателното му уреждане по начин, който да информира в достатъчна степен гражданите за подобни възможности. Достатъчно е да се разгледа ситуацията, в която автоматизирани средства за обработване на лични данни се използват чрез Tor или пък са насочени към скрити услуги в тази мрежа, за да се разбере необходимостта от законодателно уреждане на обработването на лични данни от системи с подобни възможности за търсене и намиране.

Доколкото използването на Tor от органите на досъдебното производство и на разузнаването може да включва обработването на лични данни, напр. получаване на достъп до данни извън обхвата на разследването и на лични данни, съхранявани от скрити услуги, следва да се държи сметка, че тези органи ще трябва да се съобразяват с правилата на действащото законодателство за защита на личните данни съгласно разпоредбите на чл. 1, ал. 5, т. 1-5 от българския Закон за защита на личните данни (ЗЗЛД).

Въпросът придобива още по-голяма актуалност и във връзка с предстоящото реформиране на режима за защита на личните данни в рамките на Европейския съюз. Макар и не специфично поставени в контекста на мрежата Tor, някои проблеми неизменно ще намерят проявление и в нея. Реформата ще окаже влияние върху дейността на разследващите органи, включително върху възможността за провеждане на разследване посредством Tor, когато същото включва обработването на лични данни [6]. В този смисъл независимо от обстоятелството, че тези органи може да използват Tor за анонимен достъп до определени уебсайтове или услуги, разпоредбите на законодателството за защитата на личните данни ще намери

приложение.

Нещо повече, още с подписването на Лисабонския договор ясно изпъкна желанието за закрепване на принципа, според който защитата на личните данни се прилага наравно и по отношение на полицейското и съдебното сътрудничество на наказателноправни въпроси. Предвижда се предложението за Общ регламент относно защитата на личните данни[13] да бъде допълнено от предложение за директива на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и относно свободното движение на такива данни.[14] Предложението е във връзка с проблемите, породени от прилагането на Рамково решение 2008/977/ПВР на Съвета относно защитата на личните данни, обработвани в рамките на полицейското и съдебно сътрудничество по наказателноправни въпроси, доколкото последното представлява инструмент с „*ограничен обхват и различни други празноти, които често водят до правна несигурност за отделните лица, както и за разследващите органи, а и практически проблеми при прилагането*“ [6]. След евентуалното й приемане, тази проектодиректива ще служи като основен инструмент, уреждащ обработването на личните данни за целите на разследването.

Ако до момента разследващите органи остават встрани от сянката на правилата на ЕС за обработване на лични данни, с приемането на тази директива ще се породят редица нови въпроси относно някои специфични категории данни.

Така например ще бъде поставен отново за разглеждане въпросът дали IP адресите следва да се разглеждат като лични данни. [7] Значението на този въпрос е голямо, защото признаването на IP адресите за лични данни би имало отражение върху цялата Интернет икономика, която ще следва да се съобразява със стандартите за защита на личните данни. Прилагането на разбирането за „лични данни“ към IP адресите е възможно, доколкото те са свързани с идентифицирано или подлежащо на идентифициране физическо лице и попадат в обхвата на понятието „всяка информация“ (чл. 2, б. „а“ от Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни). IP адресът е свързан с техническо устройство, посредством което се осъществява достъп до Интернет (напр. компютър или смартфон). Абонатът на услугата обаче е този, който е отговорен за действията си по време на сърфиране в мрежата. Същевременно потребителят е и този, който бива наблюдаван или следен от различни уебсайтове. Цялата тази информация във всички случаи следва да се смята за свързана със съответния потребител (вторият елемент от дефиницията), а не само със съответното техническо устройство. За да бъде идентифицирано или да бъде подлежащо на идентифициране едно лице, не е необходимо задължително притежаването на име или други лични данни, доколкото това условие ще е изпълнено и в случаите, когато съществува възможността едно лице да бъде разграничено от всички останали лица в дадена група.

Съществува съдебна практика на Парижкия апелативен съд, който в решение от

[13] COM(2012) 11 последен

[14] COM (2012) 10 последен

27 април 2007 г. се произнася по дело, свързано с P2P мрежи, че събирането на IP адреси не представлява обработване на лични данни, тъй като тези адреси се отнасят единствено до машината, а не до физическото лице, използвало същата, за да извърши правонарушение. В литературата [7] се посочва, че това тълкуване не е в съответствие с понятието за „лични данни“, възприето в европейския правен ред, доколкото директивата не изисква IP адресът да позволява идентифициране на потребителя, а само да е свързан с подлежащо на идентифициране лице. Няколко месеца по-късно друг френски съд достига до обратния извод и на 6 септември 2007 г. Първоинстанционният съд на Сен Брийо заключава, че макар и IP адресът действително да идентифицира свързаното с Интернет устройство, а не физическото лице, което го използва, същото може да се каже и за телефонния номер, който *strictu sensu* също не идентифицира пряко дадено лице, а линията, на която той е абонат. По същия начин и IP адресът, предоставен от доставчика на интернет услуги, е необходим за осъществяването на връзка на устройства с Интернет, за която едно определено физическо лице е сключило договор с доставчика. Тези решения са последвани от още две по сходни казуси и свидетелстват ясно за противоречивото разбиране и затрудненията, които съдът среща при изработването на единен подход за правната квалификация в тези случаи. Становище 4/2007 на Работната група по чл. 29 от юни 2007 г. относно понятието „лични данни“ може да служи като отправна точка при анализа. При всички положения националните транспонирания на нормите на директивата следва да се тълкуват изцяло в духа на общностното право. Това налага разбирането, че в повечето но вероятно не във всички случаи, IP адресите ще се смятат за лични данни [7].

Съществуват и други проблеми, свързани с евентуалното приемането на проектодирективата и използването на Tor от разследващите органи. Така съгласно проекта личните данни трябва да бъдат „събирани за конкретни, изрично указани и законни цели и да не се обработват допълнително по начин, който е несъвместим с тези цели“ (чл. 4, „б“) и да бъдат „съхранявани във вид, който позволява идентифицирането на субектите на данните за период не по-дълъг от необходимия за целите, за които се обработват личните данни“ (чл. 4, б. „д“). Проектодирективата провежда разграничение и между различните категории субекти на данни. Няма индикации за ограничения по отношение на разследващите органи за използването на анонимизиращ софтуер по време на разследванията, но всяко такова използване на Tor или други мрежи следва да бъде съобразено с тези правила. Това би породило практически затруднения като напр. факта, че не във всеки момент може да се определи с точност кои от обработваните данни включват лични данни и съответно дали за тях следва да се прилагат правилата за защита на личните данни, до каква степен и т.н.

Разгледаните въпроси поставят разследващите и разузнавателните органи на държавите членки на ЕС в особено положение. От една страна, те разполагат с редица технологии, които им позволяват изключително висока ефективност на разследването, но от друга страна – все по-усложняващият се регулаторен режим създава редица пречки пред осъществяването на такова разследване. Тези „пречки“, разбира се, не следва да се разглеждат само и единствено като такива, защото ограничаването на основни човешки права на гражданите на произволен принцип за разследване на всякакви престъпления или при подозрения за предстоящо

извършване на такива би довело до сериозно накърняване на конституционно и международноправно гарантирани права на гражданите. Намирането на баланса между националната сигурност и личното пространство следва да се търси в пресечната точка, където технологията, използвана от разследващите и разузнавателните органи, е поставена в ясна законова рамка, която гарантира, че ограничаването на основни човешки права е допустимо единствено в изключителни случаи.

5.2. Защита на основните човешки права

Както се посочи и в началото, анонимизиращите технологии се създават с идеята да служат за гарантиране на безпрепятственото упражняване на основни човешки права в Интернет. Въпросът за защитата на основните човешки права се поставя все по-остро с оглед на зачестяващите опити за цензуриране на Интернет и ограничаване на достъпа до информация.

Следва да се посочи, че в системата на международната защита на човешките права съществуват различни поколения човешки права, които дават рамката на международната закрила. [8] Конституционният съд на Република България също си служи с тази класификация, предложена за първи път от Георг Йелинек (така Решение № 4 от 2006 г., обн. ДВ, бр. 36 от 2006 г.). Първото поколение права са индивидуалните права – свободи, наричани „лични“, „отбранителни права“ или „негативни права“. Според Конституционния съд към тази група принадлежи и неприкосновеността на кореспонденцията, доколкото тези права защитават физическия и духовния интегритет на човешката личност и автономията и частната сфера на индивида. Второто поколение права са т.нар. икономически, социални и културни права. Третото поколение права са политическите права, които се определят като „активни“ права, а четвъртото поколение включва правото на чиста околна среда, правото на достъп до информация и някои други права, възникващи в информационното общество.

Използването на технологиите от страна на гражданите може да създаде риск от нарушаване на така установените права от практически всяко поколение права. Онлайн анонимността е призната от редица международни актове и документи, сред които Декларацията за свободата на съобщенията по Интернет на Съвета на Европа от 28.05.2003 г., Доклада на специалния докладчик на ООН (A/HRC/17/27) от 16 май 2011 г. относно насърчаването и защитата на правото на свобода на мнение и изразяване и др. С оглед на това следва да се приеме, че съществува достатъчно сериозна законова обосновка за правомерното използване на анонимизиращи технологии като Tor.

Важно е да се отбележи, че анонимността сама по себе си не представлява самостоятелно право, защото тя зависи от контекста, в който се реализира. Ако извършването на една дейност е законно, то извършването ѝ в анонимност също следва да е законно. Съответно, ако такава дейност е незаконна, тя няма как да бъде „узаконена“ от факта, че се извършва анонимно. Анонимността следва да се разглежда като съществен елемент на редица човешки права, сред които правото на свобода на изразяване, правото на лично пространство, правото на събрания, правото на сдружаване, правото на глас и др.[6].

Правото на свобода на изразяване е уредено в чл. 19, параграф 2 от Международния пакт за граждански и политически права, съгласно който всяко

лице има право на свобода на словото, което включва свободата да търси, да получава и да разпространява сведения и идеи от всякакъв вид, независимо от границите, било устно, писмено, печатно или като произведение на изкуството или чрез каквото и да е друго средство по свой избор. Факт е обаче, че редица недемократични държави нарушават повсеместно това право, налагайки цензура в онлайн пространството (напр. Китай). Tor мрежата е начин за преодоляване на тази цензура, като преодолява механизмите на защитните стени относно самоличността на източника и характера на трафика. Правото на свободно изразяване обаче не е неограничено. То търпи ограничения в определени хипотези, сред които случаите на клевета, слово, проповядващо омраза, някои случай на порнография, нарушения на авторски и сродни права, както и при опит за укриване на извършени престъпления. Въпросът и тук е в намирането на баланса при тълкуването, доколкото неоправданото разширяване на тези изключения може да влезе в остър конфликт с международно възприетите стандарти. Така забраната или неоправданото ограничаване на достъпа на гражданите до мрежата Tor може да влезе в противоречие с правото на свободно изразяване, а също и с правото на лично пространство.

Правото на лично пространство също е признато и гарантирано от Международния пакт за граждански и политически права по силата на разпоредбата на чл. 17, който гласи, че никой не може да бъде обект на своеволно и незаконно вмешателство в личния му живот, семейството му, дома или кореспонденцията му, нито на незаконно накърняване на неговата чест и добро име. Изключително честа практика е нарушаването именно на това право, дори от държави, които гарантират правото на свободно изразяване. Най-типичният пример в този смисъл е САЩ и Националната агенция за сигурност (NSA) и разработваната и систематично прилагана от нея програма за масово наблюдение и следене. Върховният комисар на ООН по човешките права отбелязва в доклада „Правото на неприкосновеност на личния живот в цифровата ера“ от 30 юни 2014 г.[15], че практиките в редица държави разкриват липса на адекватно национално законодателство и правоприлагане, слаби процесуални гаранции и неефективен контрол, които допринасят за липсата на отговорност за произволната и незаконна намеса личното пространство на гражданите. Въпреки това следва да се държи сметка за обстоятелството, че правото на лично пространство не е неограничено и абсолютно. Европейската конвенция за защита на правата на човека и основните свободи съдържа списък с изключения, които включват мерки в рамките на наказателно разследване, които на законово основание могат да ограничат правото на лично пространство. Основният въпрос и тук е свързан с пропорционалността между резултатите от подобни дейности по масово наблюдение и следене и нарушаването на личното пространство на гражданите.

5.3. Отговорност за съдържанието, което преминава през изходните точки в Tor мрежата

Отговорността на операторите за съдържанието, което преминава през изходните точки в Tor мрежата, е въпрос с голямо практическо значение. В

[15] Докладът е достъпен на английски език на уеб адрес: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc

литературата [6] се дава пример с австрийския случай от 2012 г., когато австрийската полиция претърсва апартамента на Уилям Вебер в Грац и изземва компютърен хардуер, използван за контрол на изходни точки на Tor, които се намират физически в чужбина. Неизвестни потребители на мрежата са използвали тези изходни точки за изтегляне на съдържание с детска порнография и властите са заподозрели Вебер като извършител, тъй като не им е било известно, че изходните точки не са били крайната дестинация на файловете. На 30 юни 2014 г. Вебер е осъден за помагачество при разпространение на детска порнография на лишаване от свобода за три месеца с тригодишен изпитателен срок. Поради отказа на Вебер да обжалва присъдата поради лични и финансови затруднения, не е ясно как би се произнесла втората инстанция по случая.

Според австрийското, както и според българското право, вината е елемент от субективната страна на престъплението и в случаите на помагачество, доколкото съгласно чл. 21, ал. 1 от Наказателния кодекс всички съучастници се наказват с наказанието, предвидено за извършеното престъпление, като се вземат предвид характерът и степента на тяхното участие. В съдебното следствие съдът приема като доказателства изказвания на Вебер в чат програми, съгласно които той казва, че „*на нашите сървъри може да се хоства и детска порнография*“ и „*ако исках да хостват детска порнография... аз лично бих използвал Tor*“. Тези изказвания са послужили за основа на заключението, че деецът е действал с непряк умисъл, въпреки твърденията на подсъдимия, че тези изказвания са извадени от контекста. Това решение не може да се смята за решение с общо значение относно законното използване на Tor услуги.

Решението по случая Вебер поставя за разглеждане по-общия въпрос за законността на създаването и поддържането на изходни точки в мрежата Tor и за отговорността за трафика, който преминава през тях – от гражданско- и от наказателноправно гледище. По-конкретно се поставя въпросът приложим ли е режимът за обикновения пренос по смисъла на чл. 12 от Директива 2000/31/ЕО (Директива за електронната търговия) за обикновен пренос?

Операторът на изходна точка в мрежата Tor попада в приложното поле на чл. 12, параграф 1, букви „а“ - „в“ от Директивата за електронната търговия, защото в типичния случай тази точка служи като препращаща точка (relay) и операторът няма намеса в преноса. Необходимо е обаче да се изследват въпросите дали операторът на изходна точка в Tor може да бъде определен като „доставчик на услуга“ и дали предоставянето на изходна точка в Tor мрежата е „услуга на информационното общество“.

Съгласно разпоредбата на чл. 2, б. „б“ от Директивата за електронната търговия „доставчик на услуги“ е всяко физическо или юридическо лице, което предоставя услуги на информационното общество. Според чл. 2, б. „а“ от Директивата за електронната търговия „услуги на информационното общество са услуги по смисъла на чл. 1, параграф 2 от Директива 98/34/ЕО, изменена с Директива 98/34/ЕО“. Съгласно чл. 1, параграф 2 от Директива 98/34/ЕО услуга е каквато и да е услуга на информационното общество, тоест, каквато и да е услуга, нормално предоставяна срещу възнаграждение, от разстояние, чрез електронно средство и по индивидуална молба от получателя на услугите. Дефиницията дава подробно тълкуване по три от условията, които една изходна точка на Tor лесно би покрила. Проблемът идва от тълкуването на фразата „нормално предоставяне срещу

възнаграждение“, тъй като Tor е безплатна и свободна услуга. В решението си от 11 септември 2014 г. по дело C-291/13 Съдът на Европейския съюз (СЕС) се произнася, че „понятието „услуги на информационното общество“ по смисъла на тази разпоредба обхваща онлайн информационни услуги, срещу които доставчикът не получава възнаграждение от получателя на услугите, а приходи от реклами, разпространявани на даден уебсайт.” Въпреки че това заключение е изцяло в тон с предходни становища на Европейската комисия, то не помага за определянето на правния статус на изходните точки на Tor. В същото време СЕС е сезиран с преюдициален въпрос от Районния съд на Мюнхен по дело 7 O 14719/12 относно смисъла, влаган в понятието “услуга, нормално предоставяне срещу възнаграждение” в контекста на предоставяне на свободни и безплатни Wi-Fi услуги, които не са защитени с парола.[16]

Трудно е да се прогнозира решението на съда, но то по всяка вероятно би имало значение относно това дали Tor може да се разглежда като доставчик на услуга. Ако СЕС реши, че обикновеният пренос не може да бъде прилаган по отношение на безплатни услуги, дори и по аналогия, тогава би се породил въпросът за практическият смисъл на тези услуги, чиито доставчици биха носили отговорност за пренесените данни. Решение в този смисъл би поставила ЕС в изключително неблагоприятна позиция спрямо САЩ, където има уредени изрично правила, които правилата за отговорността на доставчиците в тези случаи са ясно установени. Отговорът на този въпрос би дал отражение и върху въпросът за наблюдаване и следенето на изходните точки в Tor мрежата от страна на правоохранителните, разследващите и разузнавателните органи.

5.4. Наблюдаване и следене на изходните точки в Tor мрежата

Както се спомена по-горе, Tor може да се използва за различни незаконни дейности, обявени за такива от националните законодателства, като напр. продажба на забранени от закона стоки, разпространяване на детска порнография и др. Тези дейности са криминализирани в законодателствата на повечето държави. Много често обаче се пропуска обстоятелството, че наблюдението на трафика, който преминава през Tor, може също да бъде незаконно съгласно националното право.

В литературата не се среща задълбочен юридически анализ на дейностите, извършвани от оператора на изходна точка в мрежата Tor. Факт е обаче, че не съществува конкретно законово основание за обявяване на тази дейност за незаконна. Разбира се, не бива да се пренебрегва фактът, че операторите на тези изходни точки все пак имат достъп до трафика, който преминава през тях. Tor анонимизира произхода на трафика и осигурява криптирането му при преминаването през мрежата, но не криптира целия трафик, който преминава към Интернет. Изходната точка е в позицията да прихване трафика, преминаващ през нея – напр. лични имейл съобщения (освен ако не е приложено криптиране от край до край), достъп до потребителски имена и пароли. Дори и в случаите, когато подобно прихващане и задържане е извършено добросъвестно, напр. когато един изследовател иска да разбере какъв тип данни преминават през мрежата за целите на подобряване на качеството на услугата за потребителите, които я използват за законосъобразни цели, и идентифицира и блокира трафика, който противоречи на

[16] Понастоящем образуваното пред СЕС дело е с номер Mc Fadden/C-484/14.

императивни правни норми (детска порнография, опити за хакерски атаки др.), подобна намеса най-често би се счела за незаконосъобразна.

Според разпоредбата на чл. 2 от Конвенцията за престъпленията в кибернетичното пространство всяка страна предприема необходимите законодателни и други мерки , за да обяви за престъпление във вътрешното си право умишления и без законно основание достъп до цялата или до част от компютърна система. Страните могат да въведат като изискване престъплението да бъде извършено или в нарушение на мерките за сигурност с умисъл да се получат компютърни данни, или с друго престъпно намерение, или във връзка с компютърна система, която е свързана с друга компютърна система. Наблюдението на трафика следва да се разглежда през призмата на чл. 3, който задължава страните да криминализират прихващането, извършено чрез технически средства без законно основание. Обяснителният доклад към конвенцията свърза чл. 3 с разпоредбата на чл. 8 от Европейската конвенция за защита на правата на човека и основните свободи, който защитава личния живот и кореспонденцията.

6. Заключение

Разгледаните по-горе въпроси ще бъдат предмет и на бъдещи изследвания, доколкото техният обхват не позволява пълното им разглеждане в рамките на настоящото изследване.

Анонимността и защитата на личното пространство в Интернет е гарантирано от международния правов ред, както и от конституциите на всички демократични държави. Въпреки това, от признаването на правото на лично пространство за всеобщо човешко право до момента то никога не е било подлагано на по-сериозно изпитание. Информационните технологии и желанието за контрол над глобалния информационен поток от страна на държави и частни компании компрометират възможността на гражданите да упражняват безпрепятствано това свое право. Нещо повече, в редица случаи то се оказва застрашено или пряко нарушено, а разпространяването на класифицирана информация - единственият начин сведения за такива действия да достигнат до широката общественост.[17] Подобни постъпки обаче застрашават както личната сигурност на лицата, които ги извършват, така и националната сигурност, доколкото контролът върху информацията, която се публикува, е в ръцете на един-единствен човек.

Всичко това налага търсенето и намирането на баланс между необходимостта от гарантиране на националната сигурност и правото на лично пространство и анонимността. Използването на анонимизиращи технологии безспорно улесняват гражданите в упражняването на това им конституционно гарантирано право. Тези анонимизиращи технологии обаче крият и риска да бъдат използвани за незаконосъобразни цели и в крайна сметка да увредят други основни човешки права, които се закрилят с по-висок интензитет. Всичко това обосновава необходимостта от умерен контрол върху използването на тези технологии, подчинен на законодателни мерки, които държат сметка за действителното развитие на технологиите. Тези мерки следва да бъдат имплементирани в самите технологии (подходът *Privacy by Design*), а не да остават законодателно пожелание. Правилата на Интернет много често не следват очертаните от законодателя

[17] http://www.theguardian.com/world/2013/jun/09/nsa-secret-surveillance-lawmakers-live

императиви, защото те не са съобразени с архитектурата на световната мрежа и начина на нейното функциониране.

Предвид казаното по-горе може да се заключи, че границата на личното пространство е там, където националната сигурност се превръща от абстрактно понятие, което отваря вратата на произвола, в действителна служба в защита на най-добрия интерес на гражданите, която държи сметка за развитието на технологиите, гарантирането на основните човешки права и при всички положения се съобразява с върховенството на правото.

БИБЛИОГРАФИЯ

1. *Avdić, K, Alexandra Sandström*. Network Anonymity. Linköping University, достъпна на адрес: https://www.ida.liu.se/~TDDD17/oldprojects/2010/projects/001-1.pdf, последен достъп: 11.05.2015 г.
2. *Wiles, R., et al*. Anonymity and Confidentialit. In: NCRM Working Paper Series, 2/06, University of Southampton, достъпна на адрес: http://eprints.ncrm.ac.uk/423/1/0206_anonymity%2520and%2520confidentiality.pdf, последен достъп: 11.05.2015 г.
3. *Veen, van D*. Legal issues with on-line anonymity. Anonymity networks and the Dutch law. University of Twente, достъпна на адрес: http://referaat.cs.utwente.nl/conference/10/paper/6945/legal-issues-with-on-line-anonymity.pdf , последен достъп: 11.05.2015 г.
4. *Watson, K.D*. The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks. In: Washington University Global Studies Law Review, Volume 11, Issue 3, 2012, достъпна на адрес: http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1417&context=law_globalstudies, последен достъп: 11.05.2015 г.
5. *Rosenzweig, P.* National Security Threats in Cyberspace. Post-Workshop Report – September 2009, достъпен на адрес: http://www.americanbar.org/content/dam/aba/migrated/natsecurity/threats_in_cyberspace.pdf, последен достъп: 11.05.2015 г.
6. *Çaliskan, E., T. Minarik, A.-M. Osula*. Technical and Legal Overview of the Tor Anonymity Network. NATO Cooperative Cyber Defence Centre of Excellence, Talinn 2015, достъпен на адрес: https://ccdcoe.org/sites/default/files/multimedia/pdf/TOR_Anonymity_Network.pdf, последен достъп: 11.05.2015 г.
7. *Hustinx, P. J. Protection of Personal Data On-line: the Issue of IP Addresses*, достъпен на адрес: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-04-15_adresses_IP_EN.pdf, последен достъп: 11.05.2015 г.
8. *Друмева, Е. Конституционно право. Трето допълнено и преработено издание. Сиела, 2008*

ДИНАМИКА НА ХАКЕРСКИТЕ АТАКИ

Атанас И. Начев Виктор В. Джелепов

Шуменски университет „Епископ Константин Преславски“
e-mail: anatchev@abv.bg

Шуменски университет „Епископ Константин Преславски“
e-mail: vicdj@abv.bg

DYNAMICS OF THE HACKER ATTACKS

Atanas I. Nachev Viktor V. Dzhelepov

ABSTRACT: *The text presents the dynamics of hacker attacks, the motivation of the attacker and the purpose of cyber criminals in the past year and a half. Shown are the most commonly used techniques of hackers. The possibilities for online tracking of hacker attacks in real time.*

KEY WORDS: *hacker attack, cyber criminals*

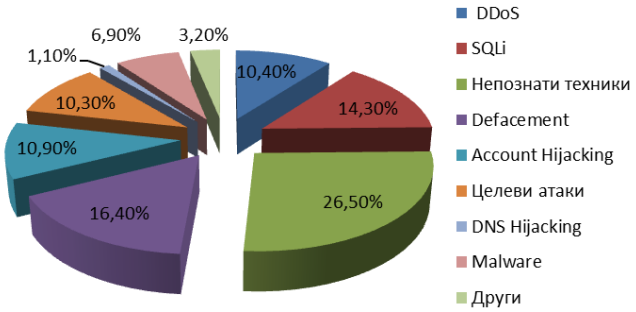
Широкото използване на информационните технологии в държавната администрация, икономиката, банковото дело, социалната сфера и пр. все по-остро поставя проблема защита на информацията. Свидетели сме на непрекъснато увеличаване на атаките по отношение на компютърните системи. Киберпрестъпниците атакуват все по-често сайтове на различни ведомства. Обект на атаки са сайтове на ДАНС, МВР, Мистерството на отбраната, Българската народна банка, Министерството на културата и дори този на православната църква. По данни на Центъра за реагиране при инциденти във връзка с информационната сигурност (CERTbg) към Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи" над 200 атаки срещу компютърните системи на държавата са засечени през 2014 година. От началото 2014 г. годината до месец октомври същата година са били атакувани 30 ведомства като са засегнати 110 IP адреса. През първите седем месеца на 2014 г. са обработени над 1300 сигнали за хакерски атаки в българското интернет пространство, които са получени от 32 732 интернет адреси. Най-фрапантен е примерът с вируса "Zeus Kins", който е засегнал 54 държавни и общински администрации, 5 университети, 9 банки, както и компаниите ЧЕЗ, НЕК, ЕОН и БТК. През януари 2015 г. бе атакуван и сайта на енергийния регулатор.

Според данни на www.statista.com над 40% от глобалния интернет трафик за атаки през втората четвърт на 2014 г. идва от Китай. На второ място е Индонезия с 15% , на трето САЩ с 13%. (фиг.1).

Фиг. 1.

Най-използваните методи за хакерска атака през 2014 г. са (фиг. 2):

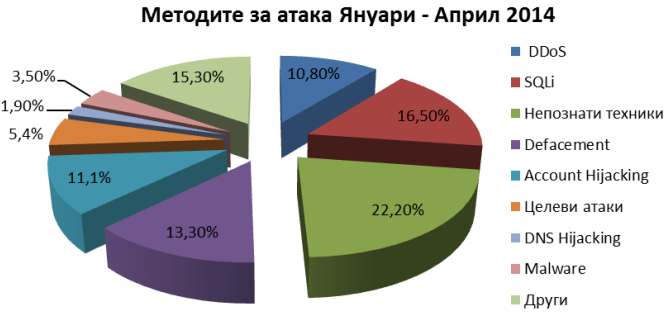
1. Defacement
2. SQLi
3. Account Hijacking
4. Целевите атаки
5. DDoS
6. Непознати техники
7. Malware



Фиг. 2

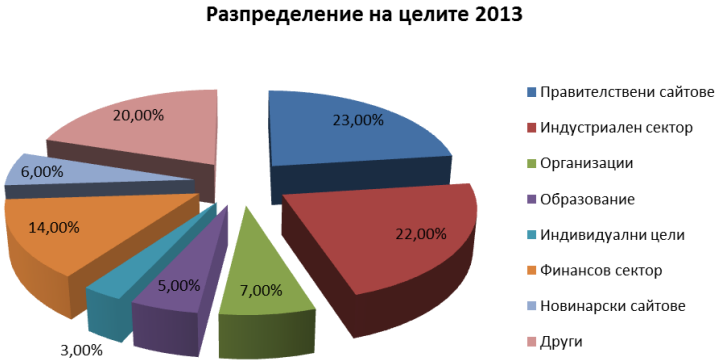
Defacement е на първо място като позната техника на атакуване (16,4% спрямо 14% за миналата година). Следва SQLi (14,3% спрямо 19% за 2013 г.), Account Hijacking (10,9% спрямо 9% за 2013 г.), Целевите атаки (10,5%), DDoS (10,4%), Malware (6,9%).

На фиг. 3 е показано разпределението на техниките за компютърни атака за периода януари – април 2014 г..



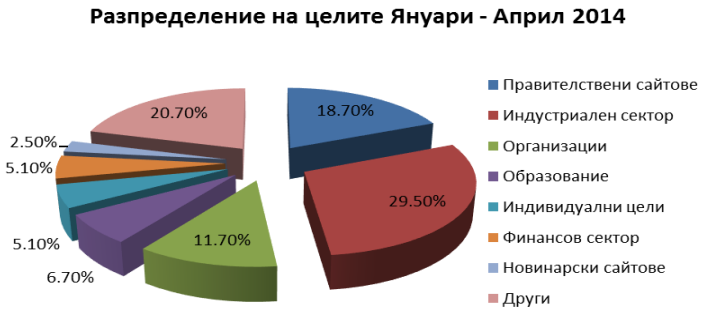
Фиг. 3

Небезинтересно е да се отбележи, че основни цели на атакуващите през 2014 г. са били, както и през 2013 г. : правителствени сайтове – 23%; предприятия и фирми – 22%; Финансови институции – 14% -фиг. 4.



Фиг. 4

За периода януари-април 2014 г. най-много атаки са осъществени по отношение на индустриалния сектор (29,5%), следван от правителствени сайтове (18,7%) и сайтове на правосъдието (15,6%). Следват сайтове на организационни структори (11.7%), обучаващи институции (6,7%) и др. (фиг. 5).



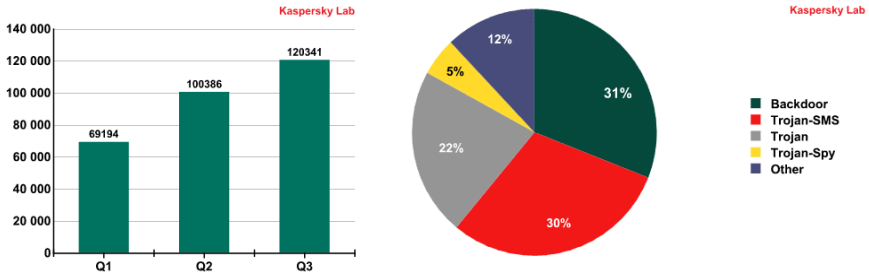
Фиг. 5

Според бюлетин на Kaspersky Lab за 2013 г. през септември Vodafone Germany е регистрирала атака, при която два милиона записи с данни са били копирани. Записите са съдържали не само имена и адреси, но също така и банкови данни.

През юли 2013 г. Apple затвори за повече от три седмици Apple Developer portal след като неизвестен нарушител източи персонална информация за много регистрирани разработчици. Малко след като инцидента придоби публичност консултант по сигурността пусна видео в Youtube признавайки за атаката.

В началото на 2014 г. в резултат на хакерска атака бяха откраднати бази данни с пароли и информация за потребители от един от най-големите онлайн търговци eBay. Атаката е компрометирала "малък брой имена и пароли на служебни акаунти", чрез които хакерите са успели да си осигурят достъп до корпоративната мрежа на eBay.

През третата четвърт на 2013 г. беше отделено много време за борба с мобилен зловреден софтуер, след появата на цял набор от нови техники и разработки от хакери пишещи Malware при мобилните устройства. Последната четвърт на 2013 г. беше несъмнено времето на мобилни атаки. Киберпрестъпниците чрез разпространение на троянски СМС се опитват да добавят интерактивност по начин чрез който да управляват своите активи. Ето защо сега хакерите използват Google Cloud Messaging за управление на своите скриптове. Разпределението на мобилен зловреден софтуер през третата четвърт на 2013 г. е полазано на фиг. 6.



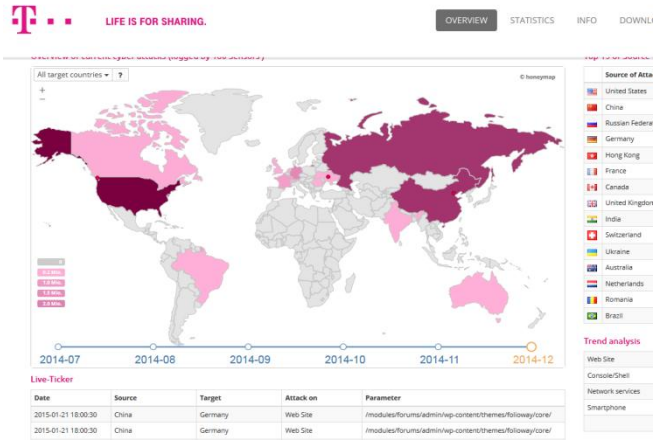
Фиг. 6

Водещата позиция при мобилен зловреден софтуер е на атаките тип задна врата (31%), като се отчита пад от 1,3% спрямо втората четвърт на 2013 г. СМС троянците (30%) бележат ръст от 2.3% спрямо предишния период и заемат втора място. Следват троянски коне (22%) и троянски коне шпиони (5%). Заедно backdoors и SMS Trojans заемат 61% от мобилния зловреден софтуер. (по данни на Касперски Лаб.). Напоследък все по-голяма популярност придобиват и атаките тип „кодиране на информацията“ с цел откуп.

По данни на Imperva броя на уеб атаките постоянно се увеличава, особено сред Cloud услугите. Щетите от кибер престъпленията в световен мащаб се оценяват на над един трилион долара годишно - само администрацията на САЩ губят над 1 милиард долара всяка година от пробиви в информационна сигурност. През 2014 г. няма сектор, който да не е бил засегнат от пробиви в сигурността или хакерски атаки.

Според CISO (Chief Information Security Officers) всеки ден жертва на Кибер престъпления стават над 1 милион души. Направена е световна класация на източниците на заплаха, като България заема 53-то място, а по Spam и Phishing атаки заемаме 41 място.

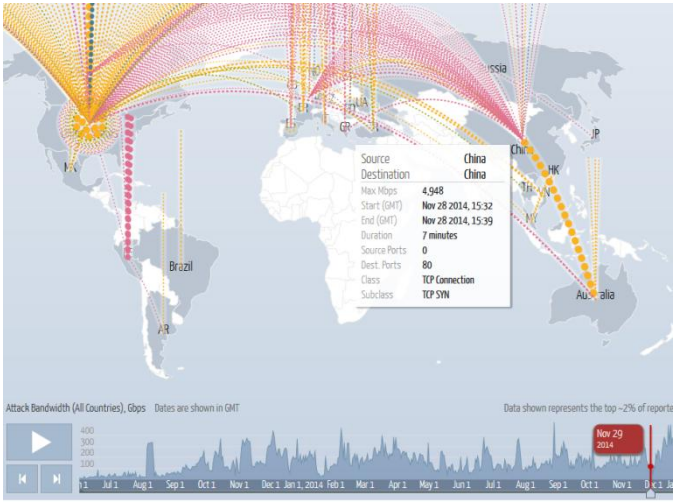
Няколко интернет сайта предлагат интерактивни карти показващи хакерските атаки в реално време. Deutsche Telekom (http://www.sicherheitstacho.eu/?lang=en) предлага интерактивна карта, която визуализира инцидентите в реално време. За нуждите на този експеримент по целия свят са разположение 180 електронни капани, сензори привличащи автоматизираните атаки, насочени към уебсайтове, мобилни телефони и уеб услуги. Картата показва типа на атаките, страната източник и срещу кого са насочени. Новият уеб портал на компанията дава възможност за генериране на интересни и подробни статистики – фиг. 7.



Фиг. 7

Google пуснаха специализирана карта на цифровите атаки Digital Attack Map – предназначена за борба предимно с DDoS (distributed denial of service) атаки (фиг. 8). Те представляват изкуствено претоварване с трафик от множество източници с цел да затруднят или блокират определени уебсайтове или отказ в обслужването на

онлайн услуги. Една трета от всички инциденти се дължат на този вид хакерски атаки, а те са около 2000 бройки дневно в световен план.



Фиг. 8

Kaspersky, която се занимава с интернет сигурност, е разработила друга интересна карта, която показва в реално време кибер атаки, засечени от защитния им софтуер (http://cybermap.kaspersky.com/)-фиг.9.

Фиг. 9

В контекста на всичко това не може да не се отбележи и фактът, че интернет се превръща в най-новото, най-масовото и най-популярното средство за контрол на общественото мнение. За пример може да се посочи „Уикилийкс", който показа, че една социална мрежа може да предизвика политическа криза едновременно в няколко държави.

ЛИТЕРАТУРА:

1. Nachev A., Zhelezov St., Assessing the efficiency of information protection systems in the computer systems and networks, Information, technology and security, № 1, Kiev, 2013.

2. Номоконов В., Тропина Т., Киберпреступность: угрозы, прогнозы, проблемы борьбы, Киев, 2013.

3. http://hackmageddon.com/

4. www. kaspersky.com

5. www.statista.com

6. https://govcert.bg/

ТЕХНИЧЕСКИ РЕШЕНИЯ ЗА ЦЯЛОСТНА ЗАЩИТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИ СИСТЕМИ В ОРГАНИЗАЦИЯТА

Преслава Р. Петкова **Огнян А. Тошков**

Адрес за кореспонденция: гр. София 1756, ул. Лъчезар Станчев – 3, Бизнес център Литекс тауър, ет. 4, Телелинк ЕАД

TECHNICAL SOLUTIONS FOR FULL PROTECTION OF THE INFORMATION AND COMMUNICATION SYSTEMS IN THE ORGANIZATION

ABSTRACT: *The following report presents examples of practical solutions for meeting the requirements, included in Annex A to ISO/IEN 27001:2013 „Information technology - Security techniques -- Information security management systems – Requirements".*

Управлението на сигурността на информацията е изключително важен въпрос за всяка една организация. Как да защитим информацията, която създаваме, придобиваме, използваме и съхраняваме по време на работа? Как да създадем такива правила и да въведем най-подходящите технически решения без да затрудним работния процес? Като цяло управлението на сигурността не е чисто технически проблем – това е съвкупност от технически и бизнес решения.

За да си отговорим на по-горните въпроси, на помощ идват стандартите. В цял свят е разпространено виждането, че за да управляваме който и да било процес от нашата дейност и този процес да ни носи стойност, трябва да се придържаме към определени правила. Тези правила не трябва да са изкуствено създадени, те трябва

да са обмислени и пречупени през дейността на организацията. Правилата трябва да бъдат създадени с цел постигане на конкретни резултати, с измерима стойност.

Когато стане въпрос за управление на сигурността на информацията, първият стандарт, който изниква в съзнанието ни е ISO 27001:2013. Взимайки под внимание неговите изисквания, ние може да сме сигурни, че ще създадем една сигурна среда за работа, сигурни канали за защита на информацията на организацията, както и да гарантираме пред всички външни заинтересовани страни, че ние поемаме ангажимент не само към нашите ресурси и активи, но и към техните такива.

В никакъв случай не е задължително да въведем система за управление на сигурността на информацията, за да бъде проверена и да получим сертификат от акредитиран орган. Ние може да използваме стандарта като ръководство за управление на сигурността на всички ценни, критични и не чак толкова критични ресурси. Този стандарт е приложим в абсолютно всяка сфера на дейност, както в частния, така и в държавния сектор.

От къде да започнем? Как да преценим какво е подходящо и необходимо за структурата, която управляваме? Какви технически решения са нужни или вече разполагаме с такива?

ISO 27001:2013 (особено след излизане на последната нова версия) предлага в себе си едно много елегантно решение за проследяване на всички аспекти на сигурността и тяхното по-лесно управление, а именно така наречените контроли, описани в приложение А на стандарта.

В настоящия доклад целим да представим едно възможно практическо приложение на контролите, обвързано с технически решения, които нашата компания препоръчва, а също така й предоставя като услуга на своите настоящи и бъдещи клиенти и партньори.

В табличен вид в таблица 1 срещу групите контроли са описани решенията, които предлагаме. Дори да въведете само няколко от тях, бъдете уверени, че вече ще разполагате с една по-сигурна организация.

Таблица 1

КОНТРОЛИ ISO 27001:2013			Как да го направим?
Клауза	**Раздел**	**ЦЕЛИ ПО КОНТРОЛА И МЕХАНИЗМИ ЗА КОНТРОЛ**	
5. Политика по сигурност на информацията	**5.1**	**Насока за управление на сигурността на информацията**	Създадени и въведени политики/писмени правила ; Периодичен преглед за изпълнимост
6. Организиране на сигурността на информацията	**6.1**	**Вътрешна организация**	Определени и документирани роли и отговорности; Списък с кон-

			такти и поддържане на връзка с тях; Анализ на риска преди стартиране на всеки нов процес;
	6.2	**Мобилни устройства и работа от разстояние**	Enterprise Mobility Management by IBM, VmWare; Cisco Identity Service Engine
7. Сигурност на човешките ресурси	**7**	**Преди наемане на работа; По време на работа; Прекратяване или промяна на службата;**	Регламентиран процес за управление на човешките ресурси; Участие на ръководството във взимане на решения за въвеждане на конкретни правила; Периодични обучения и инструктажи на служителите ;
8. Управление на активи	**8.1**	**Отговорност за активите**	Asset Management решения на IBM / RSA
	8.2	**Класифициране на информацията**	Microsoft Dynamics Retail Management System (RMS)
	8.3	**Работа с информационни носители**	Data Leakage Prevention, Endpoint Desktop Management, Enterprise Mobility Management
9. Контрол на достъпа	**9.1**	**Изисквания за дейността за контрол на достъпа**	Cisco Identity Service Engine
	9.2	**Управление на достъпа на потребителите**	Microsoft AD/ IBM Iidentity Mmanagement system / RSA Iidentity Mmanagement system
	9.3	**Отговорности на потребителите**	RSA Advanced Authentication
	9.4	**Контрол на достъпа до системи и приложения**	IDM/Microsoft AD/Other Specialized Software; Date

			Leakage Prevention
10. Криптография	**10.1**	**Криптографски механизми за контрол**	Public key infrastructure (PKI)/Password Management and other products
11. Физическа сигурност и сигурност на заобикалящата среда	**11.1**	**Сигурни зони**	Система за контрол на достъп
	11.2	**Устойства**	Разполагане на устройствата на безопасни, сигурни и защитени места
12. Сигурност на работата	**12.1**	**Процедури за работа и отговорности**	Документирани процедури; Change Management Solutions; Capacity Management Solutions; Firewall, Network Design
	12.2	**Защита от злонамерен софтуер**	AntiVirus, Advanced Malware Detection
	12.3	**Резервиране**	Backup Exec/ Symantec, IBM Tivoli Storage Manager, MS/System Center Data Protection Manager (Backup Solutions)
	12.4	**Резервиране и наблюдение**	Event Management Solutions; Backup Exec/ Symantec, IBM Tivoli Storage Manager, System Center Data Protection Manager (Backup Solutions)
	12.5	**Контрол на работещия софтуер**	Monitoring and Control with MS system centre Confi&Opp
	12.6	**Управление на техническата уязвимост**	Monitoring and Control with MSSC Confi&Opp

	12.7	**Разглеждане на одита на информационни системи**	Monitoring and Control with MSSC Confi&Opp
13. Сигурност на комуникациите	**13.1**	**Управение на сигурността на мрежите**	FW, Cisco Identity Service Engine
	13.2	**Обмен на информация**	Services and Control with Netwok Solutions (FW,Remote Access Monitoring, ISE)
14. Придобиване, разработване и поддържане на системи	**14.1**	**Изисквания за сигурност на информационните системи**	VPN, (Secure Sockets Layer virtual private network)
	14.2	**Сигурност на процесите на разработване и поддържане**	Change Management Solutions MS/CRM; IBM AppScan;
	14.3	**Данни при изпитване**	Механизми за защита на данните или използване на изкуствена тестова среда за изпитване
15. Взаимоотношения с доставчици	**15.1**	**Сигурност на информацията при взаимоотношения с доставчици**	Документирани правила
	15.2	**Управление на предоставянето на услуги от доставчици**	Control and Monitoring на достъпа на доставчици; Change Management (MS/CRM)
16. Управление на инциденти със сигурността на информацията	**16.1**	**Управление на инциденти и подобряване на сигурността на информацията**	CRM system/Incident and Problem Management / Security Information and Event
17. Аспекти на сигурността на информацията при управление на непрекъснатостта на дейността	**17.1**	**Непрекъснатост на сигурността на информацията**	Bussiness Continuity Plan Development and Automations with technical solutions (VMWare Site Recovery Manager)
	17.2	**Излишък**	Asset Management решения на IBM / RSA

18. Съответствие	**18.1**	**Съответствие със законови и договорни изисквания**	Спазване на националното законодателство и договорни изисквания с клиенти
	18.2	**Прегледи на сигурността на информацията**	SIEM/Governance Management/ RSA Advanced Security Operations Center

Предложените в таблица решения са едни от най-добрите, които се предлагат, и най-удобните и лесни за ползване. Нашите специалисти ги препоръчват като утвърдени решения и могат да съдействат при имплементацията на всяко едно от тях.

Важността на информацията и информационните процеси предизвикват все поголям интерес и внимание във всяка организация. Изработването на информационна стратегия е една от основните задачи за очертаване на бъдещето на организациите в частния и държавния сектор. Информацията е в основата и на реинженеринга на процесите, чрез който могат да се постигнат много по-високи резултати. Силата на информацията е във влиянието й върху процесите, а ефектът й пряко зависи от създадените условия за достъп до нея и за защитата й. Последното произтича от уязвимостта на информацията и информационните системи от различни атаки. Това налага анализ и разбиране на заплахите за информационната инфраструктура, дефиниране и провеждане на последователни мерки за всестранната й защита. Ако се придържаме към най-добрите практики дадени в приложение А на ISO 27001:2013 техническите решения, които предлагаме в настоящия доклад, ще изградим една защитена и сигурна среда на нашата организация.

ДЪРЖАВА И СИГУРНОСТ

АНТРОПОГЕННО ЗАМЪРСЯВАНЕ И СИГУРНОСТ

Маргарита К. Бонева **Георги В. Колев**

Шуменски университет "Епископ Константин Преславски"
Педагогически факултет

ANTHROPOGENOUS CONTAMINATION AND SECURITY

Margarita K. Boneva, Georgy V. Kolev

ABSTRACT: *The paper presents anthropogenous contamination and security*

KEY WORDS: *security, anthropogenous contamination, climate, water*

В Стратегията за национална сигурност е отделено специално място на политиката за сигурност в отношенията човек-природа. В чл.103 – чл.106 са посочени аспектите на политиката за сигурност, който включва стандартите за екологична експертиза и защита с цел опазване на околната среда и защита на екологичната сигурност. Актуално е предотвратяването, овладяването и преодоляването на последствия от промишлени аварии с изпускане на вредни емисии, трансгранично замърсяване на въздуха, водите и крайбрежната ивица, както и при наличие на заплаха за терористична дейност с използване на оръжия за масово унищожение. Въвежда се единна информационна система чрез междуинституционален механизъм за планиране, наблюдение и оценка и се създава работеща система за овладяване и преодоляване на последствията от природните бедствия с активното съдействие на гражданите и техните организации.

Антропогенното замърсяване на атмосферата, литосферата и хидросферата е основната причина за глобалната екологична криза. Тя води до изменение на климата, което влияе върху физическите и биологичните система по света, а именно:

- изменението в климата допълнително ограничава достъпа до

питейна вода. Водата, която произхожда от стопяването на ледовете, понастоящем снабдява над един милиард души. При изчезването ѝ, големи маси население ще бъдат принудени вероятно да мигрират към други части на света, причинявайки по този начин местни и световни вълнения и несигурност;

- променя се екосистемата и биологичното разнообразие като за приблизително 20-30% от растителните и животински видове, опасността от изчезване вероятно ще се увеличи, ако средната световна температура се повиши с над 1,5–2,5%;
- очаква се измененията на климата да доведат до увеличаване на риска от глад (броят на застрашеното население може да се увеличи с няколкостотин милиона);

- покачването на нивото на морското равнище ще застраши делтата на Нил, делтата на Ганг/Брахмапутра и делтата на Меконг и ще доведе до преселването на над 1 млн. души от всяка делта до 2050 г. като най-силно са засегнати малките островни държави;
- Измененията на климата ще окажат преки и косвени последици върху здравето на човека и животните. Сред най-съществените опасности, които трябва да бъдат взети предвид, са последиците от извънредни климатични явления и увеличаването на инфекциозните болести. Болестите, обусловени от климата са сред най-смъртоносните на световно ниво;
- последствията от изменението на климата в Европа и Арктика вече са значителни и измерими. Изменението на климата ще окаже сериозно въздействие върху природната среда на Европа и върху почти всички сектори на обществото и икономиката;
- температурата в Европа през последния век тя се е повишила с почти 10^0C. По-топлата атмосфера съдържа повече водни пари, но новите модели на кондензиране силно се различават между регионите. Валежите и снеговалежите значително са се увеличили в Северна Европа, докато в Южна Европа се наблюдава все почесто суша. Съществуват необорими доказателства, че почти всички природни, биологични и физични процеси (по-ранният цъфтеж на дърветата, топенето на ледниците) представляват реакция в резултат на измененията на климата в Европа и по света. Повече от половината растителни видове в Европа могат да се окажат уязвими или застрашени към 2080 г. Най-уязвимите области в Европа са:

➢ Южна Европа и целият Средиземноморски басейн, поради комбинирания ефект от високите температурни колебания и намаленото ниво на валежи в области, които вече се сблъскват с недостига на вода;

➢ планинските области и по-специално Алпите, където температурите бързо се повишават, водейки до масивно топене на снеговете и ледовете и промяна на водните потоци;

➢ крайбрежните зони, поради покачването на морското равнище, комбинирано с повишения риск от бури;

➢ силно населените алувиални долини, поради повишения риск от бури, силните валежи и внезапните наводнения, водещи до широкомащабни щети на застроените зони и инфраструктурата;

➢ Скандинавия, където се очакват много валежи, основната част, от които под формата на дъжд вместо сняг;

➢ Арктическата област, където температурните промени ще бъдат по-

съществени, отколкото на което и да било друго място на Земята.

Изменението на климатичните условия ще окаже влияние на енергийния сектор и на структурата на енергийното потребление по *няколко начина*:

- в областите, където валежите ще намалеят или ще се увеличи честотата на сухите лета, ще се намали водният поток за охлаждане на

топлоцентралите и атомните електроцентрали, както и за производството на водноелектрическите централи. Капацитетът на охлаждане на водата също ще намалее, поради общото затопляне на водата и праговете на освобождаване могат да бъдат прехвърлени;

- режимът на водните потоци ще се промени, поради изменението на структурата на валежите, а в планинските райони – поради намалената ледена и снежна

покривка. Затлачването на язовирите, използвани за водна енергия може да се ускори поради увеличения риск от ерозия;

- търсенето на отопление ще спадне, но опасността от прекъсване на електричеството ще се увеличи, тъй като летните горещини ще доведат до нарастване на търсенето на климатизация, което от своя страна ще увеличи търсенето на електричество;
- увеличаването на опасността от бури и наводнения може да застраши енергийната инфраструктура.

Основната транспортна инфраструктура с дълъг период на експлоатация, като автомагистрали, железопътна мрежа, вътрешни водни пътища, летища, пристанища и съответните начини на транспорт, се влияят от времето и климата и следователно ще бъдат засегнати от изменението му. В резултат на това:

- покачването на морското равнище ще намали защитния ефект на вълноломите и предпазните стени на кейовете;
- като цяло се очаква нарастването на опасността от щети и смущения, причинени от бури и наводнения, но също така и от горещи вълни, пожари и свличания.

Своевременните действия и адаптация ще доведат до ясни икономически ползи чрез предвиждане на потенциалните щети и намаляване до минимум на заплахите за екосистемите, човешкото здраве, икономическото развитие, имуществото и инфраструктурата.

При липса на навременно политическо решение, ЕС и държавите–членки могат да се окажат принудени да предприемат ответно, непланирано адаптиране, в много случаи по спешност, като отговор на нарастващата честота на кризите и бедствията, която ще бъде много по-скъпоструваща и ще застраши социалните и икономически системи на Европа и нейната сигурност.

Частният сектор, предприятията, промишлеността, секторът на услугите, както и отделните граждани в ЕС могат да играят важна роля при адаптационните мерки. Конкретните действия могат да са най-разнородни:

- леки, сравнително икономични мерки (опазване на водните ресурси, промени в сеитбообръщенията, датите на засяване, използване на устойчиви на суша сортове, публично планиране и информиране на обществеността);
- скъпоструващи защитни мерки и мерки за преместване (увеличаване височината на диги, преместване на пристанища, промишлености и цели градове и села от ниско разположени крайбрежни зони и алувиални долини, както и строителство на нови електроцентрали, поради неизправни водноелектрически централи);
- действия и от публичния сектор (адаптиране на териториалното планиране и използването на земята в съответствие с рисковете от внезапни наводнения, адаптиране на съществуващите норми на строителство, с цел гарантиране на защитата на дългосрочната инфраструктура срещу бъдещи климатични рискове, актуализиране на стратегиите за управление на кризи и на системите за ранно предупреждение при наводнения и горски пожари).

Всичко това ще доведе до:

- нови пазари за устойчиви на климатични влияния строителни техники, материали и продукти;
- плажния туризъм в Средиземноморските страни се очаква да се прехвърли към пролетта и есента, тъй като туристическите курортимогат да станат твърде

горещи през лятото, а благоприятните климатични условия ще превърнат Атлантическия бряг и Северно море в потенциални нови дестинации за плажен туризъм;

- адаптиране на местните системи за управление на селското стопанство в Скандинавия към по-дълги вегетативни периоди;
- застрахователен сектор (създаване на нови застрахователни продукти за намаляване на рисковете и уязвимостта преди бедствия). Застрахователните премии, предвиждащи климатичните изменения, могат да станат стимул за въвеждането на адаптационни мерки на частно ниво.

Най-важните мерки, които трябва да се вземат са:

- подобряване на управлението на бедствия и кризи;
- разработване на стратегии за адаптиране.

Измененията в климата ще доведат до рискове в:

- земеделието и развитието на селските райони (отражение върху добивите на посевите, управлението на добитъка и местонахождението на продукцията при съществени рискове за дохода на фермите и изоставяне на земи в определени части на Европа). Рисковете пред производството на храна могат да се превърнат в много голям проблем пред определени части от Европа, защото има вероятност горещите вълни, сушите и вредителите да увеличат случаите на лоша реколта, а това ще доведе до увеличаване на риска за световните доставки на храна. В този контекст следва да се оценят вероятните последици от възможното увеличаване на биомасата за енергийно производство спрямо световното снабдяване с храна.
- промишленост и услуги (измененията на климата ще засегнат клонове на промишлеността и услугите като строителството, туризма, могат да причинят преструктуриране и щети на промишлената инфраструктура);
- енергия – предоставят се нови възможности за използване на слънчевата и фотоволтаична енергия. От друга страна, по-продължителните и по-сухи лета биха засегнали други енергийни източници като ядрената енергия и хидроенергията, като същевременно нуждата от електричество за климатичните инсталации ще се засили. Това води до необходимостта от диверсициране на енергийните източници, използването на източници на възобновяема енергия, увеличаване науправлението според потребностите (demand-response management), както и енергийна система, която да е в състояние да се справя с нарастващите колебания в търсенето и в производството на енергия. Ключов проблем са сградите и затова на дневен ред е директивата за енергийната им ефективност;
- транспорт – новата транспортна инфраструктура трябва да бъде устойчива на измененията на климата. В тази връзка трябва да се адаптират конструкциите на плавателните съдове и пристанищната инфраструктура;
- здраве – изменението на климата оказва вредно влияние върху здравето чрез горещите вълни, природните бедствия, замърсяването на въздуха и инфекциозните болести. Дълготрайното отлагане на фини частици в околния въздух е причина за редица здравословни проблеми като например, хроничното обструктивно белодробно заболяване, което прави хората по-податливи на допълнителен стрес, предизвикан от климата. В ЕС е създадена рамка за борба с последиците от изменението на климата върху здравето на човека и животните, като се разглеждат различни аспекти на смъртността и заболяваемостта, причинени от изменението на климата, включително и промените в начините на пренасяне на определени инфекциозни болести, засягащи хората и животните, промените в разпространението на

алергените, които се пренасят по въздуха, поради атмосферни промени и рисковете от ултравиолетовата радиация, защото промените в климата забавят възстановяването на стратосферния озонов слой;

- вода – необходими са икономически инструменти и принципи за намаляване на потреблението на вода и увеличаване на ефективността на нейното използване. Опазването на водата трябва да се превърне в приоритет;
- морето и рибарството трябва да осигурят устойчивост на улова и рибните запаси, защото промените в климата може да засегнат структурата на разпределението и изобилието от видове планктон до хищниците на върха на хранителната верига, което може да доведе до значителни изменения във функционирането на екосистемите и в географските ареали на някои запаси;
- екосистеми и биологично разнообразие – конвенционалният натиск, който причинява раздробяването, разрушаването, прекаленото замърсяване на екосистемите трябва да бъде сведен до минимум. Необходима е устойчивост на биологичните компоненти на екосистемите: води, почви, въздух и биологично разнообразие. Специално внимание трябва да бъде отделено на интегритета, съгласуваността и свързаността на мрежата Натура 2000;
- други природни ресурси – развитие на стратегии за горите, за почвите и др. Нетните загуби на органични вещества в почвите в един затоплящ се климат са съществена причина за опасения, тъй като почвите са най-големият сухоземен източник на въглерод.

Устойчивостта на климата следва да бъде интегрирана в Директивата за оценка на въздействието върху околната среда (ДОВОС) и Директивата за стратегическа оценка на околната среда (ДСООС). Препоръката за Интегрирано управление на крайбрежната зона (ИУКЗ) призовава към стратегически подход за планиране и управление на крайбрежието.

Извършена систематична проверка как се отразява изменението на климата върху всички области на политиката и законодателството на Общността изисква *конкретни действия* в различните страни.

Изменението на климата е сериозно предизвикателство за намаляване на бедността в развиващите се страни и заплашва да унищожи много от достиженията на развитието. Най-слабо развитите страни в Африка, части от Латинска Америка и Азия и малките островни държави ще бъдат най-силно засегнати. Промените в климата може да доведат до премествания на големи маси население, включително в региони в близост до Европа. Развитите страни, които носят отговорност за по-голямата част от историческото натрупване на антропогенни емисии на парникови газове в атмосферата, ще трябва да подкрепят действията за адаптиране в развиващите се страни, защото то трябва да бъде интегрирано в стратегиите за намаляване на бедността. Европейският съюз следва да включи Русия, крайния север на Европа, Гренландия, Черноморския регион, Средиземноморския басейн, Арктика и Алпийския регион в усилията за адаптиране. Това се отнася най-вече до трансграничните райони, регионалните морета, управлението на речните басейни, функционирането на екосистемата, изследователската дейност, биоразнообразието и природата, управлението на бедствията, човешкото здраве, икономическия преход, търговията и енергийните доставки.

Анализът и развитието на добрите адаптационни практики следва да се обменят между промишлено развитите региони, изправени пред сходни проблеми, като например Япония, Югоизточна Австралия и Югозападни САЩ.

Комисията на Европейската общност работи за установяване на общ пазар за екологични технологии, който увеличава търговията с устойчиви стоки и услуги, както и прехвърлянето на технологии, особено между индустриализираните и развиващите се страни. Съвременните информационни и комуникационни системи и бъдещото им развитие, ще бъдат ключов инструмент в подкрепа на този процес на адаптиране, даващ възможност за подходящ, гъвкав и бърз отговор на изискванията за адаптиране, за наблюдение на промените на околната среда, за предвиждане и оценка на рисковете, за управление на кризисни ситуации.

Кръговратът на водата в природата включва:

- океанско звено – при изпарение от повърхността на океанските води влагата постъпва в атмосферата и във вид на валежи пада на повърхността на Земята, попада в речните и подземните води, а след това отново в океанските води;
- атмосферно звено – обезпечава образуването и падането на валежи и тяхното разпределение на повърхността на Земята. Атмосферната влага частично се стича от повърхността на Земята, попълва ресурсите от повърхностни води и формира речната мрежа и водоемите.

Повърхностните води образуват:

- почвена влага, необходима за развитието на растенията;
- зона на аерация – това е зона, наситена с въздух и влага (намираща се между земната повърхност и грунтовите води);
- обилни и устойчиви хоризонти, без налягане и образуване на грунтови води в рохкави отложени речни долини и езерни падини;
- артезиански басейни, притежаващи високо налягане.

Природната вода притежава способността да се самоочиства, т.е. да възстановява свойствата си чрез окисление и неутрализация на замърсителите. Водните източници могат да приемат отпадни води до определени граници, след което свойствата на водата се променят. При преминаване на границите естествените водоеми се превръщат в отпадни колектори, опасни за живота на човека.

Основен потребител и замърсител на прясната вода е селското стопанство. 50% от водата се губи безвъзвратно, оставайки в селскостопанската продукция или се изпарява от растенията, от повърхността на почвите и от водохранилищата, или се изхвърля като дренажна вода, оросяваща масивите.Тези води носят соли, частици от почва, остатъци от торове. Второ място по замърсяване заемат промишлените и битовите стоки ВЕЦ, ТЕЦ, замърсените води от утайниците на водоочистващите съоръжения. Основното мероприятие по защита на пресните води е тяхното очистване. Всички замърсители са различни по физико-химичните си свойства и

състав, а това затруднява очистването.

Замърсяващите вещества се разделят на:

- органични вещества от селското стопанство;
- битови и промишлени отпадъци;
- болестотворни микроорганизми;
- вируси в лошо обработените стоки;
- азот и фосфор от битови и селскостопански стоки, което увеличава съдържанието на нитратите и нитритите във водоемите;

- тежки метали;
- нефтопродукти;
- пестициди;
- миещи вещества;
- феноли.

Замърсителите са причина за:

- увеличаване на утайките поради отпадъци;
- ерозия на почвата, която води до гибел на дадени организми;
- замърсяване на дъната.

Полихлорбифенилите и детергентите (ПАВ) са екологично опасни с високата си устойчивост и способността си да се натрупват в мастната тъкан на човека и животните, в млякото и другите хидрофобни среди на живите организми. Тези вещества понижават раждаемостта при животните, а в някои случаи измират популациите. Производството на детергенти или ПАВ в света непрекъснато нараства и се измерва в милиони тонове. Тези вещества действат на биологичните мембрани, по-точно на тяхната пропускливост и мембранен потенциал, а оттук и на регулацията на метаболизма. Детергентите са добре разтворими във вода и лесно се пренасят с водните маси на големи разстояния. Замърсяват не само водните, но и наземните екосистеми. Опитите показват, че ПАВ забавят израстването на кълновете на висшите растения и при достатъчно висока концентрация (повече от 1 мг/см3) загиват. Много прахове за пране или течни препарати за миене на съдове съдържат фосфор, който стимулира растежа на водната растителност, а този растеж намалява достъпния кислород за водната фауна. Ето защо, тези препарати не трябва да попадат в реки, езера и язовири. Голям дял в замърсяването на водоемите имат отпадните битови води, особено тези от големите градове. В каналните им системи се вливат води, съдържащи хранителни и фекални отпадъци, води от пране и миене, води замърсени от занаятчийски и други производства. Тези води съдържат неорганични, органични вещества, микроорганизми, включително и болестотворни с аеробен и анаеробен начин на живот. При намаляване на атмосферното налягане от каналните шахти започва да мирише на „лошо“, т.е. от тях излизат газове (CO_2, H_2S и др.) – продукти на анаеробни микробиологични процеси.

Главен проблем на качеството на речните води в страната е органичното замърсяване от непречистени отпадъчни води. Повечето случаи на критично замърсяване от непречистени отпадни води – 16% се дължат на индустриално, смесено индустриално и битово–фекално замърсяване. На първо място това са металургичните и химичните заводи, които често поразяват живота в реките със силно токсични води. В последните години се наблюдава известна тенденция към слабо подобряване качеството на водите. Причина за това са както процесите на приватизация и прехода към пазарно стопанство, свързани с технологично обновление на производствените процеси и изграждане на пречиствателни съоръжения, така и неустановяването на дейността на неефективни, силно замърсяващи производства.

Малко хора знаят, че рапанът по принцип е хищник, който унищожава всички аборигенни дънни животни. Между другото рапаните образуват огромните колонии и отговарят за биологичното почистване и продуктивността на крайбрежните зони. Изменението на биологическия режим довежда до това, че Черно море се „разболява“ – друг става неговият цвят, прозрачността му намалява. Оказва се, че появяването на рапаните не е най-страшната екологична беда. През 1989 г. морето

изпитва още един шок: в него се появява още един чуждестранен вид -Minemiopsis leidyi. Външно той прилича на малка медуза, оказва се необикновен лакомник и изяжда всичко наред – организмите на планктона и даже ларвите на рибите. Скоро след заселването на този вид неговата биомаса достига милиарди тонове. Този хищник унищожава и ларвите на рибите. В началото на 90-те години на XX в. негативната екологична ситуация достигна своя апогей.

В края на миналия век климатичните изменения се проявяват в мощно затопляне на регионалния климат, което променя параметрите на Черно море. Сега дебелината на повърхностния слой на морето средно достига 120–160 метра, а именно там е съсредоточен целият живот. Два километра от долния слой са замърсени със H_2S и той е безжизнен. По тази причина различните въздействия на морето в т.ч. климатични и антропогенни, не влияят на целия басейн, а само на повърхностния „жив“ слой. Получава се така, че Черно море не е много устойчиво на екологичните изменения. Затоплянето води до това, че през зимата повърхностният слой на водата не се охлажда достатъчно, следователно процесът на вертикално смесване на басейна отслабва, водата в дълбоките слоеве не „оздравява“. Кислородът не достига до дълбокия слой и в резултат на това дебелината на сероводородния нараства. В последните две десетилетия тя нараства до 12 метра, което съставлява около 10% от целия кислороден слой като тази тенденция продължава и днес.

Замърсяването на морските води е резултат на изхвърляне на отпадъци в тях, на нефтени онечиствания, на отпадъчни води, строителни отпадъци, течни радиоактивни и химически отпадъци. Ежегодно във водните басейни се изхвърлят над 6 мил. тона нефтопродукти. Нефт попада в океаните и моретата и чрез вливащите се реки. В резултат 2-4% от повърхността на Тихия и Атлантическия океан е покрита с нефтен филм. При нефтени замърсявания се променя съотношението на биологичните видове, повишава се концентрацията на пестицидите, тежките метали, канцерогенните вещества, оказващи мутагеннно влияние върху морските обитатели, нарушава се газообмена между атмосферната и морската вода, променят се процесите на топлообмен, разтваряне и отделяне на O2 и CO2. В морските води се изхвърлят радиоактивни и химически вещества, както и редица боеприпаси. С комуналните и битовите отпадъци в морската вода се изхвърлят бактериално заразени води, което води до биологично замърсяване на крайбрежните води от тежки метали (As, Hg, Pb). Попаднали в морските дарове по хранителните вериги тези отрови попадат в човешките организми.

В резултат на падащите „киселинни дъждове“ крайбрежните води понижават pH, а това е свързано с невъзможност за размножаване на морски животни, риба и пр. Особено място в замърсяването на околната среда имат опасните химични вещества.

„Опасни химични вещества“ са химичните вещества, определени в &1, т. 6 на Закона за защита от вредното въздействие на химичните вещества и препарати.

„Тежки метали“ са елементите в метална форма и/или съединенията на антимон, арсен, кадмий, хром , мед, живак, олово, никел, селен, телур, талий и калай, доколкото са класифицирани като опасни. Огромно влияние върху литосферата оказва човешката дейност. В резултат на това са усвоени 55% от природните ландшафти, 20% от сушата са претърпели коренни промени вследствие застрояване, мелиорации и различни инженерни съоръжения. Голяма част от земята се отчуж-

дава, освобождава се от дървета, храсти в интерес на енергетиката (кабелни линии, антени, тръбопроводи и пр.).

Взаимодействието на човека с литосферата се осъществява по следния начин:

- разработка на богати и крупни рудни местонаходища на полезни изкопаеми, което води до изтощаване на минералните запаси;
- изменение на релефа на земната повърхност, вследствие на изкуствена промяна на ландшафта;
- изменение на баланса на веществата в горната част на литосферата и на повърхността й вследствие на антропогенното замърсяване на атмосферата и почвата;
- изменение на състоянието на надземната и подземната хидросфера;
- изменение на водно-топлинния баланс на земната повърхност;
- нарушаване на геостатичното поле в горната част на литосферата;
- изменение свойствата на планините в резултат на строителство и експлоатация на инженерни съоръжения.

Ръстът на населението през XX в. изисква увеличаване на производството на хранителни продукти, което води до развитие на селското стопанство с високи темпове. При това се достига границата на биологичната продуктивност на почвата и повишението на добивите може да бъде резултат само на внасяне на големи количества изкуствени торове. В света само в почвите се съдържат над 50 млн. тона минерални торове с над 3 млн. тона химикали, които се смесват с повърхностните води, разнасят се от ветровете и в резултат на това настъпват геохимически аномалии. На растенията е необходим азот, фосфор, калий, калций и множество микроелементи. В почвите в света се съдържат например, над 150 млн. тона азот, който е необходим на растенията. В много случаи такова високо съдържание на азот не е необходимо и в резултат на това се образуват големи количества азотни оксиди, които се включват в кръговрата на азота и предизвикват екологични катастрофи, натрупване на нитрати в хранителните продукти, в храната на животните и пр.

Нитритите лесно се окисляват до нитрати и в резултат на този процес концентрацията на нитрити в околната среда е много ниска, а на нитрати–висока. Най-разпространени са амониевият нитрат (NH_4NO_3), натриевият нитрат ($NaNO_3$), калиевият нитрат (KNO_3) и калциевият нитрат–$Ca(NO_3)_2$, наричани селитри. Всички селитри широко се използват като торове. В резултат на това в природата се образуват канцерогенните нитрозосъединения, които водят до онкологични заболявания и мутации. Растенията използват само част от внесените торове. Излишните количества водят до еутрофикация на вътрешните водоеми и крайбрежните зони на океаните.

Широко приложение в селското стопанство намират пестициди и инсектициди, които се използват за борба с редица насекоми, плесенни гъби, плевели, които унищожават реколтата.

Проблемите, свързани с пестицидите може да се сведат до привикване и устойчивост на вредителите към тези препарати и натрупването им в околната среда като последствие от това нежелателното въздействие на околната среда върху здравето на човека. Основното производство и използване на пестициди превишава 0,5 кг на човек за година. Сред пестицидите се отделя групата на персистентните (високоустойчиви) вещества (хлорсъдържащите органични пестициди, продукти на диеновия синтез, хлорциклохексан, полихлортерпени, полихлорбензени, някои производни на уреята, триазинови пестициди), които дълго – повече от 1–2 години,

а понякога значително повече се запазват в екосистемите и оказват токсични действия на живите организми.

Немаловажна екологична и екотоксикологична роля играе високата и често неспецифична токсичност, мутагенност и канцерогенност на много пестициди. При изучаване на трансформациите им в екосистемите и организмите се изясни, че някои от тези вещества дават още по-силно токсични продукти.

Пестицидите, както и други замърсители се пренасят под формата на аерозоли, под формата на пари в атмосферния въздух, с водните маси, а също и чрез организмите на мигриращите животни.

Геохимичното замърсяване на почвите е свързано с вторично осоляване при напояване в регионите, където е много топло и е малко влажно.

Значителна роля за замърсяването на околната среда с химични вредни вещества имат използваните в промишлеността за производство на лакове, целулоза, избелващи препарати, бои и др. химични съединения, защото те се отнасят към силно действащите отровни вещества, които над допустимите концентрации, поразяват човека.

В резултат на аварии в химични предприятия и хранилища, при транспортни аварии, при нарушение на технологични процеси, както и при нарушаване на правилата за съхраняване на отровни вещества всички те се намират под форма на пари, течности, аерозоли, газове и могат да поразят човешкия организъм, попадайки в него чрез органите на дишане, кожата и стомашно-чревния тракт.

ЛИТЕРАТУРА

1. Бауман, З. Глобализацията. Последиците за човека, София, 1999.
2. Бейнс, Д., Морал за 21 век, С., 2001.
3. Бонева, М. Социално-екологични аспекти на сигурността, Ф., В.Т., 2012.
4. Йончев, Д., Равнища на сигурност, НБУ, С., 2008.
5. Недев, Т., Глобализирующийся мир: бедность, богатство, тероризм, В., 2005.
6. Петров, А., Тероризъм и системи за сигурност, С., 2005.
7. Проданов, В. Глобалните промени и съдбата на България, София, 1999.
8. Слатински, Н., Измерения на сигурността, С., 2000.
9. Слатински, Н., Националната сигурност – аспекти, анализи, алтернативи, С., 2004
10. Слатински, Н., Петте нива на сигурността, С., 2010
11. Хънтингтън, С., Сблъсъкът на цивилизациите и преобразуването на новия световен ред, С., 1999.
12. Ibryamova, N., Migration from Central and Eastern Europe and Societal Security in the Europian Union, The Jean Monnet Chair, University of Miami, Florida, 2002.

СОЦИАЛНО-ЕКОЛОГИЧНИ ПРОБЛЕМИ, ПРЕДИЗВИКАНИ ОТ ВОЕННА ДЕЙНОСТ

Маргарита К. Бонева Елена Андреева

проф. д.ик. н. Маргарита Бонева – ШУ „Епископ К. Преславски“
Елена Андреева – Военна академия „Г. С. Раковски”

SOCIAL-ECOLOGICAL PROBLEMS – RESULTS OF MILITARY FUNCTION

Margarita Boneva Elena Andreeva

ABSTRACT: *The paper presents social-ecological problems –result of military function*

KEY WORDS: *security, anthropogenous contamination, military function*

Негативните аспекти на войните върху природата са свързани не само с технологиите, а и с разбирането и отношението към произтичащите от тях проблеми. Можем да определим четири основни класа на военните последици върху околната среда: съпътстващи ефекти, употребата на околната среда като оръжие, промяната ѝ за подпомагане на собствените войски или за възпрепятстване на противниковите сили, и еко-тероризъм. Военните действия могат да включват някои или всички от тези компоненти в различна степен.

След края на Пуническите войни и разрушаването на Картаген римляните посипват района със сол. Това не е единствено символичен акт, а и целенасочено увреждане на почвата с дълготраен ефект. Дори армиите от конници, снабдени с лопати са променяли околната среда в широк мащаб – отклонявайки реки за защита на крепости или пък в противоположния случай – за да лишат обсадените от вода. Холандците умишлено разрушават дигите и наводняват значителни области от своята територия през 1792 г., за да предотвратят френската инвазия. В бойните действия по време на Първата световна война в района на Алпите са предизвикани многобройни лавини за поразяване на противниковите войници. Тактиката на “изгорената земя” се използва от древността до средата на XX век.

В Южен Виетнам са унищожени повече от 1/3 от горите и селскостопанските райони, в Афганистан са отровени около 20% от водоизточниците, а в Персийския залив в продължение на няколко месеца горяха пожарите от нефтените кладенци. Гражданската война в Конго опустошава дивата природа на страната, убивайки хиляди слонове и горили.

Емисиите на парникови газове, генерирани при защитата на доставките на петрол от Близкия Изток и Персийския залив достигат до 34,4 милиона тона еквивалент на въглероден диоксид на година. Войната в Ирак и операциите за следвоенното му възстановяване се сочат като причина за още 43,3 милиона тона парникови газове годишно. Консервативната оценка на емисиите, получени в резултат от дейности в областта на сигурността и отбраната, направена след изследване на университета “Линкълн” – Небраска показват нарастване от 8 до 18 на сто.

Военната активност се отразява пряко на физическата среда в следните направления:

– замърсяване на въздух, суша и вода в мирно време;

– чрез непосредствените и дългосрочните последици от въоръжените конфликти;

– милитаризация на космоса;

– развитие на ядрените програми;

– използването на земята.

Значителни са и непреките ефекти чрез отклоняване на
средства.

Водещите Европейски армии са отговорни за освобождаването в атмосферата на повече от две трети от озоноразрушаващите вещества в озоновия слой. По време на Студената война, американските и съветските въоръжени сили произведа огромни количества опасни отпадъци. В резултат на аварии и инциденти има най-малко 50 ядрени бойни глави и 11 ядрени реактора потопени на океанското дъно. Пентагонът генерира пет пъти повече токсини от петте големи химически компании в САЩ, взети заедно, а Американската армия е най-големият източник на замърсяване на околната среда на САЩ. Разходите за почистване на обектите, свързани с отбраната се очаква да бъдат над 500 милиарда долара[1].

Заради тесните връзки между ядрената оръжейна промишленост и гражданското производството на ядрена енергия, производството на ядрени оръжия носи отговорността за замърсяване на околната среда, причинено по веригата от добива на урановата руда и преработката й през транспортирането на суровината: yellowcake (прахообразен концентрат на урана, получаван чрез различни методи за извличане и рафиниране, в зависимост от вида на рудата, обикновено чрез смилане и химическа обработка, жълт на цвят и неразтворим във вода. Съдържа около 80 % уранов оксид); MOX (От “Mixed oxide fuel” –“Mixed oxide fuel” – ядрено гориво, което съдържа повече от един оксид на делящи се елементи, обикновено се състои от плутоний смесен с природен уран, преработен уран или обеднен уран); други ядрени материали. Транспортирането се извършва с автомобилен, железопътен и морски транспорт. Рисковете произтичат и от корабите задвижвани с ядрени реактори, производство на горивни пръти и проблемите за съхраняване на ядрени отпадъци. Районите около Челябинск, Юка Маунтийн, Ханфорд, Селафийлд и Мурманск ще са под въздействието на огромните количества ядрени материали, натрупани там. Общата стойност на демонтиране на ядрените оръжия и производствените съоръжения според някои оценки (Center for Defense Information) достигнат 3,5 трилиона долара за САЩ.

Част от промените в климата чрез емисиите на парникови газове са предизвикани от военни самолети, като тези дейности са изключени от рамката на Договора от Киото.

Някои от най-известните следвоенни последствия за околната среда (комбинирана със сериозни опасности за човешкото здраве и безопасността) са:

– лъчения от ядрени взривове;

– влошаване на качеството на земеделската земя в резултат на използване на противопехотните мини;

[1] Велев, С. Военни аспекти на екологията и опазването на околната среда, С. Военна академия, 2013

– невзривени боеприпаси, възпрепятстващи селското стопанство, например мини или касетъчни бомби;

– вредни емисии при изгарянето на петролни кладенци.

Въздействие с дългосрочни отрицателни последствия е и спомената тактика на "изгорената земя" (Scorched-earth). Практика през вековете за отстъпващите войски е опустошаването на собствената територия или на тази на врага. Историческите примери включват отстъплението на Наполеон от Москва и на нацистите в Съветския съюз и в Северна Норвегия.

Използването на дефолианти от войските на САЩ по време на войната във Виетнам, опустошава около една трета от горите на територията на страната. Във всички войни, водени между 1945 и 1982 г., Виетнам загубва над 80 % от първоначалния си горски фонд, възстановяването на който може да се

осъществи след няколко поколения.

"Войната в залива" също предизвика отрицателни екологични последици. Четири до осем милиона барела петрол бяха разляти в морето. 460 мили от крайбрежната линия са претърпели огромни щети вследствие на нефтени разливи и изгарянето на кладенци. Дългосрочните ефекти могат в крайна сметка да доведат унищожение на коралите. Запалителните авиационни бомби, използвани обезвреждане на минни полета унищожават горния почвен слой и близката растителност. Боеприпасите имат радиационно и токсично въздействие. Генерирани са огромни количества отпадъци, токсични материали и между 45–54 милиона галона канализационни отпадъци в септични ями.

По време на военните действия на НАТО в Косово и Югославия бяха нанесени щети на околната среда в резултат на въздушните атаки. При пожарите в петролните рафинерии петролни продукти и химикали изтекоха в река Дунав. Изключително опасни вещества от разрушени химически инсталации попаднаха в природата. Нарушено беше биоразнообразието, регистрирани бяха повишени нива на радиоактивност в резултат на използването боеприпаси с обеднен уран. Конфликтът в Косово е първият, при който по програмата на обединените нации за околната среда (United Nations Environment Programme – UNEP) беше направена екологична оценка след конфликта. Според нея замърсяването на четири района в Сърбия е било сериозно и в степен, представляваща заплаха за човешкото здраве[2].

В Афганистан стотици хиляди противопехотни мини са разхвърляни из полетата и планинските проходи. Има доказателства, че използването на боеприпаси с обеднен уран в конфликта с Ал Кайда също са довели до замърсяване на околната среда с дългосрочни рискове за здравето.

Радиационните ефекти от бомбардировките на Хирошима и Нагасаки, последващите атмосферни ядрени опити и аварията в Чернобил и Фукушима дадоха реална представа за последствията, които биха настъпили от дори ограниченото използване на ядрени оръжия. Увреждането на екосистемата на Земята ще бъде изключително тежко, както и икономическото и социално въздействие.

Индия и Пакистан придобиват статут на ядрени държави през май 1998 г., когато Индия провежда серия от подземни тестове, последвани от подобни пакистански такива. Извършени са в пустинните райони, но е доказано, че имат екологично въздействие. Световната федерация на жертвите на ядрени тестове (The World Nuclear Test Victims' Federation) съобщава за хиляди случаи на рак от местните

[2] Бонева, М., Социално-екологични аспекти на сигурността, 2012.

жители, свързани с потреблението на млечни продукти, за които е използвана суровина от съседни райони. Съпътстващите щети са и финансови – за оръжейни програми са изразходвани огромни суми, които биха могли да бъдат използвани за защита на околната среда и справяне с бедността в региона.

Използването на химически или биологични оръжия за масово унищожение, макар и не толкова катастрофално, също ще предизвика тежко увреждания на природата, в допълнение към техните разрушителни ефекти върху хората. Химически оръжия са използвани в някои конфликти (със сериозно екологично въздействие) от Първата световна война до Ирано– Иракската война и атаките на Саддам Хюсеин срещу иракските кюрди. Има и редица недоказани твърдения за използването на т.нар. "Yellow Rain" от подкрепяните от Съветския съюз виетнамски части в Лаос и Камбоджа. За последствията от използваното в настоящия момент химическо оръжие в конфликта в Сирия (зарин) все още няма проведени изследвания.

Има предположения, че в САЩ се развива програма за култивиране на гъбички и вируси, които унощожават опиумния мак, марихуаната и коката. Те са проектирани да поразяват за кратко време високи растения като бъдат разпръсквани по време на операции за ликвидиране на тези култури. САЩ оказва натиск върху някои държави да използват тези патогенни гъби. Предполага се, че това са Колумбия и Мианмар, които имат големи райони с такива насаждения и са зони на бойни действия между бунтовнически движения и правителствата на страната. Такава стратегия носи големи опасности за заобикаляне на международните забрани и оттам – рискове за здравето и заобикалящата ги среда . Подобно на всички други биологични агенти, ще бъде много трудно да се контролират след освобождаването извън целевата зона.

Използването на сателити за военни цели е дългогодишна практика. Освен за разузнаване те са средство за насочване на ракетни системи, което предполага възможно замърсяване на космическото пространство при евентуален конфликт чрез конвенционални или ядрени експлозии.

Разработването, производството, съхранението, транспортирането и не на последно място – унищожаването на ядрени оръжия оказва своето въздействие върху околната среда и здравето на хората. Радиоактивното замърсяване от вече забранените атмосферни ядрени опити е вероятната причина за около 86000 вродени малформации и 150 000 смъртни случая в световен мащаб. В дългосрочен план то може да доведе до над два милиона смъртни случаи, предизвикани от рак. Добивът на уран, както и операциите за преработката му по цялата технологична верига водят до тежки случаи на заразяване. За унищожаване на излишъците от химически и ядрени оръжия на Русия, които представляват огромна заплаха за околната среда и сигурността правителствата от т. нар. Г–8 (вече Г–7) се споразумяха на срещата на високо равнище (в Калгари през юни 2002 г.) да отделят значителни средства за решаване на проблема. Въпреки това и след изтичане на срока по Конвенцията за забрана на разработката, производството, натрупването и използването на химическо оръжие през април 2012г. запасите не бяха унищожени и над 25 хиляди тона все още се съхраняват и представляват реална заплаха.

Много често населението на области, в които са разположени военни обекти се премества принудително. Армията използва земя (и водни обекти), необходими за живот или прехрана на местните жители. Обикновено става дума за изграждане на бази, стрелбища, складове за оръжия и тренировачни полигони. Такъв е случаят с

Туле в Гренландия, където местните инуити са разселени за да се построи в района база на САЩ. Подобни са случаите с базите в Окинава (Япония), Гуантанамо (Куба), и Диего Гарсиа. Военните действия често включват и използването на горива, експлозиви, разтворители и други токсични вещества. Когато тези вещества са използвани или складирани неправилно, те могат да проникнат в околната среда и да въздействат върху общностите в района. Често биват увреждени земеделска земя и други имоти или пък пътна инфрасруктура при използване на тежка военна техника. В земите на Ину (Канада) шумовото замърсяване, предизвикано от ниско летящи летателни средства се оказва сериозен вредител, включително и за животновъдството. Протестите на жителите на Карибския остров Вике край Пуерто Рико също са пример за напрежение, свързано с околната среда, предизвикано от военните бази, както и за пренебрегването на интересите на населението от страна на военните институции.

Освен върху околната среда, армиите въздействат непряко и чрез т. нар. "алтернативните разходи". Разработката на оръжейни системи и изследванията в областта на отбраната възлизат на 58 милиарда долара годишно. Делът на оръжията и военната екипировка заема второ място в световната търговия. Около 25 % от самолетното гориво е изразходвано от въоръжените сили, а над половината хеликоптери в света са използвани от армията. Тези огромни разходи могат да бъдат пренасочени и използвани с цел подобряването на качеството на живот, включително за екологични цели – развитието на възобновяеми източници на енергия и насърчаването на устойчивото развитие.

Държавите членки на Обединените Нации прзнават, че военните разходи са загуба на ресури. От 1976, събрания като *UN General Assembly, Social Development Summit, Habitat*, и др. са потвърдили необходимостта от намаляване на военните бюджети в световен мащаб.

Сериозно препятствия за това е влиянието на военно-промишления комплекс и по-специално това на големите корпорации, ангажирани във военната дейност. Натиск оказват не само производителите и търговците на оръжие, но и големи сектори на въздухоплаването, транспорта, металургията, електрониката и тези от комуникационно–информационния сектор. В страни като Китай и Мианмар военните пряко ръководят големи сектори на гражданската икономика. Когато представителите на тези интереси акцентират върху големия брой работни места създадени или подържани от индустрията, те не взимат в предвид възможностите, които могат да бъдат реализирани, ако ресурсите се използват по друг начин. Корпорации като Сименс са наложили в общественото пространство привлекателен екологичен профил на дейността си, който не показва ролята им в ядрената енергетика или оръжейното производство. Това прикриване е голяма пречка за осъзнаването на вредите, които се нанасят в тази област.

Това са само някои от типичните примери, характеризиращи глобалните екологични проблеми, предизвикани от военната дейност, но и те са достатъчни да се направят следните изводи:

- това са проблеми, засягащи страни от живота не само на отделни народи и региони, а буквално на цялото човечество;
- проблемите не се ограничават в тесни национални граници;
- тяхното подценяване днес ще е с необратими последствия за бъдещето.

ЛИТЕРАТУРА

1. Велев, С. Военни аспекти на екологията и опазването на околната среда, С. Военна академия, 2013.
2. Бонева, М., Социално-екологични аспекти на сигурността, В.Т. 2012.

ГЛОБАЛИЗАЦИЯТА И ГЛОБАНОТО ГРАЖДАНСКО ОБЩЕСТВО

Чавдар Л. Милков

София 1202, ул. „Будапеща“ № 38, ап. 1
milkovl@abv.bg

GLOBALISATION AND GLOBAL CIVIL SOCIETY

Chavdar L. Milkov

ABSTRACT: *Focuses on the problems of civil society in the context of new realities. European requirements for the development of civil society and good practices for the participation of citizens in decision-making in society.*

KEY WORDS: *civil society, civic participation, european practices, globalization, global society*

ВЪВЕДЕНИЕ

Понятието „гражданско общество” отразява етап от развитието на обществото като цяло. Характерно за обществото, което се нарича „гражданско” е едно ново ниво на отношенията между отделните личности, които го съставляват. В процеса на развитие и еволюция на света хората успяват да се организират, създавайки държави, едновременно с развитието на буржоазното общество, което се разглежда като начална форма на гражданско общество.

Гражданското общество е обект на изследване от теорията още от античността, но в този етап то се разглежда по-скоро в социален, културологически и политически аспект. Понятието „гражданско общество” преминава различни етапи на развитие, за да се достигне използването му в наши дни като определящо съвременната социална, икономическа и правна теория на развитите държави.

През последното десетилетие на XX век започва динамично развитие на световните процеси. Наблюдава се световна глобализация на политическо, икономическо, техническо, интелектуално, нравствено и др. ниво. Тези процеси продължават своето, още по ускорено, развитие през XXI век. Република България не прави изключение от тази световна глобализация. Особено активно се говори за това след присъединяването на България към Европейския съюз. Тогава у българските граждани се изгражда самосъзнание и самочувствие на граждани на света. Възможността за лесен достъп и трансфер на хора, стоки, услуги и капитали, довежда до естес-

твеното израстване на българското общество. Навлизат редица интернационални компании, които не само осигуряват качествени работни места, но носят опита и знанията на големи и добре развити страни.

I. СЪЩНОСТ НА ГЛОБАЛНОТО ГРАЖДАНСКО ОБЩЕСТВО

В условията на всеобхватна световна глобализация се говори и за глобално гражданско общество. Естествено е, при това бързо и лесно стопяване на границите и удобната мобилност на всеки индивид, да има очакване и развитието на гражданското общество да върви в такава насока.

Теоретичното обяснение за разбирането за глобално гражданско общество е, че това е общество в познатия смисъл, но на наднационално и международно ниво, т.е., то включва международните граждански, нестопански, неправителствени организации (НПО) и такива с нестопанска цел, както и организации, които имат икономическа печалба, но тя не е основна цел на тяхната дейност. Съществуването на глобалното гражданско общество е естествено и очаквано, тъй като светът се ориентира в развитието си към глобално управление. Като термин „глобално гражданско общество“ се използва още от 80-те години на миналия век. Някои автори предпочитат термина „международно гражданско общество“, с аргумент, че държавите съществуват отделно и имат своите граници. Дебатите по този въпрос са по-скоро следствие на различните виждания за глобализацията като цяло.

В глобалното гражданско общество се включват различни граждански и неправителствени организации, разнородни граждански съюзи и др., които могат или да работят, всяка на национално ниво и да се свързват помежду си чрез средствата за комуникация, или да се изграждат и създават като международни организации. И в двата случая, целта на подобен начин на функциониране на тези организации е не само да се използва опита и потенциала на максимален брой участници и организации, но и да се изграждат цели мрежи от еднотипни организации, които да могат да реагират на територията на различни държави.

Много често се формират подобен тип конфигурации на политическа основа. Изграждат се политически организации, чиято цел е да привлекат максимален брой привърженици на своите идеологии, като използват средства за разпространението им в много на брой и различни държави.

Управлението и функционирането на глобалното гражданско общество става предимно чрез използването на съвременните технологии и електронното пространство, където практически граници не съществуват и възможността за взаимодействие между различни държави, организации и хора е безпроблемно.

Съществуването на глобално гражданско общество се обуславя и от изготвянето и приемането на редица нормативни документи с международно действие и значение. Това позволява да се изравняват и уравновесяват правата и задълженията на гражданите на различните държави и защитата на всеки един индивидуален интерес е възможна много по-лесно.

Дейността на всички организации, които са част от глобалното гражданско общество, е насочена на по-високо интернационално ниво. Стремежът им е за постигане на отъждествяване не само на индивидуалните с националните интереси, но и да се изгради такава система, че задоволяването на националните потребности да води до една колективна, наднационална удовлетвореност.

Като цяло се приема, че тези организации, които са част от глобалното гражданско общество имат силни и затвърдени позиции на национално равнище. Те

биха могли да осъществяват контрол и да оказват влияние върху процесите в дадена държава, което би могло да доведе до много по-активна и ползотворна дейност на международно равнище.

Глобалното гражданско общество се съставя от организации с различна сфера на дейност. Те могат да бъдат политически, икономически, екологични, културни, религиозни и др., т. е., обхватът на тяхното влияние е голям и световните проблеми, които могат да бъдат решени с тяхна помощ, са не само голям брой, но и всеобхватни като теми, начин, време и място на възникване.

В условията на световна глобализация проблемите и силите за разрешаването им излизат от националните рамки и придобиват световно измерение. Това дава възможност и много по-голяма сигурност за справяне с въпроси, които имат значение за всеки един индивид по света.

В основата на изграждането на глобално гражданско общество е набралата скорост световна глобализация, като цяло. Развитието на технологиите, улеснението в комуникацията, бързото и безпроблемно придвижване чрез модернизация в транспорта и инфраструктурата, придобиването на опит и знания и др. са само част от областите и направленията на глобализацията. Напредъкът на информационните и комуникационни технологии (ИКТ) и разнообразието на възможности за връзка е предпоставка не само в международните организации, съставляващи глобалното гражданско общество, да се включат максимален брой хора, но това става и на достъпна цена. В този смисъл, разстоянията не оказват влияние върху дейността на организациите и обменът на информация и данни между тях е безпрепятствен. Освен това, чрез средствата за масова комуникация и осведоменост всеки един гражданин във всяка точка на света може да се запознае със ситуацията или развитието на конкретен казус във всяка държава. Бързият и лесен достъп до всякакъв вид информация улеснява функционирането на организациите и дава възможност за навременна реакция от тяхна страна.

Развитието на ИКТ и глобалната мрежа Интернет, виртуалното пространството създават и т. н. „виртуално гражданско общество“. Това става благодарение на различните социални мрежи, в които хората се обединяват по групи и интереси и много бързо създават организация помежду си за въздействие по различни казуси или за разпространяване на полезна информация. Това виртуално гражданско общество работи изключително в полза на глобалното такова, тъй като социалните мрежи, като цяло, обединяват хора с различни интереси и от различни националности.

Това динамично развитие на глобалния свят води до възникването на наднационални проблеми и изискването за тяхното международно разрешаване. Освен това, редица екологични проблеми, които засягат цялото човечество и всички страни по света, налагат комплексни и съвместни мерки за справянето с тях или намаляване на вредното влияние. Такъв тип проблеми са, например, изтъняването на озоновия слой и разширяването на озоновата дупка, глобалното затопляне, топенето на ледници, замърсяването на почва, вода, гори, въздух и др. Справянето с тези и подобен род трудности е въпрос на комплексни усилия от страна на всеки един жител на планетата. Именно, поради това, в тази връзка бяха създадени редица международни екологични организации, чиято цел е да провеждат разяснителни кампании навсякъде по света, да направят всеки един човек съпричастен и запознат със собственото си влияние в глобалния свят.

Съществуването на глобално гражданско общество се обуславя и от факта, че редица национални компании разгръщат своето производство и стъпват на международни пазари. Това води не само до трансфер на стоки, услуги и капитали, но и до активни взаимоотношения между съответните държави. В този случай, от защита на своите интереси и права имат необходимост не само потребителите на тези стоки и услуги, но и техните производители, които не могат да разчитат само на национална защита и законодателство.

Целта на създаването на глобално гражданско общество е да бъде бариера за безконтролно поведение в условията на глобализация. Самият процес на глобализация се свързва с редица реформи, които надскачат националните граници и са въпрос на международно сътрудничество. В този смисъл, глобалното гражданско общество има ролята да защитава основните човешки права и интереси на транснационално ниво, както всяко национално гражданско общество изпълнява тази функция в рамките на една определена територия и държава. Естествено е, че обхватът на дейността на глобалното гражданско общество е много по-голям от този на действащото такова на национално равнище. Ето защо, отговорността и очакванията към него са много по-големи.

Някои автори смятат за полезно и необходимо съществуването на глобално гражданско общество. Те са на мнение, че, в повечето случаи, държавата е неспособна да удовлетворява адекватно потребностите на своите граждани и е задължително да има механизъм, който да регулира, както държавната намеса в обществения живот, така и ощетяването на гражданите от формите на глобализация- политическа, икономическа, екологична и др.

Друг аргумент срещу изграждането на глобалното гражданско общество е, че международните граждански и неправителствени организации не са достатъчно добре развити, за да бъдат регулатор на наднационално равнище и не могат да заместят държавата в предоставянето на основни и необходими публични блага. Те могат да бъдат само балансьор в отношенията между държавата и гражданите. Освен това, формата на управление зависи не само от нагласата на гражданите и техните организации, но и от политическите и идеологически възгледи.

Транснационалните медии също могат да бъдат защитници на големи корпоративни интереси и в определени ситуации да не бъдат напълно обективни в отразяването и настройването на общественото мнение.

II. ОТВОРЕНО ОБЩЕСТВО И ИНДЕКСА ЗА РАЗВИТИЕ НА ГРАЖДАНСКОТО ОБЩЕСТВО

Щатският финансист Дж. Сорос е известен филантроп, който отделя милиарди долари за благотворителност и за финансиране на редица граждански организации. Той е създател на фондацията „Отворено общество“, както и основател на редица граждански и неправителствени организации, които действат на територията на повече от 50 държави. Основна мисия и цел на тези организации е да подпомагат структурата на гражданското общество и да разширяват методите за въздействие от страна на гражданите при вземането на управленски решения. Мрежата от организации „Сорос“ е разпространена в страни от Централна и Източна Европа, както Африка, Азия, САЩ и др. Тези организации работят в сътрудничество с институт „Отворено общество“, като целят подпомагането и развиването на отворени и демократични общества в развитите и развиващите се държави, оказват подкрепа в сферата на образованието, медиите и др. От 1990 година институт „Отворено об-

щество“ работи и в България. Той е основан като неправителствена организация, с дарение на Дж. Сорос. Дейността на института е свързана с редица програми и проекти, с подкрепа на гражданското общество и неправителствените организации, европейските и социални политики и др.

През 1997 година Световният алианс за гражданско участие (СИВИКУС) публикува „Нов атлас на гражданското общество“, в който са включени профили на гражданското общество в 60 държави от целия свят. Това е направено по примера на директора на Центъра за гражданско общество към училището по икономика в Лондон Х. Анхайер, който прави първоначално проучване в рамките на 13 държави. От 2003 година до 2006 година СИВИКУС провежда първото пълно проучване, в 53 държави. След продължителни проучвания и набиране на партньори, през 2008 година СИВИКУС стартира втора фаза на проекта с подобрена методика и с участието на нови и утвърдени партньори.

В България проектът „Индекс на гражданското общество“ по програма „Европейски политики и гражданско участие“ се прилага от 2003 година. Той се осъществява съвместно от институт „Отворено общество“- София, „Световен алианс за гражданско участие“ (СИВИКУС), както и Програмата за развитие на ООН (ПРООН). В рамките на този проект се провежда изследване в 41 страни за степента на гражданско участие и развитие на гражданското общество и за оценка на силните и слабите му страни в световен мащаб. Целта на осъществяването на подобен анализ е да се установи степента на изграденост на гражданското общество и да се дадат насоки за по-пълноценното му развитие за в бъдеще. Прилагат се качествени и количествени методи за анализ и оценка на развитието на гражданското общество.

Такова изследване в България е проведено два пъти: за периода 2003 година-2005 година и за периода 2008 година -2010 година. Докладът от проведеното първо проучване е озаглавен „Гражданското общество без гражданите“, а от второто проучване е озаглавен „Гражданското общество в България: Гражданска активност без участие“. Направеното проучване отчита промените, настъпващи в българския трети сектор след присъединяването на страната към Европейския съюз. В доклада са отбелязани, както състоянието на гражданското общество към момента, така и тенденциите и насоките за бъдещо развитие. Присъединяването на България към Европейския съюз съвсем естествено довежда до промени в редица области на обществения живот, както и във функционирането на гражданското общество. Това се дължи, както на европейските изисквания за реформи в редица области, така и на необходимостта за съвместна дейност на европейските институции.

Методологията, по която се провежда изследването, представлява анализ в пет основни направления, които образуват т. н. „диамант на гражданското общество“. Изследваните направления са: гражданско участие, степен на организация, възможност за влияние, ценности и контекст. Индексът се изчислява като от 67 количествено измерими показатели се образуват 28 групи направления, които оформят т. н. „диамант“ и се измерват по скала от 1 до 100. Размерът на „диаманта на гражданското общество“ е това, което дава представа за състоянието на гражданското общество, за степента на неговото развитие, както и за външни фактори, които влияят на неговото функциониране.

Най-ниски стойности на „диаманта на гражданското общество“ и в двете проведени проучвания има измерението „гражданско участие“. Според този анализ,

все още, се наблюдава тенденция за затвореност и ниска активност на отделните индивиди. Съществува възможност за повишаване на този показател чрез създаване на различни организации за защита на правата и интересите на по широк обхват лица.

Сравнително висока е стойността на показателя „степен на организация на гражданското общество“. Гражданското общество има добре изградена структура. Изследователите посочват, че е добре да се търсят начини за създаване на финансова устойчивост и за подобряване на връзката и разширяване на мрежата от отделните организации.

Показателят „възможности за влияние на гражданските организации“ отчита слабо влияние от страна на гражданското общество при определяне на държавната политика. Според анализаторите, все още, не е достатъчно доверието в третия сектор и то е много по-ефективно в области като образование и опазване на околната среда.

Измерението „ценности на гражданското общество“ е с относително висок резултат, което е показател за демократични практики при функционирането му. Корупцията е фактор, който води до намаляване на стойността на този показател.

С най-висока стойност от петте показателя на „диаманта“ е „контекстът на развитие“. В България има благоприятна среда за добре развито и функциониращо гражданско общество. Съществуват, обаче, негативни фактори, които изискват сериозно внимание и усилия за предотвратяването им като високо ниво на корупция, силна политическа зависимост и др.

Стойностите на петте основни показателя за гражданското общество в България се сравняват от двете фази на провеждането на ИГО, за да могат да се набележат основните тенденции в дейността на гражданското общество, да се съпостави състоянието му в периода преди и след присъединяването на страната към ЕС и да се дадат съвети и насоки за подобряване на работата му. Резултатите от проучването се обсъждат на граждански форуми, където присъстват заинтересовани лица.

III. ЕВРОПЕЙСКАТА КОМИСИЯ И ГРАЖДАНСКОТО ОБЩЕСТВО - ЕВРОПЕЙСКА ГОДИНА НА ГРАЖДАНИТЕ

2011 година е обявена за „Европейска година на доброволческите дейности за насърчаване на активна гражданска позиция“. Европейската комисия определя 2013 година за „Европейска година на гражданите“, посветена на гражданите и техните права

Този алианс е създаден с усилията на мрежа от граждански и неправителствени организации от съюза, чието намерение е активно да оказват влияние върху институциите на съюза за изграждане на стратегии и политики ориентирани към гражданите и гражданското общество.

През Европейската година на гражданите се провеждат редица семинари, както на европейско, така и на национално и местно равнище. Работят интернет-портали, чрез които всеки гражданин има възможността бързо и лесно да намира информация за съюза, както и за своите права и задължения като негов гражданин. Създават се механизми и мрежи за по-ефективната защита на човешките права, като, например, мрежата „Солвит“. Тя представлява мрежа от 30 центъра, работещи съвместно за осигуряване на защита на гражданските права и за намиране на решения на проблеми, вследствие на неправилно прилагане на европейското законодателство от националните администрации. Център от

мрежата „Солвит“ работи във всяка държава, членуваща в съюза, както и в Норвегия, Лихтенщайн и Исландия. За по-успешното протичане на Европейската година на гражданите, през 2012 година Европейската комисия прави допитване сред гражданите на съюза за основните проблеми, с които се сблъскват и за правата, които най-често биват накърнявани.

Предварителното проучване показва, че голям процент от гражданите не са запознати с правата, които имат като жители на страни, членуващи в ЕС. Една от задачите на Европейската година на гражданите е да бъдат разяснени тези права, за да могат повече граждани да се възползват от тях. През 2010 година Европейската комисия публикува доклад за гражданството на ЕС. В него се посочват основните пречки пред гражданите да се възползват от своите праваи се набелязват мерки за тяхното преодоляване. В рамките на 2013 година Европейската комисия публикува втори доклад, в който набелязва оставащите пречки за пълноценно гражданство на всеки отделен индивид и мерки за премахването им. Европейската комисия обявява2013 година за „Европейска година на гражданите“ по призив на Европейския парламент.

Създателите на алианса използват понятието активно гражданство. Дефинират го като процес на пълноценно и активно участие в управленските решения и дейности, свързани с изразяване на гражданска позиция по национални и общоевропейски въпроси.

Активното гражданство се развива в няколко основни направления- участие в обществения живот, в избори, граждански диалог, в местното самоуправление и социално гражданство.

Участието в избори е важен показател за активното гражданство. Според създателите на алианса, в Европейската година на гражданите трябва да се стимулира висока избирателна активност на гражданите на всяка една страна, членуваща в съюза при избирането на представители в Европейския парламент, тъй като това е своеобразна оценка на доверието на хората, както към институцията, така и към Съюза, като цяло.

Гражданският диалог изисква предоставянето на възможност на активни граждански организации да вземат участие в процеса науправленски решения и да получават адекватна обратна връзка с институциите. Според създателите на алианса, е необходимо да се изготви споразумение между институциите, което да даде рамката на активния граждански диалог, наред със съществуващата нормативна база, включваща договора от Лисабон и Европейската гражданска инициатива.

Целта и идеята на Европейската година на гражданите е не само да популяризира европейското гражданство, но и да допълва правото на гражданите и техните организации свободно и публично да изразяват своето мнение, което е определено в договора от Лисабон. Стремежът на алианса е да стимулира по-активна гражданска позиция по въпросите на общността и да се изгради съзнанието у всеки един гражданин на държава, членуващ в ЕС, за част от единна общност, в която гласът на всеки отделен индивид е от значение.

IV. КОДЕКС НА ДОБРИТЕ ПРАКТИКИ ЗА ГРАЖДАНСКО УЧАСТИЕ В ПРОЦЕСА НА ВЗЕМАНЕ НА РЕШЕНИЯ

На проведено заседание на Съвета на Европа в Швеция през 2007 година е направена препоръка към Конференцията на международните неправителствени

организации за изготвяне на Кодекс на добрите практики за гражданско участие в процеса на вземане на решения. В своя призив Комитетът на министрите на Съвета на Европа отчита ролята и значението на неправителствените организации за развитието на демократичността и тяхната неизменна необходимост за защита на човешките права, тъй като чрез своята дейност те допринасят за по-добрата информираност на гражданите и за тяхната активност в обществения живот и при вземането на управленски решения.

На конференция на Международните неправителствени организации (МНПО) през 2009 година е одобрен Кодекс на добрите практики за гражданско участие в процеса на вземане на решения. Изготвеният документ е приет с одобрение и от Конгреса на местните и регионални власти в Европа и от Парламентарната асамблея на Съвета на Европа.

В него се очертават рамките и механизмите за участие на граждански и неправителствени организации, както и за активността на гражданското общество при формирането на публичните политики. В изготвянето на документа вземат участие представители на гражданското общество с изграден опит. Разработен е на база на щателни проучвания в редица страни. Кодексът няма нормативен и задължителен характер. Той само дава насоки за подобряване на прилагането на демократичните механизми за участие на гражданското общество и неправителствените организации в процеса на изготвяне на публичните политики и вземане на обществено значими решения. Препоръките на Кодекса на добрите практики следва да се прилагат в страните-членки на Съвета на Европа и Беларус.

Основната задача на Кодекса е да създава общоприети европейски методики за активното участие на гражданското общество и неправителствените организации в дейността на европейските институции. Също така, да се развиват демократичните средства за участие на гражданите на местно и регионално равнище.

Създаването на Кодекса на добрите практики за гражданско участие в процеса на вземане на решения е насочен към гражданските и неправителствени организации, които развиват своята дейност на местно национално или европейско равнище, от една страна, и институциите, които са компетентни за вземане на общоевропейски политически решения, от друга. Валиден е и за националните институции на всяка страна-членка и Беларус.

В Кодекса са посочени няколко основни принципа на добрите взаимоотношения между гражданското общество и институциите. Те са: участие, доверие, отчетност и прозрачност и независимост.

Принципът на участие е основан на правото на гражданите да се включват в обществения и политически живот.

Принципът на доверие се базира на различната роля на участниците в процесите на управление. Целта на Кодекса е заимоотношенията на заинтересованите страни да се изграждат на основата на взаимно доверие за постигане на общата им цел за повишаване качеството на живот на гражданите.

Принципътна отчетност и прозрачност в дейността, както на неправителствените организации, така и на институциите, трябва да бъде спазван на всички нива.

Принципът на независимост е основан на изискването за свободно мнение на гражданските и неправителствените организации и правото им да се

противопоставят и да вземат собствена позиция по различни въпроси от тази на институциите.

Участието на ниво информация е често еднопосочен процес, при който публичните организации предоставят информация по съответния проблем без да се изисква прякото участие на граждански и неправителствени организации. Информацията е важен инструмент при осъществяването на взаимоотношенията на гражданското общество с публичните институции и макар да се приема за ниско ниво на гражданско участие, стои в основата на всички етапи на процеса.

На ниво консултация гражданското участие се изразява в допитване от страна на институциите до различни организации по съответен въпрос. Обикновено, механизмът се осъществява чрез предоставяне на информация на организациите от страна на институциите и приемане на тяхното становище по съответния проблем. На това ниво на гражданско участие инициативата се поема от публичните институции, а не от гражданското общество. Този механизъм може да се прилага на всеки етап на вземане на решения.

Инициативата за участие чрез диалог може да бъде, както на публичните институции, така и на неправителствените организации. Формите са две: общ диалог и диалог за сътрудничество. Общият диалог представлява непрекъснат процес на общуване между двете страни по различни въпроси за постигане на общи цели. Той се осъществява по различни методики като публични изслушвания, отворени срещи и др.

При диалога за сътрудничество отношенията между двете страни се създават за определен период и за конкретен въпрос, например, промени в законодателството и др. Обикновено, се осъществява чрез провеждането на срещи за обсъждане на конкретния казус. В повечето случаи, диалогът за сътрудничество е по-ефективен от общия и води до конкретни измерими резултати. Това ниво на участие може да бъде прилагано на всички етапи на вземането на решения.

Партньорството е най-активната форма на участие. При него публичните организации и гражданското общество действат в сътрудничество, като неправителствените организации запазват своята безпристрастност и независимост при изразяването на гражданската позиция. Осъществява се, най-често, чрез предоставянето на услуги от страна на неправителствени организации. Партньорството е най-висша форма на участие и може да се прилага на всички етапи от процеса на вземане на решения.

Етапите на вземане на решения са определяне на дневен ред, изработване, решение, изпълнение, проследяване и преформулиране. На всеки един етап се прилагат в определена степен изброените нива на гражданско участие.

При проучванията, направени в страните от Европейския съюз и Беларус, с цел изготвяне на Кодекса на добрите практики за гражданско участие в процеса на вземане на решения, са събрани хоризонтални механизми и инструменти за гражданско участие през целия процес на вземане на решения. Те са електронно участие, изграждане на капацитет за участие, структури за сътрудничество между НПО и публичните органи и рамкови документи за сътрудничество между НПО и публичните органи.

С напредването на технологиите и сериозното развитие и разрастване на електронното пространство е съвсем естествено да се говори за електронното участие като механизъм за гражданско участие при вземането на решения.

Възможностите, които предлага електронното участие ще доведе не само до по-голяма прозрачност и отчетност в дейността на институциите, но и до по-широко и активно участие на организираното гражданско общество. За да могат максимално да се използват инструментите за електронно участие, те трябва да бъдат приети и прилагани на всички нива и от всички участници в процеса на вземане на решения.

За използване на инструментите, свързани със изграждането на структури за сътрудничество между НПО и публичните органи, в много държави се създават и действат различни посредници в отношенията между гражданското общество и публичните институции. Това могат да бъдат служители за връзка, партньорски структури или групи от организации, експертни съвети или други форми на обединение на граждански и неправителствени организации, чиято цел е да координират взаимоотношенията на двете страни за постигане на максимално добри резултати.

В някои от страните в ЕС, където се прилагат разпоредбите на Кодекса на добрите практики за гражданско участие в процеса на вземане на решения, като инструмент за подобряване на качеството на отношенията между гражданското общество и публичната власт са приети различни рамкови документи за сътрудничество между НПО и публичните органи. Те могат да бъдат формулирани като двустранни споразумения, различни програми за сътрудничество между двете страни и др. Независимо от формулировката, тяхната цел е да се подобри координацията в диалога между заинтересованите страни и да се поставят ясни рамки и норми при осъществяването на взаимоотношенията между гражданските и публичните организации.

Във Великобритания, например, съществуват перманентно действащи работни групи, съставени от граждански и неправителствени организации, до които управляващите се допитват, консултират се и осъществяват диалог при разглеждането на важни за страната въпроси. Обикновено участниците в такива работни групи са утвърдени организации с високо доверие от страна на обществото, активно работещи за опазване на човешките права. Това са организации с дългогодишен опит, национално представени и с изградена мрежа на местно и регионално равнище.

За определяне на гражданските организации, които ще участват като представители при вземането на управленски решения и формиране на публични политики, се използват обикновено три основни подхода.

При първия подход представителните организации са поименно изброени. Те се определят от съответното консултативно звено и често са изрично посочени. Този механизъм за избор на представители на гражданското общество в процеса на вземане на решения се прилага в Унгария, Полша, Чехия и Португалия.

При втория подход представителните организации на гражданското общество се определят на по-общ принцип. При него участват обикновено браншови и икономически организации, организации за защита на потребителите и др. Такъв механизъм за определяне на граждански представители се прилага в Словения, Словакия и Естония.

При третия подход представителните организации на гражданското общество се избират чрез провеждане на конкурси. Отделните организации участват на конкурентен принцип. Този механизъм се използва рядко в страните от ЕС за

определяне на участници на гражданското общество при вземането на решения. Най-често се прилага във Великобритания и Ирландия.

Постоянно изградени консултативни звена за участие на гражданското общество в процеса на формиране на националните политики и ясно определени правила за гражданската намеса са определени в Германия, Австрия, Великобритания, Швеция, Холандия, Дания и Полша. Във Великобритания, Германия и Швеция са определени срокове, в които следва да се провеждат обсъжданията със съответните консултативни звена.

Най-често прилаганите механизми за диалог и консултация с гражданското общество при взимането на важни управленски решения в страните от ЕС са: неформална консултация, писмена консултация, събиране на коментари и предложения, фокус-групи, публични срещи, срещи с бизнес-организации, консултации с експерти, анкетни проучвания, интервюта и публикуване на информация в електронната мрежа.

Механизмът на неформалната консултация се прилага, когато въпросът, чието решение подлежи на обсъждане, е от особено значение за гражданското общество в съответната държава. Процедурата по неформална консултация не е задължителна и е обикновено допълващ механизъм. Прилага се често в страните от ЕС.

Поради трудностите, които предполага механизмът писмена консултация за допитване до гражданското общество, той се прилага като допълваща процедура. Прилагането на този механизъм отнема време за техническото му провеждане и анализ на резултатите. Прилага се често в страните от ЕС, обикновено, по въпроси, свързани с политиките на съюза.

Фокус-групите допринасят за ясното формулиране и конкретно обсъждане на обществено значимите проблеми. Участието на фокус-групи в дискусии по съответна тема или проблем предполага предварителен подбор на участващите организации, които имат опит и компетентност по съответния въпрос. При провеждането на фокус-групи се изготвя изчерпателен доклад за обсъдените теми и внесените предложения от страна на участниците. Прилагането на този механизъм отнема подълго време в сравнение с други методи, поради което, все още, се прилага рядко в страните от ЕС. Неговото приложение е по-често при въпроси с по-голямо обществено значение за по-голям кръг заинтересовани лица и в случаите, когато срокът за дискусии е по-дълъг.

Механизмът за участие на структури на гражданското общество чрез публични срещи е относително често срещан в страните от ЕС. Тези срещи са обикновено открити и дават възможност за включването на голям брой заинтересовани лица. Неудобство при прилагането на този метод при обсъждането на европейски политики и вземане на решения е, че изисква влагането на голям ресурс. След провеждането на публични консултации се изготвя подробен доклад за участниците и направените предложения.

Механизмът срещи с бизнес-организации се прилага резонно в страни с добре развити синдикални организации. При този метод се провеждат срещи обикновено със синдикални или браншови организации за обсъждане на икономическата политика на съюза, въпроси свързани с пазарната регулация и др.

Сравнително често в страните от ЕС се прилага механизмът на консултации с експерти. Той се състои в допитване до експерти с голям опит, познания и компе-

тентност в областта на обсъждания въпрос, чието мнение и позиция разширяват информацията и възможностите за действие.

Сред рядко използваните механизми за допитване до гражданското общество в страните от ЕС са анкетните проучвания. Те се провеждат чрез различни средства за комуникация като телефон, електронна поща, интернет-портали и др. Положителното при прилагането на този механизъм е, че се получава мнение на широк кръг лица и че може да се направи количествена оценка за обществените нагласи по съответния проблем. Прилага се рядко, тъй като изисква изразходването на голямо количество ресурси- финансови, човешки, технически и др.

Участието на структури на гражданското общество при обсъждане на европейските политики чрез прилагане на механизма интервю е сред най-рядко използваните. Изисква се влагането на голям ресурс за определянето на конкретните граждански организации, с които да се проведе интервюто и не дава възможност за допитване до широк кръг лица.

С напредването и развитието на технологиите и глобализацията на електронното пространство е съвсем естествено то да се използва все повече при обсъждането на европейските политики и решаването на важни общоевропейски въпроси. Механизмът представлява публикуване на документи, които следва да бъдат обсъждани, както и полезни връзки към интернет страницата, на която се намира. Публикува се и важна информация относно сроковете на консултация, възможностите за участие, същност на обсъжданата тема, както и препратки към сайтовете на основните институции на ЕС. Този метод се използва изключително често, дори и в комбинация с други от изброените механизми, тъй като осигурява информация на голям кръг хора и не изисква влагането на големи ресурси за прилагането му.

Всяка държава индивидуално определя на кой етап от процеса на вземане на решения да се включи гражданското общество. В някои страни е приета практиката диалогът с гражданите да започва още в началния етап на дискусии и консултации по съответния проблем. В други държави включването на гражданското общество и обсъжданията стават на етапа, когато има подготвен работен вариант на документ, който да регламентира правилата за разрешаване на съответния въпрос. В някои страни се предпочита гражданското участие да бъде съпътстваща част на всеки един етап от процеса на вземане на решения. Независимо от практиката, която приема всяка отделна държава, безспорна е важността на участието на структури на гражданското общество при определяне на държавните политики. В страните от ЕС сроковете за провеждане на консултации с граждански организации, са различни. Обикновено продължителността на консултациите е в рамките от 1 до 12 седмици, като този период варира според реда в съответната държава, както и сложността и важността на обсъждания въпрос. Има държави, в които формите на участие и продължителността на консултациите са строго регламентирани, в други е определен само максимален срок, а в трети правилата за гражданското участие са отворени и не съществуват ограничения за времето и начините на участие на гражданското общество в процеса на вземане на управленски решения и формиране на държавните или общоевропейските политики. В страни като Австрия, Швеция, Финландия и др. има определени максимални и минимални срокове на провеждане на консултации от страна на институциите с представители на гражданското общество, но не е изключено провеждането на дискусии и извън регламентираните срокове.

ЗАКЛЮЧЕНИЕ

За последен етап от развитието на гражданското общество се смята края на XX и началото на XXI век. В резултат на редица фактори като технологичния напредък, по-голямата икономическа свобода, все по-лесно преминаващите се граници, поради съюзи и договори между държавите, се говори вече за една по-глобална концепция за гражданите и обществото. С по-голяма сила действат и се приемат актовете на международните организации, които се ратифицират от голяма част от страните по света. Наблюдава се равноправност на отделните субекти. С разширяването на ЕС проблемите на отделните граждани на всяка държава се приемат за проблеми на общността. Нараства броя на актовете и организациите, които имат за цел да опазват правата на личността. Говори се вече не за национални, а за глобални проблеми като борбата с бедността, опазването на околната среда, ограничаването на престъпността, защита на потребителите и др., които се приемат за световни и всички държави се стремят да дадат своя принос за решаването им.

Напредъкът на технологиите улеснява общуването и достъпа на всеки индивид до информация. В XXI век капиталистическото общество се превръща в информационно. Това общество е изградено от знаещи, информирани и можещи граждани, които добре познават правата си и знаят как да потърсят защита. Този технологичен напредък, разбира се, носи и негативни последици, като появата на генномодифицирани храни, замърсяването на природата, екологични катастрофи и др. В нашето съвремие националните проблеми придобиват световно измерение, те са глобални, общи и целият свят се стреми към съвместното им разрешаване. На държавата се гледа, по-скоро, като на един спомагателен елемент с предимно социални функции, основната сила е в частния сектор.

ЛИТЕРАТУРА

1. Дарендорф, Р., След 1989. Морал, революция и гражданско общество, Дружество „Гражданин”, С., 2000.

2. Кабакчиева, П., Гражданското общество срещу държавата. Българската ситуация, Лик, С., 2001.

3. Канев, Д., Гражданското общество и правата на личността, С., 1998.

4. Кийн, Дж., Гражданското общество, ЛИК, С., 2002.

5. Кийн, Дж., Гражданското общество. Стари образи, нови визии, Лик, С., 2002.

6. Кингуел, М., Добродетели, пороци и гражданско общество, Сиела, С., 2006.

7. Кирилова, Ад., Митът за гражданското общество, Ние, 2001, кн. 2.

8. Проданов, В., Гражданското общество и глобалният капитализъм, С., 2003.

9. Сартори, Д., Теория за демокрацията. Книга 1: Съвременната дискусия, С., 1992.

10. Сартори, Д., Теория за демокрацията. Книга 2: Класическите проблеми, С., 1992.

11. Селигман, А., Идеята за гражданското общество, С., 1995.

12. Стоянов, Ж., Глобализация и гражданско общество, С., 2012.

13. Giddens, A., BeyondLeftandRight. TheFutureofRadicalPolitics, Cambridge, 2006.

14. Kean, J., CivilSociety: OldImages, Cambridge, 2003.

15. Shaw, M., GlobalSocietyand International Relations, Cambridge, 1998.

ГРАЖДАНСКОТО ОБЩЕСТВО И УСЪВЪРШЕНСТВАНЕТО НА УПРАВЛЕНСКИТЕ ПРОЦЕСИ

Чавдар Л. Милков

София 1202, ул. „Будапеща“ № 38, ап. 1
milkovl@abv.bg

CIVIL SOCIETY AND IMPROVEMENT OF MANAGEMENT PROCESSES

Chavdar L. Milkov

***ABSTRACT**: Are considered public councils and their activities as a form of civil society. Account of the role of law for the development of civil society and the forms of involvement of the same in the legislative process.*

***KEY WORDS**: civil society, community councils, legislation, management*

ВЪВЕДЕНИЕ

Гражданското общество, както и изразяването на обществено мнение, са фундамент на демокрацията. Чрез изразяване на общественото мнение гражданите дават своята оценка за управлението. И тъй като, според българската Конституция, източник на властта е народът, то той би следвало да има правото, както да контролира действията на администрацията, които, понякога, са в негов ущърб, така и да участва в процеса на формиране на държавните политики и вземане на управленски решения, както на национално, така и на местно равнище. Според Ж. Стоянов, „гражданското общество не е автономно, както от държавата и политиката, така и от бизнеса и икономиката. Очакват да е корекция и на държавата, и на пазара, и на частните собственици, да си поставя колективни, обществени, а не частни цели“ [12, с. 4].

I. ОБЩЕСТВЕНИТЕ СЪВЕТИ И ДЕЙНОСТТА ИМ КАТО ФОРМА НА ГРАЖДАНСКОТО ОБЩЕСТВО

Една от най-често прилаганите форми на гражданско участие на местно ниво, както в страните от ЕС, така и в България, са т. н. обществени съвети. Те могат да бъдат създавани в съответната общност, както по предложение на гражданите, така и по предложение на местните институции. Тяхната дейност е насочена към подпомагане на местната власт за постигане на по-добри резултати при реализирането на отговорностите ѝ, както и осъществяване на граждански контрол по въпроси свързани с местното управление. Целта е възможно най-голям кръг от хора да могат да участват в управлението на местно ниво и всеки гражданин да може да изразява своята позиция.

Когато обществените съвети се създават по инициатива на кмета и последващо решение на общинския съвет, тяхното учредяване и дейност се регламентира в нормативни актове, като Закон за народната просвета, Закон за закрила и развитие на културата, Закон за насърчаване на заетостта, Закон за социално подпомагане, Закон за юридически лица с нестопанска цел и др. В Закона за местно самоуправление и местна администрация (ЗМСМА) също е регламентирано правото на общините да дават предложения за създаване на обществени съвети с различни сфери на осъществяване на тяхната дейност.

Обществени съвети могат да бъдат създавани и по гражданска инициатива, на неправителствени и обществени организации. В този случай, учредяването им се осъществява на общо събрание, на което се определя предмета на дейност на съответния обществен съвет, участниците в него и основните цели на дейността му.

Обществените съвети могат да бъдат общински, кметски, районни за градовете с районно деление и квартални.

Положителните страни на създаването на обществените съвети са, например, стимулирането на гражданска инициатива при решаване на проблеми на местно ниво, по-голяма активност на гражданите при изпълнение на техните задължения, насърчава се съвместната дейност на гражданското общество и местната власт при осъществяване на местното самоуправление. Те допринасят за повишаване на качеството на живот на гражданите чрез реализиране на различни проекти, създава се партньорство между гражданите и местните институции и сближаване на взаимовръзката и взаимоотношенията между гражданското общество и властта.

Голяма част от обществените съвети са създадени като приложение на познатите добри практики във Великобритания, Германия и други страни, където успешно се прилага тази форма на сътрудничество между гражданското общество и институциите на местно ниво.

Създаването на обществените съвети е един от най-ефикасните начини за участие на гражданите в местното управление. Това е възможност за гражданското общество, както активно да изразява своята позиция по актуални въпроси, така и да осъществява контрол върху дейността на институциите. Тази форма е в помощ и за управляващите, тъй като, обикновено, в обществените съвети вземат участие експерти от различни области, които биха могли да допринесат за по-компетентно изготвяне на решения в различни области.

На местно равнище се предоставят публични услуги, които целят удовлетворяване на основните потребности на хората, живеещи в определената териториална единица. Повечето публични услуги са безплатни или с по-ниска цена от частния сектор, но качеството на предоставянето им е от голямо значение, тъй като те са право на всеки данъкоплатец. На местно ниво, за подобряване на комуникацията между гражданите и институциите, за повишаване на качеството на предоставяните местни услуги и за изграждане на ефективна обратна връзка, се прилага метода на т. н. „Харта на клиента“. В нея са включени въпроси за вида и качеството на предлаганите публични услуги и се дава право на всеки гражданин, който ползва съответните обществени услуги, да даде своето мнение за обслужването и да направи препоръки за усъвършенстване на дейностите на местната администрация, свързани с предоставяне на публични услуги. „Хартата на клиента“, като метод на комуникация между гражданското общество и местната административна власт, се прилага в голяма част от българските общини, включително и в столична. Като

документ, хартата няма юридическа сила, но целта й е да направи гражданите и административните служители съпричастни към процеса на предлагане на публични услуги и да подобри тяхното качество и достъпност.

Освен „Хартата на клиента“, която е иновативен подход за допитване до общественото мнение, на местно ниво се прилагат и следните методи на комуникация между гражданското общество и местната власт: информиране, убеждаване, сверяване, консултиране и партньорство.

Метод за комуникация между гражданското общество и местната власт е информирането. То трябва да бъде двупосочен процес, в който, както администрацията да има задължението да дава публична информация за своята дейност, така и гражданските и неправителствени организации (НПО) да предоставят достъпна информация за тяхната работа. Що се отнася до участието на гражданите в този процес, то е, по-скоро, пасивно и е свързано с получаване на информация за изготвянето на местните политики, но е важна основа за добрите взаимоотношения на местно ниво. Аналогично, при този подход гражданските и НПО предоставят на съответните институции информация за тяхната дейност.

Ангажимент на местната власт следва да бъде разгласяването по всякакъв достъпен начин на информация, която е от значение за гражданите на съответната териториална единица. Начините за оповестяване на информация могат да бъдат различни: пресконференции, прессъобщения, чрез средствата за масова комуникация- печатни и електронни медии и др.

В много общини, по примера на Великобритания, се изготвят етични кодекси, които регламентират отношенията на служителите и гражданите и определят правила за вида и начина на споделяне и оповестяване на различна информация. Гражданите следва да се запознаят с правилата и начините за информиране на съответната местна власт и да търсят подходи за защита на своите права и интереси, в случаите на отказ или недостъпна информация, свързана с дейността на местната администрация и формирането на местните политики.

Методи за осъществяване на комуникация между гражданското общество и местната власт са убеждаването и сверяването. И при двата метода става въпрос за вече изготвен проект, местна политика или вземане на управленско решение на местно ниво, които са факт. При първия метод, местната администрация предприема кампании, след като вече са информирани гражданите, за убеждаване на НПО в правилността на взетото решение и в ползите, които то ще донесе за местното население и бизнеса. При този метод гражданите могат да отправят своите въпроси и препоръки.

При сверяването местната администрация търси обратна връзка с гражданите по вече взето решение, за да получи мнението на обществото.

При консултирането комуникацията между гражданското общество се осъществява по конкретен въпрос, за който местната власт трябва да вземе решение. При този метод е налице диалог между двете страни, при който местните органи се допитват до общественото мнение за възможните решения и алтернативи на конкретния въпрос, а гражданското общество участва активно чрез изразяване на позиция и насоки. Подходите, които се използват за сондиране на обществените нагласи са: анкетни проучвания; социологически проучвания; консултативни съвети; Интернет; кутии, в които гражданите могат да оставят писменото си мнение; публични дискусии; фокус-групи и др. При консултирането въпросът и целта са пред-

варително определени и се избира най-подходящия подход за участие на гражданското общество в обсъждането и вземането на управленско решение. Консултацията изисква повече време за провеждането й, но дава възможност за по- високо ниво на участие на гражданското общество.

Партньорството е най-високото ниво на комуникация между гражданското общество и местната власт. При него, участието на гражданите започва от етапа на определяне на важните проблеми и решения на местните органи, минава през етапите на проучване и изследване, до крайния етап на вземане на управленското решение. При този подход гражданите на практика са участници в управленския процес- при формирането на местните политики, при изготвянето на различни проекти, при изготвянето на планове и програми. По този начин, гражданите могат да упражняват законовото си право да участват в работата на местните органи и да ги контролират.

II. ГРАЖДАНСКОТО ОБЩЕСТВО И ЗАКОНОДАТЕЛСТВОТО

Към Народното събрание (НС) на Република България е създадена Комисия по културата, гражданското общество и медиите. Според вътрешния правилник за дейността й, комисията се подпомага от щатни служители или външни експерти. За определени въпроси към комисията се създават работни групи, които осъществяват своята дейност до решаването на конкретния въпрос. След изготвянето на доклад и становище работните групи се разпускат, ако няма решение за продължаване на тяхната дейност. Заседанията на комисията са открити и имат право да присъстват заинтересовани граждани или представители на юридически лица, имащи отношение към обсъжданите въпроси. На своите заседания комисията обсъжда законопроекти, годишни отчети или други нормативни актове и документи, определени от председателя на НС. След обсъждането на конкретно определените теми комисията изготвя доклад и становище. В Интернет-сайта на НС е публикувана информация за контакти и електронна поща за кореспонденция и обратна връзка, на който всеки гражданин и представители на юридически лица, граждански и неправителствени организации, могат да отправят свои питания, относно темите, които предстои да се обсъждат, както и да получават информация за конкретното провеждане на следващо заседание на комисията, на което биха могли да присъстват, ако имат интерес.

Когато се говори за гражданско участие в законодателния процес в България, се има предвид, че гражданската страна е, все още, по-активната в изискването на достъп и информация, относно различни проектни закони, решения и др. В последните години се използват, както електронното пространство, така и медиите за осигуряване на прозрачност, достъпност и информираност на гражданите, относно обсъжданите от отделните комисии на НС проектозакони. Благодарение на напредналите информационни и комуникационни технологии (ИТК) достъпът до подобни документи е значително улеснен. В някои случаи, отделни комисии на НС търсят експертно мнение по различни въпроси, или се допитват до различни НПО. Макар да се правят усилия в насока на засилване на гражданското участие в законодателните процеси, се наблюдава едно взаимоотношение парламент-граждани, при което парламентът, по-скоро, изчерпва своите задължения за взаимна работа с предоставянето на информация по различни въпроси и, все още, е необходимо гражданите да се опитват да извоюват правото си на пряко участие в законотворчеството. Необходима е една цялостна промяна в нагласата на всеки отделен граж-

данин и на гражданското общество като съвкупност, да се намери правилния подход за усъвършенстване на взаимоотношенията парламент-гражданско общество.

Като страна в законодателния процес гражданското общество има задължението да се усъвършенства, за да може да бъде компетентно и ползотворно при своето участие. Организациите, които дават становище по различни въпроси, касаещи законотворчеството, следва да предлагат експертно мнение, което адекватно да отговаря на потребностите на обществото. Добре е представителите на гражданското общество, които представляват населението, да бъдат с богат опит в съответната сфера, който да помага да се изработват нормативни актове, които да бъдат в максимална степен отговарящи на изискванията на съвременната икономическа, политическа и социална ситуация.

В случаите, когато се предоставя за обсъждане и консултация с гражданското общество вече готов текст, той се подлага на сериозна критика и обществено недоволство. Хората търсят скрити частни интереси и проявяват съмнения към проекти, които са представени като факт на тяхното внимание. Ето защо, е необходимо съответните избрани компетентни граждански организации да участват на всички етапи на законодателния процес и да защитават общата позиция, ако се предизвикат противоречия и публично недоволство.

Разбира се, да се постигне единодушие на обществото и на всички организации е невъзможно. В зависимост от важността и публичното разгласяване на съответните теми и въпроси, се навлиза в различни дискусии и конфронтации между отделни организации. Много често институциите се възползват от тази нестабилност на гражданското общество и игнорират мнението на всички страни като вземат решения без да имат предвид обосновката и аргументите на спорещите. Следва, тези спорове да се използват градивно, за да се постигне максимално добър резултат, доближаващ се до исканията на голямата част от обществото. По всеки един въпрос се организират групи, които се приемат за ощетени от взетите решения. Нито една световна система не е изградила такива методи на действие на администрацията, като цяло, които да отговарят на всеки отделен гражданин. Целта на гражданското участие в законодателния процес е да се постигнат резултати, които да удовлетворяват максимална част от гражданите, без да ощетяват и накърняват правата на останалите.

III. ФОРМИ НА СЪПРИЧАСТНОСТ НА ГРАЖДАНСКОТО ОБЩЕСТВО В ЗАКОНОДАТЕЛНИЯ ПРОЦЕС

Целта на гражданското участие в законодателния процес е да се постигне максимална прозрачност и адекватност на нормативните документи, спрямо изискванията и потребностите на гражданите. В България няма установени правила за избора на граждански представители, но обществото поема, все повече, инициативата да се възползва от правото си на участие, контрол и въздействие над властта във всичките й форми и сфери на проявление.

1. Лобизъм

Лобизмът като понятие възниква в САЩ, като начин за гражданско влияние върху политическите решения. По-късно, през средата на XIX век, широко се разпространява и прилага във Великобритания, като метод за директно въздействие над Парламента. В днешно време схващането за лобизъм е за конкретни действия, с които се влияе директно на изготвянето на законодателни актове, с цел задоволяване и обслужване на индустриални, икономически или корпоративни интереси. Лобирането може да се разглежда и като процес на взаимодействие между обществото и властта, при който се представят частните и обществени интереси пред управляващите на съответното ниво, с цел да се въздейства върху вземането на определени политически решения. В съвремието ни, в много държави по света, съществува практиката големи корпорации да наемат лобисти, които да прокарват техните интереси в законодателните институции и по този начин да влияят върху законодателния процес. В някои държави лобирането е регламентирана дейност, с цел да бъдат избегнати злоупотреби и корупция. Като цяло, понятието лобизъм е много по-разпространено в САЩ, но широко се разпространява и в Европа, особено след създаването на Европейския съюз и приемането на общоевропейско законодателство, което засяга много по-голям брой частни лица, организации и фирми. За България това понятие, все още, е относително ново, макар в последните години да се говори, все по-често, в медийното пространство за лобистка дейност на различни нива. Поради слабото познаване и не добрата информираност по въпросите, свързани с лобизма, в България, се приема като отрицателно явление и се смята за рядко прилагано. Не винаги лобизмът се прилага в негативен план и не е основателно да се приравнява с корупцията, както често се прави. В някои случаи се лобира за обществени или екологични каузи, лобисти могат да бъдат и представители на гражданското общество.

2. Групи за натиск

Групите за натиск се формират по определен въпрос, който е обикновено с голяма значимост. Най-общо, групите за натиск са доброволни сдружения на граждани, които се събират по определен повод и за защита на обществените интереси. Те са един от новите методи за участие на гражданското общество в упражняване на властта в съвременната политическа ситуация. Тяхната дейност не е придобиване на власт, а само подкрепа на гражданското общество в сфери, където има опити за неспазване на обществените интереси. Няма ограничения и изисквания за броя на участниците в групите за натиск. В теоретичните определения групите за натиск се срещат и като различни обществени организации (фондации, сдружения и др.), НПО, групи по интереси и др. Те се зараждат в началото наXX век в САЩ, а покъсно се развиват и в Европа. Особено активно се разпространяват след края на Втората Световна война. Основната им цел е да бъдат обществен защитник пред властта и да защитават човешките права.

3. Добро управление

Когато говорим за страни в процеса на осъществяване на местното управление, разглеждаме, от една страна, местната управа, включваща органите, вземащи и прилагащи управленски решения на местно ниво и различен тип организации, от друга страна. Тези организации биха могли да бъдат граждански, финансови, политически партии, бизнес-организации, медии и др.

В последните години в България, след присъединяването на страната към ЕС, нараства вниманието и интереса към понятието „добро управление“. То навлиза като едно от основните права прокламирани в Хартата за основните права на ЕС. Според член 41 на този документ, всеки европейски гражданин има право на добро управление и администрация. Това право се разглежда по-разширено в Хартата за основните права на ЕС, отколкото в приетия от Европейския парламент през 2001 година Кодекс за добро поведение на администрацията. Докато в Кодекса се има предвид административното обслужване, доброто управление, по своята същност, се приема като една по-висша, от чисто административното управление, дейност. Доброто управление се прилага така, че да бъде адекватно в непрекъснато и динамично променящите се правила и норми и да бъде надграждащ елемент в осъществяването на управленската дейност. В съвременния динамичен и богат на информация свят гражданите не могат да бъдат удовлетворени от изпълнението на минимални изисквания. Съвременните общества имат подготовката да претендират за разширяване на техните права и за ефективно управление. Прилагането на доброто управление и неговите принципи определя ясно характеристиките на управленските органи, създава конкретни правила за тяхната дейност и стимулира професионалното отношение и изпълнение на конкретните функции.

Стратегията за добро управление е изготвена и приета на Конференция на министрите на местното и регионално управление в ЕС, проведена през октомври 2007 година във Валенсия- Испания. В тази стратегия са изброени 12-те принципа на добро управление, също така, се разясняват неговият обхват, цели, както и начините за тяхното изпълнение на национално и европейско ниво.

По същество, доброто управление се осъществява в държави с установен демократичен ред и се прилага на местно ниво. Принципите, заложени в стратегията за добро управление, са следните:

- Честно провеждане, представителност и обществено участие по време на избори- да се осигуряват реални възможности за всички граждани да упражняват правото си на глас по въпроси от обществен интерес.

- Отзивчивост- да се осигурява непрекъснато във времето посрещане на потребностите и законно обоснованите очаквания на гражданите от страна на местните власти.

- Ефикасност и ефективност- да се гарантира постигане на целите чрез оптимално използване на наличните ресурси.

- Откритост и прозрачност - да се осигурява обществен достъп до информация и да се улеснява разбирането за това, как се решават обществено значимите въпроси.

- Върховенство на закона- да се гарантира честност, безпристрастност и предсказуемост.

- Етично поведение- да се гарантира, че общественият интерес е поставен над личните интереси.

- Компетентност и капацитет- да се гарантира, че местните представители на населението, както и назначаемите служители, са в състояние да изпълняват своите задължения.

- Иновации и отвореност за промени- да се гарантира, че се извлича практическа полза от въвеждането на нови решения и добри практики.

- Устойчивост и дългосрочна ориентация- да се вземат под внимание интересите на бъдещите поколения.

- Стабилно финансово управление- да се гарантира целенасочено и продуктивно използване на обществените фондове.

- Човешки права, културно разнообразие и социално единство- да се гарантира, че са защитени всички граждани и е зачетено човешкото им достойнство, както и това, че никой от тях не е дискриминиран или изключен от обществения живот.

- Отчетност- да се гарантира, че избираемите представители на властта и назначаемите общински служители поемат и носят отговорност за своите действия.

Приетата стратегия от Валенсия набляга на няколко основни цели, които да бъдат постигнати чрез прилагане на 12-те принципа на добро управление. Част от тях са, гражданите да бъдат основен фактор при вземането на управленските решения и да бъде максимално разширено тяхното право на участие в управлението, както и непрекъснатото и всеобхватно усъвършенстване на местната администрация, съобразно принципите на добро управление и другите актове и документи на ЕС, в областта на административното обслужване и държавното управление.

Разработена е методика за оценка на доброто управление в общините, с която да се получи количествено измерение на ползите от прилагането на принципите за добро управление. Методиката за оценка се осъществява по пет критерия, които са съставени на базата на основните сфери на дейността на местната администрация. Информацията, използвана за изготвяне на оценката, е от дневен ред на заседания на общинските съвети, протоколи от тези заседания, правилници за дейността на общинските съвети и общинската администрация, годишни програми и стратегии, заповеди на кметове на общини и др.

Методиката включва изготвяне на въпросници и начисляване на различен брой точки, в зависимост от отговорите. Броят на събраните точки показва степента на прилагане на принципите на добро управление на местно ниво в съответната община. Въпросниците и начисляването на точки се прилага за всеки един от 12-те принципа по отделно, за да се установи степента на прилагане на конкретния принцип. След като бъде изчислена оценката за всеки отделен принцип се формира една обща оценка. Когато бъде получена стойността на общата оценка, съобразно резултата, общините се разделят в три групи: първата група включва общините с най-висока оценка, които прилагат много добре принципите за добро управление; втората група е на общините със задоволително прилагане на принципите на добро управление; третата група са тези с най-нисък резултат, получили най-малък брой точки, с незадоволително прилагане на принципите на добро управление. Методиката се осъществява в няколко стъпки. Първата стъпка е да бъде съставена оценяваща комисия, чийто състав е максимално 10 души и има по един представител на общинската администрация, общинския съвет, гражданския сектор, бизнеса, медиите и, когато е възможно, местен обществен защитник- омбудсман. Следващата стъпка е да бъде избран координатор на съответната оценяваща комисия. Третата стъпка е да започне събирането на информация, относно прилагането на принципите на добро управление в съответната община. Следващата стъпка е обработването на събраната информация. В последните две стъпки се изготвят описателен анализ и окончателен документ, в който се посочва общата оценка и съответно степента на прилагане на принципите на добро управление в съответната община.

IV. ДОКЛАД „ЕТ 2020“

В края на 2011 година в Брюксел е изготвен съвместен доклад на Европейската комисия и Съвета на Европа- „Образование и обучение 2020“ („ЕТ 2020“), който се отнася за изготвянето на стратегия за сътрудничество на европейските институции в сферата на образованието и обучението.

В последното десетилетие ЕС се намира в една изключително дълбока финансова и икономическа криза. Като опит за справяне с тази ситуация през 2010 година беше изготвена стратегическа програма „ЕВРОПА 2020“- „Стратегия за интелигентен, устойчив и приобщаващ растеж“. Пет са основните цели, които са заложени в стратегията, които всяка страна трябва да поставя като свой национален приоритет. Това са областите на образованието, научните изследвания и иновациите, трудовата заетост, борбата срещу бедността и енергетика и климатични изменения.

В стратегията е разгледана актуалната обстановка в рамките на ЕС и са поставени основните задачи, които да бъдат изпълнени, за да бъде преодоляна кризата и да се вземат възможните мерки за предотвратяване на бъдещи негативни процеси.

Сферата на образованието е една от ключовите цели заложени в Стратегия „Европа 2020“. В нея се набляга по-конкретно на мерките, които всяка държава, членуваща в ЕС, да предприеме в областта на образованието и насоките за провеждането на държавна реформа. Една от задачите поставени в стратегическия документ е осъществяването на превенция на ранното напускане на училище и завършването на висше образование.

В стратегията се подчертава, че държавните реформи в областта на образованието и обучението трябва да бъдат насочени към постигането на адекватност на образованието, спрямо пазара на труда. Прилаганите образователни програми следва да бъдат съобразени с потребностите на трудовия пазар от специалисти, за да се постига максимално добър резултат за реализация на получаващите съответна образователна степен. Съвместният доклад „ЕТ 2020“ е разработен въз основа на направени проучвания, относно постигнатия растеж до 2012 година. Изготвен е с цел да установи настоящата ситуация и да се приложи в подкрепа на Стратегия „Европа 2020“.

Публичните средства за образование и обучение са контролирани бюджетни средства и в голямата част от страните в ЕС е трудно постижимо дори поддържането на тяхното равнище, а в голяма част от държавите увеличаването на тези средства и предвиждането на нови инвестиции е невъзможно. Според стратегията, образованието следва да бъде основен приоритет, тъй като влагането на финансови ресурси за квалифициране на обществото ще доведе до намаляване на безработицата при реализирането на тази работна ръка, до стимулиране на икономиката и до други положителни процеси. Проучванията сочат, че много от държавите, членуващи в ЕС, вследствие на задълбочаващата се криза, са намалили драстично бюджетното перо за образование. Това, според изготвения доклад, може да доведе до сериозни негативни последици, поради произтичащите проблеми, като спадането на качеството на образованието, намаляващия интерес към по-висока квалификация и др.

Второто направление, на което се отделя внимание в доклада, се отнася за преждевременното напускане на училище. Вследствие на тежката икономическа и финансова ситуация, както в световен, така и в европейски мащаб, се наблюдава сериозен ръст на безработицата. Това води до обезверяване на гражданите в детска

и юношеска възраст за добра реализация и до увеличаване на броя на отказващите се от образователни услуги преди получаване на основно или средно образование. Проучванията показват, че в ЕС броят на лицата между 15 и 24 годишна възраст, които прекратяват образованието си и нямат трудова реализация, нараства драстично през последните години. Повече от половината от преждевременно напускащите училище остават без работа. В тази връзка, препоръките на доклада към Стратегия „Европа 2020“ и нейното изпълнение са да бъдат взети максимални мерки за предотвратяване и контрол на ранния отказ от образование.

През 2011 година от страна на Съвета на Европа, вследствие на направените проучвания, са дадени сериозни препоръки за по-сериозен контрол, проследяване и мерки за предотвратяване на преждевременното напускане на училище, към страните Австрия, Дания, Испания, Малта, Великобритания. В някои от тези страни са взети своевременни мерки и е постигнат напредък в борбата с ранния отказ от образование.

Образованието и обучението са сред основните направления включени в Стратегия „Европа 2020“. Тъй като основна задача при изпълнението на документа е постигането на интелигентен, устойчив и приобщаващ растеж, се смята, че това може да бъде постигнато чрез квалифицирането и придобиването на знания и умения на хора, които да бъдат използвани като компетентна и подготвена работна ръка. Една от целите, която е заложена в стратегията, е броят на придобиващите висше образование в ЕС във възрастовата група 30-35 годишна възраст да бъде увеличен до 40%. При проучване, направено през 2010 година, делът на висшистите в тази възрастова група е около 33,6%. За да бъде постигната тази цел, страните в ЕС трябва да продължават със своите усилия и реформи. Препоръки в тази сфера за модернизиране на системата за висше образование са направени от Европейската комисия към България, Чехия, Полша, Словакия, Малта.

Освен в направленията за подобряване на финансирането и управлението, следва да бъдат направени задълбочени реформи и за включване на различни групи с недостатъчно участие като малцинства, хора в неравностойно положение, лица с увреждания и др. Следва да бъде подобрена, както инфраструктурната база за улесняване на достъп, така и правилата за прием и обучение на различни групи в неравностойно положение. Друг проблем, върху който трябва активно да се работи, е отпадането от висше образование. Броят на лицата, които отпадат или се отказват преждевременно от висше образование е голям и би следвало те да бъдат стимулирани чрез професионално ориентиране, предварителни консултации за избор на професионално направление и др.

Стратегията за учене през целия живот се прилага в много малко страни в ЕС. В Стратегия „Европа 2020“ е заложена цел, хората на възраст между 25 и 64 годишна възраст, които са включени в програми за учене през целия живот, да достигне 15 %. Според данните за 2010 година, този дял е 9,1 %. Идеята за учене през целия живот е да обхваща периода от ранна детска и предучилищна до следтрудоспособна възраст. Това направление е особено важно, тъй като се налага схващането, че за да се постигне растеж в икономиката, всяка страна трябва да разчита на добре образовано и непрекъснато надграждащо и усъвършенстващо се общество. Познанията на хората трябва да бъдат актуални и да се приспособяват към постоянно променящата се среда. Прилагането на стратегията за учене през целия живот следва да бъде резултат от една цялостна и всеобхватна образователна ре-

форма, която да повишава качеството на образователните услуги на всички равнища. Държавите, в които има разработена и действаща цялостна стратегия в областта на образованието и обучението, са: Австрия, Кипър, Дания, Словения, Великобритания.

През 2008 година Европейският парламент и Съветът на Европа приемат Европейска квалификационна рамка за учене през целия живот. Тя се оформя като документ, свързващ системите за квалификация на отделните страни в ЕС. Нейните основни цели са да се осигурява на гражданите начин и достъп за получаване на учене през целия живот и насърчаване на гражданската мобилност в отделните страни.

Разработени са и две кредитни системи- Европейска система за трансфер на кредити (ECTS) и Европейска кредитна система за професионално образование и обучение (ECVET). Тяхната основна цел е да се насърчава ученето през целия живот, като се създава по-голяма мобилност в ЕС, единна оценъчна система и приемане на квалификационните оценки във всяка държава, членуваща в съюза.

Следващото направление, на което се обръща внимание в доклада „ЕТ 2020“, е мобилността с учебна цел. Мобилността осигурява получаването на по-големи компетенции, знания, опит и дава възможност за по-добра реализация. Обмяната на кадри и образователен опит между различните страни прави ЕС, като цяло, високо конкурентен в световен мащаб. Към 2012 година данните за мобилност с учебна цел сочат, че не е голям броят на учащите, които се включват в различни програми и използват възможността да прекарват част от обучителния си период в чужбина. Този дял е само 3 %. Трябва да бъде популяризирана тази възможност и да бъдат подробно изяснявани позитивите на всеки започващ образованието си. Основните пречки за увеличаване на мобилността са: недостатъчно средства, невладеене на чужди езици, недостатъчна информираност, относно ползите и предимствата и др.

Последното направление, на което е спряно вниманието в доклада, е свързано с новите умения и работни места. Дълбоката криза в световен мащаб променя ситуацията в почти всички страни в ЕС. В последните години държавите търсят изход и стигат до извода, че бърз напредък може да се постигне като се използват максимално човешките ресурси. Ето защо, в последните години намалява търсенето на евтина и некомпетентна работна ръка и все повече се търсят добре образовани и висококвалифицирани работници. Европейската комисия отправя препоръки към страните: България, Кипър, Чехия, Естония, Полша, Словения, Словакия, Великобритания, за подобряване уменията на трудовия пазар.

Пазара на труда се свива и се търсят възможности за по-добра координация между образованието и необходимостта от работна ръка. Проучванията и прогнозите сочат, че бъдещето ще има потребност от висококвалифицирани кадри и по тази причина усилията и реформите следва да бъдат съсредоточвани в тази насока.

Като приоритет в областта на образованието и обучението в Стратегия „Европа 2020“ се поставят стимулирането на ученето през целия живот и мобилността с учебна цел. Това се осъществява чрез прилагането на различни програми на европейско ниво. На следващо място, като основен приоритет, е да бъде подобрено качеството на предлаганото образование и обучение. За целта, следва да бъдат установени критерии за основните умения, да се създаде среда и условия за постоянно усъвършенстване на учителите и преподавателите, да се работи активно за

увеличаване на броя на хората с висше образование, да се провеждат кампании за разясняване и привличане към професионално образование и обучение, както и да се изгради адекватна система за финансиране и оценяване в сферата на образованието. Друг приоритет е създаването на равни условия и възможности, както и прилагането на превантивни мерки за намаляване на броя на ранно напускащите училище и позволяването на по-голяма гражданска инициатива. На последно място, като приоритет в стратегията, се поставя възможността за изява, инициатива и креативност. За тази цел, в процеса на образование и обучение в различни форми е желателно да се осъществява партньорство с бизнес-сектора, с гражданското общество, в различни сфери на научноизследователската дейност и др.

ЗАКЛЮЧЕНИЕ

За разлика от организациите, гражданските движения са обвързани с някаква кауза, със съвкупност от дейности, а не с интереси на своите участници, които са недоволни от нещо. Тяхната сила е в преките действия, в различни форми на гражданска съпротива, а не в представителството, типично за партиите и Парламента. Повечето социални движения не се стремят към държавната власт, а към определена автономия от държавата. „Падането на доверието към партиите повишава интереса към гражданските движения, но те не конституират политическата система, освен ако не се трансформират в партии. По начало гаранция за успеха на партиите е тяхната обвързаност с граждански движения и организации. Относително стабилното функциониране на обществото предполага определена степен на деполитизация на важни сектори от гражданското общество и готовност на организациите, не само да се противопоставят, но и да са в диалог с държавата“ [12, с. 4].

ЛИТЕРАТУРА

1. Дарендорф, Р., След 1989. Морал, революция и гражданско общество, Дружество „Гражданин”, С., 2000.

2. Кабакчиева, П., Гражданското общество срещу държавата. Българската ситуация, Лик, С., 2001.

3. Канев, Д., Гражданското общество и правата на личността, С., 1998.

4. Кийн, Дж., Гражданското общество, ЛИК, С., 2002.

5. Кийн, Дж., Гражданското общество. Стари образи, нови визии, Лик, С., 2002.

6. Кингуел, М., Добродетели, пороци и гражданско общество, Сиела, С., 2006.

7. Кирилова, Ад., Митът за гражданското общество, Ние, 2001, кн. 2.

8. Проданов, В., Гражданското общество и глобалният капитализъм, С., 2003.

9. Сартори, Д., Теория за демокрацията. Книга 1: Съвременната дискусия, С.,1992.

10. Сартори, Д., Теория за демокрацията. Книга 2: Класическите проблеми, С.,1992.

11. Селигман, А., Идеята за гражданското общество, С., 1995.

12. Стоянов, Ж., Глобализация и гражданско общество, С., 2012.

13. Giddens, A., BeyondLeftandRight. TheFutureofRadicalPolitics, Cambridge, 2006.

14. Kean, J., CivilSociety: OldImages, Cambridge, 2003.

15. Shaw, M., GlobalSocietyand International Relations, Cambridge, 1998.

СОЦИАЛИЗАЦИЯТА НА ИНДИВИДА В СЪВРЕМЕННОТО ОБЩЕСТВО

Чавдар Л. Милков

София-1202, ул. „Будапеща“ № 38, ап. 1
milkovl@abv.bg

THE SOCIALIZATOON OF INDIVIDUALS IN MODRTN SOCIETY

Chavdar L. Milkov

ABSTRACT: *Socialization is the process by which the human individual with their biological conditions, gradually acquires social experience enters into social relations and becomes a personality that can be realized in different spheres of public life and labor practices. Socialization is dvuedinen, dialectical process, which includes both absorption and create social experiences and values that develop and improve socio-biological nature of man. In her mind all interactions in the system "individual-society", including focused, organized and systematically carried interactions.*

KEY WORDS*: socialization; individual; personality; process; education; family; development.*

ВЪВЕДЕНИЕ

В съвременната културална антропология социализацията се разглежда като процес на адаптация и интеграция на индивида към определена култура, чрез усвояване на нормите, ценностите, моделите на поведение, обичаите и т.н., които обуславят тази култура (4).

„Социализацията“ е едно от ключовите понятия в съвременното социално познание. За пръв път терминът „социализация“ е използван от щатския учен Fr. Gidinsпрез 1897 година в труда му „Theoryofsocialization“, за обозначаване на социалната природа и характера на човека.

„Посредством човешката социализация, заключава П. Т. дьо Шарден, чието присъщо действие е да съсредоточава в самия него целия сноп от рефлексивните обвивки и влакна на Земята, човек намира своето продължение в самата ос на космичното завихряне на интериоризацията, и това е третият ми избор - най-решаващият от всички досега, който окончателно определя и осветлява научната ми позиция по отношение на човешкия феномен” (9, с. 245).

Дж. Дюи, П. Наторп и Е. Дюркем приемат възпитанието, преди всичко, като директно, еднопосочно въздействие. Така например, П. Наторп счита, че възпитанието не зависи толкова от психиката на детето, а, преди всичко, от условията на живот. Дж. Дюи е убеден в пряката зависимост на социализацията от характера на обществото.

Според З. Фройд, социализацията, по своята същност, е един антихуманен акт. Обществото може да обуздае човешките пориви, да ги потиска и да ги превръща в хуманна база на културата. Това влияние на социума върху природния характер на човека, т. е., върху естествените му нагони, З. Фройд нарича сублимация.

Според Е. Дюркем, „социализацията е процес на превръщането на биологичното същество в човек по пътя на интериоризирането от индивида на социалния опит,

културата, нормите и ценностите на обществото. Същевременно социализацията е процес на адаптация на човека към социалната среда“ (по 1, с. 129)

Дж. д’Аркас смята, че социализацията идва като резултат от общуването, подпомагащо формирането на уникални личности, без да се стига до индивидуализъм.

За Е. Фром, характерът на човека е оформен от изискванията на света, създадени от собствените му ръце. Характерът на членовете на всяко общество се оформя от нормите, чрез които то функционира.

Социализацията е процес, при който човешкият индивид със своите биологични предпоставки, постепенно овладява социален опит, навлиза в социални отношения и се превръща в личност, която може да се реализира в различните сфери на обществения живот и трудовата практика. Социализацията е двуединен, диалектически процес, който включва, както усвояване, така и създаване на социален опит и ценности, при който се развива и усъвършенства социално-биологичната природа на човека. При нея се имат предвид всички взаимодействия в системата „индивид-общество“, в това число целенасочените, организирани и планомерно осъществявани взаимодействия.

В този контекст се поставя ударението върху формирането на цялостната личност. Научаването на четенето за учителя е неразделна част от процеса на ученето, как да се живее в нашето многослойно общество. Учебната активност най-добре се развива в училище (започва в детската градина като първи етап в образователната ни система, продължава в начална училищна степен). Моментът на постъпване на детето в социална институция, каквато е училището, е преломен в живота му, защото тогава се отключва възможността за пряко влияние на множество фактори, въздействащи върху цялостната му социализация.

Очевидно е, че социализацията е изключително сложен феномен, чиято същност трудно може да се отрази от обобщените и кратки определения, но безспорно тя е най-съществения компонент на връзката „общество-личност”.

Като изходна позиция приемаме постановката на Е. Илиенков. „Процесът на възникването на личността се проявява като процес на преобразуване на биологично определения материал чрез силите на социалната действителност, съществуваща преди, извън и напълно независимо от този материал.

Понякога този процес бива наричан „социализация на личността”. Според нас, това название е несполучливо, тъй като предполага, че личността е съществувала и преди нейната „социализация”. В действителност, „социализира” се не личността, а естествено-природното тяло на новороденото, което тепърва предстои да се превърне в личност в процеса на тази „социализация”, т. е., личността тепърва трябва да възникне. Актът на нейното раждане не съвпада нито по време, нито по същество с акта на раждането на човешкото тяло, с деня на физическата поява на човека на този свят” (5, с. 223).

В съвременната щатска психология широко застъпено е виждането за социализацията като long-lifeprocess, т. е., процес, който не спира в нито един момент от живота на човек, до дълбока старост. В подкрепа на горното, могат да се приведат множество доказателства. Едно от тях е фактът, че в съвременния динамичен свят на хората често им се налага да се адаптират към бързо променящите се условия на средата и да се ресоциализират, а адаптацията и ресоциализацията са части от поглобалния процес на социализацията.

Способността на човека да се включва успешно в сложния жизнен цикъл, без продължителна специализирана подготовка, е твърде голяма, но съвременното социално поведение, социалните отношения образуват такъв лабиринт, из който детската личност не може да се придвижва адекватно, без продължително формиране на поведенчески образци и усвояване на конвенционални значения с помощта на други хора. Ролята на „значимите други" в процеса на социализацията е особено показателна, в случаите, когато, по силата на някакви причини, отделни деца се окажат „емоционално изолирани" през първите години на живота си.

I. АСПЕКТИ И ФАКТОРИ ЗА СОЦИАЛИЗАЦИЯТА

Управлението, обяснението и прогнозирането на социализацията на децата не са възможни без разкриването на механизма и динамиката ѝ през различните възрастови периоди и при различни социални условия.

1. Аспекти на социализацията

В тази връзка, педагогическата социология, като наука, извежда следните значими аспекти на социализацията:

- На първо място е развитието на самосъзнанието на децата. Индивидуалността, според И. Кон, „се създава само в процеса на общуването на индивида с другите хора, чрез усвояването на определена система от социални роли и културни ценности" (6, с. 16). Развитието на самосъзнанието на децата чрез социализацията отразява не само съвременната социална структура, но и динамиката в промените и тенденциите в нейното развитие. В процеса на социализацията си човек се реализира като субект на обществените отношения.

- Друг важен аспект на социализацията е ролевото развитие на децата. Например, ученикът има статут на ученик, в семейството е син или дъщеря, а сред връстниците си приема различни роли, в зависимост от значимите и незначими направления на съвместните дейности.

- Третият аспект е познавателният. Овладявайки възможностите за пълноценно включване в системата на първоначалния минимум обществени отношения, детето неизбежно опознава тези обществени отношения и развива способността си да разсъждава абстрактно за тях.

- Следващият аспект е мотивационният. Процесът на социализация винаги поражда и се съпътства от определени мотиви, от определена мотивационна сфера. Колкото по-многостранен и интензивен е процесът на социализацията, толкова по-богата е мотивацията, която се поражда. Тя, от своя страна, води до необходимо включване в повече социализиращи системи и цялостното формиране на личността протича по-ускорено и по-пълноценно.

- Последният аспект е свързан с ценностната ориентация на децата. Още в определенията на различните автори за същността на социализацията се подчертава, че в процеса на обществеността приспособяване се усвояват социални и културни ценности. Те варират силно, в зависимост от конкретно-историческите условия и, поради това, ценностните ориентации, формирани чрез процеса на социализация, отразяват особеностите на обществените структури и отношения, богатството на културата на дадено общество.

2. Фактори за социализацията на индивида

Факторите за социализацията могат да бъдат разделени на външни и вътрешни, но и двата вида произхождат от обществото. Външните фактори, като цяло, са под формата на награди и наказания, или липсата им. Те действат на принципа на под-

креплението и предполагат наличието на мотивация и ценности у личността. Вътрешните източници на социален контрол по правило са интернализирани външни източници. След като у човек се формира стабилен набор от ценности, нагласи и мотиви, той е склонен в своето социално поведение да се ръководи от тях, независимо от моделите и подкрепленията, които му се представят, а понякога дори и въпреки тях.

Водещи руски и западни автори отнасят към механизмите на социализацията подражанието, заразяването, убеждението, внушението, уподобяването, идентификацията, адаптацията, ръководството, примера, модата, лидерството, заимстването, ученето. Многообразието на посочените механизми не е проучено задоволително. Те са много повече от изброените тук, но това са едни от най-ясно изразените и „мощни“ прояви, установени от социалните учени.

Я. Глински диференцира няколко стадия на социализация, първият от които е този на ранната социализация. Обхваща периода на ранното и предучилищно детство.

Тогава човешкият индивид придобива първите необходими знания и опит. На този етап се формират основните свойства и качества на личността.

Опитите да се обособят общи стадии на социализацията среща големи трудности, главно, поради обстоятелството, че социалното съзряване на личността е твърде разнородно и неравномерно. Някои изследователи разграничават три, други- четири стадия. Всички автори, обаче, подчертават решаващото значение на ранната социализация. В специализираната литература тя се нарича „първична”.

Следващият стадий се назовава обобщено „вторична” социализация. Това разграничение на „първична” и „вторична” социализация не се споделя от всички автори, тъй като „вторичната” е, всъщност, продължение на един и същи процес, но на други качествени равнища.

Много автори смятат, че социализацията не е характерна само за детството. През юношеството, младостта и зрялата възраст човек продължава да се приобщава към нови групи, да усвоява нови роли, да придобива нов статус, да функционира в нови социални общности с различно предназначение. Смята се, че между социализацията в детството и тази в зряла възраст има значителни различия. Въпреки това, между тях съществува тясна връзка. Ако между приобщаването в детството и това в зряла възраст се появи продължително прекъсване, последното дава отражение върху целия последващ живот на човека.

Ранната социализация на децата осигурява елементарна подготовка, а това, което човек трябва да усвои, за да задоволи потребностите на зрялата възраст, най-често, се придобива в самите нови ситуации, в които попада. Ето защо, определени изследователи наричат социализацията през детството и, особено, през юношеството, антиципационна.

Всяко следващо поколение идва със своите особености и заема подобаващото му място в обществената структура. Позицията на зрялата възраст в тази структура неизбежно си взаимодейства с тази на новото поколение. Процесът на въздействието е взаимен. Тези взаимоотношения изменят непрекъснато източниците на очакванията и разкриват нови перспективи пред личността.

Показаното разнообразие на идеи за социализацията дава основания и за частично анализиране на процеса, чрез конкретни технологични стъпки, при търсене на промяна и устойчивост на резултатите в процеса. В този контекст, социализаци-

ята би могла да се разглежда като процес на „мотивирано изразяване и самоутвърждаване на личността в условията на живот, чрез самоизява и творчество” (2, с. 20).

II. СЕМЕЙСТВОТО КАТО ВОДЕЩ ФАКТОР В ПРОЦЕСА НА СОЦИАЛИЗАЦИЯ НА ДЕЦАТА

Ролята на семейството за социализацията и възпитанието на детето, разглеждана в исторически план, не е постоянна. Тя зависи от мястото, което обществото отрежда на семейството сред своите структури, от значимостта, която му предава. Като се започне с първобитното общество и се стигне до началото на XIX век, отношението към детето е амбивалентно. От една страна, детето се схваща като собственост, с която родителите могат да разполагат, както намерят за добре, от друга страна се смята за чест да имаш деца. Родителите се стремят, не толкова да дисциплинират детето, колкото да помагат за неговото индивидуално развитие.

Очевидно е, че за да се стигне до днешната представа за родител и деца, обществото е изминало дълъг и противоречив път.

Максимално обобщени, основните положения за мястото и ролята на родителите за формиране на личността могат да бъдат сведени до следното:

- Родителите са първото социално обкръжение на личността. Тяхната роля е толкова голяма и толкова специфична, че не може да се изпълнява от никоя друга социална институция.

- Родителите полагат основите на личността, а те в голяма степен определят нейния по-нататъшен облик.

- През родителите се пречупва влиянието на другите социални фактори, като училище, общество, масмедии, култура, демографски и миграционни процеси, спорт, връстници.

- Родителите изграждат първата представа за бъдещето собствено семейство.

Родителите едновременно са социален институт и малка социална група. Като институт, те се управляват от нормите, законите, санкциите на обществото и задоволяват социални потребности. Като малка социална група, те носят нейните основни белези, но имат, едновременно, формален и неформален характер. Формален, доколкото в него „не може да се влиза и излиза”, като в приятелските кръгове, а неформален, защото създадените норми и ценности, независимо дали съвпадат с общоприетите, са специфични за всяко семейство. Колкото „по-отворено” е семейството към обществото, толкова повече нормите и ценностите на обществото ще бъдат норми и ценности на семейството.

Единствено в семейството съществува проявление на родителска любов, тези проявления са специфични за всяко семейство и в тези отношения детето играе различни роли: социални, психологически и полови. Тяхното овладяване зависи, както от представата на родителите за самата роля, така и от начините за реализиране на тази проява. Ако, обаче, представите на родителите за ролите на детето са детерминирани изцяло от социокултурни и етнокултурни стереотипи и не държат сметка за индивидуалните особености и потребности на детето, семейното възпитание ще повтаря традициите и шаблоните в тяхното съдържание и механизми.

Родителските отношения дават основание за типологизиране на семействата (например, хармонично, вулканично, семейство-санаториум, семейство-театър, семейство с кумир, като във всяко от тях се обуславят принципите, методите, фор-

мите и средствата, чрез които родителите осъществяват възпитателната си позиция).

Отношенията между родителите в семейството определят начина, по който детето възприема света. Той може да бъде психологически адекватен и оптимистичен (присъщ е на деца с благополучни семейни отношения, родителите се отнасят към тях с любов и строгост), неоснователно оптимистичен (родителите са превърнали децата си в център на семейния живот и са ги изолирали от различните трудности) и адекватно-песимистичен (при децата от неблагополучни семейства, при които семейните отношения се превръщат в доминираща тема или настроение за детето). Семейството отрежда на новороденото собственото място в обществото и това в значителна степен предопределя кръговете на общуването му впоследствие, възможностите му да усвоява социален опит с една или друга стойност. Това, само по себе си, играе важна роля в по-нататъшната активност и социална ориентация на детето.

Родителското възпитание е тясно преплетено със социализацията и трудно може да се отличи от нея.

На първо място, това може да се обясни с особеностите на семейството като първична социална система. В семейството тези, които социализират децата и тези, които ги възпитават, са едни и същи, това са родителите.

На второ място, това е следствие от статуса на възпитанието на системата на семейните ценности.

Ако възпитанието на децата е значимо за родителите, но те смятат, че то е задължение на училището и учителите, а в семейството го свеждат до поддържането и до личния си пример, на преден план ще изпъкне социализацията.

Ако семейството е ориентирано към „социално лекомислие" и възпитанието не е сред семейните ценности, то влиянието му върху децата ще бъде стихийно-социализиращо.

За социализиращо влечение на родителите може да се говори и в семейства с много нисък материален, образователен и професионален статус. В тях, обикновено, има много деца, които по подражание усвояват модела на социално поведение на своите родители.

Най-важната функция на родителите в семейството е възпитателната, от това как тя ще се реализира са заинтересовани обществото и личността. Обществото, защото му е необходим определен тип личност, която се съобразява с нормите и ценностите в него и съдейства за неговото развитие, а личността, защото, не само социалната й реализация, но и личният й живот, до голяма степен, зависят от социо-емоционалния модел, който е усвоила в семейството.

Демографската структура на семейството е свързана с доминиращия тип семейство, в което вертикалните вътрешно-семейни контакти са стеснени до две поколения- родители и деца. От педагогическа гледна точка, това има противоречиво значение. От една страна, върху децата оказват въздействие само родителите и по този начин възможността за конфликти значително се ограничава, от друга страна, възпитателната позиция на родителите става трудно поддаваща се на изменения. Убедени в своята правота, те рядко се обръщат към училището, дори когато неговата помощ е очевидно необходима, всичко това прави взаимодействието между тях трудно осъществимо и недостатъчно ефективно.

Броят на децата в семейството също има значение. Днес тенденцията е към семейства с едно или две деца, общото за тях е че разполагат с по-големи възможности, било то материални или духовни, за задоволяване потребностите и интересите на децата, за по-често и разнообразно общуване между тях, за по-високо равнище на интелектуалното им развитие. Възпитанието на единственото дете има своя специфика и свои трудности. По-вероятна е, например, неразумна родителска любов, което води до израстването му като егоист и егоцентрик, контактите с училището, обикновено, са епизодични и понеже децата не създават грижи с успеха и дисциплината, най-важните проблеми са нравствените и се подценяват.

При семейства с две деца един от проблемите е взаимодействието между самите деца. Взаимодействието с училището се пречупва през ролята, която родителите определят на съответното дете в семейните отношения и поведението им към него. Ако статусът на детето е различен от този в семейството, взаимодействието между училището и семейството сериозно се затруднява.

Тясно свързани с броя на децата са „полюсите в раждаемостта"- от една страна, семейства с много деца, а от друга, твърде много семейства с едно дете. При това положение, възпроизводството на значителна част от децата става на възможно най-ниско социално равнище, защото високата раждаемост се осъществява в социални среди с ниско материално, културно, квалификационно и образователно равнище. Стига се дотам, че някои родители трябва да бъдат убеждавани в необходимостта децата им да ходят на училище и да учат. Сериозни промени има и в структурата на раждаемостта. М. Михайлов посочва, че „по експертна оценка т.нар. социализирани слоеве в България са около 75% срещу 25% маргинални (които не спазват обществения морал и закони). В структурата на раждаемостта тази пропорция е приблизително обърната - около 30% от ражданите деца са от социализираните слоеве, а 70% са от маргиналните. Това е изключителна деформация на структурата на раждаемостта" (7, с. 16).

Все по-актуална днес става т.нар. непълна семейна структура или непълни семейства - семейства само с един родител. Тази алтернатива става по-широко разпространена и е алтернатива на традиционното семейство. В тези семейства, много често, емоционалният свят на детето е деформиран, ценностите са променени, а когато родител е майката, децата са силно конфликтни. Децата от тези семейства обикновено се учат по-лошо от останалите, имат лошо поведение в училище, груби са в общуването си и попадат в лоши среди.

Важно място заема образованието на родителите, то е свързано с успеха на учениците. Колкото по-добро е то, толкова по-висок е успехът на децата. Тази зависимост се запазва и в по-горните класове, когато децата вече имат привички за самостоятелна работа и не им е необходима непосредствената помощ на родителите. Понякога, по-високо образованите родители общуват с децата си по-неохотно, отколкото хората с по-ниско образование, т. е., тези които могат да осигурят на децата си по-разнообразно общуване не го желаят, особено, а тези, които го желаят (хората с по-ниско образование) не могат да го осигурят. От принципно важно значение е културното равнище на поколенията в семейството, съответствието или разминаването между тях.

Оформят се две култури - едната на децата, а другата на родителите. Всяка от тях е със свои знания за света, свое отношение, специфична ценностна информация. В културен аспект важна е и насочеността на родителите - тя може да бъде

трудова, потребителска и творческа. Трудовата е свързана с отношението към труда като средство за съществуване, като удовлетвореност от него; потребителската - с мястото на материалното и духовното в йерархията на семейните ценности; творческата- с разгръщането на личностния потенциал.

За семейното възпитание, често пъти, най-важна се оказва насочеността на майката, а това произтича от мястото и ролята й в това възпитание. Изследванията показват доминиращата потребителска насоченост на майката, особено в семействата с традиционен тип отношения.

Много често се случва родителите да не са осведомени за живота на своите деца и само в драматични ситуации, например, изключване от училище или противоправна постъпка, са способни да активизират вътрешно семейното общуване. Това е тактиката на „мирно съвместно съществуване", от позиции на ненамеса и емоционална изолация. Има и семейства, които поддържат прекалено тесни отношения между деца и родители, най-често, на децата с майката, това е т. н. „тактика на опеката".

Семейството, като елемент от микросоциалната среда, е един от най-съществените фактори на първичната социализация в ранното детство. Основен компонент от социализацията на малкото дете са неговите отношения с родителите. Съобразно ролята си в структурата на семейството, родителят има възможност да прибягва до трите форми на власт, а именно, принуждаваща (насилие), компенсаторна (възнаграждение) и условна (убеждение или друга по-скрита сила).

Според класификацията на тактиките на А. Петровски, те са пет: диктат, опека, конфронтация, мирно съвместно съществуване, сътрудничество.

Диктатът, това е тактика, която се основава върху категоричните изисквания на родителите. Тук детето не обсъжда и не оспорва изискванията, а просто ги изпълнява, то е обект на диктата. Друга характеристика е честото приложение на наказанията и много рядко на поощренията. Целта на тази тактика е послушанието на детето. Тя потиска самостоятелността и инициативата на детето, не зачита неговото достойнство и създава дистанция между родители и дете.

Проявява се в две основни форми- автократична (абсолютна родителска власт) и авторитарна (детето формално има право на мнение, но никога на решение).

Опеката е тактика, при която на преден план се поставят интересите на детето, но то е пазено от всякакви опасности. Родителят приема поведението на единствен и възможен помощник, той изисква пълна информация от детето под претекст, че иска да му помогне, но истинската причина е че иска да знае всичко за детето, за да може да го моделира, според разбиранията си. Тук няма насилие, а манипулиране на детето - родителят го сравнява с другите деца, за да покаже неговото превъзходство и се стреми да поддържа у него висока самооценка, най-често, завишена. За детето в това семейство се казва, че е единствената радост в живота. При тази тактика, физически наказания не се прилагат, доминират поощренията, задълженията на детето са сведени до минимум, особено трудовите. Основната родителска грешка тук е, че родителите гледат на детето само като на дете, независимо на колко години е то, много често, детето вижда единствения изход по време на пубертета във бягството от родителите, израства несамостоятелно и неспособно да се съпротивлява на различните ситуации.

Тактиката на открития конфликт се нарича конфронтация. В семейството има два свята, които непрекъснато враждуват помежду си- това е война без победител.

Всяка от страните се стреми да причинява страдание и болка на другата. Ролята на детето е ролята на Пепеляшка и, много често, то трудно създава собствено здраво семейство.

При тактиката на мирно съвместно съществуване в семейството има два свята. Те не се конфронтират, а, напротив, всеки е за себе си. За детето, това е една наложена принудителна свобода, нежелана от него, а, по същество, това е тактика на скритата зрителска безотговорност- родителите не се интересуват от него, но представят поведението си като загриженост. Така детето става егоист, иска да накаже родителите си за безразличието им и за собствения им егоизъм.

Тактиката на сътрудничеството е основана на доверието и уважението на детето, то има място в семейния диалог, не само с право на мнение, но и на решение. Проблемите се обсъждат заедно, одобряват се от всички и се вземат решения, не се прилагат физически наказания, между родителите и децата няма постоянни и трайни конфликти, а когато има, те са с временен характер.

ЗАКЛЮЧЕНИЕ

Социализиращите функции на семейството в първите десетилетия на XXI век се характеризират с повишена сложност и динамичност, поради зачестилите ситуации в семейната среда (количествен скок на разводи, отглеждане на дете от един родител) и глобалната тенденция за промяна на социалните норми и ценности, по отношение на семейната среда. В тези изменени условия е още по-важно родителите да полагат съзнателни грижи и усилия за формирането и развитието на личността на детето, тъй като под влияние на стреса от натиска на обществените промени, родителският им „инстинкт" може да ги подведе към прилагане на по-лесни за тях методи и стил на възпитание- демонстриране на безпрекословна власт, авторитаризъм, физическо или психическо насилие, безразличие на потребностите на детето и др.

Желателно е педагозите да познават семейната среда на децата, с чието възпитание и обучение са ангажирани, за да бъдат в състояние да прилагат индивидуален подход в педагогическото взаимодействие, не само въз основа на установените у тях психофизиологични характеристики на всяко от децата, но и съобразно условията, в които тези характеристики са формирани.

ЛИТЕРАТУРА

1. Андреев, М., Педагогическа социология, Народна просвета, С., 1988.

2. Борисова, В., Социализация и ресоциализация, УИ „Св. Климент Охридски, С., 2001.

3. Бъргър, П., Т. Лукман, Социално конструиране на реалността, Критика и хуманизъм, С., 1996.

4. Енциклопедичен речник по социология, С., 1996.

5. Как се ражда личността, Под ред. на Р. Косолапов, С., 1983.

6. Кон, И., Психология на средношколеца, Народна просвета, С., 1995.

7. Михайлов, М., Социологът: 70% от децата са от маргиналните слоеве, 24 часа, 16. 09. 2004.

8. Парсънз, Т., Социализацията на детето и интернализирането на социални ценностни ориентации. Структура на „базовата личност" , В: Социология на личността, Наука и изкуство, С., 1990.

9. Шарден, П. Т. дьо, Човешкият феномен, Аргес, С., 1994.

ФУТУРОЛОГИЧЕН РАКУРС КЪМ ГЛОБАЛНАТА СИГУРНОСТ. НЕОБХОДИМОСТ ОТ ДЪЛГОСРОЧНО ПРОГНОЗИРАНЕ В ОБЛАСТТА НА НАЦИОНАЛНАТА СИГУРНОСТ НА БЪЛГАРИЯ

Соня Б. Илиева Веселина Н. Илиева

Шуменски университет „Епископ Константин Преславски”
Педагогически факултет, ул. „Червени ескадрони” № 22, гр. Шумен

FUTUROLOGICAL PERSPECTIVE TO GLOBAL SECURITY. NEED FOR LONG-TERM FORECASTING IN THE NATIONAL SECURITY OF BULGARIA

Sonya B. Ilieva Veselina N. Ilieva

“Konstantin Preslavsky” – University of Shumen
Pedagogical Faculty, 22 Cherveni eskadroni str., Shumen

ABSTRACT: *The science futurology largely allows to identify global threats, security - national and global level. Since its establishment until today it has the task to predict future threats to humanity today can be avoided. Specify the various theoretical developments in this context. Bulgaria needs indispensable connection between such futurology and national security, as well as international and national environment is a field in which threats arise, undermining national security.*

KEY WORDS*: futurology, national security threats, conflicts, crises, long-term forecasting*

През цялото си развитие човечеството търси начини за установяването на алтернативни реалности при избора и вземането на решения за своето бъдеще. Това от своя страна означава изграждане на някакви прогнози. В този контекст, изследванията на бъдещето в съвременността бележат непрекъснато нарастват.

Динамиката в социалната и национална сигурност, свързана с цялостната промяна и разрешаването на проблеми в нея, както и подпомагане за вземане на решения, свързани с човешкото благоденствие, човешките права и социалната справедливост.

Науката Футурология в голяма степен дава възможност за идентифициране на глобални заплахи, свързани със сигурността – на национално и глобално ниво.

Още през далечната 1932 г. в Би Би Си - излъчване писателят **Хърбърт Уелс** [15, с.89-91], призовава за създаването на специални научни звена, които да изучават бъдещето и предлага въвеждането на научно звание „професор по Форсайт” (Футурология), който ще анализира и посочва пътищата за приложение на новите технологични открития. Но институционализирането на науката за дългосрочно прогнозиране започва десетина години по-късно. Нейното наименование, символизиращо научен поглед в бъдещето - Футурология (от лат. Futurum - бъдеще и от гр. Λόγος-учение) е предложен от социолога **Осип Флетхайм** (1909-1998) през 1943 г. в писмо до писателя Олдъс Хъксли. През 1971 г. той пише своята книга “Футурология - битката за бъдещето” [7]. В нея той излага възгледите си, че едно човечество, изоставено на произвола на динамичното развитие на техниката и на естестве-

ните науки, не може да навлиза сляпо в бъдещето, ако не иска да заплати с осакатяване и дори с упадък. А една Футурология, която е нещо повече от утопия, трябва да се опита да обедини прогностиката с планирането и философията на бъдещето в една нова общност, при което към философията на бъдещето трябва да спадат и политиката, и педагогиката на бъдещето. Футурологията трябва да даде отговор на петте предизвикателства, заплашващи човечеството: 1.елиминирането на войната и институционализирането на мира; 2.ликвидирането на глада и мизерията и стабилизирането на числеността на народонаселението; 3.побеждаването на експлоатацията и подтисничеството и демократизирането на държавата и обществото; 4.премахването на безогледната експлоатация на земи и находища и охраната на природата и човека от самия него; 5.отстраняването на вътрешните опустошения и на отчуждението и създаването на нова творческа човешка личност "хомо хуманус".

Разрешаването на тези проблеми, според Флехтхайм, може да се изрази накратко в следното: институционализиране на световния мир; планиране на световното население и осигуряване на достатъчни средства за живот за всеки индивид; хуманизиране на държавата и демократизиране на обществото; опазване на природната среда от безогледна експлоатация; развитие на човека до съзидателно същество и творец.

Целта на Футурологията [4] е да изследва вероятните, възможните и предпочитани събития в бъдещето, както и на гледните точки, които стоят в основата на подобни очаквания. В този контекст тя може да бъде част от различни науки или човешки практики и разбирания – напр. философия, изкуство, мода и т.н. За да се обяснят различни вероятности за бъдещи тенденции Футурологията търси модели в миналото и настоящето, екстраполира ги в бъдещето и по някакъв начин го премоделира или както пише **Х. Кан** [8] - превръща немислимото в мислимо.

В контекста на написаното за Футурологията, може да се обобщи, че тя е наука за **изучаване на бъдещето и заплахите, които крие то както за глобалната сигурност на планетата, така и за сигурността на отделните човешки същества**, които я населяват.

Показателни в това отношение са редица **футурологични прогнози**, в които са представени тези заплахи:

Около 70-те години на XX век става невъзможно да се говори за развитие на човешкото общество, без да се отчитат екологичните проблеми на национално и глобално ниво. Обобщено това звучи като: няма Футурология, без екология [2]. За това говори книгата на американския социолог **Робърт Фолк** „Нашата планета е в опасност" (1971). Редица автори излизат с решителни произведения по посока замърсяването на околната среда, изчерпването на природните ресурси, обезлесяване, израстването на суперградовете и т.н. Това поражда необходимостта от национални и наднационални организации и институции, работещи по екологични проблеми на глобалното общество. За тези процеси може да се съди по книгата на американските футуролози **М. Сертон и Б. Барток** „Оценка на технологиите в динамична среда" (1974).

Основният принос на **Херман Кан**, свързан с РАНД Корпорейшън, известен ядрен стратег и системен теоретик, създател на Институт Хъдзън [8] са стратегиите, които разработва по време на Студената война, измежду която „да съзерцавам

немислимото" – бъдеща ядрена война, като за разработването й използва Теорията на игрите.

Но по-впечатляващи са прогнозите, които той, заедно с **Антъни Винер** публикуват под надслов „Година 2 000" (или „Година 2 000"), в която се посочват 100 технически нововъведения, свързани с идващия XXI век: масово приложение на лазерите; създаването на структурни материали с висока степен на якост; нови летателни апарати; по-дългосрочно и по-надеждно прогнозиране на времето; широко използване на ядрени реактори за производство на енергия; нови и евтини техники за надежден контрол върху раждаемостта; промяна на възможностите за промяна на пола; автоматизирани системи за банкиране и одитиране; всепроникващо присъствие на компютри; лични пейджъри и може би джобни телефони и т.н. Всичко посочено до тук вече е факт.

Херман Кан, заедно с **Уилям Браун и Леон Мартел** написва книгата „Следващите 200 години" (1976), посветена на 200 годишнината от създаването на САЩ, където представят оптимистичен сценарий за икономическите условия до и след 2176 година.

Жак Атали (р.1943) смята, че днес, в съвременността ще се реши какъв ще бъде света през 2050 г. и как ще изглежда през 2100 г. [5], [6], [1]. От днешните действия на човечеството зависи дали нашите деца и внуци ще живеят в мир или ще се окажат в ад и ще ни проклинат; дали въобще ще им оставим обитаема планета. Силно вярвайки в прогреса на човешките общества той пише [1, с.21]: „Аз вярвам, че прогресът не е линеен и неговото овладяване е възможно. С всяка следваща възраст децата променят стратегията си, за да организират своето развитие. Защо същото да не се отнася за обществата, които днес трябва да променят толкова радикално стратегията на развитието си и да скъсват решително със своето минало, за да оставят бъдещето да се самосъздаде? Разбира се задвижването на една такава промяна изисква единство на интересите на класите, на социалните групи, способни да наложат колективно тази промяна и имащи интерес от нея."

Атали смята, че това, което формира днес човешкото общество е пазарът. Той формира така наречената от него хиперимперия – необятна и планетарна, създаваща търговски богатства и ново отчуждение, огромни състояния и ужасяваща нищета. Според него природата варварски се експлоатира в името на пазара. В резултат на изчезването й човечеството ще стане артефакт и постепенно ще изчезне. В борбата за пазари човечеството ще се впусне в опустушителни битки с помощта на мощни оръжия, които към този момент са непознати. Тези войни Атали нарича хиперконфликти, при които ще се противопоставят държави, религиозни групировки, терористични организации и бандити-единаци. Това може да доведе до унищожаване на човечеството.

Историята на петдесетте следващи години Атали описва като преход от хиперимперии към хипердемокрации чрез хиперконфликт: до 2035 г. ще настъпи краят на американската империя; след това ще следват една след друга три вълни на бъдещето – хиперимперия, хиперконфликт и хипердемокрация. Двете вълни a priori ще бъдат смъртоносни, а третата a priori ще бъде невъзможна. Въпреки всичко, Атали вярва в победата около 2060 г. на хипердемокрацията – висша форма за организация на човечеството, висша форма на свободата – двигател на историята.

В поредицата от авторите, които се вписват измежду тези, които прогнозират бъдещите глобални заплахи могат да се впишат и имената на **Бертран Де Жувенел, Реймънд Кърсуайл, Джон Нейсбит** и др.

Опасностите, които предстоят пред човечеството, ако то не предприеме решителни мерки за тяхното преодоляване, са в основата на създаването на футурологичния кръг, наречен **РИМСКИ КЛУБ**, основан през 1968 г. Неговите членове правят едни от първите задълбочени изследвания свързани с дългосрочното прогнозиране и бъдещето на човешкото общество [189], [187]. Той е един от първите безспорни индикатори за възникващо световно съзнание по отношение на бъдещето на човешкото общество. Негова основна изследователска проблематика са глобалните предизвикателства и съдбата на човечеството.

Основател на Римския клуб е **Аурелио Печеи** [12], [13], който твърди, че последиците от развитието на производството, науката и техниката е достигнало такова ниво, което променя и застрашава съществено не само условията на живот на планетата, но и самото качество "човек". Изходът от тази катастрофална ситуация Печеи вижда чрез налагане на мерки за управление или по-точно ограничаване на самоунищожителната и безразсъдна дейност на човека и най-вече чрез усъвършенстването и преобразуването на самия човек и неговите ценности.

От 1970 г. до 2013 г. Римски клуб издава 54 доклада, като се посочват концептуално онези от тях, които „бият камбаната" за събуждане на човечеството пред глобалните заплахи за сигурността на човечеството:

Джей Форестър от Масачузетския технологически институт, разработва модели за бъдещото състояние на световната икономика [12]. Според него модели, изтощаването на запасите от суровини ще доведе през идващото столетие до спадане на ръста на производство, а впоследствие до регресиране числеността на населението на планетата и западане на цивилизацията. Неговият асистент **Денис Медоуз** смята, че непрекъснатият възход на обществото е илюзорен. Докладът / Книгата на Медоуз и неговата група - „Пределите на ръста" [3], [11], предизвиква футурологична сензация. Ключови процеси в това изследване са: 1.ръстът на световната човешка популация; 2.ръстът на промишленото производство; 3.производство на храни; 4.намаляването на природните ресурси; 5. темпове на замърсяване на природната среда. Докладът показва, че ако темповете в тези пет пункта продължават да растат, то още в първите десетилетия на XXI век процесите на глобална катастрофа ще бъдат необратими. Подавайки параметрите на тогавашните глобални процеси в компютъра той връща сигнал към изследователите: катастрофа.

Ервин Ласло (Унгария / САЩ) и неговата изследователска група написват доклад в два тома, който излиза през 1977-1978 г. с наименованието „Целите на човечеството" [9], [10]. В първи том се разглеждат подробно регионалните аспекти на целеполагането в големите световни региони. За тази цел са привлечени специалисти от цял свят, включително от бившия СССР, независимо от Студената война. Анализира се дейността на големи международни организации и корпорации, международната безопасност, продоволствието, енергетиката и минералните ресурси, общото глобално развитие. Формулира се призив за извършване на световна революция за установяване за постигане на световна солидарност в името на осъществяване на глобални цели. Вторият том детайлно показва хода на самото изследване.

Един от последните доклади на Римски клуб е написан на Йорген Рандърс през 2012 г. Той кореспондира едновременно с Първи доклад на Римски Клуб „Границите на растежа" от 1972 г., както и теоретичните постановки на Аурелио Печеи отразени в „Човешките качества". Тенденциите, които Й. Рандърс посочва се изразяват в следното: Около 2040 г. населението на света чувствително ще намалее, като работещата част от него ще покаже най-високо нива през 2030 г. БВП ще се увеличава, но не с очакваните бързи темпове. Този извод корелира с общото застаряване на населението и с това – намаляване растежа на производителността. Енергийната ефективност ще продължава да нараства, но потреблението на енергия ще достигне своя връх през 2030 г. В същото време средната глобална температура ще се повиши с два градуса, което ще доведе до сериозни проблеми на земята. Надпреварата за природни ресурси ще бъде задълбочена, но все пак биологичният капацитет на света ще бъде използван максимално. Авторът посочва, че градовете ще стават все по-богати източници на метали, докато в същото време ще намаляват природните източници. В същото време зоологическите градини ще са последното убежище за много застрашени видове животни. Знанието няма да бъде повече ограничен ресурс, благодарение на Интернет, който освен това ще доведе до размиване на понятията „частно" и „публично". Но това разширяване на знанията в никакъв случай няма да доведе в повечето случаи до по-рационални решения, защото знанието само по себе си не е достатъчно, за да се промени поведението, когато са намесени силни интереси. Най-важният извод, към който насочва доклада е: идва криза и за целта е необходимо да се разработят нови цели за съвременното общество. Целта на обществото е да се увеличи общата удовлетвореност от живота, а не само всеки човек да допринася за БВП.

Посочените доклади на Римския клуб отразяват главните насоки на възможните проблеми в областта на глобалната сигурност, на все по-обвързващите се световните пространства и космополитни механизми. За съжаление те не успяват да респектират в достатъчна степен държавите. Но от тях става ясно, че е нужно да се реализират начини за създаване на блага, щадящи планетата и нейните обитатели.

Освен Римски Клуб в областта на дългосрочното прогнозиране на бъдещите заплахи, предстоящи пред човечеството работят и още две организации:

1. **Корпорация РАНД** (RAND Corporaton - USA), създадена по време на Втората световна война. Именно в рамките на тази организация през 1964 г. се ражда Методът Делфи (Делфийски метод) за дългосрочно прогнозиране, с огромен научен потенциал, включващ сътрудничеството на учени Нобелови лауреати;

2. **Институт Хъдзън** (Hudson Institute – USA). Основан от футуролога Херман Кан, институтът помага за управлението на бъдещето чрез интердисциплинарни изследвания в отбраната, международните отношения, икономиката, здравеопазването, технологиите, културата и правото. Чрез своите изследвания и дългосрочни прогнози насочва държавници, политици, световни лидери и правителства към разумно управление на бъдещето.

Изучаването на "алтернативни светове" и на "желания образ на бъдещето" стои като важна задача и пред други футурологични центрове възникнали още през 60-те г. на XX в., преди всичко в САЩ: **центрове за изучаване на бъдещето** към университетите Станфорд, Хъдзън, Портланд, Принстън и Южно-Калифорнийски и др. Световно известни научни институти изучаващи бъдещето на човешкото общество са тези в Менло-Парк и Ню Йорк.

Изложеното дотук съдържание експлицилра проблемът за **необходимост от дългосрочно прогнозиране на заплахите, стоящи пред националната сигурност на България.**

Правилното прогнозиране на събитията в дългосрочен план е от изключително важно значение за дефиниране на задачите на една държава във всяка област. Преди изготвяне на военна доктрина, концепция за национална сигурност или стратегически преглед на отбраната трябва да се определи ясно средата, в която държавата ще съществува за период поне от 15 години. Според данни от различни официални източници, ЦРУ също се ориентира към един хоризонт на прогнозата от 15-20 г. В икономическата област големите компании също се опитват да оценят перспективите си за следващите 15 години. Възможностите на петролния пазар се изчисляват за 20-30 години напред. Оръжейната промишленост планира развойната си дейност за следващите 20 години.

В този контекст стои и необходимостта от дългосрочно прогнозиране на социалните конфликти, рискове и заплахи за националната сигурност на Република България. Всички посочени заплахи могат и да не настъпят, но които следва де се имат предвид, да се прави своевременно необходимото за предотвратяването им и да се насочва управлението на процесите съобразно тях и доколкото зависи от възможностите на страната да им влияе или да ги избегне чрез съответната политика и държавнически решения.

За страната ни такива заплахи могат да бъдат групирани в глобален, регионален и национален мащаб.

А. В глобален мащаб:

1. Евентуална **дестабилизация на международната система**, намаляване на ролята на фактори като важни международни организации и размиване на ценности и принципи в международните отношения. Опитите за налагане на еднополюсна система ще бъдат съпроводени с политическа и икономическа конфронтация и преки сблъсъци за предотвратяване възникването на нови центрове на сила и намаляване ролята на националния суверенитет на държавите.

2. **Икономически и финансови трусове** с по-дълбоки и дълготрайни въздействия в глобален мащаб, икономическа дестабилизация на региона и България в резултат на интереси и конкурентни борби на световни икономически центрове или мощни транснационални компании.

3. Сращване на **организирана международна престъпност** с капитала и противопоставяне на държавни интереси.

4. Принципно **нови видове въоръжения**, които биха попаднали в диктаторски режими или терористи и биха могли да се използват срещу един континент, регион или отделна държава.

Б. В регионален мащаб:

1. Изостряне на нерешени **териториални спорове** и исторически вражди, неустановен статут и амбиции на някои млади нации към експанзия. Очертаващите се събития в съседни региони ще влияят негативно и на проблемите в нашия регион.

2. **Етнически конфликти** в Югоизточна Европа и въздействието им върху мира и сигурността в региона, водещи до затрудняване на общорегионални инициативи, транспортни и транзитни потоци и други. Разрастването на дейността на секти и фундаменталистки религиозни организации, финансирани от други държа-

ви и континенти, които подкопават демократичната същност на държавното устройство, нарушават правата на човека и водят до назряване на конфликти в обществото.

3. Разрастване на **организираната престъпност**, търговията с наркотици и хора, превръщането на неукрепнали близки страни от региона в центрове за подготовка на терористични актове и включването неизбежно и България в нея, поради възловото й географско място.

В. В национален мащаб

1. Задълбочаване на **демографската криза** и отражението й върху различни области. Намаляване на **интелектуалния и професионален потенциал** на нацията вследствие на емиграцията на младото поколение и влошаване качеството на образованието. Запълване на освободеното от емигриращите пространство от граждани от други държави с друго равнище на развитие, потенциал, култура и религия, криминогенност и т.н.

2. **Загуба на стратегически позиции** в региона и изпадане в икономическа, енергийна или друга зависимост, създаващи условия за ограничаване на растежа и развитието ни в ущърб на националните интереси.

3. **Изоставане във военнотехнологично отношение** вследствие нарастване на разликата в тази сфера не само между Европа и САЩ, което е факт и днес, но между нови структури в Централна Европа и новите страни - членки на НАТО, което би оставило България в позиции за изпълнение само на спомагателни задачи и би намалило ролята й на партньор, който да влияе върху вземането на решения, касаещи Югоизточна Европа.

4. Възникването на **екстремистки групировки** вследствие на продължително безуспешно икономическо развитие, съюзяването им с такива от други страни и активизиране дейността им на наша територия. Евентуална невъзможност да спрем проникването на **международната престъпност** и израстването и утвърждаването на българска такава от мафиотски тип, която да наложи своята воля в държавата и да диктува икономически интереси.

5. **Ответни терористични актове** от организации и страни, срещу които е участвала Република България съвместно със съюзнически въоръжени сили, като се отчитат всички нови форми и средства на тероризма. Допускане на неконтролируемо разрастване на проблемите с **ромското население** и манипулирането му от вътрешни и външни фактори за дестабилизиране на държавата.

6. Дългосрочното проникване и влияние на различни **секти и на ислямския фундаментализъм**, финансирането им от чужди организации и държави, очевидния им стремеж за перспективно настаняване и противопоставяне на национални и религиозни традиции.

7. Налагане на тенденцията към разграничаване и **обособяване на групи от населението въз основа на социални, етнически и/или религиозни различия.** Напускане конституционната плоскост за единната политическа нация и създаване на условия и насърчаване на стремежи към преференции, ограничен суверенитет или пълна независимост на групи от населението.

Готова ли е България да отговори на тези предизвикателства в бъдеще? Това е задачата на дългосрочното прогнозиране в сферата на националната сигурност. То има задача да се минимизират рисковете за обществото.

Изложеното съдържание предполага формулирането на следните

обобщения и изводи:

1. Чрез теоретичните и практически разработки в областта на Футурологията се налагат на обществото определен тип полезни действия за овладяване на социалните заплахи, подкопаващи глобалната и националната сигурност. Откриват се възможностите, с които тези заплахи биха могли да бъдат преодолени.

2. Това води до поставяне бъдещето на глобалната и националната сигурност в един континуум с настоящето.

3. Дългосрочното прогнозиране в сферата на националната сигурност има защитна (охранителна) функция спрямо бъдещето.

4. Чрез методите на Футурологията се прониква в общественото и експертното съзнание, като се откриват нагласи за бъдещото развитие на глобалната сигурност.

5. Прилагайки методите на Футурологията е възможно да се научи не само какво следва в бъдещето, но и това какво мислят самите хора за обществото. Те отразяват структурата на мисленето на обществото, което е социално обусловено, т.е. изследва се самата негова рационалност. Това в много голяма степен определя стратегиите за глобална и национална сигурност, които се изграждат в обществото.

6. Футурологичните анализи в системата на сигурността подпомага преодоляването на футурофобията (страх от бъдещето). Този страх произтича от неясното бъдеще, както и от заплахите, които носят в себе си социалните конфликти заплашващи сигурността на обществото.

7. Приложени в сферата на националната сигурност, футурологичните методи водят до яснота за мерките и политиките, които могат да се приложат за да бъдат поставени хората в състояние на относително спокойствие за своята лична сигурност.

ЛИТЕРАТУРА

1. **Атали, Жак**, Слово и средство, София, 1996
2. **Бестужев-Лада, И.В., Наместникова, Г.А.,** Социальное прогнозирование, курс лекции, Москва, 2001
3. **Медоуз, Д**., Пределы роста, Москва, 1988
4. **Турчин, А., Батин М.,** Футурология. XXI век: бессмертие или глобальная катастрофа, изд. БИНОМ, 2012
5. **Atalli, J.,** Une Breve Histoire De L'Avenir, Arcade, 2009
6. **Attali, J.,** A Brief History of the Future /2006/, Arcade Publishing, 1st english-language ed. 2009
7. **Flechtheim, O.,** Futorologie – Der Kampf un die Zukunft, Köln, 1970
8. **Kahn, H.,** Thinking About the Unthinkable, New York: Horizon Press, 1965
9. **László, E., Bierman, J.,** Goals in a Global Community: The Original Background Papers for Goals for Mankind, Pergamon Press, 1977
10. **László, E., et al.,** Goals for Mankind: On the New Horizons of Global Community, New American Library Signet Hutchinson, 1977
11. **Meadows, D., Randers, J., William, W. Behrens, W.,** The Limits to Growth . New York, New York, USA: Universe Books, 1972
12. **Peccei, A.,** Before It Is Too Late, with Daisaku Ikeda, Kodansha America, 1985
13. **Peccei, A.,** One Hundred Pages for the Future, Pergamon Press, 1981
14. **Peccei, A.,** The Human Quality, Pergamon Press, 1977

15. **Wells, H.,** Wanted: Professors of Foresight! Futures Research Quarterly V3N1 (Spring), (1932) 1987

СЕКЮРИТИЗИРАНЕ НА СОЦИАЛНИТЕ КОНФЛИКТИ, ЕКСПЛИЦИРАЩИ ПРОЦЕСИ В НАЦИОНАЛНАТА СИГУРНОСТ

Соня Б. Илиева Веселина Н. Илиева

Шуменски университет „Епископ Константин Преславски”
Педагогически факултет, ул. „Червени ескадрони” № 221 гр. Шумен

SECURITIZATION OF SOCIAL CONFLICTS, EXPLICIT PROCESSES IN NATIONAL SECURITY

Sonya B. Ilieva Veselina N. Ilieva

“Konstantin Preslavsky” – University of Shumen
Pedagogical Faculty, 22 Cherveni eskadroni str., Shumen

ABSTRACT: *The problem of "securitization" of social conflicts first place by N. Slatinski, in the context of the demographic crisis. This report attempts to broaden the understanding of this concept in otnoshennie poverty, unemployment and employment; health; education; migration and emigration, etc. Covered data show that Bulgaria ripen social conflicts that give rise to certain risk groups jeopardized national security.*

KEY WORDS: *National security, social security, social conflicts, securitization of social conflict risk groups in society*

Проблемът за **секюритизацията** на определени страни от обществения живот се поставя в светлината на научнато обяснение от българския изследовател на проблема **Николай Слатински** [13]. Според него, когато става дума за сигурност трябва да се подхожда към нейните проблеми изключително внимателно и отговорно. Защото тези проблеми са неизменно екзистенциални. Те се управляват, и то отчасти успешно, само докато водят до количествени, и много трудно, когато водят до качествени промени. Един проблем става проблем на сигурността (или както се казва, той се **секюритизира**), ако в резултат от него възникват качествени промени и обществото не може да го преодолее без значими структурни трансформации.

Според **Николай Слатински** [13] сред главните рискове за националната сигурност е опасността от демографски колапс на българския етнос и оттук – на коренна промяна на демографската и етническа картина на нашата нация. Той смята, че България трябва да се обърне с лице към своя тежък демографски проблем, защото той вече се е “**секюритизирал**”, т.е. за България трайно, дълбоко и дългосрочно той се е превърнал в проблем на нейната национална сигурност!

Към проблемите, секютиризиращи националната сигурност, **Николай Слатински** добавя [13]: *увредената природна среда*, ниското *качество на*

храната, стресът, агресията, насилието, личната несигурност – социална и физическа, развратът в редица медии. И още – все по-влошаващият се в здравен, в образователен и квалификационен разрез *качествен състав на населението*. Като той има предвид под индикатори за качеството на населението: са главно *образованието* – ниво на грамотност на възрастните хора, дял на учащите; *здравното състояние* на населението - средна продължителност на живота, заболеваемост, трудоспособност).

В контекста на посоченото може да се определи социалната сигурност като фундаментална част от националната сигурност. В продължение на тази теза някои изследователи, измежду които **Арнолд Уолферс** [18, pp. 147-165], пише: „Сигурността, в обективен план, измерва отсъствието на заплахи за постигнатите обществени ценности, а в субективен план – отсъствието на страх, че тези ценности могат да бъдат накърнени, атакувани, застрашени." Тя още може да може да се определи като относително устойчиво състояние на нацията, характеризиращо се с обективни външни и вътрешни условия, при които в достатъчно висока степен са защитени от съвременните рискове и заплахи жизненоважните национални интереси и благодарение на които, това състояние поражда в обществените настроения господстващо чувство на сигурност [5, с.18]. В най-общ план „национална сигурност" е защитеност и реализиране на националните интереси като съвкупност от интересите на държавата, обществото и личността.

Едно кратко определение представено в Доклада за човешко развитие за 1994 г. поставя ударението върху въпроси като: „оцеляването, ежедневието и достойнството на хората [19]**",** което дава представа за акцента на националната сигурност върху социалната сигурност, **до** ненарушен достъп до възможностите за човешко развитие.

Социалната сигурност на всяко общество е в изключително голяма корелация с със социалните конфликти, които са налице във функционирането на обществената система. А Социалните конфликти в сферата на социалната сигурност очертават проблематиката на *социалното включване и социалното изключване***,** които пряко влияят върху националната сигурност.

От тази гледна точка по надолу са посочени релациите между социална сигурност – социални конфликти в социалната сфера – национална сигурност:

Демографски проблем

Настъпилите в края на XX век сериозни промени в демографската картина на България продължават да оказват сериозно влияние и през първото десетилетие на XXI век. Броят на населението, независимо от затихващата емиграционна вълна, в резултат преди всичко на отрицателния естествен прираст продължава да намалява от 7891 хил. през 2001 г. на 7668 хил. през 2005 г. и на 7606 хил. в края на 2008 г. Темпът на намаляване на населението връща страната в 1946 г., когато обаче съотношенията са били други – висок естествен прираст, висока раждаемост и ниска смъртност [7], [8], [9].

Очевидно *смъртността* се очертава като един от най-сериозните демографски проблеми за страната. От 1990 г. до днес България е единствената страна в Европейския съюз, в която смъртността бележи непрекъснато увеличение и е на най-високо равнище – над 14‰.

Противоположна е картината при *раждаемостта*. Вече почти цяло столетие продължава системното намаление на нейното равнище, за да се стигне в края на миналия век до екстремни стойности от 7,0 ‰ (1997 г.). В първите години на XXI век ражданията се увеличават, за да стигнат до равнището около 10‰, с което днес България се нарежда сред страните със средно европейско равнище на раждаемост. Това показва, че страната ни навлиза с отрицателен естествен прираст на населението. Всяка година населението намалява с над 40 хиляди души и тази тенденция вероятно ще продължи през следващите няколко десетилетия.

Миграционните процеси, които застрашават националната сигурност, в началото на XXI век се съпровождат от някои особености. След масовата емиграционна вълна в началото на 90-те години на миналия век, процесът на емигриране от страната постепенно затихва.

Вътрешната миграция продължава да бъде главния фактор в обезлюдяването на отделни региони. Наблюдава се и обратна миграция към селата, но в преобладаващата си част това са хора на пенсионна възраст, които са все още жизнени и с възможност за работа в дребно лично стопанство, с цел осигуряване на допълнителен доход в натура.

При запазване на сегашните тенденции на изменение на населението в селата, водещи до свиване на техния демографски и икономически потенциал, приносът на селските райони в бъдещото развитие на страната ще става все по-малък.

Труд, заетост и безработица

Проблемите на заетостта винаги са актуални. Значими и актуални са те от гледна точка на социалната реализация на личността, свързани с поддържането на състояние на активност през целия живот в резултат на вложените в нея инвестиции и превръщането им в човешки капитал и отношението на всички тези изброени процеси към националната сигурност на България.

Икономическата криза през последните години задълбочава проблемите в социалната система. Броят на хората под прага на бедност расте, като в края на 2012 г. е 1 673 хил. души (22.3% процента от населението на страната). Процентът на хората без работа за период над 12 месеца на годишна база расте с 22% от 2008 г. насам. Размерът на социалните помощи и обезщетения, изплащани от НОИ, е нараснал 6 пъти през последното десетилетие – до 1 040 милиона през 2012 г. България е квалифицирана и като страната с най-висок риск от бедност и социално изключване в Европейския съюз – 49.1% от населението за 2011 г. Данните свидетелстват, че сегашната социална система е неефективна и не изпълнява основните си функции на задоволително ниво [29].

Доходи, разходи, потребление, бедност

Продължаващото доходно разслоение и наличието на елементи на фрагментация на обществото като последица на подобно разслоение продължават да бъдат едно от предизвикателствата пред развитието на страната и националната сигурност. Значим сам по себе си, проблемът с доходите на населението придоби още по-сериозно звучене след присъединяването на страната към ЕС.

Категорията на бедните у нас не е хомогенна група с изчистен социален профил. Формира се т.нар. симптом за формиране на траен "културен модел на бедността". Способността му да се възпроизвежда в следващото поколение крие сериозни рискове от зараждане на "втора генерация бедни", което би било непознато предизвикателство за българската реалност през най-новата ни история.

Картографирането на бедността в страната очертава драстични различия в териториален план. Относителният дял на бедните по общини варира от 1.8% в столицата София до 53.8% в община Бойница, област Видин. Съществени са различията в профила на бедност в градовете и в селата. Градската бедност е парична, докато бедността в селата е очертана от липсата на работа, некачествени или недостъпни здравеопазване, образование и социални услуги. В селата натуралното потребление продължава да формира значителна част от общото потребление за сметка на доходите от работна заплата или предприемачество.

Образование

Корелацията между образование и национална сигурност е лема за всяко общество. Образованието на населението в дадена страна е един от съществените показатели, характеризиращ реалните възможности за нейното развитие, качеството на живот и сигурността й. Това негово значение обяснява включването му като структурообразуващ елемент на индекса за човешкото развитие в Програмата за развитие на ООН.

Данните от изследването „Взаимоотношения между поколенията и половете" потвърждават диференциращата роля на възрастта върху образователната структура на населението и позволяват да се проследят измененията. При двете вълни на изследването се очертава положителна промяна сред най-младата възрастова група. Нараснал е относителният дял на завършилите средно образование с 10,3 процентни пункта. Близо с толкова е намалял относителният дял на завършилите основно образование (с 10,1 процентни пункта). При най-възрастните промяната е с отрицателен знак. Увеличил се е относителният дял на завършилите само основно образование с 5 процентни пункта.

В началото на XXI век образователната структура на населението в селата продължава да е по-неблагоприятна в сравнение с тази на населението в градовете.

Получените резултати от социално-демографското изследване „Взаимоотношения между поколенията и половете" показват, че очерталите се негативи между образованието в градовете и селата не са преодолени. Ярко изразена е тенденцията относителният дял на лицата с висше образование да нараства с нарастването на размера на населеното място. Така относителният дял на населението от селата с висше образование е 6,4 пъти по-малък от този на София, 4,7 пъти от този на големите градове и 3,2 пъти от тези в градовете. При основното образование тенденцията е обратна на описаната при висшето образоватние, а именно – относителният дял на населението с основно образование от селата е с 5,9 пъти по-голям от този в София, - 3,5 пъти от този на големите градове и с 2,1 пъти на градовете. По отношение на средното образование между градовете почти не съществува разлика.

Закрити са значителен брой училища в селата и учениците се пренасочват в средищните училища. Поради нерешените проблеми със социалната инфраструктура много от децата, подлежащи на задължително образование не посещават средищното училище, което допълнително увеличава разрива в образованието между града и селото.

Средният годишен дял на отпадналите ученици е 14,9% за закритите училища спрямо 6,2% за незакритите. Само през лятото на са закрити около 300 училища. За тях средният дял на напусналите обучението ученици е 11,3% спрямо 4,9% за незакритите училища.

Ниското образование на някои слоеве от населението, както същевременно развиващият се процес на „изтичане на мозъци" от България неминуемо ще доведе до срив в националната сигурност и именно тези процеси е необходимо дългосрочно да се прогнозират, за да се овладеят в името на сигурността на нацията.

Здраве и здравеопазване

Значимостта на здравето като интегрален показател за социално-икономическото развитие както на всяка отделна страна, така и на цели региони трудно може да бъде подценена, тъй като имат директна връзка с националната сигурност.От своя страна Мадридската рамка описва здравето като най-чувствителен индикатор за благосъстояние и свобода [17].

Общата смъртност в страната през последните десетилетия непрекъснато нараства. От 1990 г. повишението на смъртността средно на десетилетие е с 1 пункт на 1000 души. Особено висок е този показател в селата. Със стартово равнище от 18,6‰ през 1990 г. смъртността в селата нараства на 25,4‰ през 2008 г. В градовете този показател е съответно 9,4‰ и 12,1‰ [9]. Ярко изразените различия в стойностите на смъртността в градовете и селата са едно от най-силните доказателства за неравенствата между населението в двата типа населени места. Съществени са различията в общата смъртност и от гледна точка на регионалното разпределение на населението. Показателят сочи твърде големи различия в отделните региони за планиране [14], [15], [16].

Инвалидност. За общия брой на лицата с увреждания в България може да се съди по данните от преброяването през 2001 г., или като се изведе индиректно и сравнително точно от данните на НОИ. Така може да се твърди, че относителният дял на инвалидите в България във времевия интервал януари 2001 г. − юни 2009 г. се движи от 4,8% до 6,4% от общия брой на населението [15].

Три други репрезентативни изследвания през последните години сочат определени данни за инвалидността сред младите хора. Интерпретирайки емпирични данни от различни източници може да се твърди, че почти всеки 10-и млад човек в България е с увреждане - *регистриран или самоопределил се*, и изпитва сериозни или средни по тежест ограничения във възможностите да извършва своите ежедневни дейности и да изпълнява присъщите за него социални роли.

Една от основните причини за съществуването на увреждванията / инвалидността са хроничните заболявания. Данните от изследването „Взаимоотношения между поколенията и половете", и от двете вълни ясно показват тази тенденция [2], [3].

Двата основни недостатъка на здравната система, пораждащи социална несигурност и тласкащи населението на България в полето на неверие към националната сигурност са - неефективност и несправедливост.

Реформата в здравеопазването доведе до значителен финансов натиск върху домакинствата, особено като се има предвид влошения здравен статус на населението. Ниското равнище на доходи на населението затруднява достъпа до здравеопазване. Това се отнася особено за бедните и уязвими слоеве от него. Особено затруднен е достъпът на представителите на етнически малцинства.

Крайно недостатъчни са средствата НЗОК за покриване стойността на лекарствата. По данни на Европейската Федерация на фармацевтичната индустрия българските пациенти, в сравнение с тези от останалите европейски страни, плащат за лекарства относително най-много от собствения си джоб - 56%, т.е. само 44% се покриват от НЗОК. Средно за ЕС това съотношение е 18 към 82%.

Всичко това налага извода, че бедните, ако искат да се лекуват стават по-бедни, а ако се откажат от лечение стават по-болни. Това изключително дълбоко подкопава националната сигурност.

Формиране на рискови групи в обществото

В резултат на социалните конфликти в българското общество се формират т.нар. *рискови групи,* които са събирателен образ на тези конфликти и които подкопават социалната сигурност.

Формирали се в рамките на сегашното състояние на обществото те представляват сериозна заплаха за националната сигурност, поради което е необходимо дългосрочно да бъде прогнозирано тяхната екстраполация в бъдещето. Без да се претендира за изчерпателност, по надолу са описани по-характерните рискови групи на българското общество.

Лица с асоциално поведение

Теоретично могат да бъдат дефинирани различни и разнообразни социално-демографски сегменти, чрез които се подпомага разбирането и вникването в дадени процеси на националната сигурност [10], [11].

Анализът на *извършителите на престъпления* (за разлика от други анализи) не може да се направи задоволително, ако пропуснем да интерпретираме тенденциите и като абсолютни величини. Това е вторият аспект на анализ, за който стана дума по-горе. Необходимостта от подобен анализ произтича от факта, че предмет на анализ са не само дялове и тенденции, а и човешки личности, всяка с уникални характеристики.

Настъпилата през 1989 г. промяна на политическата система е довела институциите, отговорни за броя на осъдените лица (полиция, съд, прокуратура и т.н.) да изпаднат във вакуум и практически да сведат работата си до функционален минимум както по отношение на непълнолетните, така и по отношение на пълнолетните извършители на престъпления. Това създава впечатление за състоянието на нефункционалност.

Извънбрачни съжителства, извънбрачни деца, самотни майки

През последните десетина години традиционно набираните данни за структурата и състава на семействата и домакинствата започнаха да се обогатяват с данни за предпочитаните форми на съжителство. Така според преброяването на населението от 01.03.2001 г. в съжителство без брак живеят 314 718 души. По официални данни през 2009 г. са сключени 25 923 юридически брака, които са с 3 717 по-малко от тези през 2007 г. Намалението на броя на сключените бракове води и до намаляване на коефициента на брачност - от 3.9‰ през 2007 г. на 3.6‰ през 2008 година и 3,1 ‰ през 2014 г., което се дължи предимно на разпространението на т.нар. фактически партньорства.

Формира се устойчива *тенденция на нарастване на абсолютния и относителния дял на извънбрачно родените деца.* По данни на НСИ средногодишния темп за нарастване на техния брой е близо 4% .

Считано от 2000 г. насам, най-характерният процес е формирането и утвърждаване на *нов тип семейно поведение* в страната – *съжителство с партньор без официално сключен брак*.

В рамките на населението като цяло официалният юридически се запазва като масово предпочитаната форма на съжителство за българското население. Съжителството без брак варира в относително тесни граници –между 7,2% и 7,6% [2], [3].

Възрастни хора

Нарастване делът на възрастното население е глобален проблем, но в българските условия той има отношение към националната сигурност. По – надолу са дадени някои специфични характеристики на проблемите, свързани със застаряването на българската нация. Извън грубата статистика, следва да се подчертае на първо място и това, че този процес е свързан с различни отношения, в които са свързани възрастните хора.

София е областта с най-висок относителен дял на населението в трудоспособна възраст – 66.5%, следват областите Благоевград и Смолян с по 64.7%. С най-нисък дял на населението в трудоспособна възраст е област Видин – 54.8%.

Нарастващият дял на хората над 65-годишна възраст поставя сериозни предизвикателства пред социалноосигурителната система, системата за социално подпомагане, здравеопазването и образованието, които по същество са елементи, върху които почива националната сигурност на България.

Безработни хора

Въпреки постигнатия напредък през последните 10 години и създаването на законови гаранции, все още съществуват редица предизвикателства и проблеми в областта на заетостта, социалната закрила, бедността и социалното включване.

Съотношението безработни жени : мъже е 54.7%:45.3% (при 54.6%:45.4% през 2010 г., 57.7%:42.3% през 2009 г. и 62.5%:37.5% през 2008г.) [14], [15], [16].

Обезкуражените лица на възраст 15-64 навършени години са 13.3% от икономически неактивните лица в същата възрастова група.

Основните два проблема в областта на заетостта, които подкопават националната сигурност са: *1.Високо ниво на безработни и икономически неактивни лица, с ясно изразена диференциация по региони.* Липсата на заетост е една от основните причини за увеличаване на бедността, предоставянето на социалните помощи и социалната изолация; *2.Изолиране на определени социални групи от пазара на труда.* Предлагането на работни места е изключително ограничено за нискоквалифицираните лица, хората с увреждания, имигрантите, лицата, живеещи продължителен период от време в социална изолация и бедност.

Бедни хора

Икономическата криза през последните години задълбочава проблемите в социалната система. Броят на хората под прага на бедност расте, като в края на 2014 г. е над 25% процента от населението на страната). Размерът на социалните помощи и обезщетения, изплащани от НОИ, е нараснал 6 пъти през последното десетилетие – от 169 милиона през 2001 г. до 1 150 милиона през 2014 г. В същото време, социалната среда се е влошава, като делът на бедните след социалните трансфери, насочени към тях, продължава да нараства.Тези данни и обстоятелства неимоверно подкопават социалната и национална сигурност на страната.

Показаната теоретична и емпирична информация насочват към обосноваването на следните **обобщения и изводи:**

1. Социалната сигурност, като фундаментална част от националната сигурност предполага: гарантиране на индивида и семейството срещу рискове, които е възможно да настъпят при тяхното съществуване; създаване предпоставки за сигурност на индивидите и семействата, че равнището и качеството на техния живот няма да бъдат сериозно нарушени, доколкото това е възможно, при евентуално възникване

на икономически и социални рискове; тя предполага осигуряване не само на финансови средства, но и система от услуги за обслужване на населението.

2. В прехода към пазарна икономика непрекъснато се увеличава броят на индивидите и семействата, нуждаещи се от социална сигурност, което изисква и разработване на ефективни механизми в тази връзка.

3. Секюритизираните социални конфликти, представляващи заплаха за националната сигурност са: систематично намаляване на раждаемостта; нарастването на относителният дял на извънбрачните живородени спрямо всички живородени деца; високата смъртност; намаляване на относителният дял на младите генерации и се увеличаване делът на възрастните; различията в равнището на раждаемостта сред населението от отделните етнически групи води до днешните различия между етническия състав на децата и младежите и на населението като цяло; недоброто икономическо и здравно състояние, социалната изолация, несигурността. формирането и утвърждаването на нов тип семейно поведение - съжителство с партньор без официално сключен брак и др.

ЛИТЕРАТУРА:

1. **Ангелов, А.,** Системата за национална сигурност в новите условия. София, 2000
2. **Бюлетини на НОИ** 2000 – 2014
3. **Взаимоотношения между поколенията и половете**, Социално-демографско изследване, София, БАН, 2004
4. **Емелянов, С., Езеров, В.,** Исследовательские методы научно-технического прогнозирования, /обзор/, МЦИНТИ, Москва, 1974
5. **Милина, В.,** Политически аспекти на сигурността, 2003, Министерство на отбраната, ВА „Г.С. Раковски", София, 2003
6. **Моргунов, Е.В.,** Метод «Форсайт» и его роль в управлении технологическим развитием страны, Глава коллективной монографии «Проблемы развития рыночной экономики», под ред. чл.-кор. РАН В.А. Цветкова, М.: ЦЭМИ РАН, С. 97-113, 2011
7. **Население 2005**, НСИ, София, 2006
8. **Нива за средноевропейски достижения в образованието и обучението** (Bench markes). Решение № 8981 на Съвета на министрите на Европейския съюз от 7 май 2003 г.
9. **Преброяване на населението и жилищния фонд, 2001**, т. 6, кн. 4
10. **Престъпления и осъдени лица**, НСИ, 2001-2007
11. **Престъпления и осъдени лица**, София, НСИ, 1990-1991
12. **Рачев, В. и др**. Национална и международна сигурност. София, 2005
13. **Слатински, Н.,** Сигурността: същност, смисъл и съдържание, Изд. „Военно издателство" ЕООД, София, 2011 63
14. **Статистическа панорама**, НСИ, 2007
15. **Статистически годишник**, НСИ, 2007 – 2010
16. **Статистически справочник**, София, НСИ, 2010
17. **Marinker M.,** The Madrid Framework, Eurohealth 11(1): 2-5,200

18. **Walfers, A.,** National Security as an Ambiguous Symbol, in: Discord and Collaboration: Essays on International Politics. Johns Hopkins University Press, 1962, pp. 147-165 [210 Human Development Report 1994
19. **Human Development Report**, www.undp.org/hdro/e94over.htm

МЕНИДЖЪРЪТ И КРИЗАТА

Красимир М. Марков

Шуменски университет „Епископ Константин Преславски”
Педагогически факултет, катедра „Педагогика и управление на образованието”

THE MANAGER AND CRISIS

Krasimir M. Markov

ABSTRACT: *The article discusses the peculiarities of behavior and the role of the manager in a crisis in the organization*

KEY WORDS: *manager behavior, crisis*

Всяка една криза в зависимост от своя характер влияе по различен начин на обществото и на поведението на хората в него. Това, което е валидно като закони на поведение в обществото принципно се проявява и в организационна среда, което налага мениджърът в организацията да се съобразява с възможностите за действие в нови условия поставящи пред него сложни за решаване задачи влияещи много силно върху състоянието на организацията. Вече сме имали повод да описваме проблемите на антикризисното управление, но там става дума за мобилизиране на силите на организацията чрез управленски подходи с оглед превенция на криза. А тук става дума за това, че управлението преминава от антикризисно в екстремално, т.е. променили са се условията, кризата вече е настъпила, нейните последствия се чувстват осезаемо и трябва да се вземат бързи и нестандартни мерки. Тези нестандартни мерки се заключават в предлагането на също толкова нестандартни схеми свързани с управлението на производството, финансовия маркетинг, продажбите, персонала и т.н. в зависимост от структурата и особеностите на организацията. Видимо в условия на криза това от което трябва да се започне естествено е финансовата дисциплина, управлението на стагниращото производство и продажби, но в крайна сметка основната тежест в условия на криза пада върху управлението на персонала, тъй като хората пряко чувстват нейното влияние като страх от съкращение, намаляване на заплащането и т.н. [4].

За да обсъждаме поведението на мениджъра в условията на криза, както вече подчертахме това означава, че кризата вече е започнала следователно нейните реални последици се чувстват, което пък от своя страна означава, че е преминало

достатъчно време от нейното въздействие, за да се направят определени изводи и да се направи съответен анализ на кризисното управление.

Условията в България дават богата възможност за изучаване на поведението на мениджъри управляващи организации в състояние на криза. Нещо повече влошената социално-икономическа, демографска и екологична обстановка дава възможност да се проучи това поведение в условията на различни типове кризи, което пък от своя страна позволява да се направят обобщени изводи даващи най-обща представа какво би трябвало да бъде поведението на мениджъра при управлението на персонала в условията на криза. Бихме могли да откроим няколко характерни черти отличаващи поведението на мениджърите в условията на криза, които се заключават най-вече в следното [7]:

Първо – характерна черта на поведението на мениджърите проявяваща се в кризисния период, това е липсата на готовност на голяма част от тях да реагират адекватно на критичната ситуация. Периодът до 2002-2009 година се характеризираше с относителна стабилност и сравнително устойчиви темпове на развитие на страната, което позволи да се развият фирми и организации управлението на които се осъществяваше в тези относително спокойни условия. Мениджърите на тези нови организации не бяха както професионално, така и психологически готови към промяната на тези относително благоприятни социално-икономически условия в неблагоприятни, когато започна през 2009-2010 година и продължава и досега. Промяната наложи необходимостта да се вземат бързи и точни решения в различни аспекти на дейността включително и променяне на самия предмет на дейността на фирмите с оглед на тяхното оцеляване, и в това число разбира се, и в аспект на управление на персонала. Наложи се мениджърите да си отговарят на въпроси, които не си бяха задавали преди това и които можем да формулираме по следния начин – Какво да правим?; Какви решения да вземем?; Кое поведение би било най-ефективно? Някои от изследванията в световен мащаб [4] показват че много от мениджърите включително завършили и магистърска степен по бизнесадминистрация не са били подготвени и нямат познания затова как се изменя управлението при критични обстоятелства и какви методи да се приложат. Голяма част от тях, а и все още сега, приемат кризата като непредсказуемо явление, като стихийни действия на непреодолими сили. В действителност обаче икономическата теория учи, че кризите са предсказуеми и логично следват след фазата на ръст в условията на циклично функциониране на икономиката. Познаването на този икономически механизъм означава, че мениджърите от различните нива предварително следва да имат набелязан план не само за действието в условията на стабилното развитие, но и за действията в условията на криза. Ако такъв план съществува предварително и хората са запознати с него това означава, че ще имаме добри условия да съхраним психическата си устойчивост и да не допускаме грешки на незнанието.

Второ – като втори проблем налагащ се като извод от първия е, че не съществува необходимото бизнеспланиране, което да бъде насочено към постигане на определени тактически оперативни и стратегически цели. Неподготвеността на мениджърите, общо взето ни довежда до извода, че при настъпването на период на криза се появяват непредсказуеми проблеми, което затруднява поставянето на различните цели, а оттам прави планирането и прогнозирането на развитието на организацията невъзможни. Практиката обаче показва, че независимо от въздействието на такива непредсказуеми и непредвидими фактори, които затрудняват пос-

тигането на целите и по същество саботират постигането на плановете някои от планираните и посочените като цели достижения на организацията могат да бъдат осъществени и се осъществяват. Не бива да се пренебрегва и факта, че когато хората виждат една организация да работи по относително планов и целенасочен начин това влияе дисциплиниращо върху тяхното организационно поведение и в крайна сметка води до увереност в постигането на определените цели[1].

Трето – в условията на настъпила кризисна ситуация много мениджъри се опитват да намалят възнагражденията на работещия персонал. Независимо от съществуващите ограничения като наличието на минимална фиксирана работна заплата те могат да се заобикалят с назначаването на намален работен ден и др. Много често, за да се обоснове намаляването на заплатата мениджърите предлагат тактиката на заплаха, че е по-добре да намалят заплатата отколкото да съкратят човека. Изправени пред възможността да останат без работа голяма част от хората се съгласяват да работят при намалено възнаграждение. Това обаче води до няколко негативни последици, които най-общо бихме могли да опишем по следния начин, от една страна голяма част от персонала губи вярата, че организацията в която работи е способна да се справи с възможните предизвикателства, а от друга страна част от високо квалифицирания персонал започва да си търси друга работа и съответно възнаграждение, адекватно на квалификацията им [2].

Четвърто – следващият проблем, който възниква когато анализираме поведението на мениджърите в кризисна ситуация се заключава в неразумните съкращения на персонала. Естествено е, че има логика в условията на криза при намаляване на обема на произведената и реализираната продукция организацията да се освобождава от част от персонала. Проблемът е, че това освобождаване често се осъществява не на базата на един точен разчет, който да задържи квалифицираните и опитни кадри, а на базата на принципа обоснован от Захари Стоянов като „зетьошуробаджанакизъм" или пък по съвсем непонятни критерии, умозрително съставени от някой от ръководството. Практиката показва, че има много случаи, когато мениджъри освободили се от квалифицирани кадри много бързо осъзнават, че тяхната липса в организацията не само не решава, а съвсем задълбочава кризисната ситуация, но при опита да ги върнат отново на работа се оказва, че те вече са си намерили подходяща такава. Естествено е, че съществуват разнообразни методики и критерии за оценка на качествата на персонала, прилагането на които би позволило в условията на криза мениджърите да запазят квалифицирания и опитен персонал. За съжаление обаче тези технологии не се познават и не се спазват от мениджърите, особено от висшето ниво [3].

Пето – ако приемем, а то би трябвало да е така, че мениджърът е лидер в организацията то би следвало да се спазва един от принципите на лидерството, мениджърът със своето поведение да показва готовност за преодоляване на проблемите и давайки пример да мотивира персонала за борба с трудностите. За съжаление обаче част от мениджърите поради своята неподготвеност като квалификация от една страна и като психика от друга страна сами изпадайки в депресия губят възможност за оценка на перспективата, а оттам и своята вяра в бъдещето на организацията. По този начин те вместо да мотивират подчинените си създават дезорганизация и хаос тъй като най-вече в такъв момент проявяват принципи на невъздържаност, избухливост или малодушие, което пък от своя страна поставя под съмнение вярата на подчинените не само в организацията, а и в самия мениджър.

Оттук нататък каквито и обосновани решения те да предлагат на персонала, той или ще ги приема с големи резерви и съмнения, или директно ще ги отхвърля. Бедата е там, че непознавайки основите и идеите на лидерството мениджърите често го разбират като командване, но дори и самото командване означава, че заповедите, за да бъдат изпълнени правилно и точно трябва да бъдат облечени мотиви и цели.

Шесто – може би една от най-разпространените грешки в етап на криза е, че мениджърите страхувайки се да разкрият пред персонала действителните мащаби на случващото се, произтичащите от това проблеми и възможностите за тяхното разрешаване започват да крият информацията от подчинените си. Психологията учи, че отсъствието на информацията за хората се явява източник на фрустрация и стрес, което води до снемане на работоспособността. Опитът от екстремални и кризисни ситуации учи, че в своевременно и обективно предоставената оперативна информация на хората дава възможността за набелязване на реален план за действие, а в някои случаи включително и спасява човешки животи. Най-добрият подход би бил ако ръководителят предоставя тази информация на базата на лични срещи с персонала от всички нива. Така от една страна той е сигурен, че обективната информация е стигнала неизкривена до персонала от различните нива, а от друга страна това съкращаване на дистанцията показва на персонала загрижеността на ръководството. Естествено е, разбира се умния мениджър да прецени коя информация е необходимо да поднесе на подчинените от гледна точка на практическата полза за организацията [6].

Седмо – всичко казано дотук в крайна сметка опира до изключително важния проблем за мотивирането на персонала. И тук бедата е в непознаването от мениджърите от различните нива на възможните схеми и управленски подходи за мотивиране на персонала. В крайна сметка дори и това каква схема или какъв подход ще използваме зависи от самия мениджър, организационната структура и качеството на персонала, т.е. тук определени рецепти няма, а има творчество, но идеята при всички положения е в крайна сметка една, хората да разберат, че ръководството ги цени като специалисти и като личности, а оттам и да осъзнаят, че те са необходими на своята организация. Мотивирането на персонала би могло да се осъществи по метода на пробата и грешката, но това е труден метод, който от една страна изисква много време и натрупан опит, а от друга страна всички тези опити и грешки рефлектират върху членовете на организацията и трупат неверие във възможностите на ръководството [1].

Осмо – мениджърите в България в голямата си част не са любители на идеята да разходват средства за повишаване на квалификацията на персонала. Изключвайки така наречените тиймбилдинги, които не са нещо лошо, но имат много съмнителни цели в наши условия разходването на средства за квалификация на персонала като правило се счита за нещо излишно, най-малко поради идеята, че мениджърът счита, че ако му е необходим квалифициран служещ или работник може да си го намери на пазара на труда. В условията на криза на разходването на средствата за квалификацията на персонала общо взето се гледа като нещо не така разумно. Идеята всъщност на разсъжденията на мениджърите е уж логична, след като съкращаваме ресурсното обезпечение на организацията от гледна точка на финанси, персонал или техническо оборудване няма никакъв смисъл да влагаме средства за обучение и квалификация на персонала. Тази логика обаче практиката показва, че е

напълно погрешна, тъй като всяка криза би могла да се разглежда не само като проблем, бедствие и т.н., но и като възможност за разкриване на допълнителни ниши от една страна, а от друга страна това време на намалено производство или услуги, което означава и намалена заетост на персонала е съвсем разумно да бъде оползотворено за неговата квалификация и преквалификация за постигане на нови цели от всякакъв характер. Още повече, че се появиха обучаващи организации достатъчно квалифицирани да извършват тази услуга, а цената на услугата се снижи значително в сравнение с тези отпреди 10/15 години [4].

Всички коментираме колко трудни са условията за бизнес в България, необходимостта от чужди инвестиции, отпускане на европейски средства и т.н., оправдаваме се с кризата, която настъпи през 2009 и продължава и досега, но забравяме, че един основен елемент и може би най-важния за развитието на икономиката на страната е ефективният мениджмънт, който включително съдържа в себе си възможността за ефективно управление в условията на криза или кризисни ситуации. Съществува голямо количество информация базирана на световния опит включваща в себе си и умение да се реагира адекватно в условията на кризисната ситуация. Остава само мениджърския състав да осъзнае необходимостта от изучаването и прилагането на този опит, но видимо това в наши условия се оказва най-трудно.

ЛИТЕРАТУРА:

1. Бонева, М. Социална манипулация и сигурност, Сборник научни трудове на НВУ „В. Левски", Факултет „Артилерия ПВО и КИС", Шумен, 2014, с.75-81
2. Бонева, М., Г. Колев. Глобалната икономика и сигурността на държавата. Сборник научни трудове на НВУ „ В. Левски", Шумен, ч. II, 2013, с. 30 – 37.
3. Бонева, М., Г. Колев. Измерения на социалната криза в България. Сборник научни трудове на НВУ „В. Левски", Факултет „Артилерия ПВО и КИС", Шумен, 2014 ,с. 93-100.
4. Марков, К. Организация, управление, промяна. ВТ., 2014
5. Чередниченко, И., Тельных, Н. Психология управления. М., 2004
6. Щербатых, Ю. Психология стресса и методы коррекции. СПб., 2006

ЗА НЯКОИ ПРОБЛЕМИ НА ПСИХОЛОГИЧЕСКИЯ СТРЕС

Красимир М. Марков

Шуменски университет „Епископ Константин Преславски”
Педагогически факултет, катедра „Педагогика и управление на образованието”

ABOUT SOME PROBLEMS PSYCHOLOGICAL STRESS

Krasimir M. Markov

ABSTRACT: *Discuss peculiarities of emotional stress, the reasons for its occurrence and possible ways to overcome the consequences.*

KEY WORDS: *emotional stress, coping strategies*

Сравнително доскоро в България се обръщаше по-малко внимание на емоционалния или психическия стрес като основно се коментираше физиологичния механизъм на развитието на стреса и неговите последици в аспект на така наречените заболявания на стреса. Не можем обаче да не отчетем психичните последици възникващи в резултат на преживения стрес проявяващи се като посттравматично стресово разстройство, емоционално напрежение и рефлектиращи определени психични преживявания. Вероятно вниманието беше насочено към физиологичните последици от преживяването на стреса тъй като те по-пряко се чувстват както от потърпевши, така и от околните. Същевременно обаче трябва да подчертаем, че психическите последствия от преживения стрес са не по-малко значими за човека и неговото обкръжение. Дотолкова, доколкото стресовото преживяване на определена ситуация или стресор се поражда от обективни външни или вътрешни причини, но се преживява субективно е необходимо да изясним субективните причини за пораждането на емоционален стрес. Авторите изследвали този проблем [4] считат, че има де групи субективни причини предизвикващи стрес. Към първата група причини се отнасят тези, които имат относително статичен и постоянен характер, а във втората група се отнасят тези, които имат динамичен характер. Независимо от това обаче, и в двата случая стресът се предизвиква от разминаването между очакваните събития и реалността. Как бихме могли да групираме тези субективни причини.

Относително постоянни причини отнасящи се до трайните характеристики на личността на човека:

– несъответствие на човешките генетични програми на съвременните условия – вече е доказано, че повечето реакции, които човек проявява в резултат на биологични и физични въздействия имат рефлекторен характер и са генетично програмирани. Авторите занимаващи се с този проблем отчитат, че природата е подготвила човека за дейност в условията на повишено физическо натоварване, периодично гладуване и влияние на различни температурни разлики, докато съвременния човек живее в условия на уседналост, температурен комфорт и задоволеност от храна. Доказано е [3], че по своята природата хората са много устойчиви

към природни фактори, но проявяват повишена чувствителност към социалните фактори към които още не са изработени вродени механизми за защита;

– стрес предизвикан от реализация на негативни родителски програми – знаем, че част от програмите на поведението на човека се закодират в главата на детето от неговите родители, учители или други лица от времето когато детето приема външните въздействия безкритично. Независимо как ще наречем тези програми неосъзнати нагласи, житейски принципи или родителски сценарии, те оказват съществена роля върху по-нататъшния живот на човека. Тези нагласи могат да бъдат полезни за детето, но тогава, когато то расте и се променя в съответствие с условията на живот те често усложняват изпълнението на неговите социални роли правейки поведението неадекватно на тях и съответно предизвиквайки стрес [1];

– стрес предизвикан от механизмите на психологическа защита и когнитивния дисонанс – емоционалният стрес наричаме такъв, защото върху поведението на човека като източник на стрес влияят неговите емоции, които предизвикват спонтанни реакции независимо, че човек се опитва да си обясни нещата разумно и логично. Съвсем естествено е, че в този процес, за да оправдае възникналите емоции разума се стреми да използва псевдологични механизми, които обикновено наричаме механизми за психологическа защита. Ако детето използва така наречените примитивни механизми или още механизми от първи род, това би могло да бъде обосновано. Проблемът възниква тогава, когато зрелия човек използва тези примитивни механизми, тъй като не е успял да ги преработи в механизми от втори или висш вид;

– стрес предизвикан от неадекватни нагласи и убеждения на личността – човек по принцип разсъждава относително полярно – добро или зло, красиво или грозно и т.н. Съвършено естествено е, че условията на живот предизвикват и поява на оценка на явленията в околния свят делейки преживяванията на добри или лоши и съответно отношението на проява на оптимизъм или песимизъм. Нормално хората не са твърди оптимисти или твърди песимисти. Счита се, че [4] поведението на хората се проявява по така наречения закон на нормалното разпределение, т.е. хората могат да бъдат и оптимисти и песимисти в зависимост от ситуацията. Но при определени хора обикновено такива, които изповядват крайни религиозни или политически убеждения оценките стават полярни и нещата се виждат или прекалено оптимистични, или прекалено песимистично, което при ситуации на разминаване с обективната действителност довеждат до емоционален стрес;

– стрес предизвикван от невъзможността за реализация на актуални потребности – развивайки своята теория за потребностите и съответстващата им мотивация в резултат на определени изследвания Е. Маслоу структурира така наречената пирамида на потребностите. Независимо, че учени като Невис доказаха, че тази пирамида не е общовалидна навсякъде и потребностите могат да променят своята йерархия от значение е да отбележим факта, че дори и актуализирайки своите потребности по йерархия, ние винаги оценяваме тези, които са субективно важни за нас. Ако тази оценка на субективно важните потребности се срещне с невъзможността те да бъдат реализирани се поражда емоционален стрес. Разбира се когато коментираме това във връзка със статичните причини пораждащи психологическия стрес трябва да подчертаем, че тук оценката е върху така

наречените висши потребности по Маслоу свързани с принадлежност, уважение и себереализация;

– стрес предизвикван от неадекватна реализация на условните рефлекси – вече говорихме за програмите, които се закодират в човешкия организъм било генетично или в ранна възраст под влиянието на родителите или другите елементи на околната среда. Тук обаче става дума за програми изработвани в процеса на живота [2], така наречените условни рефлекси. В хода на нашия живот човешкия мозък се учи да разпознава сигнали, които посочват настъпването на важни за организма събития. Това са неща свързани с такива моменти в нашия живот като храненето, служебни взаимоотношения и т.н., сигналите за които човек възприема и след това действа по определен начин. Но ако тези сигнали се разминат с нашите очаквания това поражда дискомфорт в организма и съответно емоционален стрес;

– стрес породен от неадекватното разчитане на времето – една от най-честите причини за стреса са размитите времеви граници на психичното състояние. Това се случва ако човек отделя голямо емоционално значение на миналото или на бъдещето [5]. Разглеждайки този проблем А. Елкин определя следните признаци при които човек изпитва стрес породен от неефективното използване на времето: усещане за непрекъснато бързане; недостиг на време за хобито и общуването със семейството; постоянно закъсняване; отсъствие на план за разпределяне на времето; неумение да се делегират пълномощия на други хора; неумение да се откаже на хора отнемащи ни времето; периодично възникващо усещане за непълноценно или напразно използвано време [5].

Динамични причини, пораждащи възникването на психичния стрес:

– условията на работата и на живот са една от най-съществените динамични причини за възникването на стрес – тук могат да влязат преди всичко битовите проблеми свързани с необходимост от осигуряване на живота и бита, възможни ремонти, семейни отношения, транспортни проблеми свързани с придвижване до работно място или до роднини, родители и т.н., проблеми свързани с работата, несигурност на работното място, ниско или рядко заплащане, информационно претоварване или недостиг на информация и т.н. Както и проблеми свързани с географските и екологичните особености на населеното място – замърсяване, запрашаване, периодични наводнения и др.;

– политически и икономически фактори предизвикващи емоционалния стрес – преките икономически причини влияещи върху пораждането и появата на емоционален стрес рефлектират върху от една страна повишените разходи за обезпечаване на ежедневното съществуване, възникването на непредвидени разходи или невъзможност за връщане на кредити с много висока лихва, което съчетано с ниските доходи, безработицата и несигурността за собственото бъдеще естествено поражда емоционален стрес. Към политическите причини пораждащи такъв стрес бихме могли да споменем най-общо неефективна политическа власт както на държавно, така и на общинско ниво и неефективна държавна политика в областта на икономическите реформи, законодателството и т.н.;

– извънредни обстоятелства – към извънредните обстоятелства отнасяме факти и явления, които натоварват екстремално човешката психика, ограничават възможността на човек да реагира и по този начин водят до появата на психичен или емоционален стрес. Това могат да бъдат природни катастрофи, бедствия,

технически аварии, криминални посегателства и престъпления, и тежки заболявания.

Възможни пътища за преодоляване на емоционалния стрес

Независимо от различните причини пораждащи емоционалния стрес съществуват определени пътища или методи за преодоляване на вредното му влияние. Съвсем естествено е, че тези методи и пътища би следвало да се подбират в зависимост от причините породили стреса. За стресорите от първа група видимо е необходимо от една страна да освободим съзнанието си от травмиращата ситуация, а от друга страна да преразгледаме своето отношение към неприятните факти и да ги преоценим. В зависимост от човека би могло да се използват различни техники като медитация, съсредоточаване върху дишането, масаж на раменете, рационализация или посещение на психотерапия. За преодоляване на стресорите от втората група най-адекватни ще са методите насочени към усъвършенстване на поведенските навици включващи тренинг на общуването, тренинг на управление на времето и разбира се тренинг за формиране на увереност в собствените сили. Автори като Щербатых разпределят методите на проявление на стреса съобразно типа на стресорите в следните варианти [4]**:**

Област на мъдрото възприемане:

- релаксация на раменния пояс;
- дълбоко дишане;
- визуализация;
- рационална терапия;
- рефрейминг.

Област на конструктивните действия:

- избор на правилна стратегия;
- поставяне на адекватни цели;
- тренинг на социалните навици;
- тренинг на увереност в себе си;
- тренинг на управление на времето;
- използване на принципа на Парето.

Област на субективния стрес:

- преодоляване на оценъчния подход;
- формиране на навици за позитивно мислене;
- промяна на неадекватните убеждения;
- блокировка на нежелани мисли;
- рационална терапия.

Област на саморегулирането:

- автотренинг;
- невролингвистично програмиране;
- тренинг за увереност в себе си;
- релаксация;
- дишане;
- биологична обратна връзка.

Независимо какъв подход ще изберем, за да търсим възможност за преодоляване на последствията от емоционалния стрес е необходимо да осъзнаем, че добра е тази копинг стратегия, която помага на организма да се справи с

нежеланите последствия, което означава в крайна сметка, че всеки сам следва да прецени и подбере тази стратегия, която действа при него. Освен това е необходимо да се запомни и това, че за да се набележи ефикасна лична стратегия за преодоляване на емоционалния стрес. Човек трябва да осъзнае причините, които са го породили и обстоятелствата при които той е възникнал, както и степента на отражение на тези обстоятелства в емоционалната и поведенската му сфера. Само тогава набелязаните лични стратегии ще бъдат ефикасни. В противен случай съществува реалната опасност личността да си набележи „стратегии" като алкохолизъм, наркомания, агресивно поведение и др.

ЛИТЕРАТУРА:

1. Бонева, М. Социална манипулация и сигурност, Сборник научни трудове на НВУ „В. Левски", Факултет „Артилерия ПВО и КИС", Шумен, 2014, с.75-81
2. Судаков, К. В. Индивидуальная устойчивость к стрессу. М., 1998
3. Чередниченко, И., Тельных, Н. Психология управления. М., 2004
4. Щербатых, Ю. Психология стресса и методы коррекции. СПб., 2006
5. Элкин, А. Стресс для „чайников". М., 2005

НЯКОИ ПРОБЛЕМИ НА ПСИХОФИЗИОЛОГИЧНИТЕ ОСНОВИ НА УПРАВЛЕНИЕТО

Красимир М. Марков

Шуменски университет „Епископ Константин Преславски"
Педагогически факултет, катедра „Педагогика и управление на образованието"

SOME PROBLEMS OF PSYCHOPHYSIOLOGICAL MANAGEMENT BASICS

Krasimir M. Markov

ABSTRACT: *Discuss the impact of fatigue on performance and psycho-physiological characteristics of man in normal conditions and in estremalni*

KEY WORDS: *management, psychophysiology, performance, fatigue*

Човекът като активно и действащо същество си поставя конкретни цели и работи за тяхното изпълняване при конкретните ситуации. Изпълнението на тези цели освен организация на дейността изисква и конкретен разход на енергия, която зависи от функционалното състояние на човека към момента. Функционалното състояние се описва на основата на появата, изменението и проблемите във функционирането на физиологичните системи на организма, има се предвид централната нервна система, сърдечно-съдовата система, двигателната, ендокринната и т.н., както и сривовете при протичането на психичните процеси и субективните прежи-

вявания на човека. В литературата се е наложило следното определение на функционалните състояния: „Функционалното състояние на човека се разбира като интегрален комплекс от характеристиките на тези функции и качества на човека, които пряко или косвено обуславят изпълнението на дейността“.

Състоянието на човека е винаги уникално, тъй като се определя от конкретната ситуация и наличието на много други субективни фактори. Тази уникалност предопределя многообразието на частните случаи на функционално състояние, но независимо от това в литературата се определят някои общи категории функционални състояния:

- състояние на нормален живот и дейност;
- гранични състояния;
- патологични състояния.

За критерии служещни за класифициране на определено функционално състояние към някои от посочените групи ни служи от една страна качеството и надеждността на извършената дейност, а от друга цената на тази дейност измерена като разход на физически, материални ресурси, време и т.н. Затова разглеждането на едно или друго функционално състояние към определен клас налага разглеждането на всеки един отделен частен случай. В литературата се разглежда пример със състоянието „умора“, счита се, че това състояние не бива да се разглежда като недопустимо за организма независимо, че води до снижение на ефективността на дейността и се явява очевидно следствие на изразходвани психофизиологически ресурси. Прието е да се смята, че недопустима се явява такава степен на умора, при която ефективността на дейността преминава долните граници на надеждността на дейността или се появяват симптоми на натрупване на умора водещи до обща преумора на организма.

Както при проблема със стреса, така и тук прекомерното напрежение на физиологичните и психичните ресурси на човека е потенциален източник на възникване на заболяване. Това е и критерия, който разделя нормалните от патологичните състояния, които са обект на изследване от медицината. Тъй като споменахме одеве за преумората трябва да кажем, че тя се явява основа на патологично състояние от невротичен тип. Това налага категориите психофизиологични състояния отнасящи се към граничния тип да бъдат считани за недопустими тогава, когато се планира, организира и осъществява определена дейност. Това означава, че те изискват при възникването си провеждането на съответните психофизиологични мерки при разработването на които непосредствено участие трябва да вземат и психолозите.

Според друга класификация на функционалните състояния, използваща като критерий ответната реакция на човека на изискванията на изпълняваната дейност. Съгласно тази класификация функционалните състояния на човека се делят на две групи:

- състояние на адекватна мобилизация;
- състояние на динамично разсъгласуване.

Състоянието на адекватна мобилизация се характеризира със съответното напрежение на физиологичните и психичните сили на човешкия организъм насочени към реализацията на определена дейност. Ако това напрежение премине нормалните граници и доведе до претоварване на организма се появява състоянието на динамично разсъгласуване. Това се случва като правило когато усилията на орга-

низма превишават изискванията на определената дейност за нейното извършване. Разбира се в тази класификация на основата на двете полярности, които посочихме можем да поместим между тях всички функционални състояния на работещия човек. Анализът на състоянието на човека в процеса на продължително изпълнявана дейност като правило се провежда с проучване на фазите на динамичната работоспособност, вътре в които вниманието се насочва върху характерните особености на формирането и развитието на умората. Това дава отговор на въпроса защо инженерната психология, екстремалната психология и ергономията поставят в центъра на предмета на изучаването си работоспособността и умората. Те приемат, че умората е естествено състояние на организма възникващо при нарастване на напрежението в хода на продължително извършвана работа. То физиологична гледна точка наличието на умора е свидетелство за изтощение на вътрешните сили на организма и преминаването на същия към по-неизгоден за него начин на функциониране. Като пример можем да посочим усиленото сърцебиене, за да нарасне обема на кръвотока, засилват се двигателните реакции, което води до нарушение на устойчивостта на отделните вегетативна функции, което води до затруднение при изработването и осъществяването на условните рефлекси и се осъществява върху цялостното състояние на организма. С нарастването на умората се наблюдават значителни изменения в протичането на различните психични процеси [ ]: повишават се абсолютния и диференциалния праг на чувствителността; нараства продължителността и яркостта при последователните образи; намалява се скоростта за реакция и т.н. Същевременно умората води до разпад при изпълнението на сложните двигателни навици. Най-ярко се проявяват признаците на умора с нарушението на вниманието, снижава се неговия обем, затруднява се превключването и разпределението му. Разбира се умората влияе и върху процесите осигуряващи запомнянето и съхранението на информация. Доказано е, че умората води до затруднение при извличане на информация, която се съхранява в дълговременната памет. Наблюдава се и снижаване на показателите за качеството на работа на кратковременната памет. Всичко това затруднява процеса на мисленето, което се насочва към стереотипни способи за решаване на задачите и ситуациите в случаи, когато се изисква творчество за тяхното решаване, а от друга страна се нарушава и целенасочеността на интелектуалния акт.

Всичко изброено дотук неминуемо довежда до трансформация на мотивите за дейността. Ако на ранните етапи на умората все още се съхранява така наречената делова мотивация, в последствие тя преминава в мотиви за прекратяване на дейността или бягство от нея, ако дейността продължи това води до формиране на отрицателна емоционална реакция.

Авторите изучаващи този проблем [ ] определят при анализа на трудовата дейност четири етапа на работоспособност:

- етап на преработване;
- етап на оптимална работоспособност;
- етап на умора;
- етап на последния порив.

След приключването на тези етапи започва така нареченото разсъгласуване на трудовата дейност. За възстановяване на оптималното ниво на работоспособност следва да се прекрати предизвикващата умора дейност за толкова време, колкото е необходимо за пасивен и активен отдих. Ако продължителността на този период на

почивка е недостатъчен за организма настъпва натрупване на умора. Като първи симптом на хроничната умора можем да отчетем някои своеобразни субективни усещания заключаващи се в: чувство за постоянна умора; повишена уморяемост; сънливост; вялост и бавност и т.н. В началните етапи на развитието на хроничната умора тези обективни признаци са слабо проявени, но за настъпването на хроничната умора можем да съдим по това, че все по-кратки стават фазите на оптимална работоспособност и все по-дълга необходимостта от почивка.

Занимавайки се с този проблем учените [ ] са стигнали до извода, че за изследване на състоянието на работещия човек се използва категорията напрежение. Степента на напрежение на дейността се определя от структурата на процеса на труда в частност от интензивността, наситеността и натовареността на трудовата дейност. От тази гледна точка напрегнатостта се разглежда като изискване предявено от конкретните видове труд към човека. От друга страна напрежението на дейността може да се опише с психофизиологични загуби, които вече описахме като цена на дейността и които са необходими за постигане на поставените цели.

Приема се, че има две основни категории състояние напрегнатост:

- специфична – определяща динамиката и интензивността на психофизиологичните процеси и стояща в основата на изпълнението на конкретните видове дейност;
- неспецифична – характеризираща общите психофизиологични ресурси на човека и осигуряваща като цяло нивото на изпълнение на дейността.

Като логичен извод от проблема за умората и неговото влияние върху човешкия организъм възниква работоспособността. В повечето случаи тя се разбира като способност за работа в определен ритъм за определено количество време [ ]. Характеристика на работоспособността е нервнопсихичната устойчивост, темпа на дейността и умората на човека.

Естествено е работоспособността да е променлива величина, която има предел, който зависи от конкретни условия:

- здраве;
- качество на храната;
- възраст;
- резервни възможности на човека (сила и подвижност на нервната система);
- санитарно-хигиенни условия на труда;
- професионална подготовка и опит;
- мотивация.

Счита се, че сред задължителните условия осигуряващи работоспособността на човека и предотвратяващи преумората, важно място заема доброто редуване на труда и почивката. Този режим трябва да бъде установен при отчитане на особеностите на конкретната професия, характера на изпълняваната дейност, конкретните условия на труда и индивидуално-психичните особености на хората участващи в трудовия процес. От това в крайна сметка зависи честотата, продължителността и съдържанието на почивките в хода на работния ден.

Екстремалните условия налагат и своя специфика върху дейността извършвана в подобни ситуации. Към екстремални условия на дейността отнасяме следните:

- монотонност – самите физиологични особености на мозъка посочени още от Сеченов и Павлов сочат, че за работоспособно състояние на главния мо-

зък е необходима минимална сума от раздразнения влияещи върху висшия отдел на големите полукълба;

- изменение на възприятието на пространствените структури – под пространствена ориентировка се разбира способността на човека да оценява своето положение според насочеността на силата на тежестта и според различните обкръжаващи го обекти. Тези компоненти са функционално тясно свързани, но съществуват условия при летците, космонавтите при които тази ориентировка се губи, което изисква от организма повишена степен на напрежение, пораждаща стрес и същевременно много висока степен на подготовка и тренировка на организма за пространствено-времева ориентация в условия различни от обичайните;
- ограничена информация – в екстремални условия се наблюдават няколко възможни ограничения на постъпващата към човека информация, от една страна ако тези условия се заключават в изолация за продължително време на такъв човек му липсва информацията за близките, при което се развива състояние на тревожност и депресия и се нарушава съня. Друг възможен вариант на недостиг на информация е когато тя е на различен от езика, който ползваме, което затруднява нейното обработване и разбиране. В такива случаи говорим за информационен глад;
- самота – продължителната самота неизбежно предизвиква изменение в психичната дейност. Случаи с хора останали сами на необиктаеми острови, на ледени късове или лодки в океана показва, че при тях се развива депресия. Същевременно говорейки за така наречената „психоза на старите моми“ Е. Кречмер определя като една от причините за нейното възникване относителната изолация. По тази причини реактивни състояния и халюцинации могат да се развият не само при посочените случаи, но и при самотни пенсионери, вдовци и т.н.;
- групова изолация – в състояние на групова изолация попадат хора при експедиции в сложни условия в относително откъснати краища по земното кълбо. При тях характерно е развитието на конфликтността, агресивността, развиващи се в психологично състояние, когато и най-спокойния човек се ядосва, озлобява се и накрая преминава в ярост, тъй като неговото полезрение непрекъснато се стеснява от механизма на афекта и в обкръжаващите го започва да вижда само недостатъците. В крайна сметка като резултат се увеличава броя на изолираните и отхвърлени членове на групата;
- заплаха за живота – всяка една теория за определяне на риска се основава на допускането, че всеки вид човешка дейност съдържа в себе си възможността за аварии и катастрофи. Заплахата за живота влияе по специфичен начин на психичното състояние на хората. Възниква психично напрежение обусловено от необходимостта доколко дейността, която извършваме е безопасна.

Тези фактори действащи в екстремални ситуации не действат изолирано, а като правило в съвкупност, което още повече утежнява тяхното въздействие върху човешкия организъм. За тяхното преодоляване е необходимо човешкия организъм в някаква степен да се адаптира към определените екстремални условия.

Независимо от конкретните проявления на екстремалните условия психичната адаптация към екстремални условия и реадаптация към обичайните условия преминава през следните етапи:

- подготвителен;
- стартово психично напрежение;
- остри психични реакции на входа;
- преадаптация;
- завършващо психично напрежение;
- остри психични реакции на изхода;
- реадаптация.

Етапът на преадаптация при определени обстоятелства може да се смени с етап на дълбоки психични изменения. Между тези два етапа лежи етапа на неустойчивата психична дейност.

В заключение на обсъждането на проблема за работоспособността и умората бихме могли да кажем още един техен ключов елемент. В крайна сметка хората дори натрупващи знания и опит, остаряват. Естествено, че това понижава работоспособността и повишава уморяемостта, което налага определен начин на организация на дейността на застаряващия персонал. При всички случаи трябва да различаваме биологичното от календарното стареене. Като решаващо значение за човека и неговата работоспособност има биологичното стареене.

В хода на човешкия живот организма се подлага на въздействия, които предизвикват съответните изменения в биологичната структура на организма и в нейните функции. Времето, когато се появяват структурни и функционални изменения характеризира отделните възрастови групи, но в крайна сметка е индивидуално за съответния човек. Това означава, че с нарастването на възрастта могат да се получат съществени различия между биологичната и календарната възраст на човека. Доказано е, че рационалната трудова дейност на възрастния човек позволява той по дълго да съхрани работоспособността си, да отложи биологичното стареене чувствайки се полезен за определен човек или за организация.

ЛИТЕРАТУРА:

1. Бонева, М. Социална манипулация и сигурност, Сборник научни трудове на НВУ „В. Левски”, Факултет „Артилерия ПВО и КИС”, Шумен, 2014, с.75-81
2. Бонева, М., Г. Колев. Глобалната икономика и сигурността на държавата. Сборник научни трудове на НВУ „В. Левски”, Шумен, ч. II, 2013, с. 30 – 37.
3. Бонева, М., Г. Колев. Измерения на социалната криза в България. Сборник научни трудове на НВУ „В. Левски”, Факултет „Артилерия ПВО и КИС”, Шумен, 2014 ,с. 93-100.
4. Марков, К. Организация, управление, промяна. ВТ., 2014
5. Чередниченко, И., Тельных, Н. Психология управления. М., 2004
6. Щербатых, Ю. Психология стресса и методы коррекции. СПб., 2006

МЕДИЙНИ ДОБРИ ПРАКТИКИ ЗА ИНФОРМИРАНОСТ НА ОБЩЕСТВОТО ПО ПРОБЛЕМИТЕ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Веселин Ц. Целков **Сибила К. Кусева**

УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ
ГР. СОФИЯ, 1784, БУЛ. "ЦАРИГРАДСКО ШОСЕ" 119

MEDIA GOOD PRACTICES FOR PUBLIC AWARENESS ON PERSONAL DATA PROTECTION ISSUES

Veselin Ts. Tselkov **Sibila K. Kuseva**

UNIVERSITY OF LIBRARY STUDIES AND INFORMATION TECHNOLOGIES

SOFIA, 1784, BLVD. "TSARIGRADSKO SHOSE" 119

***ABSTRACT**: The report presented the media best practices of the Commission for Protection of personal data for public awareness on the issues of personal data protection in the Republic of Bulgaria. Based on the strategic principles and priorities are defined directions and mechanisms for informational impact. Many media good practices are presented such as the use of websites, social networks and blogs, other services from the Internet, commercials and spots brochures and more. A perception is derived that the media should be viewed not only as a corrective, but also as a tool to influence society and one of the main factors contributing to the proper functioning of the personal data protection system.*

***KEY WORDS:** Post-quantum cryptography, Lattice-based cryptography, Hash-based cryptography, Code-based cryptography, Multivariate-quadratic-equations cryptography*

„Суверенитетът на общността, региона, нацията, държавата има смисъл само ако произтича от единствения истински суверенитет – суверенитета на човешкото същество." – Вацлав Хавел

ВЪВЕДЕНИЕ

Информацията и знанията в съвременното общество се превръщат в основни продукти и определят характера на развитието на цивилизацията. Затова и съвременният етап на развитие на човечеството се нарича етап на Информационното общество. В него доминираща роля играят комуникационните и информационни технологии. Характерни са следните особености:

- Засилване на ролята на информацията в живота на обществото;
- Нараства броят на заетите в информационните технологии, комуникациите и в производството, както и делът на информационни продукти и услуги;
- Нараства проникването на телефони, радио, телевизия, Интернет;
- Нараства влиянието на средствата за масова информация;
- Като част от процеса на глобализация се създава глобално информационно пространство, осигуряващо на хората по-ефективно взаимодействие и лесен достъп до световните информационни ресурси.

Част от информационното пространство заема и информацията за защита на неприкосновеността и личните данни на хората в Република България.

2. ИНФОРМИРАНОСТ НА ОБЩЕСТВОТО

Информираността на обществото е непрекъснат процес.

Стратегически принципи и приоритети в работата на Комисията за защита на личните данни през годините

- ...
- Информираност на обществото
- Обучение
- …

Основни проблеми

- Не знание за проблема със защита на личните данни
- Не оценяване на важността и заплахите
- Не познаване на нормативната база
- Не знание какво да се прави при нарушаване на правата

Направления за въздействия

- Хората
- Органите на държаната власт и местното самоуправление
- Частните фирми и компании

Механизми

- Използването на медиите

Необходимо е те да се разглеждат не само като коректив, но и като инструмент за въздействие върху обществото и един от основните фактори способстващи за правилното функциониране на системата за защита на личните данни.

  - Електронни
  - Други
- Интернет
  - Web-страницата на КЗЛД
  - Социалните мрежи
  - Материали и банери в най-популярните страници
  - Връзки между страницата на КЗЛД и страниците на:
    - Държавните институции
    - Браншовите организации
    - Неправителствените организации
- Информационен бюлетин
  - Новите тенденции
  - Промените в регулаторната рамка
  - Практиката на КЗЛД
- Връзки с неправителствени и браншови организации
  - Програма „Достъп до информация”
  - ...

- Семинари
  - Журналисти
  - Главни секретари на министерства и ведомства
  - Браншови организации
- Примери
  - Видео клип
  - Специално приложение в Web-страницата на КЗЛД
  - Информационни брошури

o Специално пощенско клеймо „28 януари - Европейски ден на защитата на личните данни"

  - Дни на отворените врати
  - Публични лекции с академичната общност
  - Съвместни и/или изнесени заседания
  - Информационно-рекламни материали
  - Магнитни носители
- Информационни брошури

Информационните брошури могат да бъдат с обща насоченост или насочени към отделни целеви групи

  - 10 години КЗЛД
  - Вашата лична карта
  - Видеонаблюдение
  - Интернет и децата
  - Съвети за родители
  - Вашето Шенгенско пространство
- Съвместни и/или изнесени заседания
  - Срещи
    - С областни управители и кметове
    - Тематични – КРС, КЗП и др.
  - Открити заседания
  - Пресконференции с журналисти

o Отворени врати за среща с граждани и администратори на лични данни

  - Обучение

o Приложение на Закона за електронните съобщения (дискусии със заинтересованите страни по места - прокуратура, съдии и др.)

- Информационно-рекламни материали с бранд: **„2012 година - 10 години Комисия за защита на личните данни. 28-ми януари - Европейски деня за защитата на личните данни"** - брошури, тефтери, значки, плакети, чаши, химикалки, календари, както и преносими памет-устройства (flash memory) с информационно съдържание.
- Магнитни носители

3. ЗАКЛЮЧЕНИЕ

В доклада са представени част от добрите медийни практики на Комисията за защита на личните данни за информираност на обществото по проблемите на защитата на личните данни в Република България. На базата на стратегическите принципи и приоритети са дефинирани направленията и механизмите за информа-

ционно въздействие. Представени са множество добри медийни практики, като използването на електронни страници, социални мрежи и блогове, други услуги от интернет пространството, рекламни клипове и заставки, информационни бюлетини, брошури и др. Изведено е разбирането, че е медиите да се разглеждат не само като коректив, но и като инструмент за въздействие върху обществото и един от основните фактори способстващи за правилното функциониране на системата за защита на личните данни. Част от резултатите се използват в тематични курсове в Университета по библиотекознание и информационни технологии и са основа на различни изследвания.

ЛИТЕРАТУРА

1. Денчев С., Информационна среда за трансфер на технологии, Издателство "Захарий Стоянов", 166 стр., София, 2003 год.

2. Денчев, С., Ц. Семерджиев, И. Попов, Н. Костова. Концепция и политика за информационна сигурност. Част 2. Библиографски указател. Изд. «За буквите – О письменехь» , София, 2008 г., 496 стр., ISBN-978-954-8887-36-6.

3. Семерджиев, Ц. Сигурност и защита на информацията. - С.: Софттрейд, 2007 г. – 228 стр., ISBN-978-954-327-034-7.

4. Семерджиев, Ц. Стратегически информационни системи. - С.: Софттрейд, 2007 г. – 440 стр., ISBN-978-954-334-052-1.

5. Целков, В., Сигурността и защита на личните данни в процеса на глобализация, СВУБИТ, Научна конференция „Глобализация и сигурност", 6 юни 2009 г.

6. Целков, В. Модели на защитени взаимодействия в компютърни системи и мрежи, За буквите – О писменехь, София, 2008, 234 стр.

7. Държавен вестник, Република България

ФИНАНСОВА СИГУРНОСТ ИЛИ СИГУРНОСТ НА ФИНАНСОВАТА СИСТЕМА - КОНЦЕПЦИЯ ЗА ИЗСЛЕДВАНЕ

Станимир Ст. Станев

Университет по библиотекознание и информационни технологии. Институт за научни изследвания и обучение на докторанти (ИНИОД), гр. София

FINANCIAL SECURITY OR SECURITY OF THE FINANCIAL SYSTEM - CONCEPT STUDY

Stanimir St. Stanev

***ABSTRACT**: In the research I will discuss two different type of concept study on the financial security.*

***KEY WORDS**: financial security; financial system.*

Интересът към изследване на сигурността е безспорен. Без нейното детайлно разглеждане, трудно бихме изследвали и деривативните категории, като национална сигурност, икономическа, финансова и др. видове сигурност. Естествено, всяка субкатегория от множеството на сигурността изисква и поставянето му в конкретното отношение към цялото с всички необходими връзки.

Действащото законодателство на Република България не съдържа определение за финансова сигурност, поради тази причина е необходимо научно-теоретичното осмисляне на това понятие, като обществено явление или в по-тесен смисъл, като икономическа категория.

Дуализмът в изследването на финансовата сигурност, от една страна, се проявява в изучаване на обективните защитни свойства на финансовата система, като механизъм за противодействие на влиянието на опасни фактори и сили, а от друга страна, са охранителните функции на държавата и създадените за тази цел институции.

Тази двупосочност в дефинитивното определяне „полето на действие“ на финансовата сигурност, поставя и разграничителна черта към концепцията за нейното изследване, от перспектива на повече социално или повече икономическо съдържание и структура. Акцентът ще е: финансовата сигурност научна категория от общата теория на националната сигурност ли е или финансовата сигурност, е сигурност на финансовата система и това ограничава изследователската рамка предимно в макроикономически измерения.

Като отправна точка при изследване на финансовата сигурност, би могло да се използва етимологичния ракурс.

Както следва от самата фраза "финансова сигурност", понятието е съставно и представлява два отделни термина "финанси" и "сигурност", всеки от които носи специфично значение. Финанси (на латински: *financia* — наличност, доход) - един общ икономически термин, който има за базис- финансови средства и ресурси,

разглеждани в тяхното създаване, движение, разпределение, преразпределение и използване.

Съвременното разбиране за финансите е парични отношения, които изразяват процесите, свързани с формирането и разходването на фондовете на държавата, от стопанските субекти и индивидите. Дейността на държавата, свързана със събиране, разпределение (преразпределение) и използването на държавни и общински средства, е финансова дейност на държавата. Икономическите отношения, които тя поражда, могат да бъдат диференцирани в зависимост от формите и методите на събиране, и разпределение на тези средства. Група от еднородни отношения образуват финансовите институти. Съвкупността от финансовите отношения и връзките между тях образуват финансовата система.

Финансовата система е интегриран елемент на икономическата система обслужваща икономическите субекти, които имат излишък или недостиг на парични средства. Това е и най-използваното структурно определение за финансовата система на една страна, което обаче има няколко ограничения, тъй като се отнася само за финансовата система и нейните институционални елементи. Такъв едностраннен подход не отразява функционалната основа, и съответно функционалната структура на финансовата система, като система, която осигурява натрупването, разпределението и преразпределението на средства от различни икономически субекти (държави, организации, домакинства), които функционират по различен начин.

В българската литература преобладава функционалния подход към съдържанието на финансовата система. Финансовата система се разглежда в два аспекта:

1) като съвкупност от финансови институти, т.е. съвкупност от различни видове парични отношения;

2) като съвкупност от държавни органи и институции.

По този начин основа за тълкуването на финансовата система, се базира на принципа на разделяне на различните функционални области и дялове на конкретни финансови взаимоотношения.

Понятието "сигурност" като комплексно многостранно и социално явление е тясно свързано с взаимодействието в системата „природа-човек/личност/-общество“. Взаимодействието, води до развитието на всички обекти от обкръжаващата действителност.

Съществуват голям брой оригинални дефиниции и подходи за изследване на категорията сигурност, където акцентът или основата е поставена върху такива характеристики, като: система, съвкупност от отношения, защитеност, способност, съвкупност от условия и фактори , безопасност и др[1,2].

Обзора на научната литература свързан със сигурността ни води към извода, че полиаспектното разглеждане на сигурността е факт. Към момента са известни поне пет групи дефиниции за понятието сигурност:

- първата група включва дефиниции, характеризиращи сигурността, като състояние на защитеност на интересите на личността, обществото и държавата;
- втората, като свойство на системата;
- третата разглежда сигурността, като съвкупност от държавни органи изпълняващи специфична дейност;
- четвърта характеризира сигурността, като отсъствие на заплаха или опасност;
- пета дефинира сигурността, като определено състояние;

Различните дефиниции ни дават основание да твърдим, че съществуват няколко основни подхода за изследване на сигурността.

Първият подход се основава на обектното разбиране на сигурността, като проява на обектите да запазят своята устойчивост при различни негативни влияния. Именно в този контекст, сигурността се разбира като определено свойство /атрибут/ на системата.

Вторият подход се основава на подчертаване на субективния характер на сигурността. Субективното разбиране на сигурността през призмата на ценността и интереса.

Третият определя сигурността, като състояние [3] и по-широкото разбиране, като състояние на защитеност[4].

Като обект на изследване на сигурността би следвало да бъде и обкръжаващата среда. Нито личността, нито обществото, нито държавата може да бъде с гарантирана сигурност без да се гаранитра сигурността на обкръжаващата среда.

Обект на изследване на сигурността, би следвало да бъде и социалния ред, като система от отношения и институции, и обществено съзнание. Корелирайки с обекта на изследване на финансовата сигурност на Р.България, в съвременни условия, обект на изследване би следвало да бъдат системата от финансови отношения и институции, чиято основна и определяща съставна част е валутния борд.

В съвременната научна литература, изследваща проблемите на сигурността се наблюдават и два ясно различими контекста при избор на подход.

Първият се основава на сравнение на сигурността с несигурността, тяхната диалектика и семантическа определеност. При този подход сигурността се възприема, като хипотетично отсъствие на опасност или заплаха, като защитеност и способност да се противодейства на заплахи.

Вторият разглежда сигурността в по-широк смисъл от гледна точка на вътрешната организация, функционирането и саморазвитието на даден обект. Тук сигурността се разглежда, като свойство на обекта и система за саморазвитие.

От теоретично познавателна гледна точка и двата контекста на изследване на сигурността са принципно непротиворечиви и допълващи се при изследване на сигурността като социален феномен. При определянето на заплахите и опасностите обаче, изборът на определен контекст е ключов и определящ впоследствие при разработването на механизъм за защита.

Разглеждайки финансовита сигурност в широк и тесен смисъл, и анализирайки тази категория от гледна точка на социално-икономическото или само икономическото, се обосновава изводът, че задължителен подход е изследването на финансовата сигурност от гледна точка на общата теория на сигурността и нейното място, като елемент на националната сигурност.

Това се налага по три основни причини:

- първата е свързана с фундаменталността на категорията сигурност, нейната многостранност и всеобхватност на множеството от съдържателни отношения и форми на външни прояви и взаимодействия с други явления от обективната реалност.

- втората, с разбирането за финансовата сигурност като изследователски обект, трябва да се базира на естеството на финансовата система, но без да се ограничава само в своите дистрибуторски функции на преразпределение и натрупване на финансови средства и ресурси.

- третата е, че сигурността като научна категория поставя по-сериозни изисквания към корелиращите с нея обекти на изследване, като в случая с финансовата сигурност трансформира и изискване за качество на функциониране на финансовата система.

Всичко това позволява да се обобщи, че всички гореспоменати гледни точки относно концепцията за финансова сигурност, като системно явление, предполага известно сходство по отношение на параметрите му с другите видове сигурност. Това дава възможност да се подчертаят някои основни елементи:

На първо място, финансовата сигурност е неразделна част от системата за национална сигурност;

На второ място, изследването на проблемите на финансовата сигурност са с основен предмет на защита финансовите дейности на държавата;

Трето, обществените отношения във финансовата сфера се регламентират от правни норми и се гарантират от държавни институции;

Четвърто, състоянието на обществените отношения във финансовия сектор, трябва да осигури надеждна защита на "националните интереси" на държавата.

ЛИТЕРАТУРА

1. Прохожев А. А. Национальная безопасность: к единому пониманию сути и терминов // Безопасность. 1995. N 9. С. 11 и др.
2. Глебов И. Н. Национальная безопасность Российской Федерации: проблемы правового регулирования. СПб., 1999. С. 45 и др.
3. Бельков О. А. Понятийно-категориальный аппарат национальной безопасности // Безопасность. 1994. N 3. С. 91 и др
4. Степашин С. В. Безопасность человека и общества (политико-правовые вопросы): Монография. СПб., 1994. С. 6 и др.
5. Дидык В. Финансовая безопасность в системе экономической безопасности государства. В: Закон и жизнь, 2009.
6. Дидык В. Вопросы правового регулирования в области обеспечения финансовой безопасности США. В: Закон и жизнь, 2009.
7. Абалкин Л. Экономическая безопасность России: угрозы и их отражение. В:Вопросы экономики. 1994.
8. Абдурахманов М. Основы национальной безопасности России. Под общей редакцией Манилова В.Л. М.: Друза. 1998.
9. Аксенов В., и др. Мировой финансовый кризис и экономическая безопасность России: анализ, проблемы и перспективы. М.: Экономика. 2010.

БОРБАТА С НЕЛЕГАЛНОТО РАЗПРОСТРАНЕНИЕ НА НАРКОТИЦИ И НАРКОТРАФИКЪТ В СВЕТА

Велико П. Петров **Николай Й. Досев**

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

COMBATING ILLEGAL DRUG DISTRIBUTION AND DRUG TRAFFICKING IN THE WORLD

Veliko P. Petrov **Nikolai J. Dosev**

ABSTRACT: *This report aims to acquaint the reader with the fight against illegal distribution of drugs and drug trafficking in the world. Recent years brought new challenges regarding drugs - increases the dynamics of the emergence of new psychoactive substances appear new chemicals for their production, new ways of trafficking and innovative distribution channels. Drug phenomenon is a matter of national and international significance and combat it must be fought globally. To limit the supply of drugs crucial importance targeted, coordinated and effective action by law enforcement authorities at national, regional and international levels. There are new instruments that will: target major criminal networks for cross-border drug trafficking by exploring minimum common aggravating or mitigating circumstances; improve the definition of offenses and sanctions, and thirdly, they would introduce higher requirements for reporting by Member States.*

KEYWORDS*: the fight against illegal distribution of drugs, and drug trafficking, psychoactive substances.*

Още в началото на човешкото развитие започва историята и на разпространението и употребата на наркотици (в религиозните обреди, в медицината и бита на хората), като ги превръща в съставна част от живота, а също възниква и проблемът с тяхната злоупотреба. Разрешение на този проблем търсим и днес. По данни на Службата на ООН за борба с наркотиците и престъпността, изнесени в последния й доклад за наркотиците за 2014 г., средно около 243 милиона души по света на възраст от 15 до 64 г. или близо 5,2% от възрастното население. Злоупотребата с наркотици е определяна като „бедствие за отделния индивид" и „социална и икономическа опасност за човечеството". Щом съществува такъв проблем, ще се търсят и мерките, които ще са в състояние да го ограничат или да намалят вредите и рисковете, които той поражда.

Употребата, движението и контролът върху наркотичните вещества са обект на международното законодателство. Първа стъпка в това направление е свиканата през 1909 г. Шанхайска конференция по опиума. В работата й вземат участие представители на 13 страни, които си поставят за цел да се предотврати нелегалния внос на наркотици в Европа и САЩ от азиатския район. Положено е началото на международния контрол, дава се тласък на международното сътрудничество и правна помощ в тази насока, но липсват конкретни норми и договорености за ограничаване употребата и разпространението на наркотици.

Следващите усилия са конференцията в Хага от 1912 г. и приетия първи документ „Международно споразумение за опиума". Независимо от международните проекти и сътрудничество, консумацията се увеличава драстично и не се постига използване на наркотиците предимно за лечебни и научни цели. Следва споразумението от Женева (1925 г.), допълнено през 1931 г. с нови мерки за контрол. Създаден е и Консултативен комитет по борбата срещу търговията на опиум и други опасни за здравето на човека лекарствени вещества, като през 1946 г. неговите функции преминават към Комисията по упойващите вещества на Организацията на обединените нации (ООН)[3].

Усилията и волята на редица държави да ограничат нелегалното разпространение на наркотици водят до приемането на международни конвенции, които въвеждат мерките за контрол върху упойващите и психотропни вещества. Ядрото на международния забранителен режим спрямо наркотиците може да се посочат договорените под егидата на ООН следните три акта:

– Единната конвенция по упойващите вещества от 1961 г.;

– Конвенцията за психотропните вещества от 1971 г.;

– Конвенцията на ООН за борба срещу незаконния трафик на упойващи и психотропни вещества от 1988 г.

Изискванията на тези документи са въведени в националните законодателства на страните, които са ратифицирали конвенциите. Република България е ратифицирала и трите международни конвенции в областта на контролираните субстанции. Те са разработени от Световната здравна организация (СЗО) и приети от Общото събрание на ООН по предложение на Фармацевтичния отдел на световната организация. Списъците с веществата, обект на контрол по смисъла на конвенциите периодично се обновяват, като включват вещества, за които е доказано че:

– предизвикват състояние на зависимост;

– имат стимулиращо или депресивно въздействие върху централната нервна система (ЦНС), предизвикват халюцинации или нарушения на двигателната активност, мисловната дейност, поведението, възприятията или настроението;

– с тях се злоупотребява или имат вредно въздействие, представляващо проблем за общественото здраве и обществото.

Приетата през 1961 г. и допълнена през 1972 г. **„Единна конвенция за упойващите вещества"** е създадена от 73 държави с цел да се въведе единен международен документ за контрол на упойващите вещества и да се осигури контрол над производството и суровините. Счита се, че е необходимо да се въведат ефикасни мерки за борба с наркотиците от държавите членки, и че действията на международната общност трябва да бъдат координирани и да се ръководят от едни и същи принципи с оглед запазване физическото и морално здраве на човечеството. „Незаконен трафик" означава култивирането или всеки трафик на упойващи вещества, които противоречат на целите на тази конвенция.

Подписана във Виена през 1971 г. „**Конвенция за контрол на психотропните вещества**" има същите цели, както и конвенцията за упойващите вещества, а именно - да обедини усилията на държавите в борбата срещу злоупотребата с психотропни субстанции. Като психотропна субстанция се дефинира всяка субстанция от природен или синтетичен характер, включена в четирите части на конвенцията,

[3] Контрол на упойващи и психотропни вещества. Политики за ограничаване разпространението на наркотични вещества, http://www.pharmfac.net/Lectures_Social_pharmacy_Doc_Getov/4_Lecture_Narcotics%20control%20and%20prevention.pdf

а препарат е всеки разтвор, смес или всяко физично състояние, съдържащо една или повече психотропни субстанции. „Незаконен трафик" означава фабрикацията или трафикът на психотропни вещества, извършвани в нарушение на разпоредбите на тази конвенция.

В Член 20 са дадени „Мерки срещу злоупотребата с психотропни вещества" и те са:

1) Страните вземат всички подходящи мерки за предотвратяване злоупотребата с психотропни вещества и за навременното разкриване, лечение, превъзпитаване, постлечебно наблюдение, възстановяване на трудоспособността и социалната реинтеграция на засегнатите лица и координират усилията си за постигането на тези цели.

2) Страните съдействат, доколкото е възможно, за подготовката на кадри в областта на лечението, постлечебното наблюдение, възстановяването на трудоспособността и социалната реинтеграция на лицата, които злоупотребяват с психотропни вещества.

3) Страните съдействат за запознаване на лицата, на които това е необходимо в работата, с проблемите на злоупотребата с психотропни вещества и предотвратяването й, а също така съдействат за запознаване на населението с тези проблеми, ако съществува опасност, че злоупотребата с тези вещества може да вземе широки размери.

В Член 21 съдържа „Борба срещу незаконния трафик". Като отчитат надлежно своите конституционни, правни и административни системи, страните:

a) осигуряват в национален мащаб координация на дейността по предотвратяване и преследване на незаконния трафик; за тази цел би било полезно те да определят подходяща служба, която да отговаря за тази координация;

b) взаимно си оказват съдействие в борбата срещу незаконния трафик на психотропни вещества и по-конкретно незабавно предават на другите пряко заинтересувани страни по дипломатически път или чрез компетентните органи, определени от страните за тази цел, копие от всеки доклад, изпратен от тях до генералния секретар съгласно чл. 16 във връзка с разкриването на случай на незаконен трафик или с изземване;

c) тясно си сътрудничат помежду си и с компетентните международни организации, в които те членуват, с цел да водят координирана борба срещу незаконния трафик;

d) осигуряват оперативното осъществяване на международно сътрудничество между съответните служби, и

e) осигуряват в случаите, когато за целите на съдебно преследване се налага предаване между страни на съдебни документи, предаването на адреса на определените от страните органи да става оперативно; тази разпоредба не нарушава правото на страните да изискват съдебните документи да им бъдат изпращани по дипломатически път.

Тези две конвенции кодифицират материята, свързана с борбата с незаконната търговия с наркотици и психотропни вещества и очертават насоките за сътрудничество между държаните по този проблем. В чл. 354 от НК на Република България се предвижда наказание лишаване от свобода до 10 години и глоба за извършителите на тези престъпления. В Иран, Ирак, Малайзия и други страни не само за разпространение, но и за употреба на наркотици се предвижда смъртно наказание.

Третата конвенция „**Конвенция за борба срещу незаконния трафик на упойващи и психотропни вещества**" от 1988 г. Съставена и подписана във Виена на 20 декември 1988 г., конвенцията влиза в сила от 11.11.1990 г. Към 1 януари 2005 г., има 170 страни които са страни по нея, сред които и Република България (обн. ДВ. бр.89 от 19 октомври 1993 г.). Тя се отнася за прекурсорите и химичните вещества често използвани при незаконното производство на упойващи вещества и психотропни субстанции под международен контрол.

През 2009 г. са приети Политическа декларация и План за действие на ООН за международно сътрудничество за постигане на интегрирана и балансирана стратегия за справяне с международния проблем с наркотиците, в която се казва, че намаляването на търсенето и предлагането на наркотици са взаимно подсилващи се елементи на политиката за борба със забранените наркотични вещества, както и политическата декларация на ООН относно ХИВ/СПИН.

През последните 15 години Европейската комисия спомогна за изготвянето на цялостен и балансиран отговор на Европейския съюз (ЕС) на проблема с наркотиците в рамките на стратегията на ЕС за наркотиците (2013-2020 г.). Двата основни правни инструмента на ЕС в областта на политиката срещу наркотиците - за трафика на наркотици[4] и за появата на нови наркотици (нови психоактивни вещества)[5] - са съответно от 2004 и 2005 г. През последните години обаче се появиха нови предизвикателства: нови начини на трафик на наркотици и на химикали, използвани за тяхното производство („прекурсори на наркотични вещества"), бързата поява на нови наркотици и иновационни канали за разпространение на тези нови вещества.

В Плана за действие за изпълнение на Програмата от Стокхолм за периода 2010-2014 г.[6] Европейската комисия пое ангажимент да приеме мерки за засилване на защитата срещу тежките престъпления и организираната престъпност. Сега, след като Договорът от Лисабон вече е влязъл в сила, отговорът на Европа на проблема с наркотиците трябва да бъде силен и решителен, като бъде насочен както към търсенето, така и към предлагането на наркотици. Новите законодателни актове, в чието приемане ще участва Европейският парламент и които ще бъдат изпълнени от държавите-членки, ще бъдат подложени на контрол от Европейската комисия и в крайна сметка от Съда на Европейския съюз. Комисията се ангажира да даде нов тласък на политиката на ЕС за борба с наркотиците. В предложението си „Бюджет за стратегията „Европа 2020" Комисията обещава финансова подкрепа, за да може да се отговори на бъдещите предизвикателства, които поставят наркотиците. Бюджетът на ЕС трябва да бъде насочен към финансиране на дейностите, които имат ясна добавена стойност, които включват: борба с новите наркотици, разработване на иновационни практики за превенция или лечение и трансгранично сътрудничество в областта на правоприлагането и обучението[7].

[4] Рамково решение 2004/757/ПВР на Съвета от 25 октомври 2004 г. за установяване на минималните разпоредби относно съставните елементи на наказуемите деяния и прилаганите наказания в областта на трафика на наркотици, ОВ L 335, 11.11.2004 г., стр. 8—11.

[5] Решение 2005/387/ПВР на Съвета от 10 май 2005 г. относно обмена на информация, оценката на риска и контрола върху новите психоактивни вещества, ОВ L 127, 20.5.2005 г., стр. 32–37.

[6] Европейският съвет на 10-11 декември 2009 г. прие Програмата от Стокхолм, която представлява цялостна рамка за инициативи в областта на правосъдието и вътрешните работи. С цел превръщането на тези политически цели в конкретни предложения Комисията подбра няколко ключови действия, които трябва да приеме през периода 2010—2014 г., COM(2010) 171 окончателен.

[7] Съобщение на комисията до Европейския парламент и до Съвета, Към по-решителен европейски отговор на наркотиците, Брюксел, 25.10.2011, COM (2011) 689 окончателен

В Европейския съюз нормативната уредба за борба с нелегалното разпространение на наркотици и наркотрафика е следната:

– Рамково решение 2004/757/ПВР на Съвета от 25.10.2004 г. за установяване на минималните разпоредби относно съставните елементи на наказуемите деяния и прилаганите наказания в областта на трафика на наркотици, ОВ L 335, 11.11.2004 г.;

– Решение 2005/387/ПВР на Съвета от 10.05.2005 г. относно обмена на информация, оценката на риска и контрола върху новите психоактивни вещества, ОВ L 127, 20.5.2005 г.;

– Директива на Съвета 92/109/ЕИО от 14.12.1992 г. за производство и пласиране на пазара на някои вещества, използвани при незаконното производство на наркотици и психотропни вещества;

– Директива 2001/8/ЕО на Комисията от 08.02.2001 г. за замяна на приложението към Директива 92/109/ЕИО на Съвета за производството и реализацията на някои вещества, използвани за незаконно производство на наркотици и психотропни вещества;

– Регламент (ЕО) № 273/ 2004 на Европейския парламент и на Съвета от 11 февруари 2004 г. относно прекурсорите на наркотичните вещества;

– Регламент (ЕО) № 111/ 2005 на Съвета от 22 декември 2004 г. за определяне на правила за мониторинг на търговията между Общността и трети страни в областта на прекурсорите;

– Регламент (ЕО) № 1277/ 2005 на Комисията от 27 юли 2005 г. за установяване на правилата за прилагане на Регламент (ЕО) № 273/ 2004 на ЕП и на Съвета относно прекурсорите на наркотичните вещества;

– Регламент (ЕО) № 111/ 2005 на Съвета за определяне на правила за мониторинг на търговията с прекурсори на наркотични вещества между Общността и страни извън Общността;

– Регламент на Комисията (ЕО) № 260/2001 от 08.02.2001 г. заменящ Приложението към Регламент на Съвета (ЕИО) № 3677/90 за въвеждане мерки за прекратяване отклоняването на определени субстанции с цел незаконно производство на наркотични средства и психотропни вещества;

– Регламент (ЕИО) № 3769/92 на Комисията от 21.12.1992 г. за прилагане и изменение на Регламент (ЕИО) № 3677/90 на Съвета относно определяне на мерки, които трябва да се предприемат с цел да се ограничи отклоняването на някои вещества за незаконно производство на наркотични и психотропни вещества;

– Регламент (ЕИО) № 3677/90 на Съвета от 13.12.1990 г. относно определяне на мерки, които трябва да се предприемат с цел да се ограничи отклоняването на някои вещества за незаконно производство на наркотични и психотропни вещества;

– Решение 2001/419/ПВР на Съвета от 28.05.2001 г. за предаване на проби от контролирани вещества;

– Решение на изпълнителния комитет от 22.12.1994 г. за сертификата по член 75 за пренасяне на наркотици и/или психотропни вещества;

– Стратегия на ЕС за борба с наркотиците (2013-2020 г.).

В стратегията на ЕС за борба с наркотиците са предвидени, за периода 2013-2020 г., всеобхватната политическа рамка и приоритетите за политиката на ЕС за борба с наркотиците, определени от държавите-членки и институциите на ЕС. До

2020 г. приоритетите и действията в областта на забранените наркотични вещества, подпомагани и координирани посредством стратегията на ЕС за борба с наркотиците, следва да са постигнали цялостен ефект върху основните аспекти на положението с наркотиците в ЕС. Те следва да осигурят високо равнище на защита на здравето на хората, социална стабилност и сигурност чрез съгласувано, ефективно и ефикасно прилагане на мерки, интервенции и подходи за намаляване на търсенето и предлагането на наркотици на национално, европейско и международно равнище и чрез свеждане до минимум на потенциалните косвени отрицателни последици от изпълнението на тези действия.

На европейско равнище рамката за координирани действия се състои от законодателството на ЕС в областта на наркотиците и многогодишните стратегии и планове за действие. Националните правителства и националните парламенти носят отговорността на национално равнище за приемането на необходимите за решаване на проблемите с наркотиците законодателни, стратегически, организационни и бюджетни рамки.

През 1999 г. с целта да уреди обществените отношения, свързани с контрола върху наркотичните вещества и прекурсорите, в съответствие с изискванията на международните договори, по които Република България е страна, от българското правителство е приет „**Закон за контрол на наркотичните вещества и прекурсорите" (ЗКНВП),** изменян и допълван многократно**,** последно изм. ДВ. бр.53 от 27 Юни 2014 г. Законът е напълно хармонизиран и съгласуван с Единните конвенции на ООН за упойващи и психотропни вещества, конвенцията за борба с незаконния трафик на вещества и прекурсори и Европейското законодателство.

С този закон Република България урежда:

1) Организацията, правомощията и задачите на държавните органи осъществяващи контрол върху производството, преработването, търговията, употребата, съхранението, вноса, износа, превозването и отчетността на наркотични вещества;

2) Мерките срещу злоупотребата и незаконния трафик с наркотични вещества и прекурсори;

3) Научноизследователската и експертна дейност, свързана с наркотични вещества и прекурсори за тяхното производство.

Наркотично вещество е всяко упойващо и психотропно вещество, включено в приложенията на закона, което може да предизвика състояние на зависимост и има стимулиращо или депресивно въздействие върху ЦНС, предизвиква халюцинации или нарушения в двигателната функция, мисловната дейност, поведението, възприятието и настроението, както и други вредни въздействия върху човека.

Наркотичните вещества са разделени на две главни групи в закона, според риска, които носят за общественото здраве: вещества с висока степен на риск и рискови вещества. Освен това в Закона са определени също:

– всички растения, съдържащи упойващи и психотропни вещества, забранени за използване в страната;

– вещества, използвани при производство на упойващи и психотропни вещества, класифицирани като прекурсори.

През последните години в редица страни от ЕС се наблюдават тенденции на развитие на наркопазара към разпространение и употреба на наркотични вещества, които не са поставени под контрол и забрана, съгласно нормативната уредба, т. нар. „дизайнерски наркотици". В резултат от това страните най-силно засегнати от

проблема като Великобритания, Румъния, Прибалтийските републики предприеха законодателни мерки за поставянето на въпросните вещества под контрол. Това създаде предпоставки престъпни групи, разпространяващи „дизайнерските дроги" да се установят и осъществяват дейността си в България.

Поради обществената значимост на проблема и по-бързото поставяне на нови вещества под контрол се направиха промени в закона, обн. в ДВ бр.61 от 09.08.2011 г. като е издадена „**Наредба за реда за класифициране на растенията и веществата като наркотични**" , която е в сила от 10.11.2011 г. Основна предпоставка за иницииране на законодателни промени е наложилата се през последните две години в Р. България трайна тенденция в насока увеличаване трафика и разпространението на нови психоактивни вещества, т.нар. „дизайнерски наркотици".

Наказателният кодекс на Република България съдържа редица разпоредби, претърпели значително развитие от 1975 г. досега, особено с измененията през 2000 и 2002 г., инкриминиращи деяния, свързани с режима на наркотичните вещества, техни аналози или прекурсори, включително и действия в престъпна група. Престъпленията срещу правната уредба на наркотиците, Наказателният кодекс (в чл.354 и чл. 242) предвижда няколко групи такива деяния. Първата група обхваща деянията, свързани с разпространението на наркотици. Втората група престъпления включват неразрешеното придобиване или държане на наркотични вещества и техни аналози. Третата група престъпления са свързани с нарушаване на установени правила за работа с наркотични вещества. Четвъртата група престъпления са свързани с подтикването на други лица към употреба на наркотици. Петата група престъпления обхваща даването на смъртоносна доза от наркотично вещество на друго лице. Шестата група престъпления са свързани със създаването на условия за употреба на наркотични вещества. Седмата група престъпления обхващат различни случаи на отглеждане на растения с цел производство на наркотични вещества. Последната група престъпления обхваща трафика на наркотични вещества. В тази група попада преди всичко пренасянето на наркотични вещества през границата на страната без надлежно разрешение.

Други документи уреждащи обществените отношения, свързани с контрола върху наркотичните вещества и прекурсорите в Р. България са:

1) Правилник за организацията и дейността на Националния съвет по наркотичните вещества, приет с ПМС № 91 от 7.04.2011 г., Обн. ДВ бр. 31 от 15.04.2011г.;

2) Наредба № 7/2001 г. на министъра на здравеопазването, за условията и реда за издаване на разрешителни за внос и износ на наркотични вещества и техните препарати (Обн. ДВ. бр. 17 от 25.02.2011 г.);

3) Наредба за условията и реда за разрешаване на дейностите по чл. 73, ал. 1 от ЗКНВП приета с ПМС № 122/09.05.2011 г., обн. ДВ, бр. 38/17.05.2011 г.;

4) Наредба № 8 от 07.09.2011 г. за условията и реда за осъществяване на Програми за психосоциална рехабилитация на лица, които са били зависими или са злоупотребявали с наркотични вещества (Обн. ДВ. бр. 75 от 27.09.2011 г.);

5) Правилник за функциите и организацията на Експертния съвет по лечение на зависимости (Обн. ДВ. бр. 34 от 29.04.2011 г.)

Противодействието на производството, разпространението и търговията с наркотични вещества, както и за ограничаване на наркопрестъпността в страната, е

особено актуално с оглед изпълнението на Националната стратегия за борба с наркотиците и Плана за действие по нейното прилагане, както и във връзка с реализиране на ангажиментите, произтичащи от Стратегията на ЕС за борба с наркотиците. Трафикът, разпространението и употребата на наркотици в страните от Европейския съюз, включително и в България, следват общо установените в световен мащаб тенденции. Борбата с наркопрестъпността в България е първостепенен приоритет в работата на Министерството на вътрешните работи. Противодействието на престъпленията, свързани с наркотици, е организирано в съответствие с Националната стратегия за борба с наркотиците, която се основава на балансиран и всеобхватен подход към синхронно атакуване на проблемите на търсенето и предлагането на наркотични вещества[8].

От казаното до тук могат да се направят следните изводи:

1. За организираната наркопрестъпност е задължително да бъде съобразена с някои общи признаци, които я определят като „класически" тип организирана престъпност като:

– тя е съвкупност от престъпления, свързани с наркотици в сферата на производството, трафика и разпространението;

– функционира посредством престъпната дейност на лица, професионално заети в конкретно противоправно действие;

– извършителите на наркопрестъпления са обединени в трайни (устойчиви), организирани и добре защитени формирования;

– формированията във всяка една от сферите на нарко-бизнеса може да съществува самостоятелно, със своя специфична структура;

– отделните формирования могат да бъдат подструктури или разклонения на престъпна система на регионално, междурегионално и транснационално равнище.

2. Трафикът на наркотици представлява незаконна търговия, която включва производството, дистрибуция и продажба да вещества, забранени от закона. Всъщност той е многослоен проблем и не се ограничава само до производството и реализацията, но обхваща и други аспекти, засягащи както националната, така и международната сигурност. Наркотрафикът е част от трансграничната престъпност, от реализацията на наркотици се финансират терористични организации, той е и престъпление, предикатно на изпирането на пари.

3. Наркопрестъпността и нейното негативно влияние в много сфери на обществения и социалния живот се отнасят към факторите, застрашаващи сигурността и здравето на обществото. Тя е един от престъпните феномени, оценявани като заплаха за страните от Европейския съюз. Трафикът на наркотици и свързаното с него разпро странение са едни от най-доходоносните престъпни дейности, които имат структуроопределящо значение за организираната престъпност като цяло[9].

4. Последните години поднесоха нови предизвикателства, касаещи наркотиците – нараства динамиката на поява на нови психоактивни вещества, появяват се нови химикали за тяхното производство, нови начини на трафикиране и иновационни разпределителни канали.

---

[8] Информация от МВР относно „Противодействие на незаконния трафик, производство и разпространение на наркотични вещества и прекурсори", *www.mvr.bg/NR/rdonlyres/03AD6773-BABE-46B5-993B.../0/*

9 Димитър Георгиев, "Трансгранична престъпност и международно сътрудничество", Национална конференция, 30 и 31 януари 2012 г., Централен военен клуб – гр. София, стр.3.

5. Явлението наркотици е въпрос от национално и международно значение и борбата с него трябва да се води в световен мащаб. За ограничаване на предлагането на наркотици ключово значение имат целенасочените, координирани и ефективни действия на правоприлагащите органи на национално, регионално и международно ниво.

6. Предлагат се нови правни инструменти, които ще:

- бъдат насочени към големите престъпни мрежи за трансграничен трафик на наркотици, като бъдат разгледани минималните общи утежняващи или смекчаващи обстоятелства;

- подобрят дефинициите на престъпленията и санкциите, и трето, ще въведат по-високи изисквания за докладване от страна на държавите членки[10].

ЛИТЕРАТУРА:

1. Контрол на упойващи и психотропни вещества. Политики за ограничаване разпространението на наркотични вещества,http://www.pharmfac.net/Lectures_Social_pharmacy_Doc_Getov/4_Lecture_Narcotics%20control%20and%20prevention.pdf

2. Единна конвенция по упойващите вещества от 1961 г., изменена с протокола от 1972 г., изменящ единната конвенция по упойващите вещества от 1961 г., Ратифицирана с Указ № 634 на Президиума на НС на НРБ от 22.08.1968 г. - ДВ, бр. 67 от 1968 г. В сила за Република България от 24.11.1968 г. Закон на НС от 12.01.1994 г. за оттегляне на резервата по чл. 48, т. 2 - бр. 8 от 27.01.1994 г. Резервата оттеглена на 6.05.1994 г. Издадена от МВР, обн., бр. 87 от 15.10.1996 г. В сила за Република България от 17.08.1996 г. - дата на влизане в сила на Протокола от 1972 г. - ДВ, бр. 86 от 1996 г.

3. Конвенция за психотропните вещества, Указ № 690 на Държавния съвет от 5.04.1972 г. за присъединяване - ДВ, бр. 30 от 1972 г., в сила от 16.08.1976 г. Закон на НС от 12.01.1994 г. за оттегляне на резервата по чл. 31 - ДВ, бр. 8 от 27.01.1994 г. Резервата оттеглена на 6.05.1994 г. Издадена от МВР, обн., ДВ, бр. 40 от 2.05.1995 г., попр., бр. 83 от 1.10.1996 г.

4. Конвенция на Организацията на обединените нации за борба срещу незаконния трафик на упойващи и психотропни вещества Приета от конференцията на нейното 6-о пленарно заседание на 19 декември 1988 г. Ратифицирана със закон на Народното събрание от 15.07.1992 г. - ДВ, бр. 60 от 24.07.1992 г. Издадена от Министерството на външните работи, обн., ДВ, бр. 89 от 19.10.1993 г., в сила за България от 23.12.1992 г., попр., бр. 58 от 29.06.2001 г.

5. Стратегия на ЕС за борба с наркотиците (2013-2020 г.) Обн. С ОВ. бр.402 от 29 Декември 2012г.2012/С 402/01

6. Информация от МВР относно „Противодействие на незаконния трафик, производство и разпространение на наркотични вещества и прекурсори”, www.mvr.bg/NR/rdonlyres/03AD6773-BABE-46B5-993B.../0/

7. Китан Китанов, Организираната наркопрестъпност, криминологични проблеми и превантивна дейност на полицията, София 2008 г.

[10] Становище на Европейския икономически и социален комитет относно „Съобщение на Комисията до Европейския парламент и до Съвета –Към по-решителен европейски отговор на наркотиците“, COM(2011) 689 final, Брюксел, 24 май 2012 г.

8. Рамково решение 2004/757/ПВР на Съвета от 25 октомври 2004 г. за установяване на минималните разпоредби относно съставните елементи на наказуемите деяния и прилаганите наказания в областта на трафика на наркотици, ОВ L 335, 11.11.2004 г., стр. 8—11.

9. Решение 2005/387/ПВР на Съвета от 10.05.2005 г. относно обмена на информация, оценката на риска и контрола върху новите психоактивни вещества, ОВ L 127, 20.5.2005 г., стр. 32–37.

10. Европейският съвет на 10-11 декември 2009 г. прие Програмата от Стокхолм, която представлява цялостна рамка за инициативи в областта на правосъдието и вътрешните работи. С цел превръщането на тези политически цели в конкретни предложения Комисията подбра няколко ключови действия, които трябва да приеме през периода 2010—2014 г., COM(2010) 171 окончателен.

11. Съобщение на комисията до Европейския парламент и до Съвета, Към порешителен европейски отговор на наркотиците, Брюксел, 25.10.2011, COM (2011) 689 окончателен.

12. Съобщение на Комисията до ЕП, Съвета, Европейския икономически и социален комитет и Комитета на регионите, Установяване на пространство на свобода, сигурност и правосъдие за гражданите на Европа, План за действие за изпълнение на Програмата от Стокхолм, Брюксел, 20.04.2010, COM(2010) 171 окончателен.

13. Становище на Европейския икономически и социален комитет относно „Съобщение на Комисията до Европейския парламент и до Съвета –Към порешителен европейски отговор на наркотиците“, COM(2011) 689 final, Брюксел, 24 май 2012 г.

14. Димитър Георгиев, “Трансгранична престъпност и международно сътрудничество”, Национална конференция, 30 и 31 януари 2012 г., Централен военен клуб – гр. София, стр.2.

15. Нели Кирилова, доклад „Контрабанда в глобализиращия се свят. Рискове пред ЕС от новосъздаващите се демокрации. Място и роля на България”, сборник на центъра за европейски и международни изследвания „Арабската пролет: надежда за промяна и предизвикателства пред Европейската външна политика и политика за сигурност, София, 2012 г.

МЕХАНИЗЪМ ЗА ГРАЖДАНСКА ЗАЩИТА НА ЕВРОПЕЙСКИЯ СЪЮЗ

Велико П. Петров

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

CIVIL PROTECTION MECHANISM OF THE EUROPEAN UNION

Veliko P. Petrov

ABSTRACT: *This report introduces the reader to the European Civil Protection Mechanism, which aims to facilitate reinforced cooperation in civil protection assistance interventions , and its purpose is to provide support in the event of major emergencies which may require urgent intervention . The new provisions in the revised EU legislation on civil protection establish the framework for the implementation of multispectral management policy disaster risk by encouraging an integrated approach to all natural and manmade risks in all phases of the cycle of disaster management (prevention, preparedness, response).*

KEYWORDS*: European Civil Protection Mechanism, disaster management, prevention, preparedness, response.*

Почти всички видове природни бедствия могат да сполетят Европейския съюз, така както и другите региони по света. Всяка година бедствията са причина не само за човешки жертви, но и за щети на стойност милиарди евро, засягащи икономическата стабилност и растежа. Бедствията могат да имат трансгранични последици и потенциално да застрашат цели райони в съседни държави[11]. Природните и причинени от човека бедствия все повече засягат безопасността и сигурността на гражданите на Европейския съюз и налагат да бъдат подобрени действията му при управлението на бедствия.

Законодателството на ЕС в областта на гражданската защита включва две решения на Съвета за създаване съответно на *Общностен механизъм* и *Финансов инструмент* (ФИГЗ). Механизмът подпомага и координира подготовката и използването на помощта в натура от държавите-членки (екипи, експерти и оборудване) за държави, които искат международна помощ при всички видове природни или предизвикани от човека сериозни извънредни ситуации в рамките на ЕС и извън него[12].

Европейският механизъм за гражданска защита[13] е създаден през 2001 г. с цел улесняване на засиленото сътрудничество в рамките на спасителните операции в областта на гражданската защита и е предназначен да осигури средства за подкрепа при изключително спешни случаи, в които се налага бърза намеса, в частност

11 Зелена книга относно застраховането срещу природни и причинени от човека бедствия, Страсбург, 16.4.2013, COM(2013) 213 final

12 Работен документ на службите на комисията, обобщение на оценката на въздействието, придружаващо Решение на ЕП и на Съвета, относно Механизъм за гражданска защита на Съюза, Брюксел, 26.1.2012 г., SEC(2011) 1630 окончателен/, стр. 3

13 Решение 2001/792/ЕО, Евратом на Съвета от 23 октомври 2001 г. за създаване на механизъм на Общността за поощряване на засиленото сътрудничество в рамките на спасителните операции в областта на гражданската защита

спешните случаи в контекста на управлението на кризите, визирани в дял V от Договора за Европейския съюз.

Действията на ЕС в областта на гражданската защита по линия на Механизма и ФИГЗ са изправени пред три основни предизвикателства:

1) непрекъснатото увеличаване на броя, силата и сложността на бедствията;

2) бюджетни ограничения предвид настоящата икономическа ситуация;

3) системни ограничения, които са присъщи за сегашния мандат на Механизма, намаляващи ефективността, ефикасността и съгласуваността на реакцията на ЕС при бедствия.

Механизмът има няколко недостатъка, свързани с реагирането при бедствия, готовността за тях и тяхната превенция[14]:

1) Основаните на реакцията и *ad hoc* механизми ограничават ефективността, ефикасността и съгласуваността на европейската реакция при бедствия. Механизмът не е в състояние да гарантира наличността на помощта в случай на необходимост и не позволява целесъобразно планиране на действия при извънредни ситуации.

2) Критични недостатъци в средствата за реагиране поради недостатъчни количества, проблеми с графика или споделянето. Недостатъци възникват по отношение на средствата за справяне с рисковете с малка вероятност/силно въздействие, специализираните средства, свързани с високи разходи, и „хоризонталните“ средства.

3) Ограничените транспортни решения и тежките процедури затрудняват оптималната реакция: липсата на добър достъп до транспорт може да предотврати предоставянето на помощта; счита се, че процедурите за искане на финансова помощ от ЕС за транспорт пораждат прекомерна административна тежест по отношение на действията за бързо реагиране.

4) Ограничена готовност за обучение и учения: възникнаха проблеми, свързани с несъвместимостта на оборудването, процедурите за сътрудничество, готовността на отделните организации и доверието в способностите на партньорите. Без помощ от ЕС участващите държави няма да могат да повишат своите нива на готовност за широкообхватни и трансгранични събития.

5) Липса на интеграция в областта на превенцията: липсва обща рамка за управление на риска на равнище ЕС в секторните политики за превенция, при което различните елементи могат да се обединят за по-ефективно свързване на превенцията с действията за готовност и реакция.

През януари 2006 г. Комисията предложи механизмът да бъде преразгледан въз основа на досегашния опит и да се предвиди подходящо правно основание за бъдещи действия. Решение № 2007/779/ЕО, Евратом на Съвета[15] имаше за цел да отговори на зачестилите и все по-сериозни природни и предизвикани от човека бедствия. Освен това Решение № 2007/162/ЕО, Евратом на Съвета[16] предоставя възможност за финансирането на дейности, насочени към превенция, подготвеност и по-ефективни действия в областта на реагирането, по-специално на такива, които

14 Работен документ на службите на комисията, обобщение на оценката на въздействието, придружаващо Решение на ЕП и на Съвета, относно Механизъм за гражданска защита на Съюза, Брюксел, 26.1.2012 г., SEC(2011) 1630 окончателен/, стр. 4

15 Решение № 2007/779/ЕО, Евратом на Съвета от 8 ноември 2007 г. за създаване на Общностен механизъм за гражданска защита (преработен вариант)

16 Решение на Съвета от 5 март 2007 г. за създаване на финансов инструмент в областта на гражданската защита (ФИГЗ)

са предприети чрез сътрудничество между държавите членки и осъществявани в рамките на механизма. Общата сума за действия и мерки, които да бъдат финансирани по силата на Решението за ФИГЗ, е определена на 189,8 млн. EUR за периода 01.01.2007 г.–31.12.2013 г. Решението за механизма и Решението за ФИГЗ бяха отменени, считано от влизането в сила на 1 януари 2014 г. на решението за Механизма за гражданска защита на Съюза[17].

Законодателството и действията на ЕС в областта на гражданската защита, включително решенията за механизма и за ФИГЗ преди влизането в сила на Договора от Лисабон през 2009 г., бяха основани на универсалната разпоредба на член 308 от Договора за ЕО, която дава право на Съвета да действа (с единодушие), когато това е необходимо за постигане на целите на Договора в областите, в които Договорът за ЕО не предвижда друго правно основание. В новия член 196 на Договора от Лисабон, който е посветен на гражданската защита, вече тя беше официално призната като самостоятелна политика.

До началото на 2010 г. гражданската защита е в рамките на компетентността на члена на Комисията, отговарящ за околната среда. След това е прехвърлена на Генералната дирекция на Комисията „*Хуманитарна помощ и гражданска защита*“ (наричана по-нататък ГД ЕСНО) с оглед на по-доброто оползотворяване на полезните взаимодействия и за да се засили съгласуваността на операциите за реагиране на ЕС.

Механизмът за гражданска защита на ЕС (МГЗЕС), който през 2013 г. бе съставен от 32 държави (28 държави — членки на ЕС, плюс Македония, Исландия, Лихтенщайн и Норвегия), които си сътрудничат в областта на гражданската защита, е създаден с цел подпомагане на техните усилия за предотвратяване, подготовка и реагиране при природни или причинени от човека бедствия на територията на ЕС или извън нея. Подкрепата може да бъде под формата на помощ в натура, оборудване и екипи или да включва изпращането на експерти за извършване на оценки. Тя разчита на държавни ресурси и ако е необходима помощ в държави извън ЕС, обикновено се осъществява успоредно с хуманитарната помощ. Оперативното ядро на МГЗЕС е Координационният център за реагиране при извънредни ситуации (ERCC), с който може да бъде установена връзка денонощно, седем дни в седмицата.

Защитата, осигурявана съгласно Механизма за гражданска защита на Съюза (или Механизма на Съюза), следва да обхваща преди всичко населението, но също така и околната среда и имуществото, включително културното наследство, срещу всички видове природни и причинени от човека бедствия, включително екологични бедствия, замърсяване на морската среда и извънредни ситуации, свързани с остри здравословни проблеми, които възникват на територията на Съюза или извън него. При всички тези бедствия може да се наложи съдействие от гражданска защита и друга спешна помощ съгласно Механизма на Съюза в допълнение към способностите за реагиране на засегнатата държава. По отношение на бедствията, причинени от терористични актове, ядрени или радиационни аварии, Механизмът на Съюза следва да обхваща само действията за готовност и реагиране в областта на гражданската защита.

Механизмът на Съюза представлява явен израз на европейската солидарност, чрез осигуряване на практически и своевременен принос за превенцията на бедст-

17 Решение № 1313/2013/ЕС на Европейския парламент и на Съвета от 17 декември 2013 г. относно Механизъм за гражданска защита на Съюза

вия и готовността за тях и за реакцията при бедствия и непосредствена заплаха от бедствия, без да се засягат съответните водещи принципи и механизми в областта на гражданската защита.

Механизмът на Съюза трябва да отчита съответното право на Съюза и международните ангажименти, да използва възможностите за полезно взаимодействие със съответните инициативи на Съюза, например европейската програма за мониторинг на Земята (Коперник), Европейската програма за защита на критичната инфраструктура (EPCIP) и общата среда за обмен на информация (CISE)[18].

В управлението при бедствия е изключително важна, ролята на регионалните и местните власти, ето защо е необходимо те да бъдат подходящо включвани в дейностите, предприемани в съответствие с националните структури на държавите членки.

Превенцията има решаващо значение за защитата от бедствия и налага предприемането на по-нататъшни действия, както се посочва в Заключенията на Съвета от 30.11.2009 г. и в резолюцията на Европейския парламент от 21.09.2010 г. относно съобщението на Комисията, озаглавено „Подход на Общността за превенция на природни и причинени от човека бедствия“. Механизмът на Съюза следва да включва обща политическа рамка за действията на Съюза за превенция на риска от бедствия, чиято цел е да се постигне по-високо ниво на защита и устойчивост срещу бедствия чрез предотвратяване или ограничаване на техните въздействия и чрез насърчаване на култура на превенция, включително надлежно разглеждане на евентуални въздействия на изменението на климата и нуждата от подходящи действия за адаптация.

Във връзка с това оценките на риска, планирането на управлението на риска, оценката на способността за управление на риска, извършвани от всяка държава членка на национално или на съответното поднационално равнище с участието по целесъобразност на други служби, прегледът на рисковете, извършван на равнище на Съюза, както и партньорските проверки имат основно значение за осигуряване на интегриран подход за управлението при бедствия, обединяващ действията за превенция на риска, готовност и реагиране. Механизмът на Съюза включва обща рамка за обмен на информация относно рисковете и способностите за управление на риска, без да се засяга член 346 от ДФЕС, който гарантира, че нито една държава членка не следва да бъде задължавана да предоставя информация, чието разкриване тя счита за противоречащо на основните интереси на нейната сигурност.

Механизмът на Съюза включва обща политическа рамка, насочена към непрекъснато подобряване на степента на готовност на системите и службите за гражданска защита, на техния персонал и на населението в рамките на Съюза, което включва програма за учения, програма за извлечени поуки, както и програми за обучение и мрежа за обучение на равнището на Съюза и държавите членки в областта на превенцията, готовността и реагирането при бедствия, както се изисква в Заключенията на Съвета от 27.11.2008 г. относно европейското обучение в областта на управлението при бедствия.

Да продължава изграждането на *модули за операции за оказване на помощ* в областта на гражданската защита, състоящи се от ресурсите на една или повече държави членки, чиято цел е да бъдат напълно оперативно съвместими. Тези моду-

18 Решение № 1313/2013/ЕС на ЕП и на Съвета от 17.12.2013 г., относно Механизъм за гражданска защита на Съюза, стр. 1

ли се организират на равнището на държавите членки и са подчинени на тяхното командване и контрол.

Мобилизирането и координирането на операциите по оказване на помощ се улеснява от Механизма на Съюза, който се състои от *Координационен център за реагиране при извънредни ситуации* (ERCC), *Европейски капацитет за реагиране при извънредни ситуации* (EERC) под формата на доброволно обединяване на предварително заделени от държавите членки способности, обучени експерти, *Обща система за комуникация и информация при извънредни ситуации* (CECIS), управлявана от Комисията, и точки за контакт в държавите членки.

За подобряване на планирането на операциите за реагиране при бедствия съгласно Механизма на Съюза и повишаване наличността на ключови способности, е необходимо да се развие EERC под формата на доброволно обединяване на предварително заделени капацитет от държавите членки и структуриран процес за установяване на евентуални пропуски в капацитета.

В операции по оказване на помощ в отговор на бедствия извън ЕС, Механизмът на Съюза следва да улеснява и подпомага действията, предприемани от държавите членки и Съюза като цяло, с оглед да се насърчи последователността на международната дейност в областта на гражданската защита. Помощта, предоставяна по линия на Механизма на Съюза, следва да се координира с ООН и съответни други международни участници, за да се оползотворят максимално наличните ресурси и да се избегне излишно дублиране на усилията.

Механизмът за гражданска защита на Европейския съюз („Механизмът на Съюза“) има за цел да засили сътрудничеството между Съюза и държавите членки и да улесни координацията в областта на гражданската защита с цел подобряване на ефективността на системите за превенция, готовност и реагиране при природни и причинени от човека бедствия.

Механизмът на Съюза насърчава солидарността между държавите членки чрез практическо сътрудничество и координация, без да засяга първостепенната отговорност на държавите членки да защитават населението, околната среда и имуществото, включително културното наследство, при бедствия на територията си, както и да обезпечават своите системи за управление при бедствия с достатъчен капацитет, така че те да могат да се справят системно и по подходящ начин с бедствия с характер и величина, които могат с основание да се очакват и за които трябва да бъдат подготвени.

Чрез Механизма на Съюза се подпомага, допълва и улеснява координирането на действията на държавите членки при изпълнението на следните общи специфични цели:

а) постигане на високо ниво на защита срещу бедствия чрез предотвратяване или ограничаване на потенциалните въздействия, чрез насърчаване на култура на превенция и чрез подобряване на сътрудничеството между службите за гражданска защита и съответни други служби;

б) повишаване на степента на готовност за реагиране при бедствия на равнище на държавите членки и на Съюза;

в) улесняване на бързо и ефикасно реагиране при бедствия или непосредствена заплаха от такива; както и

г) увеличаване на обществената осведоменост и готовност за бедствия.

Прилагат се следните определения:

– „*бедствие*“ означава всяка ситуация, която има или може да има тежки последици за населението, околната среда или имуществото, включително културното наследство;

– „*реагиране*“ означава всяко действие, което се предприема при искане за помощ в съответствие с Механизма на Съюза в случай на непосредствена заплаха от бедствие или по време на бедствие или след него и което цели овладяване на непосредствените неблагоприятни последици;

– „*готовност*“ означава състояние на подготвеност и способност на човешките и материалните ресурси, структури, общности и организации за ефективно бързо реагиране при бедствие, като това състояние е постигнато в резултат на предварително предприети действия;

– „*превенция*“ означава всяко действие, насочено към намаляване на рисковете или смекчаване на неблагоприятните последици от бедствие за населението, околната среда и имуществото, включително културното наследство;

– „*ранно предупреждение*“ означава своевременното и ефективно предоставяне на информация, което позволява да се предприемат действия за избягване или намаляване на рисковете и неблагоприятните последици от бедствия, както и за улесняване на готовността за ефективно реагиране;

– „*модул*“ означава самостоятелна и независима структура на способностите на държавите членки, определена предварително въз основа на задачите и потребностите, или подвижен оперативен екип на държавите членки, представляващи комбинация от човешки и материални ресурси, която може да се опише с оглед на способността за намеса или според задачата(ите), която(ито) може да поеме;

– „*оценка на риска*“ означава цялостен междусекторен процес за установяване, анализ и оценка на рисковете, който е предприет на национално или подходящо поднационално равнище;

– „*способност за управление на риска*“ означава способността на държава членка или нейните региони за ограничаване, адаптиране или смекчаване на рисковете, (въздействието и вероятността за възникването на бедствие), установени в оценката на риска, до равнища,които са приемливи за тази държава членка. Способността за управление на риска се оценява от гледна точка на техническия, финансов и административен капацитет за предприемане на адекватни:

а) оценки на риска;

б) планиране на управлението на риска с оглед на превенцията и готовността;

в) мерки за превенция на риска и за готовност за посрещането му;

– „*подкрепа от приемащата държава*“ означава всяко действие, предприето на етапите на готовност и реагиране от държава, която получава или изпраща помощ, или от Комисията, за отстраняване на предвидимите препятствия пред международната помощ, предоставена чрез Механизма на Съюза. Тя включва подкрепата от държавите членки за улесняване на транзитното преминаване на тази помощ през територията им;

– „*способност за реагиране*“ означава помощта, която може да се предостави чрез Механизма на Съюза при поискване;

– „*логистична подкрепа*“ означава основното оборудване или услуги, необходими на експертните екипи, посочени в член 17, параграф 1, за изпълнение на техните задачи, наред с другото. комуникации, временно настаняване, храна или транспорт във вътрешността на страната.

Някои от задачите изпълнявани от Комисията в областта на превенцията са:

а) действия за подобряване на базата от знания за рисковете от бедствия и улесняване обмена на знания, най-добри практики и информация, включително сред държавите членки с общи рискове;

б) подкрепа и насърчаване на дейностите на държавите членки по оценка и картографиране на рисковете чрез обмен на добри практики, както и улесняване на достъпа до специфични знания и експертен опит по въпроси от общ интерес;

в) осъществяване и редовно актуализиране на междусекторен преглед и картографиране на рисковете от природни и предизвикани от човека бедствия;

г) насърчаване обмена на добри практики за подготовка на националните системи за гражданска защита с цел справяне с последствията от изменението на климата;

д) насърчаване на използването на различни фондове на Съюза, с които може да се подпомага устойчива превенция на бедствия;

е) изтъкване на значението на превенцията на рисковете и оказване на подкрепа на държавите членки в дейностите им за повишаване на осведомеността, предоставянето на информация и обучението на обществеността.

Целите на Механизма ще бъдат изпълнени чрез финансовия инструмент за гражданска защита. Чрез този иструмент ще се финансират дейности в три направления:

• готовност и реагиране при бедствия включени в механизма за гражданска защита на ЕС;

• предотвратяване (изследване на причините за бедствието, предвиждане, обществена информация) и готовност (засичане, обучение, създаване на мрежи, упражнения, мобилизация на експерти) в границите на Съюза;

• допълнителен транспорт в отговор на действия по механизма за гражданска защита.

Координационен център за реагиране при извънредни ситуации (ERCC). ERCC гарантира денонощен (24/7) оперативен капацитет и обслужва държавите членки и Комисията за постигане на целите на Механизма на Съюза.

Новите разпоредби в преразгледаното законодателство на ЕС относно гражданската защита[19] установяват рамката за изпълнение на многосекторната политика за управление на риска от бедствия, като насърчават възприемането на цялостен подход за всички природни и предизвикани от човека рискове във всички фази на цикъла на управление на бедствията (превенция, подготовка, реагиране).

В периода между 2010 г.–2014 г. ЕС реагира на повече от 80 извънредни ситуации по света:

- тройното бедствие в Япония;
- гражданската война в Сирия;
- горските пожари в Южна Европа и на Балканския полуостров;
- наводненията в Централна Европа и на Балканския полуостров (Сърбия, Босна и Херцеговина);
- епидемията от ебола в Западна Африка;
- конфликта в Украйна.

19 Решение № 1313/2013/ЕС относно Механизъм за гражданска защита на Съюза.

През януари 2014 г. влезе в сила ново законодателство за гражданската защита, което осигурява рамка за по-тясно сътрудничество в следните области:

- предотвратяване на природни бедствия;
- оценка на риска;
- подготвеност и планиране, включително по-често провеждане на съвместни обучения и учения на европейските екипи по гражданска защита.

Изводи:

1. Управлението на бедствия от страна на Съюза следва да се основава на интегриран подход, който да обхваща целия цикъл на бедствието, състоящ се от предотвратяване, подготвеност, реагиране и възстановяване, при действията в границите на Съюза и извън тях. Управлението на бедствия от страна на ЕС се основава на два основни принципа:

– отговорността на държавите-членки за предоставяне на необходимата защита на своите граждани с оглед на съществуващите рискове и заплахи;

– солидарността между държавите-членки за взаимопомощ преди, по време на и след бедствия, ако катастрофите надхвърлят националния капацитет или засегнат повече от една държава-членка.

2. Бъдещите действия на ЕС следва да се ръководят от целта за намаляване на уязвимостта при бедствия, като се създаде стратегически подход за предотвратяване на бедствия и като се подобрят подготвеността и начините на реагиране при зачитане на националната отговорност.

3. Въз основа на новото законодателство и предходни съобщения и заключения на Съвета, основните действия за подпомагане на прилагането на рамката на ЕС за управление на риска от бедствия включват:

– оценка и анализ на риска: На базата на наличните национални оценки на риска Комисията изготви първоначален многосекторен преглед на рисковете в ЕС, като отчете, където е възможно и целесъобразно, бъдещото въздействие на изменението на климата и необходимостта от адаптация към това изменение; прилагайки последователен подход, до края на 2015 г. държавите членки трябва да изготвят национални оценки на свързания с различни опасности риск, които да бъдат последвани от оценка на националния капацитет за управление на риска и подобрени планове за управление на риска;

– насърчаване на ученето и обмена на опит с цел подобряване на управлението – популяризиране на и подкрепа за извлечените поуки и партньорските оценки с цел да се стимулира ученето във всички държави членки и да се направлява напредъкът към по-нататъшно развитие и прилагане на политиките и практиките за управление на риска;

– освен това в момента са в процес на разработване **напътствия за предотвратяване на бедствия въз основа на добри практики,** обхващащи взаимно свързани теми (управление, планиране, данни, комуникация и информация по отношение на рискове, научни изследвания и технологии);

– наличност на данни, достъпност, споделяне и съпоставимост, включително постоянна работа с държавите членки и международните партньори

(в това число UNISDR и IRDR[20]) за установяване на европейски стандарти и протоколи за отчитане на загубите в резултат на бедствия[21];

– интегриране на управлението на риска от бедствия: съображенията за предотвратяване и управление на риска бяха интегрирани в редица ключови политики и финансови инструменти на ЕС за подкрепа на устойчивите инвестиции (т.е. политика на сближаване, транспорт и енергетика, научни изследвания и иновации, защита на критичната инфраструктура, трансгранични заплахи за здравето, оценка на въздействието върху околната среда, зелена инфраструктура, интегрирано управление на крайбрежната зона, селско стопанство, сигурност в областта на продоволствието и прехраната, управление на водите и на риска от наводнение, предотвратяване на големи промишлени аварии);

– използване на застраховането като инструмент за управление на бедствията – Зелената книга относно застраховането срещу природни и причинени от човека бедствия[22] има за цел да ангажира частния сектор и да изследва начините за ефективно използване на застраховането като стимул за осъзнаване на риска, превенция и ограничаване на последиците;

– силни взаимодействия с дейностите по адаптиране към изменението на климата, както е посочено в Стратегията на ЕС относно адаптирането към изменението на климата[23], във взаимосвързани области като споделянето на данни и знания, оценката на рисковете и уязвимостта, устойчивостта на градската среда, разработването на европейски стандарти за устойчива на климатичните изменения инфраструктура, съответствието между националните стратегии за адаптиране и плановете за управление на риска, проследяването на устойчивите на изменението на климата инвестиции[24].

– наука и иновации за управление на риска от бедствия: През 2013 г. Комисията стартира инициатива съвместно с държавите – членки на ЕС, за изрично определяне и подобряване на научно обоснованите съвети за намаляване на рисковете и реагиране при неотложни ситуации. Освен това програмата за научни изследвания „*Хоризонт 2020*“ ще подпомогне разработването на съобразени с предизвикателствата подходи за подобряване на устойчивостта при бедствия (като мониторинг, превенция, прогнозиране, ранно предупреждение, повишаване на осведомеността, смекчаване на последствията от и приспособяване към изменението на климата, комуникация при кризи, трансфер на технологии, предварителна стандартизация);

– работа за отстраняване на трансграничните въздействия (посредством макрорегионални проекти и стратегии, като стратегията за Балтийско море, стратегията за река Дунав или регионалните морски стратегии) **и дейности за сътрудничество** със страните кандидатки и потенциални кандидатки, както и други съседни страни;

20Интегрирани проучвания относно риска от бедствия, http://www.irdrinternational.org.

21De Groeve, T., K. Poljansek и L. Vernaccini, 2013 г. „Отчитане на загубите в резултат на бедствия: препоръки за европейски подход“ (Recording Disaster Losses: Recommendations for a European approach). Служба за публикации на Европейския съюз, доклади за научни и технически изследвания EUR 26111. ISBN 978-92-79-32690-5, DOI: 10.2788/98653 (онлайн), http://publications.jrc.ec.europa.eu/repository/handle/111111111/29296.

22COM(2013)213, 16.4.2013 г.

23 COM(2013)216, 16.4.2013 г.

24Оказване на принос за постигане на целта на ЕС за финансиране на 20% от свързаните с климата инвестиции от бюджета на ЕС.

– **повишена степен на готовност** за реагиране чрез доброволно обединяване на предварително заделен от държавите членки капацитет за реагиране при бедствия, по-добро планиране на реагирането, мрежа за обучение, засилено сътрудничество между властите в областта на обученията и упражненията[25], и укрепени системи за ранно предупреждение[26]. Освен това посредством космическите програми на ЕС като „Галилео“ и „Коперник“ в световен мащаб се предоставят нови оперативни услуги за управление на извънредни ситуации[27].

4. В „Окончателен доклад за изпълнението на Стратегията за вътрешна сигурност на ЕС за периода 2010-2014 г.“[28] от 20.6.2014 г. са посочени целите и основните постижения от ЕС през периода 2010-2014 г. Като пета цел е посочена „*Подобряване на устойчивостта на Европа спрямо кризи и бедствия*“ и се определиха четири ключови действия:

– пълноценно използване на клаузата за солидарност;

– разработване на подход, обхващащ всички опасности, за оценяването на заплахите и рисковете;

– свързване на различните центрове за ситуационна осведоменост;

– разработване на Европейски капацитет за спешно реагиране при бедствия.

ЛИТЕРАТУРА:

1. Зелена книга относно застраховането срещу природни и причинени от човека бедствия, Страсбург, 16.4.2013, COM (2013) 213 final.

2. Съобщение на Комисията до Европейския парламент и Съвета, Окончателен доклад за изпълнението на Стратегията за вътрешна сигурност на ЕС за периода 2010-2014 г. Брюксел, 20.6.2014 г., COM(2014) 365 final.

3. Решение 2001/792/ЕО, Евратом на Съвета от 23.10.2001 г. за създаване на Механизъм на Общността за поощряване на засиленото сътрудничество в рамките на спасителните операции в областта на гражданската защита (ОВ L 297, 15.11.2001 г., стр. 7).

4. Решение 2007/779/ЕО, Евратом на Съвета от 08.11.2007 г. за създаване на Общностен механизъм за гражданска защита (ОВ L 314, 1.12.2007 г.,стр. 9).

5. Решение на Съвета от 05.03.2007 г. за създаване на финансов инструмент в областта на гражданската защита (ФИГЗ).

6. Работен документ на службите на Комисията, обобщение на оценката на въздействието, придружаващо Решение на ЕП и на Съвета, относно Механизъм за гражданска защита на Съюза, Брюксел, 26.01.2012 г., SEC(2011) 1630 окончателен.

7. Решение № 1313/2013/ЕС на ЕП и на Съвета от 17.12.2013 г., относно Механизъм за гражданска защита на Съюза, ОВ L 347, 20.12.2013 г., стр. 924

8. Доклад на комисията до ЕП и Съвета за последващата оценка на Общностния механизъм за гражданска защита и на Финансовия инструмент в областта на гражданската защита за периода 2007–2013 г. , Брюксел, 18.02.2015 г., COM(2015) 61 final.

25 Решение № 1313/2013/ЕС относно Механизъм за гражданска защита на Съюза.

26 Например EFFIS (Европейската информационна система за горски пожари) или EFAS (Европейска система за осведоменост във връзка с наводненията).

27 Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите, Рамковата програма за действие от Хього в периода след 2015 г.: Управление на риска с цел постигане на устойчивост, Брюксел, 8.4.2014 г., COM(2014) 216 final, стр. 7 и 8.

28 Съобщение на Комисията до Европейския парламент и Съвета, Окончателен доклад за изпълнението на Стратегията за вътрешна сигурност на ЕС за периода 2010 - 2014 г. Брюксел, 20.6.2014 г., COM(2014) 365 final

9. Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите, Рамковата програма за действие от Хього в периода след 2015 г.: Управление на риска с цел постигане на устойчивост, Брюксел, 8.4.2014 г., COM(2014) 216 final

10. Хуманитарна помощ и гражданска защита, *http:// europa.eu /pol /hum/ index_bg.htm*

ПОЛИТИКА НА ЕВРОПЕЙСКИЯ СЪЮЗ В ОБЛАСТТА НА ХУМАНИТАРНАТА ПОМОЩ И ГРАЖДАНСКАТА ЗАЩИТА

Велико П. Петров

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

EUROPEAN UNION POLICY IN THE FIELD OF HUMANITARIAN AID AND CIVIL PROTECTION

Veliko P. Petrov

ABSTRACT: *This report aims to acquaint the reader with the policies of the European Union's humanitarian aid and civil protection and implementation mainly through its Directorate-General "Humanitarian Aid and Civil Protection" (ECHO). Referred to are the numerous threats facing the European Union and its Member States, such as earthquakes and tsunamis; fires; floods and landslides; industrial and nuclear accidents; terrorist attacks; natural disasters and major pandemics. Observed a dramatic increase in the number and severity of natural and man-made disasters affecting the Union and its citizens, as well as other countries and regions worldwide. Improving coherence and coordination between the EU and its Member States in response to a disaster or protracted crisis is a key issue for improving the effectiveness of the overall assistance provided by the EU.*

KEYWORDS*: Directorate-General "Humanitarian Aid and Civil Protection" (ECHO), a disaster, humanitarian aid, civil protection,*

Европейският съюз и неговите държави-членки са изправени пред множество заплахи, като например: земетресения и цунами; пожари, включително горски пожари; наводнения и свлачища; промишлени и ядрени аварии; терористични атаки; природни бедствия и големи пандемии; наблюдава се драстично нарастване на броя и сериозността на природните и предизвиканите от човека бедствия, които засягат Съюза и неговите граждани, а също така и други държави и региони по света.

В Европа честотата и мащабите на големите суши и горските пожари са се увеличили, което означава, че следва да се доразвият съответните научни изследвания с оглед подобряването на механизмите за оценяване на риска, на системите за предотвратяване и на средствата за борба с тези явления. Засилването на последи-

щите от изменението на климата и изчерпването на природния капитал допълнително ще увеличат вероятността от по-чести и по-силни природни бедствия.

Големи трагедии по света, като земетресението в Хаити и наводненията в Пакистан, показаха, че основните инструменти, с които разполага ЕС за реагиране при бедствия (*хуманитарна помощ* и *механизъм на ЕС за гражданска защита*), функционират добре по отношение на своето предназначение и при стеклите се обстоятелства, но също така като има предвид, че съществува жизнена необходимост допълнително да се засили координацията на реакцията на Европейския съюз при бедствия както в неговите граници, така и извън тях и че съществува възможност за подобрения по отношение на ефективността, ефикасността, съгласуваността и видимостта на помощта на ЕС като цяло.

Хуманитарните действия имат многовековна история на солидарност, коренящa се в духа на хората, оказващи помощ на жертвите на кризи. Целта на хуманитарната помощ е да спаси живота и да предостави незабавна помощ на хората, изправени пред тежка криза, която е резултат от природно бедствие или конфликт. През последните трийсет години се отделя повече внимание на принципите, качеството и професионализма при предоставянето на международна хуманитарна помощ[29]. Европа има дългогодишни традиции в областта на хуманитарната дейност, с които може да се гордее, и е родина на много от най-реномираните хуманитарни организации в света. Хуманитарната дейност представлява морален императив за проява на солидарност и облекчаване на страданието на хора, засегнати от природни бедствия или бедствия и катастрофи, предизвикани от човека.

Хуманитарната помощ, предоставяна от ЕС, подпомага и подкрепя най-нуждаещите се хора в трети държави. Тя се оказва животоспасяваща за тези, които са засегнати от природни или причинени от човека бедствия, и подготвя общностите, които са жертва на чести кризи, да се справят с последиците от бъдещи извънредни ситуации. В допълнение към хуманитарната помощ **операциите за гражданска защита** осигуряват непосредствена подкрепа чрез екипи от експерти, спасително оборудване и наблюдение на разразяващи се бедствия в реално време както на територията на Европейския съюз, така и извън нея[30].

Операциите на Европейския съюз имат също така за цел предотвратяване или намаляване на страданията и защита на интегритета и достойнството на хората чрез предоставяне на помощ и защита в случаи на хуманитарни кризи. Комисията също способства за координацията с и между държавите членки в областта на хуманитарните действия и политика, за да се подобрят ефективността и взаимното допълване на хуманитарната помощ.

Определението за принципите е посочено в Етичния кодекс на международното движение на червения кръст и полумесец и неправителствени организации (НПО) за помощ при бедствия и в Резолюция 46/182 на Общото събрание на Обединените нации.

Основните хуманитарни принципи[31] са четири и те са:

[29] Съобщение на Комисията до Европейския парламент и Съвета, Към постигане на европейски консенсус относно хуманитарната помощ Брюксел, 13.6.2007, COM (2007) 317 окончателен.

[30] Доклад на Комисията до Европейския парламент и Съвета, Годишен доклад относно политиките на ЕС в областта на хуманитарната помощ и гражданската защита и тяхното изпълнение през 2013 г., Брюксел, 28.8.2014 г., COM(2014) 537 final

[31] Тук не се има предвид широкото значение на термина в смисъл на „принципи на международното хуманитарно право" (каквито са, например, принципът за защита правата на човека или неприкосновеността на цивилното население), а тясното значение на термина в смисъл на „*принципи на хуманитарното действие*"

– **хуманност** – постулира безусловно и неотменно хуманно отношение към пострадалите и съхраняване на личното им достойнство**;**

– **безпристрастност** – предоставянето на хуманитарна помощ следва да бъде основано само на обективните нужди, а не да се определя от субективни оценки (например, дали получателят е „виновен" или „невинен", „заслужаващ" или „не заслужаващ" помощ и пр.) или на критерии като националност, раса, религия, пол, богатство и др.;

– **неутралност** – предоставящият хуманитарна помощ (държава, организация и пр.) следва да бъде неутрален от идеологическа гледна точка, както и да не бъде ангажиран по никакъв начин – пряко или косвено – във военни действия на място (в случай че се провеждат такива)**;**

– **независимост** – хуманитарните организации следва да определят и прилагат политиката си независимо от политиката или действията на правителствата[32].

Днес участниците в хуманитарни действия са изправени пред особени предизвикателства. Хуманитарните кризи се случват все по-често и имат по-сериозни последствия, като са свързани с измененията на климата, промяната на конфликта, увеличаване на борбата за достъп до енергия и природни ресурси, крайната бедност, лошото управление и разпадащите се държави.

Главната жертва е цивилното население, като по-голяма част от него живее в развиващите се страни. Съществува нарастваща тенденция за незачитане или очевидно нарушаване на хуманитарното и международно право. Хуманитарната помощ е една от главните външни политики на ЕС. ЕС като цяло е водещ хуманитарен донор в света и европейците са силно ангажирани в подкрепа на хуманитарни действия, а това налага голяма отговорност и очаквания за ЕС.

„Европейската хуманитарна помощ променя живота на стотици хиляди хора, които знаят, че Европа е сила, застъпваща се за онези всеобщи ценности, които са от съществено значение за превръщане на света в по-добро място за живеене."

ЕС е един от най-големите донори на хуманитарна помощ в света: Европейската комисия и държавите членки осигуряват съвместно около 50 % от световното финансиране за спешна хуманитарна помощ. Генерална дирекция „Хуманитарна помощ и гражданска защита" (ECHO) е основното действащо лице на ЕС в тази област, като финансира операции за хуманитарна помощ, провеждани от различни партньори (неправителствени организации, агенции на ООН и международни организации) и координира политиките и дейностите на държавите членки. ECHO подкрепя също така ефективни мерки за предоставяне на хуманитарна помощ в целия свят. През 2013 г. ЕС предостави 1 353 милиарда евро за хуманитарна помощ, за да помогне на 124 милиона души в над 90 страни извън ЕС. Европейският парламент и Съветът на ЕС действат като съзаконодатели при определянето на насоките на политиката на ЕС за предоставяне на хуманитарна помощ. Освен това Парламентът следи предоставянето на хуманитарна помощ и се застъпва за определянето на бюджетни средства, съответстващи на хуманитарните нужди[33].

Правното основание за предоставянето на хуманитарна помощ е чл. 214 от Договора за функционирането на Европейския съюз (ДФЕС), а преди Договора от Лисабон за правно основание служеше чл. 179 от Договора за Европейската общ-

[32] Международното хуманитарно сътрудничество – основни принципи, действащи лица и направления, bdi.mfa.government.bg / projects /7-ihc.pdf

[33] Справочник за Европейския съюз – 2015, Хуманитарна помощ, FTU_6.3.2, стр. 1

ност. Правното основание за създаване на Европейски доброволчески корпус за хуманитарна помощ е чл. 214, параграф 5, а чл. 21 от Договора за Европейския съюз (ДЕС) определя принципите на цялата външна дейност на ЕС (чл. 21, параграф 2, буква ж) и се отнася до хуманитарната дейност.

Разпоредби и правила относно предоставянето на хуманитарна помощ (включително относно финансовите инструменти) са изложени в Регламент (ЕО)№ 1257/96 на Съвета от 20.06.1996 г. относно хуманитарната помощ и същият не е изменян досега, докато други инструменти бяха основно преработени в хода на подготовката за многогодишната финансова рамка (МФР) за периода 2007-2013 г. За периода 2007-2013 г. за инструмента за хуманитарна помощ бяха разпределени 6,62 милиарда евро. Поетите от ЕС годишни ангажименти се завишаваха редовно, така че да съответстват на нови хуманитарни нужди.

В „*Европейски консенсус относно хуманитарната помощ*“ от 2007 г., подписан от трите институции на ЕС (Съвета, Комисията и Парламента) е очертана Общата рамка на политиката за хуманитарна помощ. Там са дефинирани общата визия, целите на политиката и принципите по отношение на редица въпроси, като:

– международното-хуманитарно сътрудничество;
– добрите практики за донорство;
– намаляването на риска и подготвеността;
– гражданската защита;
– гражданските и военните отношения.

Предвижда се по-координиран и съгласуван подход за предоставяне на помощ (една част от тези средства се предоставя директно от държавите членки, но голяма част произхожда от бюджета на ЕС), като свързва хуманитарната помощ и помощта за развитие, така че да се даде възможност на ЕС да откликва по-ефективно на нарастващите нужди. Срокът на плана за действие за изпълнение на консенсуса изтече през 2013 г., а новата рамка за изпълнение е понастоящем в процес на обсъждане.

Службата за хуманитарна помощ на Европейската общност (ЕСНО) е създадена като централен орган за осигуряване и координиране на европейската хуманитарна помощ още през 1992 г. През 2004 г. ЕСНО се превръща в генерална дирекция (ГД) на Европейската комисия и запазва съкратено си наименование. През 2010 г. в мандата на ЕСНО е включена и гражданската защита с оглед осигуряването на по-добра координация и реакция при бедствия в рамките на ЕС и извън него.

От своето създаване до сега ЕСНО е насочила повече от 14 милиарда евро от общия бюджет на ЕС за близо 150 милиона души, които са засегнати от бедствия и конфликти в над 140 страни. ЕСНО се разрасна през годините: повече от 300 служители работят в нейното седалище в Брюксел и се подпомагат от широка мрежа от експерти (над 400) и работещи местни служители в 39 държави. Самата генерална дирекция не изпълнява програми за хуманитарна помощ, тя по-скоро финансира операции, провеждани от нейните партньори. Основните задачи на ЕСНО са да осигурява средства, да следи за разумното управление на финансите и да гарантира, че стоките и услугите на нейните партньори достигат засегнатото население ефективно и бързо, така че да отговорят на действителните нужди.

След настъпването на природно бедствие или друго събитие, изискващо хуманитарна помощ, експертите по хуманитарна помощ на ЕСНО извършват първона-

чална оценка на ситуацията на място и след това въз основа на тази оценка средствата биват изплащани бързо. Този подход „*основаващ се на потребностите*“ определя дейността на ЕСНО. Помощта се предоставя чрез повече от 200 партньори – включително агенциите на ООН, неправителствени организации (НПО) и международни организации като Международното движение на Червения кръст и Червения полумесец, с които ЕСНО е сключила предварителни договорни споразумения. Структурата на ЕСНО гарантира, че средствата се използват прозрачно и че партньорите носят отчетна отговорност.

През 2013 г. и 2014 г. ЕС финансира операции в редица извънредни ситуации, предизвикани от природни бедствия, като:

– тайфунът „Хаян“ връхлетя Филипините през ноември 2013 г. и предизвика невиждани дотогава поражения и опустошение. Той е сред най-мощните в историята и причини смъртта на хиляди души, разселване на около 4 милиона души и засегнатитев са между 14 и 16 милиона души;

– в целия регион на Сахел проточилата се продоволствена криза с изхранването продължи да излага на риск живота на милиони хора (около 16 милиона души бяха изложени на риск от липса на храна, а 8 милиона от тях се нуждаеха от спешно продоволствено подпомагане);

– четири години след унищожителното земетресение в Хаити през 2010 г. хуманитарните нужди все още са големи. От първоначално нуждаещите се 1,5 милиона души все още 130 000 са разселени, страната все още е огнище на най-голямата епидемия на холера в света и е в състояние на структурна продоволствена несигурност;

ЕС предостави хуманитарна помощ за справяне с последиците от следните природни бедствия:

• суши в: Камбоджа, Виетнам, Лаос, Мексико, Джибути и Етиопия;

• наводнения в: Бангладеш, Камбоджа, Виетнам, Лаос, Индия, Етиопия, Кения, Мозамбик, Нигерия, Сейнт Лусия, Сейнт Винсънт и Гренадини;

• циклони/урагани/тропически бури във: Филипините, Бангладеш, Камбоджа, Виетнам, Доминиканската република, Куба, Хаити, Ямайка, района на Тихия океан;

• земетресения във: Филипините, Индонезия;

• епидемии: Афганистан, Буркина Фасо, Сомалия, Демократична република Конго, Нигерия, Зимбабве, Кения, Доминиканската република, Мексико, Лаос, Киргизстан.

В **причинените от човека кризи**, ЕС подпомогна операциите за предоставяне на помощ в няколко конфликта, а някои от тях вече се смятат за **продължителни и сложни кризи:**

– *мащабният конфликт и гражданската война в Сирия*, при които е налице голям наплив на сирийски бежанци в съседните държави, сред които Ливан, Турция, Йордания и Ирак, още от самото начало изискваха голям по мащаб хуманитарен отговор от страна на ЕС (от насилието са засегнати около 9,3 милиона души и се нуждаят от хуманитарна помощ на територията на Сирия, вътрешно разселени лица са около 6,5 милиона, а броят на бежанците в съседни държави са над 2,3 милиона). Комисията предостави многосекторна хуманитарна помощ на бежанците и приемните общности в съседните държави, както и на засегнатите групи на тери-

торията на Сирия, като основните сектори бяха подслон, нехранителни продукти, продоволствия, водоснабдяване, канализация и хигиена, здравна помощ и защита;

– ЕС предостави значителна хуманитарна подкрепа (77 милиона EUR) на населението на *Северно Мали*, засегнато от продължаващия въоръжен конфликт (70 % от здравните заведения функционираха, а около 900 000 души се смята, че са имали полза от целенасоченото продоволствено подпомагане).

– в хуманитарен план *Централноафриканската република* (ЦАР) е в бедствено положение от декември 2012 г. и дълго време широката международна общност не обръщаше голямо внимание на кризата. ЕС отпусна на ЦАР хуманитарна помощ в размер на 39 милиона EUR, с което се превърна в основния международен донор на страната.

Особено внимание ЕС отделя на т. н. „*забравени кризи*“ по света и разпредели 15 % от общия размер на финансирането за подпомагане на хората, които са в ситуация на често продължителни бедствия, на които международната общност почти не отделя внимание.

Операции за гражданска защита – Комисията се стреми да насърчи и улесни сътрудничеството между 32-те държави, участващи в *Механизма за гражданска защита на ЕС* (МГЗЕС), с цел да се подобри предотвратяването, повиши готовността за защитата от бедствия (природни, технологични или причинени от човека) в Европа и извън нея.

Координационен център за реагиране при извънредни ситуации (ERCC) е създаден през май 2013 г. в рамките на ГД „ЕСНО” като наследник на Центъра за мониторинг и информация (ЦМИ) и е оперативното ядро на МГЗЕС. Неговите основни предимства са:

– капацитет да работи по няколко протичащи едновременно извънредни ситуации в различни часови зони;

– осъществяване на непрекъснат мониторинг по отношение на конкретни опасности; събиране и анализ на информация за бедствия в реално време;

– изготвяне на планове за разполагане на експерти, екипи и оборудване;

– работа с държавите членки с цел да се набележат наличните активи и да се координират усилията на ЕС за реагиране при бедствия, като съобразява предложената помощ с нуждите на засегнатата от бедствие страна.

Той действа също така като информационен център и входен пункт за исканията за помощ от страна на държавите – членки на ЕС.

Като обединява в едно Кризисното звено за хуманитарни кризи и Мониторинговия и информационен център (МИЦ) за гражданска защита, ERCC осигурява засилено сътрудничество между операциите на гражданската защита и хуманитарната помощ. Той предоставя на ЕС платформа за координиране при сериозни кризи.

Помощта от ЕС включва още две структури: Механизма за гражданска защита на Съюза и Европейския доброволчески корпус за хуманитарна помощ.

Механизмът за гражданска защита на Съюза е създаден през 2001 г. и включва 32 държави (28-те държави членки плюс бивша югославска република Македония,Исландия, Черна гора и Норвегия). Решение № 1313/2013/ЕС, прието на 17.12.2013 г., определя като правно основание член 196 от ДФЕС относно гражданската защита и гарантира финансирането на механизма до 2020 г.

Европейският доброволчески корпус за хуманитарна помощ е предвиден в член 214, параграф 5 от Договора от Лисабон и беше създаден през март 2014 г. като инициатива „Доброволци на ЕС за хуманитарна помощ“. Като укрепва способността на ЕС за реагиране при хуманитарни кризи, инициативата има за цел да се повиши устойчивостта на уязвимите общности в трети страни. Нейният бюджет в размер на147,9 милиона евро ще позволи между 2014 и 2020 г. да бъдат обучени и изпратени на място около 4 000 доброволци, както и да бъде развит капацитетът на същия брой местни служители.

От 2009 г. насам координацията с държавите членки се осъществява главно в рамките на работната група на Съвета „Хуманитарна и продоволствена помощ“ (COHAFA), в която участва Комисията. На стратегическо равнище COHAFA има съществен принос за повишаване на съгласуваността и взаимното допълване на дейностите на ЕС и на държавите членки в областта на хуманитарната помощ.

От казаното до тук могат да се направят следните изводи:

1) Броят на бедствията продължава да нараства в световен мащаб и тази тенденция ще продължи поради изменението на климата. Това налага още по-ефективни хуманитарни действия. Силно ударение в последните години се постави върху:

– повишаването на бързината и ефективността;

– отстраняването на дублирането на процеси и действия;

– гарантирано получаване на подходящата помощ в подходящия момент от най-нуждаещите и намирането на начини за постигане на по-големи резултати с по-малко средства.

2) Мандатът на ГД „ЕСНО” включва както *хуманитарната помощ*, така и *гражданската защита*. Чрез тези два основни механизма Европейският съюз вече може да осигури бърза и ефективна хуманитарна помощ на хората, засегнати от непосредствени последици от бедствия.

3) Постоянно нараства несъответствието между глобалното нарастване на хуманитарните нужди и все по-недостатъчните налични финансови ресурси за адекватен отговор на тези нужди, което означава, че донорите трябва да положат повече усилия, за да отговорят на бедствията по по-ефективен начин, като използват още по-добре ограничените си ресурси.

4) По отношение на природните бедствия ЕС възприе двупосочна стратегия:

• бърз отговор чрез осигуряване на хуманитарна помощ и чрез улесняване и координиране на помощта за гражданска защита;

• готовност при бедствия чрез набелязване на географските райони и населението, които са най-уязвими към природни бедствия и за които се създават специални програми за готовност при бедствия. През 2015 г. ЕС продължава да предоставя подкрепа на програмите DIPECHO[34] в Южен Кавказ (Армения, Азербайджан и Грузия), Карибите, Централна Америка, Южна Америка, Тихия океан, южната част на Африка и Централна Азия.

5) *Механизма за гражданска защита на ЕС* бе задействан многократно (при искания за помощ, предварителни сигнали и мониторинг), повечето от тези случаи бяха свързани с природни бедствия (изключително студено време, бури, горски пожари, наводнения, тропически циклони, земетресения, цунами), а други - с при-

[34] DIPECHO (готовност при бедствия ECHO) е специална програма, посветена на готовността при бедствия. Тя е насочена към силно уязвими общности, живеещи в някои от най-изложените на бедствия региони в света.

чинени от човека бедствия (създаване на бежански лагери поради граждански размирици, химически аварии и транспортни произшествия).

6) Приоритетите на ЕС на ниво политики в областта на *хуманитарната помощ* включваха ефективност на помощите, насоченост към резултати и въздействие. През 2013 г. беше преработено законодателството за *гражданска защита,* а с него се подобрява планирането на Европейските операции за реагиране при бедствия, осигурява се по-ефикасно, ефективно и съгласувано управление на бедствията през идните години.

7) Политиките на Европейския съюз в областта на хуманитарната помощ и гражданската защита демонстрират ангажимент за подпомагане на нуждаещите се в рамките на Съюза и извън него, когато те са най-уязвими. Тази помощ допринася за изпълнението на една от стратегическите цели на външната дейност на ЕС, както е посочено в член 21 от Договора за Европейския съюз. Подобряването на съгласуваността и координацията между ЕС и неговите държави членки в отговор на бедствие или продължителна криза е ключов въпрос за подобряване на ефективността на цялостната помощ, предоставяна от ЕС.

Литература:

1. Съобщение на Комисията до Европейския парламент и Съвета, Към постигане на европейски консенсус относно хуманитарната помощ Брюксел, 13.6.2007, COM (2007) 317 окончателен.

2. Доклад на Комисията до Европейския парламент и Съвета, Годишен доклад относно политиките на ЕС в областта на хуманитарната помощ и гражданската защита и тяхното изпълнение през 2013 г., Брюксел, 28.8.2014 г., COM(2014) 537 final

3. Международното хуманитарно сътрудничество – основни принципи, действащи лица и направления, *bdi.mfa.government.bg/projects/7-ihc.pdf*

4. Справочник за Европейския съюз – 2015, Хуманитарна помощ, FTU_6.3.2

5. Доклад на Комисията по околна среда, обществено здраве и безопасност на храните от 19 юли 2011 г., Към укрепване на реакцията на ЕС при бедствия: ролята на гражданската защита и на хуманитарната помощ (2011/2023(INI))

6. Решение № 1313/2013/ЕС на Европейския парламент и на Съвета от 17.12.2013 г. относно Механизъм за гражданска защита на Съюза

7. Регламент (ЕО) № 1257/96 на Съвета от 20 юни 1996 г. относно хуманитарната помощ;

8. Политиките на Европейския съюз, Хуманитарна помощ и гражданска защита, „Подпомагане на жертвите на бедствия и конфликти и защита на лицата, изложени на риск", http://www.horizonti.eu/europe-direct/files /NA 7012029 BGC 002 .pdf

9. Хуманитарна помощ и гражданска защита, http://europa.eu/pol /hum /index_bg.htm

10. MEMO-13-1120_BG, Ново законодателство за укрепване на европейската политика за управление на бедствия, Европейска комисия, Брюксел, 10.12.2013 г.

11. Съобщение на Комисията до Европейския парламент и до Съвета, Междинен преглед на плана за действие на Европейския консенсус относно хуманитарната помощ: осъществяване на ефективни хуманитарни действия на ЕС, основани на принципи Брюксел, 8.12.2010, COM(2010) 722 окончателен

ПОДХОД ЗА ПОДОБРЯВАНЕ НА БЕЗОПАСНОСТТА НА ПРОМИШЛЕНИТЕ ОБЕКТИ ЧРЕЗ ДИАГНОСТИКА И ЕКСПЕРТИЗА НА ЖИЗНЕНИЯ ЦИКЪЛ

Христо А. Десев

Национален Военен Университет " В. Левски" гр. Велико Търново
Факултет "Артилерия ПВО и КИС" гр. Шумен

APPROACH TO IMPROVE SAFETY OF INDUSTRIAL PROJECTS THROUGH THE DIAGNOSIS AND EXPERTISE OF LIFE CYCLE

Hristo A. Desev

ABSTRACT: *The growing value of losses and financial costs reasonably guide the efforts of the state to take initiatives to harm reductio. Policies safety management must reorient to raise emergency protectivity prevent events and accumulation of skills for effective treatment outcomes and reduction.*

KEY WORDS: *emergency protectivity, operational reliability, sustainability of the design parameters*

Природните и техногенни катастрофи се превръщат все по-често в наше съпътстващо ежедневие. Нарастващата стойност на загубите и финансовите разходи логично насочват усилията на държавата към предприемане на инициативи за намаляване на щетите.

Анализът на мероприятията за управление на риска, реализирани в досегашни събития, показват, че действащата стратегия не осигурява необходимото ниво на безопасност. Необходима е преоценка на съществуващите стереотипи за основните принципи и подходи за намесата на държавата в управлението на техногенните рискове. Политиките за управление на безопасността трябва да се преориентират към повишаване на аварийната защитеност, предотвратяване на събитията и натрупване на способности за ефективно третиране на последствията и съкращаване на посткризистния етап. Стремежът към изграждане и поддържане на стройна и многофункционална система за комплексно решаване на проблемите при бедствията и авариите, в целия им аспект на действие, е постижим с действия за прогноза, оценка на риска, превенция, дейности по ранно предупреждение и ликвидиране на последствията.

В по-голямата си степен можем да считаме, че управлението на техногенния риск се свежда до разработване и реализация на програми за осигуряване на мониторинга, предотвратяване на аварии и защита на процесите на производство.

Редукцията на заплахите от производствени дейности за населението и екосистемите следва да е продукт от развитието на три направления: мониторинг, ограничаване и защита.

Мониторингът е процес на постоянно наблюдение и събиране на информация за обектите, изследване на параметрите на технологичното производство, изхвър-

лянето на вредни вещества и състоянието на околната среда в зоната около предприятията.

Ограничаването лимитира времеви и пространствени параметри за персонала към производствата и условията на работа, които са източници на заплаха, а за населението определя санитарни зони, изключващи вредни въздействия.

Защитата обединява в едно цяло мерки за безопасност и мерки за защита. Първите не допускат ситуации на въздействие от вредните фактори върху персонала в процеса на нормална работа. Мерките за защита са физическите бариери срещу разпространение на елементите на поразяващите фактори при нормална работа и авария.

Целите на такъв тип управление са държавна инициатива и трябва да са насочени към достигане на приемливи нива на риска. Реалните мерки могат да обхващат:

- преглед на състоянието на обектите;
- повишаване на технологичната безопасност на производствените процеси и експлоатационната надеждност на оборудването.;
- разработване на инженерно технически мерки за намаляване на загубите за конкретни обекти определена територия;
- разпределение на промишлените мощности върху територията на страната от гледна точка на техногенната безопасност;
- провеждане на държавна експертиза по надзора и контрола на техногенната безопасност;
- деклариране на промишлената безопасност и лицензиране на различните дейности в областта на промишлената безопасност;
- поддържане в готовност на сили за реагиране и осъществяване на мерки за защита на персонала и населението в прилежащите територии.

Декларирането на промишлената безопасност е в основата на дейността на държавните институции по надзора на промишлените мощности и непрекъснатия мониторинг на обектите.[2]

Разкриването на основните опасности от аварии в технологичната сфера, започва в процеса на проектирането на системата и позволява в следващите етапи (конструиране, производство и експлоатация) значително да се подобри противодействието на катастрофалните произшествия.

Основно изискване за разкриване на опасностите се постига с предварителното определяне на някои параметри:

- използвани материали - входящи суровини, междинни производства и крайни продукти;
- вид на производствените операции - характера на производствения процес;
- топография на системата - разположение на отделните елементи (с възможна детайлизация) и пространственото разположение с други системи.

Тези параметри са в процеса на последователно разглеждане през призмата на потенциалните заплахи. Често голямата част от технологичните дейности се обследват в смисъла на случайните опасности: пожари, взрив, радиация, вибрации, отровни вещества, електротоков удар, механични повреди и др. Потенциалните опасности следва да приемат общ показател за измеримост (човешки загуби, финансови загуби и др.). След сравняване на опасностите, тази с най- висока стойност се детайлизира в съответствие с набор от принципни технически решения, водещи

до намаляване на заплахата. Така например, ако изходящото производство е с токсични параметри и е заплашено от възникване на пожар, то при проектиране на такава технология трябва да се предвидят хранилища за такива продукти с по-висока степен на противопожарна защита.

Такъв подход при процеса на проектиране позволява да се изгради производство с висока съчетаемост на елементите и възможност за по-добро взаимодействие между отделните елементи и между технологиите и околната среда.

Решаващо значение за високата безопасност има изследването на техническите системи в процеса на въвеждане в експлоатация и контрола им през целия жизнен цикъл. Извършената експертиза определя промените в експлоатационните характеристики, намаляването на ресурса, нарушения в изискванията за безопасност, заложени в проектната документация. За нейното провеждане е препоръчително да се проучат и вземат в предвид няколко важни фактори:

- нарушения на безопасността, които изискват подробно изследване на заплахата от отделни детайли или цели производства;
- в процеса на експлоатация, ремонтни дейности на системата е имало произшествие или нещастен случай;
- процесът на цялостна експлоатация показва, че технологичната система притежава висок потенциален риск на опасности (загуби, замърсявания);
- техническата система има дълъг експлоатационен период;
- техническата система е била подложена на значителни промени от технологично или елементно естество;
- изследванията се провеждат последователно или в комбинация с други паралелни системи.

Провеждането на експертиза на безопасността на система, намираща се в експлоатация, изисква допълнителен ресурс от време, необходимо на екипа за издирване на технологични схеми и стари инструкции за експлоатация. Подготовката на екип и разработване на ефективна форма за извършване на препоръчителните действия и оценка на резултатите се определя от персоналните особености на всяка система.

Резултатите от изследванията и тяхната регистрация се превръщат в "архив", картотека на опасностите, като екипите обобщават и представят документи и сведения:

- технологични карти, инструкции, хистограми, подкрепящи извършената експертиза;
- доклади на отделните екипи, подкрепени с резултати от технически измервания;
- регистрация на промени в "архива" се въвеждат ако:
  - ✓ има изменения в производствено-техническата система или в целия процес;
  - ✓ поява на нова информация за опасни вещества и нов заплахи;
  - ✓ промени в техническите подобрения на същия технологичен процес.

Създаването на "архив" и събирането на отчетни документи съответства на определени формуляри, които са източници за следващи контроли на безопасността. Съдържанието на "архива" е предмет на отчетността във фирмата-производител и част от декларацията за безопасност.[4] Тя съдържа описание на техническа систе-

ма и данни за оценка на обекта. Описанието е инициращ документ и той следва да съхранява информация за основните показатели на обекта:

- топография на обекта (местност, сгради, допирни зони със съседни обекти - училища, автомагистрали и др.);
- описание на производствения процес и възприетата технология;
- конструктивни особености и използвани суровини и материали;
- устойчивост на конструктивните параметри - високо налягане, високи температури, обеми от суровини и др.;
- зони за опасност (зони на взривове, зони за разпространение на отровни вещества, радиация);
- възможности за достъп в производствената зона и сградите, пътища за евакуация;
- места за разполагане на системите за контрол и средствата за автоматична защита;

Описанието на производствения процес и възприетата технология са обем от сведения, които разкриват заплахите към експлоатацията на системата. Те са основата за разработване на мероприятия за повишаване на безопасността:

- предназначение на производството;
- основни операции - химически реакции, термични процеси, процеси при високо налягане, очистване на атмосферния въздух и отпадните води;
- описание на процесите - температурни граници, разход на материали, шумове, вибрации и др.
- енергоемкост на производството - електрическа енергия, природен газ, сгъстени елементи (въздух, водород, кислород, пропан-бутан и др.);
- системи за автоматична вентилация и гасене.

Допълнително в оценката се обобщават обемите и вида на опасните вещества, произведени в общия технологичен процес и техните характеристики (температура, налягане, токсичност). Анализират се формите и състоянието на веществата, при които те се намират в производството, възможностите за тяхното неконтролирано смесване и опасностите, които биха се получили от това.

На основа на анализа на производствения процес, състоянието на системата и използваните опасни вещества се изработват изводи за общата опасност на обекта и мерките за предотвратяване на заплахите за населението и околната среда.

Окончателната оценка се оформя след развитието на сценарии на възможните последствия от аварии, които могат да имат въздействие върху персонала, околното население и природната среда. За такава оценка се разработват:

- описание на вероятната авария (пожар, повреда на клапан, разрушение на тръбопроводи и др.);
- оценка за изпускане и възможните количества енергия или опасни вещества;
- дисперсиране на изпуснатите количества вещества в атмосферата и анализ на токсичните концентрации;
- оценка на въздействието (летални изходи, разрушения в инфраструктурата).

Промишлените производства не притежават абсолютна безопасност и подробната оценка на заплахите, уязвимостите и опасностите не гарантират нулева вероятност от аварии. По тези причини в общия регистър от дейности се включват и мерките за намаляване на влиянието и снижаване на последствията, предвидени в

законовите норми, обхващащи разработване на план за защита и предприемане на контролни дейности. [3]

Цялостната дейност по разкриване, експлоатация или ликвидация на опасните производства се провежда под контрола на органите на местна власт и обществото. Процесите по разработването и експлоатирането на производства с опасни рискове се извършва в строга последователност и в съответствие с определените изисквания. Те са отговорност на ръководителите на обекта, които трябва да изпълняват определени изисквания:

- производителят да има лиценз за експлоатация на техническо опасен обект;
- да има обучен и подготвен персонал за работа в опасна среда;
- да се извършва контрол на изискванията за безопасност;
- да са осигурени прибори за технически контрол на опасните лъчения, изпускани отровни вещества и др.;
- да извършват периодична диагностика и експертиза на безопасността;
- периодично да извършват проверка на производствената дейност и да отстраняват предписанията на контролните органи;
- да разработят мерки за защита на персонала, населението и околната среда;
- да анализират и отстранят причините за аварията;
- да информират местните органи за управление при авария;
- да предприемат преустановяване на опасното производство при авария, инцидент или при промяна на техническите параметри на експлоатация;
- да провеждат мероприятия по локализиране и ликвидиране на последствията от аварии.

Действията по локализиране и ликвидиране на последствията от техногенните аварии също са отговорност на организацията, експлоатираща конкретното производство. Тя е отговорна да разработи планове, да поддържа собствена система за диагностика и контрол, да обучава персонала и собствени аварийни органи, да създава финансов ресурс за тези дейности.

В практически план не съществува еднозначна стратегия, която да решава проблема с безопасността в техносферата. Възможните подходи за решението ѝ следва да се търсят в следните направления:

- разпределение на отговорностите по веригата производител - население, обществена организация - власти;
- търсене на оптимални взаимодействия между оператора и техниката (технологията) чрез оперативни реализации;
- изграждане на потенциално опасните обекти с присъщи за тях системи за диагностика и защита от аварии.

ЛИТЕРАТУРА:

1. Ветошкин А., Таранцева А. Техногенный риск и безопасность. Пенза 2002.
2. Директива 96/82/ЕС (Севезо) за контрол на риска от големи аварии, приета на 9 декември 1996 г. допълнена с Директива 2003/105/ЕО.
3. Закон за опазване на околната среда, Обн., ДВ, бр. 91 от 25.09.2002г.
4. Lees F.P. Loss Prevention in the Industries. Butterworths, London, 1980.

СЪЩНОСТ И ЗНАЧЕНИЕ НА СЪПЪТСТВАЩИТЕ ЗАГУБИ

Калоян А. Илиев

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

NATURE AND SIGNIFICANCE OF COLLATERAL DAMAGE

Kaloyan A. Iliev

ABSTRACT: *Leading militarily states implement fundamental reform (transformation) of the armed forces to adapt to threats, risks and challenges of the new information age. Military construction in these countries are subject to the new military strategy, the essence of which is the purpose of the war (military conflict) to be achieved in the shortest possible time and with minimal losses.*

KEYWORDS: *incidental loss, armed forces, local conflict, military operations, collateral objects, methodology for assessment of collateral damage.*

Военните операции в настоящия момент и тези, проведени през последните години, показват, че е необходимо постоянно изменение в целите, задачите, структурата и организацията на съвременните армии.

Анализът на такива операции показва, че структурата за коалиционните сили в Ирак, Афганистан, Косово, Босна и Херцеговина постоянно претърпяват изменения в числеността, задачите, целите и приоритетите в зависимост от конкретната обстановка на операцията и определения желан краен резултат.

В съвременната среда на сигурност по-голяма част от операциите са съвместни по своята същност. Това е така поради естеството на съвременните заплахи и необходимостта от справяне с тях, което не е възможно да се постигне чрез използване на способностите само на един вид въоръжени сили.

Това налага, както при планирането, така и при провеждането на операциите, да се прилага съвместния подход.

В света съществуват много организации и най-вече НАТО и Европейския съюз, които поддържат, ръководят и изпълняват политика при възможност да не се нанасят огневи удари или да не се допускат съпътстващи загуби при нанасянето им в съвременните военни конфликти по света. При ангажиране на сили от НАТО, на които сме свидетели от последните проведени операции в Косово, Афганистан, Ирак, Либия, когато се планират и нанасят огневи удари задължително се отчитат и нивата на съпътстващите загуби.

Съпътстващите загуби са определени като неумишлено или случайно наранени или поразени хора и/или обекти, които не са валидни военни цели по време на нанасянето на огневи удар. Тези загуби няма да се смятат за нарушение на правото, когато са съпоставими с очаквано военно предимство от атаката (JP 1-02, JP 3-60).

При планиране и управление на операциите обединеният щаб е отговорен за политика без нанасяне на удари, за които не е извършена оценка на съпътстващите

загуби. Щабът изпълнява тази си функция чрез структура за управление на разузнаването на военни цели MTIMS (Military Target Intelligence Management Structure), в сътрудничество с бойните командвания и службата за разузнаване. Ролята и специфичните характеристики на политика без нанасяне на удари, за които не е извършена оценка на съпътстващите загуби, са следните:

• Развиване на обща политика и ръководство за оценка на съпътстващите загуби.

• Съгласуване с бойните командвания, службите, агенциите за бойна поддръжка и обединената група за техническо координиране ефективността на боеприпасите за определяне на оперативните изисквания, които осигуряват рамката на методиката за оценка на съпътстващите загуби.

• Осигуряване на контрол за цялостното обучение при изучаване на методиката за оценка на съпътстващите загуби.

• Поддържане на база от данни от обучени и сертифицирани анализатори (включваща име, звание, дата на обучение, резултат, обучен от..., валидност на последната промяна), която да валидира искания за службите от бойните командвания или организациите, желаещи да имат обучение в курс за изучаване на методиката, както и да координира акредитацията на този курс.

• Валидиране на нова информация за съпътстващи загуби преди нейното включване в методологията.

• Осигуряване преглед на таблиците за гъстотата на населението, за да осигури стандартизираното им издаване за използване.

• Преглеждане и координиране на изискванията за автоматизация; осигуряване прегледа и развитието на автоматизираните програми за гарантиране на политика, обучаване и синхронизиране на програмите.

• Известяване структурите на министерството на отбраната, когато се съставят нови таблици за радиуса на съпътстващите загуби за боеприпасите и техниките на нанасяне на удари.

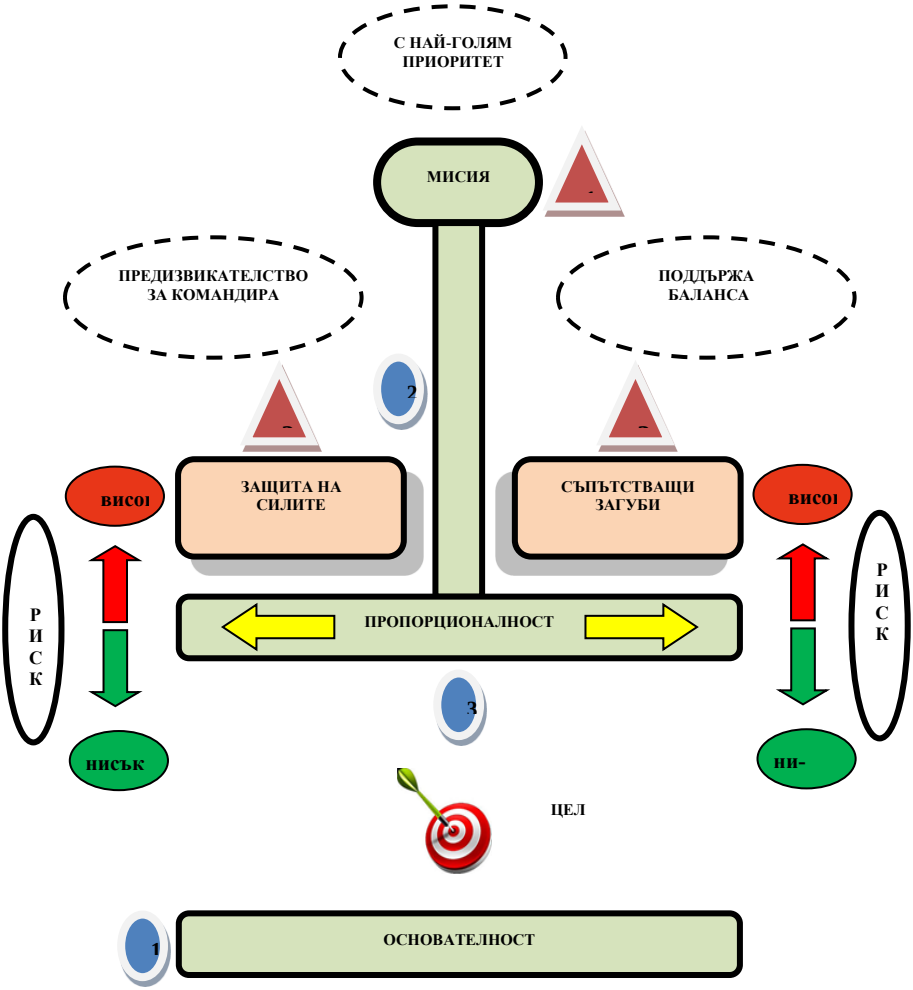
В САЩ и НАТО е създадена Обединена техническа група за координи-ране ефективността на боеприпасите (ОТГКЕБ). Това е обединена организа-ция, управлявана от център по логистика. Тя ръководи работни групи, които се фокусират върху специфични аспекти на избора на огневото средство (weaponering), ефекта от него и съпътстващите загуби.

На тази група следва да се възлагат следните отговорности:

- Развиване и публикуване на информация за ефективността на конвенционалните оръжия. Групата, в координация с щаба, следва да развива, поддържа и разпространява таблици, отнасящи се до оценката на съпътстващите загуби, които пък са основа за оценка на съпътстващите загуби;
- Изработване на таблици за оценка на съпътстващите загуби, отделно от приетите нормативни документи, когато се приемат на въоръжение нови образци оръжия. Таблиците следва да се изготвят не по-малко от два пъти годишно и се разпространяват от групата до потребителите;
- Допринасяне за техническо допълване на приетите нормативни документи, едновременно с развиването и пускането в употреба на нови продукти и нови данни за ефекти на огневите средства;
- Одобряване на средства, източници и методи използвани за изобразяване или калкулиране на стойностите на радиуса на ефекта за съпътстващи загуби, към

таблиците, отнасящи се до оценката на съпътстващите загуби и данните за ефективността на огневите средства.

Въз основа на предложенията на тази група командващият на съвместните сили може да вземе решение за поразяване на различни по характер цели, които допринасят за постигане целите на операцията. (фиг. 1).



Фиг. 1

При вземане на такова решение следва да се използват два принципа – оперативен и правен.

Оперативните са постигане целта на операцията - мисията, защита на собствените сили, недопускане на съпътстващи загуби.

Правните положения са основателност, необходимост, пропорционалност.

Правото налага да се нанасят удари само по военни обекти, да е налице въздържане от целенасочено поразяване на цивилно население и сгради (жилища, болници, училища, религиозни обекти и т.н.). То също изисква допусканите цивилни жертви и разрушения да не са крайни при постигането на определен военен успех.

Правните принципи при вземане на решение за нанасяне на огневи удари по цели са три:

- Първи - дали е налице правната основателност за нанасяне на удар по дадена цел.
- Втори - необходимо ли е да се нанесе огневи удар по целта.
- Трети – задължително е употребата на пропорционална сила за огнево въздействие по целта.

Несъблюдаването на тези положения може да предизвика прекомерни отрицателни ефекти върху цивилните и да бъде нарушение на правото. Нещо повече, политическите лидери и военачалниците могат да станат обект на масирана критика, която да повлияе тежко на военните цели, съюзниците, партньорите или националните цели. Командващите на операциите в НАТО оценяват високо съхраняването на живота на цивилните. Военнослужещите от всички нива трябва да демонстрират тези ценности при използването на сила за изпълняване на поставените военни задачи и недопускане на съпътстващи загуби.

При разглеждане на съпътстващите загуби е необходимо да се имат предвид защитените уязвими невоенни обекти (съпътстващи обекти), целите с двойно използване и живите щитове.

Обекти, определени от международното право като цивилни (невоенни), се смятат за защитени. Познаването им е основното за развитие на процеса за поразяване на целите и те задължително се описват при правилата за бойно поведение на всяка операция (Operational ROE). Правилата за бойно поведение (ROE) са издадените от компетентните военни власти нормативни положения, които очертават обстоятелствата и ограниченията, при които въоръжените сили ще започнат и/или продължат бойните действия с насрещни сили (JP 1-02).

Защитените уязвими невоенни обекти са разделени в две категории, като определяща е тяхната чувствителност. Използват се кодове за всяка цел, обработена от разузнаването със стандартизирано описание (табл. 2).

КОД НА ЦЕЛТА:	ОПИСАНИЕ НА ГРУПИ ЦЕЛИ:
778XX	ДИПЛОМАТИЧЕСКИ ОФИСИ, ЧУЖДЕСТРАННИ МИСИИ И НЕПРАВИТЕЛСТВЕНИ ОРГАНИЗАЦИИ;
776XX	РЕЛИГИОЗНИ, КУЛТУРНИ И ИСТОРИЧЕСКИ ИНСТИТУЦИИ;
434XX	МЕДИЦИНСКИ СЪОРЪЖЕНИЯ;
721XX	МЕДИЦИНСКИ УЧИЛИЩА;
496XX	ЦИВИЛНИ УЧИЛИЩА (НО НЕ И ВОЕННИ УЧИЛИЩА);
75300	БЕЖАНСКИ ЛАГЕРИ;
75900	ВОЕННОПЛЕННИЧЕСКИ ЛАГЕРИ;

КОД НА ЦЕЛТА:	ОПИСАНИЕ НА ГРУПИ ЦЕЛИ:
775XX	ДЪРЖАВНИ ЗАТВОРИ;
43210	СЪОРЪЖЕНИЯ НА КАНАЛИЗАЦИОННАТА СИСТЕМА;
439XX	ЯЗОВИРИ;
438XX	ДИГИ И ДРУГИ ВОДНО КОНТРОЛИРАНИ СЪОРЪЖЕНИЯ;
77700	БИБЛИОТЕКИ.

Таблица 2

Първа категория защитени уязвими невоенни обекти включва:

• дипломатически офиси, чужди мисии и неутрална невоенна собс-твеност на други нации в зоната на операцията;

• религиозни, културни, исторически институции и структури;

• международни организации (ООН, НАТО) и неправителствени органи-зации (Международния комитет на Червения кръст и Червения полумесец, „Амнести Интернешънъл“), собственост, оборудване и личен състав;

• медицински съоръжения (цивилни и военни);

• обществено-образователни струкури – невоенни училища, колежи, университети и институти;

• бежански лагери;

• пленнически лагери и държавни затвори;

• съоръжения, които след поразяване ще доведат до замърсяване на питейна вода, потоци и реки;

• язовири или диги, чието поразяване може да предизвика наводняване на цивилни области.

Втора категория защитени уязвими невоенни обекти включва останалите обекти, определени като защитени от военното право:

• невоенни помещения за настаняване;

• цивилни места, включващи стадиони, паркове, театри, супермаркети и райони за възстановяване;

• обществени съоръжения, предназначени за пренасяне на електро-енергия, петрол или вода за консумация от цивилните, бензиностанции, транспортни съоръжения, пожарни, пощи, полицейски участъци и финансови институции;

• земеделски складове;

• съоръжения с непознато предназначение.

• защитените уязвими невоенни обекти могат да бъдат променени (за САЩ от президента или министъра на отбраната), като това се отразява в правилата за бойно поведение.

Цели (обекти) с двойно използване (предназначение) – Dual-Use Target – военно и цивилно, са:

• съоръжения за командване и управление на високо правителствено равнище;

• инфраструктура на националната комуникационна система;

• медийни центрове;

• национални електрически и петролни съоръжения;

• индустриални мощности и обществени съоръжения, осигуряващи поддръжка за цивилното население и военната кампания.

Цели с двойно предназначение също може да бъдат обекти, защитени от правото, но заети от бойци (combatants). Защитени от правото структури, заети от бойци, изпълняващи военна задача, губят правната защита и се смятат за военни цели.

На базата на текущите разузнавателни данни командирите са отговорни да определят преобладаващата функция на защитени от правото структури и дали целта е с двойно предназначение. Правилата за бойно поведение за всяка операция осигуряват права и/или забрани за поразяване на цели с двойно предназначение.

Независимо от действащите правила за бойно поведение цивилните, работещи в границите на цел с двойно предназначение, трябва да бъдат смятани като съпътстващи загуби при оценката им, съгласно методиката за оценка на съпътстващите загуби (Collateral damage estimation methodology – CDM).

Живи щитове са цивилни или невъоръжени лица, разположени около действаща военна цел, за да се възпрепятства поразяването ú. В някои случаи живите щитове са в съучастие и доброволно подкрепят действията на противника. В този случай те губят статута си на защитени и са валидни военни цели. В други случаи неприятелската страна може насила да принуди цивилни да прикриват военни цели. Тези лица са защитени и няма да бъдат поразявани (обстрелвани). Само недоброволни живи щитове следва да бъдат вземани предвид за оценка на съпътстващите загуби. Ако статутът на живите щитове не е ясен, се прилагат най-рестриктивните правила и те трябва да бъдат защитени като уязвими невоенни обекти (съпътстващи обекти).

Съпътстващи обекти (Collateral objects) са цивилни и невоенни обекти, структури, машини и материали, които не поддържат дейностите и/или функциите на противниковите военни или бойни способности.

От изложеното по-горе е видно, че водещите във военно отношение държави, който са участвали във военните конфликти през последното десетилетие са оценили важността от отчитането на съпътстващите загуби.

За да може да има съвместимост в работата на щабовете в Българската армия с тези в НАТО, е необходимо създаването на техническа група във всеки щаб, която да е отговорна за координиране ефективността на използване на боеприпасите по различните по характер цели на бойното поле и тя да дава необходимата информация на командващия на съвместните сили за вземане на решение за въздействие по целите с отчитане на съпътстващите загуби.

ЛИТЕРАТУРА:

1. НП-3, Доктрина за провеждане на операциите, С., 2012 г.
2. Национална отбранителна стратегия, С., 2011 г.
3. Стратегия за национална сигурност, С., 2011 г.
4. MC – 471/1 – NATO Targeting Policy – 2007.
5. Joint Targeting Cycle and Collateral Damage Estimation Methodology (CDM)
6. JP 1-02, Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 2010.
7. JP 3-60, Joint Publication 3-60, Joint Targeting, 2007.
8. http://www.dtic.mil/doctrine/training/trainingsystem.htm, 25 януари, 20,00

РЕД ЗА ОЦЕНКА НА СЪПЪТСТВАЩИ ЗАГУБИ

Калоян А. Илиев

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

PROCEDURES FOR EVALUATION OF COLLATERAL DAMAGE

Kaloyan A. Iliev

ABSTRACT: *Strategic environment is influenced by unpredictable and dynamic political, social, technological and military processes. Conflicts are complex and difficult to predict and control. This requires flexible policy development, organization, doctrine, operational concepts, and above all the capabilities of future forces and command structure of the Armed Forces.*

KEYWORDS: *evaluation of collateral damage, techniques to reduce collateral damage, armed forces, local conflict, military operations, methodology for assessment of collateral damage.*

Настъпилите и настъпващите изменения в световен и регионален мащаб, в резултат на подписаните договорености и политически съюзи довеждат до създаването на нова постоянно изменяща се система от международни отношения, основаващи се на взаимното уважение и стремеж за сигурност и сътрудничество чрез споделяне на сили и средства за поддържане на мир.

В много от страните членки на НАТО е възприет определен ред за оценка на съпътстващи загуби и най-вече при нанасяне на огневи удари. Проблемът не е развит в компонентните командвания и в тактическите формирования, при което този ред не дава пълен отговор на въпроса „Каква е взаимовръзката между средствата за въздействие, средствата за разузнаване, оценка на бойните загуби и намаляване до минимум на съпътстващите загуби, при поразяване на различни по характер цели от оперативните и тактическите звена?".

До 2010 г. съществуват няколко методики за оценка за съпътстващите загуби (МОСЗ) при нанасяне на огневи удари (САЩ, Великобритания и др.).

Методиката на Великобритания определя четири нива за съпътстващи загуби, като определя и нивото на командващите, даващи разрешение за нанасяне на удари за всяко от тях. Методиката на САЩ използва пет нива, като всяко има поднива:

„Ниско" и „Високо" – например „Ниво 3 ниско".

По своята същност реда за оценката следва да включва общи стандарти, методи, техники и процеси, и те да се прилагат при планирането на съвместната огнева поддръжка с цел оценка и минимизиране на съпътстващите загуби.

Реда за оценка на съпътстващите загуби следва да бъде използван постоянно по всички нива на командване, да поддържа общи стандарти и да осигурява командирите и щабовете с обща процедура при вземането на решения.

Този ред за оценка следва да подпомага командирите да преценят риска срещу военната необходимост и пропорционалността за използване на сила в процеса на вземане на решение. При това резултатите от оценката следва да станат средство за

командващия на съвместните сили (командирите на компоненти) за спазване на принципите на международното право. Освен това оценката следва да бъде баланс между наука и изкуство, която показва най-добрия резултат за потенциални загуби на съпътстващи обекти.

За уеднаквяване на процедурата при планиране на операциите днес в НАТО е приета методиката за оценка на съпътстващите загуби на САЩ. Тя включва общи стандарти, методи, техники и процеси, прилагани при планиране на огневите удари с цел оценка на съпътстващите загуби, както и използване на всички способи за тяхното намаляване. Подпомага командирите да претеглят риска срещу военната необходимост и преценка на пропорционалността за използване на сила в процеса за вземане на решение. Накратко, методиката е средство за командващия за съблюдаване на правото.

Методиката за оценка на съпътстващите загуби е баланс между наука и изкуство, която показва най добрия резултат за потенциални щети на съпътстващи обекти.

Като наука методиката използва комбинация от данните от резултати от научни експерименти, вероятност, исторически наблюдения и комплекс от моделиране на оценки на съпътстващи загуби.

Науката обаче е ограничена от количеството и надеждността на събраните и анализираните ефекти за боеприпасите и целите. Освен това тя не може винаги да съвпада с динамичната и оперативната обстановка. Изкуството в методиката не е само допълващо. Офицерите по целите/за огнева поддръжка (targeteers/fire supporters), разузнавачите и операторите трябва да използват общата експертиза, опита и последните разузнавателни данни, за да приспособят науката към оперативната среда. Взети заедно, науката и изкуството в методиката за оценка на съпътстващите загуби осигуряват важна информация, за да може командващият да я прецени в обстановката и да определи ефектите за поразяване на определена цел с използване на огневи удари.

Важно е да се спомене, че информационната операция (IO) е основна част от стратегическата комуникационна кампания, която пък е елемент на военната стратегия.

Правилното управление на процеса за недопускане на съпътстващи загуби спомага до голяма степен за успеха на информационната операция, а оттам и за изпълнение на плана за стратегическа комуникационна кампания.

Методиката за оценка на съпътстващите загуби подпомага използването на конвенционални боеприпаси през всички фази на военния конфликт. Тя осигурява командващите с информация за ефекта на боеприпасите, инци-дентни обстоятелства и техники за намаляване ефекта на боеприпасите.

Техническите данни и процеси в методиката са извлечени от ком-пютърно моделиране, изпитване на оръжия и наблюдения при бойни действия. Тези източници съдържат в някаква степен грешки и неизвестност. МОСЗ не предрича резултата от използване на оръжието. Оперативната среда, надеждността на оръжието и достоверността на разузнавателните данни са първичните фактори за оценка на съпътстващите загуби от бойното използване.

Методиката следва устойчив процес, генерира очаквани величини и нито анализаторите, нито командващите трябва да остават с впечатлението, че тези величини са абсолютна истина, наука и изключително точни данни.

Резултатите от методиката не са единствените данни при вземането на решение. Целите на операцията, правото, правилата за бойно поведение, характеристиките на целите, рискът за собствените войски и стратегическият риск са пример за други фактори, които допринасят за вземането на решение.

Специфичните правила за бойно поведение, приети за дадена операция от военното командване на НАТО, определят праговете за допустими съпътстващи загуби. Например за цивилни жертви (невоенни лица): число (Non combatant Casualty Cut-Off Value – NCV), което за Афганистан е „0“, а за Ирак – „29“. Праговете са обвързани с правилата за бойно поведение, като определят и изискванията, и реда за докладване и отговорности при допустими съпътстващи загуби на стратегическо, оперативно и тактическо ниво. МОСЗ трябва да се прилага напълно и изчерпателно при специфичните съображения за операциите. Тя следва да бъде относително гъвкава да посрещне скоростта и темпото за провеждане на операцията. МОСЗ трябва да остане приложима при промените на оперативната обстановка и достатъчно обща за повечето географски области или области на конфликти.

МОСЗ трябва да бъде прилагана постоянно по всички нива на коман-дване, да намалява до минимум объркването, да поддържа общи стандарти и да осигурява командирите и щабовете с обща процедура при вземането на решение. Командващите обаче могат да изследват използването на нови техники за намаляване въздействието на боеприпасите, като прилагат следните правила и ограничения:

• Техниките за намаляване на съпътстващите загуби (mitigation techni-ques), непосочени изрично в тази методика, не могат да бъдат представени като част от оценката.

• Командващият (или оторизираните за нанасяне на удари) трябва да бъде информиран за допусканията, грешките, фактите и придружаващите техники за намаляване на съпътстващите загуби.

Командващите прилагат методиката, концепциите и изводите за пла-ниране на огневите удари най-вече до оперативното ниво. МОСЗ е гъвкава за прилагане по време, важни моменти от операцията и е предназначена за обучен анализатор бързо да изготви оценка на съпътстващите загуби.

МОСЗ обаче няма намерение да забрани на командващия да порази важните цели – критични по време (TST/time sensitive targets – цели, оп-ределени и поразявани със средствата на командващия на съвместните оперативни сили).

В допълнение МОСЗ не ограничава командира за самозащита в съот-ветствие с правото. Когато използването на сила за самозащита е необходимо, включително в ситуации при войски в боен контакт, естеството, продължителността и обсегът на действие не трябва да превишават необходимото за отговор на неприятелски дейности или демонстрираното неприятелско намерение.

Концепцията за пропорционалност при самозащита не следва да се бърка с опитите за намаляване на съпътстващите загуби и другите догми на правото при военните операции.

МОСЗ усъвършенства ефективността на операцията и е в съответствие с обичайното международно право.

Тази методика директно подкрепя установяването на целите като „критични“. Ограничения и изключения МОСЗ има предвид всички конвен-ционални боеприпаси в САЩ. Тя не се прилага за ядрено оръжие, информационни средства или непоразяващи оръжия.

Оценката за съпътстващи загуби, както е определена в МОСЗ, не се използва

при стрелба с право мерене (противотанкови оръдия, танкове), атакуващи вертолети и изтребители, въоръжени с оръдия с калибър под 105 мм. Рискът от съпътстващи загуби от тези системи е представен при попадането на боеприпасите в района на целите, а не от експлозията (разрива). Правните концепции за пропорционалност, необходимост и основателност са отчитани при стрелбата с право мерене.

МОСЗ не отчита грешките на оръжейните системи, грешките при попаденията на разривите или измененията в начина за поразяване на целите. МОСЗ допуска, че оръжейните системи ще функционират както са конструирани и ще поразяват целите за постигане на желания ефект.

МОСЗ не отчита неизвестни преминаващи цивилни или оборудване в близост до района на целите. Това включва коли и цивилни по път и всичко друго, чието присъствие в областта на целите не може да бъде предвидено. Изключително право на командващите от всички нива е да се стараят да определят (предвиждат) наличие на цивилни или имущество в района на целите и да отлагат огневите удари, когато е възможно.

МОСЗ не отчита индивидуалните коригирания на огъня при артилерийския огън. Командирите трябва да остават осведомени и да изстрелват минимален брой маркиращи или целеуказващи боеприпаси, за да постигнат желания ефект за поразяване на целта.

МОСЗ не се използва при касетъчните боеприпаси или усъвършенстваните конвенционални боеприпаси след трето ниво на оценка на съпътстващите загуби, поради по-големия риск от неексплодирали боеприпаси и ограничените възможности за избор на средство за намаляване на риска от съпътстващи загуби.

Боеприпасите с реактивен двигател за увеличаване на далекобойността, минохвъргачките и морските оръдия не се използват при нива по-големи от „3“, поради чувствителното увеличаване на балистичната грешка и значителното увеличаване на риска при тяхното използване в градски условия.

Докато МОСЗ може да бъде приложена във всеки географски район, ефектът от боеприпасите може да варира в различни условия. Най-общо МОСЗ и данните за ефективността на оръжията, като база за околност и терен, използват комбинация от равен терен, заоблени хълмове и мека почва. Пустинните области и джунглите, както и областите с каменист терен могат да променят ефекта от използването на боеприпасите. Командирите трябва да отчитат всяко условие на района на целите при оценка на съпътстващите загуби.

Процеса за изготвяне на оценка за съпътстващи загуби при нанасяне на огневи удар по определена цел от списъка на целите се поразява, след като бъдат изготвени и взети предвид отговорите на пет базови въпроса:

1. Има ли положителна идентификация на целта (характеристика, място, време)?

2. Има ли защитени съпътстващи обекти, цивилни, недоброволни живи щитове или значителни уязвими съоръжения в обхвата на ефективното поразяване на оръжието, което ще използваме?

3. Може ли да се намалят щетите на тези защитени обекти, поразявайки целта с друго оръжие или с друг метод, при които ще бъде изпълнена бойната задача?

4. Ако не се отговори положително на третия въпрос, колко цивилни (съпътстващи загуби) ще бъдат ранени или убити при атаката?

5. Ще бъдат ли съпътстващите загуби прекалено големи във връзка с очакваното военно предимство и дали се нуждаем от разрешение от старшото командване за

атакуване на целта, базирано на действащите правила за бойно поведение? В пето ниво „Високо“ или „Ниско“ се определят дневно, нощно или епизодично очакване на загуби в личен състав?

Съществуват пет етапа (едновременно и нива) на оценка на съпътстващите загуби (ОСЗ) (схема. 1):

ОСЗ 1 (CDE 1): Утвърждаване на целта/Първоначална оценка

ОСЗ 2 (CDE 2): Общо/Оценка на размерите на целта

ОСЗ (CDE 3): Избор на огнево средство за поразяване

ОСЗ 4 (CDE 4): Прецизна оценка

ОСЗ 5 (CDE 5): Оценка на жертвите

При ОСЗ 1 се работи по следните въпроси:

1. Има ли положителна идентификация на целта – Да/Не

2. Определени ли са границите на целта спрямо други обекти – Да/Не

3. Поразяването на целта оторизирано ли е от правилата за бойно поведение – Да/Не

4. Целта с двойно предназначение ли е – Не/Да

5. Има ли наличие на обекти в поразяващия радиус на боеприпасите – Не/Да

6. Съществува ли риск от поява на облак отровни газове или радиоак-тивен облак – Не/Да

7. Съществува ли риск от наводнения, свлачища и т.н в района – Не/Да

ОСЗ 1– Ниска/Висока

При отрицателни отговори на първия и третия въпрос се прекратява изпълнението на задачата. При положителни отговори на шестия и седмия въпрос се осъществява задължително допълнителна оценка.

При ОСЗ 1 „Висока“ се преминава към ОСЗ 2:

1. Проверяват се минималните размери на целта и възможността тя да се порази с огън от закрита огнева позиция или неуправляеми бомби. При „Да“ се преминава към трето ниво, а при „Не“ се смятат единствено високоточни средства за поразяване на целта.

2. Обща оценка на високоточните оръжия (единични или касетъчни). Има ли обекти в зоната за поразяване? При „Не“ – приема се ниско ниво, а при „Да“ се приема високо ниво и се преминава към ОСЗ 3:

1. Измерва се и се записва разстоянието от точката на прицелване в зоната за поразяване с авиационни бомби или артилерийски боеприпаси до най-близкия уязвим обект.

2. Необходимо ли е използване на боеприпаса без техники за намаляване на неговото поразяване? При „Да“ – висок риск за щети, се преминава към пето ниво.

3. Може ли да се избере огнево средство при ОСЗ 3, със съответните данни за радиуса на поразяване на уязвимите обекти (в метри или футове). При „Да“ се приема ниско ниво, а при „Не“ се преминава към ОСЗ 4:

1. Оценяване и записване на структурата (тип на постройката, материал за построяване, брой на етажи, размери и т.н.) на уязвимите обекти.

2. Избиране на огнево средство.

3. Сравняване на радиуса за поразяване – дали е по малък от разстоянието до уязвимите обекти.

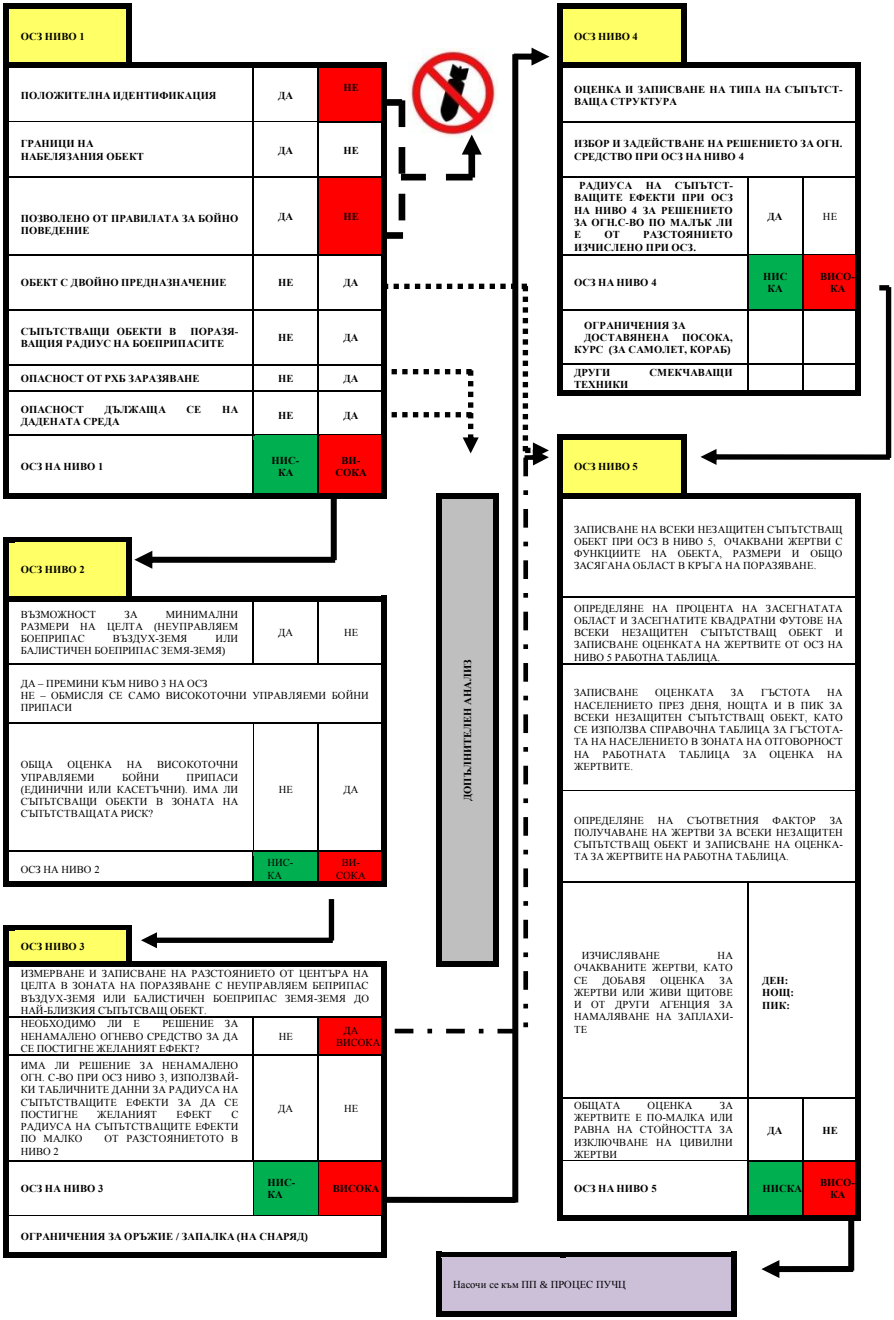


Схема 1. Модел за оценка на съпътстващите загуби (вариант

КРАЙНА ОЦЕНКА НА СЪПЪТСТВАЩИТЕ ЗАГУБИ					
ОСЗ НИВО	**НИСКО / ВИСОКО**	**КЛАС НА ОРЪЖИЕТО /ВИСОКОТОЧЕН БОЕПРИПАС/ АВИАЦИОНЕН НУРС/ БАЛИСТИЧЕН БОЕПРИПАС И ДРУГИ/**	**ОГРАНИЧЕНИЕ ЗА ИЗБОР НА С-ВО ЗА ПОРАЗЯВАНЕ**	**ГЛАВНИ ОГРАНИЧЕНИЯ**	**ОЦЕНКА НА ЖЕРТВИТЕ**
ОСЗ : ____					**ДЕН: __ НОЩ: __ ПИК: __**

Схема 2. Крайна оценка на съпътстващите загуби (вариант)

4. При „Да“ – ниско ниво, а при „Не“ – високо ниво, се преминава към ОСЗ 5:

1. Записване на всеки незащитен обект в нивото за очаквани жертви с функциите на обекта, размери и общо засягана област в кръга на поразяване.

2. Определяне на процента от засегнатата област – в квадратни футове за всеки обект и записване в работна таблица на хартия.

3. Записване на дневен, нощен и епизодичен очакван брой хора за съответните сгради (обекти).

4. Определяне на съответния фактор за получаване на жертви (1 или 0,25).

5. Изчисляване на очаквани жертви за ден, нощ, епизодични събития (табл. 4).

6. Общият брой на очакваните жертви не надминава числото NCV (по-малко или равно на допустимо число жертви съгласно правилата за бойно поведение). При „Да“ – ОСЗ 5 е „Ниско“, а при „Не“ – „Високо“.

Ако числото на очакваните жертви е по високо от NCV, целта не може да бъде поразена с решение на командващия на театъра на военните действия.

При такива ситуации се използват различни техники, като намаляване на поразяващите елементи или тяхното действие, които се постигат чрез:

1. Взривател на закъснител е първата техника за намаляване на осколките, ударната вълна и високата температура. Използва се при оценката от трето ниво нагоре.

2. Дистанционният взривател е първа техника за намаляване на падащите предмети и проникването на боеприпаса към основата на сградата.

3. Дистанционният взривател е втора техника за намаляване на ударната вълна и грешката при стрелбата. Ударната вълна се разнася бързо на открито, намалявайки три пъти силата от наземния взрив. Това е техника, която се препоръчва при четвърто ниво и при използване на артилерийски боеприпаси.

4. Защитни сгради (щитове) се използват само при налична структура и определен терен, намиращ се между желаната точка на прицелване и уяз-вимите обекти. Методът не може да се прилага за намаляване поразяването на развалините при наличие на хора извън сградите.

5. Промяната на ъгъла на атаката е първа техника за намаляване на ефекта от грешката при стрелбата. Бомбите имат тенденция да падат по-далече от точката на примерване.

6. Промяната на ъгъла на атаката е втора техника за намаляване на ефекта от осколките. Повечето осколки поразяват в предните квадранти от 270 до 90 градуса във връзка с ъгъла на атаката.

За постигане на оперативна съвместимост на националните формирования в многонационалните съвместни оперативни сили са необходими единни стандарти

при планиране на операциите, както във Въоръжените сили на Република България така на страните формиращи тези сили.

За да има определена съвместимост в работата на щаба на националните съвместни сили, компонентните командвания и тактическите формирования, в техния състав следва да се възприеме определен ред за оценка на съпътстващите загуби, който да отговаря на възприетите методи на работа в останалите страни членки на НАТО.

Ето защо е необходимо в щабовете на съвместното командване на силите, компонентите и тактическите формирования на Българската армия да се разработи и възприеме определен ред за оценка на съпътстващите загуби на различни нива за въздействие по целите и той да отговаря до известна степен на възприетия ред за оценка в останалите страни членки на НАТО.

ЛИТЕРАТУРА:

1. НП-3, Доктрина за провеждане на операциите, С., 2012 г.
2. Национална отбранителна стратегия, С., 2011 г.
3. Стратегия за национална сигурност, С., 2011 г.
4. MC – 471/1 – NATO Targeting Policy – 2007.
5. Joint Targeting Cycle and Collateral Damage Estimation Methodology (CDM)
6. JP 1-02, Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 2010.
7. JP 3-60, Joint Publication 3-60, Joint Targeting, 2007.
8. http://www.dtic.mil/doctrine/training/trainingsystem.htm, 25 януари, 20,00

НОВОНАЗНАЧЕНИТЕ ОФИЦЕРИ – ИЗРАСТВАНЕ И ПРОБЛЕМНИ ПРАГОВЕ

Станчо Г. Станчев

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

THE NEWLY APPOINTED OFFICERS - GROWTH AND PROBLEM THRESHOLDS

Stancho G. Stanchev

ABSTRACT: *This report presents some views on the problems faced by young officers at the beginning of their professional career.*

KEYWORDS: *young officers, realization, career development.*

Един от основните критерии за образователна ефективност на всяка обучаваща организация е „професионалната реализация" на кадрите, които създава. Процедурата, която осигурява реализацията на една такава цел, в контекста на мениджмън-

та на образованието, все още не е еднозначно дефинирана и апробирана в практиката. Това възпрепятства възможността за непрекъснат контрол и усъвършенстване системата за управление качеството на обучение на военнослужещите в Националния военен университет. В Тълковния речник термина „реализация" се представя, като осъществяване, прокарване на някакъв план и др. В този смисъл да реализираш нещо ще рече: 1. Да осъществиш да приложиш на дело. 2. Да постигнеш, да се докажеш. Така тълкувано понятието реализация на випускника би следвало да има връзка с вътрешната мотивация на личността в постигане на възможно най-добри резултати в работата, развитие в кариерата и осъществяване на мечтите.

„Има ли граница човешката мечта?" Все още вековете не са дали пълен отговор на този въпрос, както и на другия: „Защо основно сред младите хора изобилства от мечти?" Ясно е едно - ако само за миг си представим, че всички мечти и желания на младите хора се сбъднат, Земята ще заприлича на невероятно красиво разцъфнало дърво.

От друга страна, древните римляни са казвали, че колкото и да е силна дадена река при извора си - и най-слабата преграда може да я спре и да издигне непреодолим за нея праг, докато по-надолу, когато набере сили водата би разбила много по здрави и по-големи прагове! Тук ние поставяме нашите два въпроса - само за цъфтежа и за извирането ли са им стигнали силите и ако не, кой и как им пречи. И още нещо: нужно ли е да се заблуждаваме и да търсим проблемите не там, където са и да не виждаме праговете, които понякога се издигат пред едни, а пред други се монтират ескалатори, за да се придвижват по-бързо нагоре? Но не е ли в това причината, която унищожава плодовете в едните, и в другите?

Длъжни сме да назовем гласно тези прагове и да съдействаме за създаването на оптимални условия за изграждането на офицерите като инициативни, смели, със собствено мнение по всички въпроси, но с една обща цел - защитата на мира и отечеството.

Колкото и невероятно да звучи, първият праг пред младите офицери се издига още във Военния университет. Не е ли погрешна тоталната уравниловка? Без разлика на успеха и качествата всички курсанти получават едно звание. Нещо повече, след две-три години от производството посредственият курсант по силата на прослуженото време е станал командир на батарея, а като негови подчинени пристигат лейтенанти отличници. На какво ще се научат те от него? От друга страна, ако говорим за целесъобразни реформи, не е ли време да се потърсят някои по-смели и решителни промени? Сега през целия период на обучение курсантите са поставени при едни и същи условия на живот (изолираният от външната среда казармен начин). А защо след първата или втората година те да не са свободни след учебните занятия? По този начин бъдещите офицери няма да израстват под „похлупак". Те ще са опознали по-добре своите съвременници и бъдещи подчинени. След време срещата с тях няма да придобие формата на сблъсък, за което ще стане дума по-нататък. От друга страна, ще се извърши естествен подбор - склонните към нарушения, неумеещите да се самоконтролират и психически неустойчивите ще отпаднат преди да завършат Военния университет. Ще останат онези от тях, които няма да изхвърлят още през първите години „маршалския жезъл".

И все пак, както се казва в народната поговорка, това са само *бели кахъри* пред онези, които очакват младите офицери във военните формирования. Не рядко се оказва, че нагласата за професионално реализация не зависи толкова от тяхната

теоретична и методическа подготовка, а от интелекта и професионализма на техните командири, от микроклимата в офицерския колектив. Ще отчетем ли най-после, че стремежът за лъжливо представяне цели задоволяването на личните вкусове и капризи на отделни началници. Този стремеж води до опасни явления, като проявите на опекунство, недоверие и изземване на задълженията. От желание за „по-добро" иззехме задълженията на сержантите, като по този начин ги обезличихме, а сега сме тръгнали да обезличаваме взводните командири. Като че ли не им вярваме. От тези действия на практика понякога идва и резултатът - всяка дума на взводния командир да се диктува или заповядва И сами се превръщаме на такива, като искаме те, само послушно да изпълняват нашите нареждания. А къде са творчеството, креативността и инициативата на младия офицер, децентрализацията и делегиране на правомощия на подчинените, чрез даване на свобода на действията им в подкрепа естествено на намеренията на старшия командир?

В повечето случаи не многото работа, а лошите взаимоотношения, болните амбиции на някои по-старши командири, недостатъчната им подготовка за работа с хора, довеждат до грубост, до търсене на „цаката" и незачитане на личното достойнство на младия офицер. А това е поредният праг, преди да дойде разочарованието.

Образно казано, младият офицер излиза на „армейската сцена", когато главните герои – кадровите войници и останалите офицери - вече са заели своите места. Той се вклинява между тях и от двете му страни започва въздействие. От една страна, офицерите, имащи известен опит, му показват „добрите страни на службата", а от друга - кадровите войници му въздействат, чрез прилагане на методиката на „старото куче".

Как да реагира лейтенантът, в чиито представи войникът е изглеждал другояче? И тук започва сблъсък, от който ще паднат поне две-три листенца от цвета на мечтите. Редникът заплашва и заявява на своя взводен командир: „Не се занимавайте с мен, защото имам връзки!"

Естествено възниква въпросът, не е ли лъже-демокрация „грижата за редника", която демонстрират някои откъснали се вече от войнишките маси началници? Не е ли тя, която създава условия офицерът да бъде зависим от войника?

По-късно същият този редник отказва да изпълни заповед. Започва ходене по мъките - обяснения, обещания и пак нарушения. Дори и пред инспектората редникът заявява: „Младите офицери са зависими от нас - ако не поразим целите, на тях се карат, ако докладват за наше нарушение - пак те са виновни, че не умеят да работят индивидуално с нас. Виждал съм как им се карат."

Не е ли това още един праг пред младите офицери?

Искаме офицерите да водят методически издържани занятия, да бъдат всеотдайни, да постигат добри и отлични резултати подразделенията им, като естествено, следим педантично как изпълняват задълженията си, а не виждаме нито нуждите им, нито чуваме критиката им. Не е ли време да се види, че от грижи се нуждае младият офицерът, който с цената на много условности се стреми да изпълни функционалните си задължения? Този офицер има необходимост от жилище, какъвто по право се полага на всеки гражданин на страната ни, от време за повишаване на своята обща и професионална култура, от време за отдих и почивка. Ако той всеки ден не придобива и разширява знанията си, то решително ще изостане от своите

връсници в цивилния живот. Не е ли това пореден праг, който за мнозина офицери става непреодолим?

Сега често препоръчваме нестандартно мислене. Модно е, но то не е по-малко опасно от стандартното, ако е само мислене, а не действие, което да разкъса оковите на старото и да води до положителен резултат. Ето го противоречието според нас - съществуването на стандартното и нестандартното, и то в една и съща верига - висши, старши и младши офицери. Казваме открито, че ако не се преустрои генералът, безсмислено е да се иска това от лейтенанта, но как да се преодолеят натрупаните с години комплекси?

Мисля, че примери, в които се поставят прагове пред младите офицери, могат да се изброят немалко, но самото изброяване няма да доведе до премахването им. То само ще напомни, че има над какво да се замислим. Иначе ще остане като загадка: как при производството си младите офицери говорят за мечти и високи отговорности при изпълнение на задълженията си, а след няколко месеца и тонът, и мислите на повечето от тях са съвсем други - коренно противоположни от първоначалните нагласи.

ЛИТЕРАТУРА:

1. Андреев, М. "Процесът на обучението: Дидактика", УИ "Св. Кл. Охридски", С. 1996.

2. Чернов, А., С. Миллер. Профессионализм, компетентность выпускника высшего военного учебного заведения.

3. Гиндев, Е. Научен подход в управленските практики.-Военен журнал, 2007, № 1

4. Гюргаков, И. Пътища за повишаване на ефективността в обучението в системата на военното образование. - Военен журнал, 2012, № 2.

5. ACT Evaluation of Education and Training (E&T) Directive – Директива на Съюзното командване по трансформацията за оценка на обучението и подготовката; Bi-SC Directive 75-2 – Директива за обучение, подготовка, провеждане на учения и оценка (ETEED).

ПРЕГЛЕД НА ВОЕННИЯ БАЛАНС И СХВАЩАНИЯ ЗА БОЙНОТО ИЗПОЛЗВАНЕ НА АРТИЛЕРИЯТА НА СЪСЕДНИТЕ СТРАНИ НА РЕПУБЛИКА БЪЛГАРИЯ

Станчо Г. Станчев

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

REVIEW OF MILITARY BALANCE AND PERCEPTIONS OF COMBAT USE OF ARTILLERY IN THE NEIGHBORING COUNTRIES OF REPUBLIC OF BULGARIA

Stancho G. Stanchev

ABSTRACT: *This report examines the military potential of the neighbors of the Republic of Bulgaria and understanding of the combat use their artillery.*

KEYWORDS: *armaments, military balance, artillery, combat use.*

В анализ, публикуван от американската експертна мрежа за глобални политически и военни прогнози (World Security Network), се твърди, че Балканите са една от най-тежко въоръжените зони в Европа.

Поради разположението си, Балканите ще рефлектират всяка промяна в баланса на силите в Русия, Близкия изток и Западна Европа и в този смисъл остават изключително важен регион, чието развитие трябва да се следи отблизо. Във военно-отбранително отношение на Балканите стават големи промени, а военният потенциал на няколко държави расте. Поради явните и скрити регионални напрежения няма никаква гаранция за мирен 21-ви век на Балканите. Така че - Балканите остават приоритетен регион за геостратегически анализ.

В анализа на балканския военен баланс, публикуван от World Security Network се поставя силен акцент върху необходимостта от поддържане на експертно знание за Балканите заради важността на бъдещата политика спрямо региона. От особено значение е наблюдението на развитието на военния потенциал. Този анализ се фокусира върху военно-отбранителните тенденции в 4 балкански държави: Гърция, Турция, Сърбия и Румъния.

Независимо че Сърбия все още не е членка на НАТО, тя няма да избегне реформите на въоръжените си сили, които другите три държави вече провеждат. Тези реформи, твърди се в анализа, са ръководени най-вече от американската визия за модерна армия: подвижна, гъвкава, способна за бързи действия дори на "нетрадиционни военни театри" като Афганистан. Не само Америка, Европа има същата визия за своите сили за бързо реагиране, диктувана от новите заплахи като тероризма. Всичко това означава изграждане на високо подвижни структури, създаване на голяма бойна сила и професионални армии.

Друга импликация на модернизирането на армиите е уеднаквяване на военната инфраструктура във всички страни-членки на ЕС или НАТО. Реформите, с които

това трябва да се постигне включват крайно непопулярното съкращаване на военния състав. Но по-малкият брой на военния персонал освобождава средства за закупуване на скъпи нови оръжия, произвеждани в Америка и от водещите производителки в Западна Европа. Установените големи военни сили на Балканите – Гърция и Турция, вече влагат милиарди в модерно въоръжение. През последните 20 години те са похарчили над 100 милиарда евро за нова военна техника. Сега тези разходи се увеличават главоломно, струпвайки още оръжия на Балканите, а развитието на останалите балкански държави променя завинаги баланса на силите в региона с последици за цяла Европа.

В **Гърция**, реформите на отбраната променят изцяло формата на оперативните дейности и планирането за всички родове войски. Съставът на армията - включително най-високите рангове - е намален с една трета. Остарялата техника - самолети, бойни кораби, танкове - се подменя със свръхмодерна. Гръцката армия например е придобила 170 най-модерни бронирани танка, за 1.7 милиарда евро. Моделът – "Леопард", - е смятан за най-съвършеният в света от гледна точна на сигурността и боеспособността му.

Списъкът на гръцките военни придобивки е дълъг, но ето някои от тях: 20 транспортни хеликоптера за 657 милиона евро, 4 подводници U214 за 1,5 милиарда евро. Голямо внимание е отделено на новите самолети - 80 F-16 от "Локхийд Мартин", 15 самолета "Мираж", и голям брой други специализирани бойни и транспортни самолети. Гърция вероятно ще закупи други 60 нови бойни самолета.

Сухопътните войски на Гърция се състоят от четири армейски корпуса (АК) и две командвания. Първи и Четвърти АК отговарят за защитата на северните и източните граници на страната. 1-ви АК включва пехотна дивизия, две пехотни и две бронирани бригади. 4-ти АК се състои от две дивизии (две моторизирани пехотни бригади) и бронетанкова дивизия (три бронирани бригади). Втори АК служи като резерв. Той е съставен от една пехотна и една моторизирана пехотна дивизия. Трети АК е за бързо реагиране в рамките на НАТО. Състои се от пехота бригада и няколко по-малки единици за различни цели.

Танковият парк на Гърция включва: 353 съвременни немски „Leopard – 2"; 526 стари немски „Leopard 1"; 503 доста стари американски M48A5 и 240 M60A3. Общо 1622.

Бойните машини на пехотата са както следва: 243 френски - БРМ VBL; 401 (от бившата ГДР) - BMP-1; 1789 американски бронетранспортьори - M113 и 501 собствени „Leonidas" (произведен по австрийски лиценз).

Артилерия: 418 американски самоходни артилерийски установки (САУ) - M109; 25 от най-новите немски (155 мм) САУ - PZH-2000; 12 стари американски САУ - M107 (175 мм) и 145 M110 AU (203 мм). Има повече от 700 буксирни оръдия и пет хиляди минохвъргачки, 152 РСЗО (116 Чехословашки RM-70 (40 х 122 милиметра) и 36 на Американски MLRS (12 х 227 mm); 196 руски ПТРК „Корнет" (базирани на джипове); 262 „Фагот"; 366 американски „Тоу" и 400 френски „Милан".

Традиционната балканска неприятелка на Гърция – **Турция**, също планира значителна редукция на военните си сили и създаване на полупрофесионална армия през следващото десетилетие. Сред придобивките на Турция са 4 бойни самолета "Боинг" 737, отделно 1600 противотанкови управляеми ракетни установки за около 485 милиона евро.

Турските сухопътни войски са съставени от четири полеви армии (ПА).

1-ва ПА със зона за отговорност европейската част на страната и Черноморския пролив. Съставена е от пехотна дивизия и три армейски корпуса (АК). 2-ри, 3-ти и 5-ти АК.

2-ра ПА отговоря за защитата на югоизточната част на страната и границите със Сирия и Ирак. Именно тя се бори срещу кюрдите. Съставена е от три АК (4-ти, 6-ти и 7-ми АК).

3-та ПА поема защитата на североизточната част на страната и границите с Грузия и Армения. В състава и са включени два АК (8-ми и 9-ти АК).

4-та ПА защитава югозападната част на страната, (брега на Егейско море), както и за Северно кипърската турска република. На остров Кипър е разположен 11-ти АК в състав две пехотни дивизии и една бронирана бригада.

Въоръжение на Турция:

Тактически ракети: 72 американски ATACMS и най-малко 100 от собствени J-600T, реплика на китайската B-611.

Танкове: 326 съвременни немски „Leopard 2A4", 410 стари немски „Leopard 1A3", 1027 по-стари M60 и в 1482 напълно остарели M48A5.

Бойни машини на пехотата: 789 бойни разузнавателни машини „Cobra" и 370" „Акреп", 650 бойни машини на пехотата „AIFV", повече от 6000 ВТР. Всички тези машини са собствено производство. В допълнение, жандармерия, съставена 323 БТР-60РВ и 535 БТР-80, както и 25 немски „Condor".

Артилерия:

На въоръжение са 1267 САУ, 1932 буксирни оръдия, около 10 000 минохвъргачки. Почти всички артилерийски единици са стари с изключение на произведените в Турция по южнокорейски лицензa 240 САУ Т-155 и 225 гаубици „Panther" (и двата образеца са - 155 мм).

Значително внимание е отделено на реактивните системи за залпов огън. На въоръжение са 12 бр. РСЗО (227 мм), 80 бр. РСЗО Т-300 „Kasigra" (най-новите китайски WS-1) (302 мм), 24 бр. собствени буксирни системи RA7040 (70 mm), 130 бр. Т-122 „Сакария" (Съветски ВМ- 21 на турско шаси), повече от 100 бр. Т-107 (стара китайска Type 63 (107 мм).

Противотанкови системи: 365 бр. американски ПТРК „Тоу" (в това число самошодни - 173 бр. M901, 48 ACV), 80 бр. руски „Корнет" и 268 бр.съветската „Малютка", 186 стари немски „Cobra", 340 бр.нови шведски „Eriks", 392 бр. стари френски „Милан".

Схващанията за бойното използване на артилерията в армиите на Турция и Гърция се основават на възприетите концепции. През 2010 г. в Лисабон е приета Стратегическа концепция за отбраната и сигурността на държавите – членки на Организацията на Северноатлантическия договор, която в настоящия момент е залегнала в полевите устави на сухопътните войски на НАТО. Главната идея е едновременното поразяване на групировките на войските на противника по цялата дълбочина на оперативно-стратегическото построение чрез използване на целия арсенал от наличните обикновени сили и средства (най-вече ракетни войски и артилерия).

Според специалистите в НАТО при равни други условия изходът на боя ще зависи не толкова от съотношението между традиционните показатели на силите и средствата (броя на подразделенията, танковете, артилерията и др.), колкото от

постигнатото предимство в системите за управление, разузнаване, радиоелектронна борба и бойните възможности на обикновените средства за поразяване.

Съгласно посочената по-горе концепция артилерията е основен елемент за огнева поддръжка. Според уставите в Турция и Гърция предимствата на артилерията са: да осигурява огнево въздействие при всякакви метеорологични условия и особености на местността; да позволява бързо пренасочване на огневата поддръжка; да дава възможност на командира на маневрените формирования, който се нуждае от огнева поддръжка да поразява обекти, разположени в дълбочина на противника; да използва боеприпаси с различно предназначение.

За най-ефективно решаване на задачите по огневата поддръжка се създава групировка на артилерията. Групировката на корпусната артилерия е предназначена за: нанасяне на огневи удари по противника на далечните подстъпи и осигуряване на бойните действия на войските действащи в зоната за прикритие; огнево въздействие по подхождащия и настъпващ противник; указване на огнева поддръжка на бригадите от първия ешелон; борба с артилерията на противника; осигуряване на контраудара с резерва. Възможен е следния състав: 2-3 дивизиона 203,2-мм самоходни гаубици; 1-2 дивизиона 155 - мм самоходни гаубици (смесен артилерийски дивизион за Гърция); батарея РСЗО или батарея АТАСМ5.

Артилерията на бригадата често се усилва с артилерийския полк на корпуса, или част от него. В организационно отношение тя може да включва два дивизиона 155- мм гаубици, един дивизион 203,2- мм гаубици (смесен артилерийски дивизион за Гърция) и един дивизион 175-мм мм оръдия. Артилерията на бригадата в Турция включва дивизион 203,2-мм с.г., дивизион 155-мм САУ, дивизион 105мм САУ. В армията на Гърция артилерията на дивизията включва два три дивизиона 155мм гаубици и смесен дивизион, а артилерията на бригадата - дивизион 155-мм САУ. Организационно артилерията на бригадата е изградена така, че да изпълнява точно определени задачи. Обикновено по един дивизион се придава на всеки полк (батальон).

При настъпление усилията на артилерията са насочени на направлението на главния удар, за нанасяне на решително огнево поразяване на противника, което да доведе до промяна на съотношението на силите и средствата до 6-8 към 1 в полза на настъпващите.

При отбрана схващанията предвиждат огънят да се планира за прегражданe на най-вероятните направления за настъпление на противника. Освен това може да бъде планирано провеждането на контраподготовка за намаляване на вероятния ефект на противниковата огнева подготовка, дезорганизиране на неговите сили и нарушаване на управлението му.

Провеждането на контрабатарейната борба се планира, както при воденето на настъпателни, така и при отбранителни действия.

С въвеждането на автоматизираната системи за управление на огъня (Питагорас в Гърция) нарастват възможностите за разузнаване, с което бригадите в гръцката армия увеличава способностите си за водене на контрабатарейна борба. По настоящем тя се планира и провежда в два Варианта: активна и превантивна:

- за превантивната контрабатарейна борба е характерно това,че артилерийските средства на противника се подават преди да са използвани бойни действия. Успехът й зависи от способността на бригадата да използва пълноценно наличния комплект от разузнавателни средства и бързо да обработва непрекъснато постъпващата информация.

- активната контрабатарейна борба се характеризира с това, че артилерийските средства на противника се подавят с началото на тяхната огнева дейност. Препоръчва се тази борба да се води тогава, когато бригадата разполага с по-малко време за изпълнение на задачата, или с по-малко разузнавателни средства.

За изпълнение на тези задачи артилерийските подразделения се развръщат в боен ред. За развръщане в боен ред им се назначават позиционни райони. Размерите на позиционните райони могат да бъдат: за 155-мм и 203,2-мм дивизиони и смесения дивизион 2,5 до 4,5км по фронта и 2 - 3 км в дълбочина; за 105-мм дивизиони 1,5 - 2,5км по фронта и в дълбочина. Позиционния район на всяка батарея може да бъде с размери 500 - 1000м по фронта и дълбочина. На всяка батарея се назначава основен и запасен район за огневи позиции. За водене на разузнаване, и обслужване на стрелбата на огневите подразделения се създават предни артилерийски наблюдатели. Броят им може да бъде 2-4 за всяка батарея. Отдалечението ще се определя от възможностите на средствата за разузнаване (средно 1 - 2км от предния край).

Отдалечението на позиционния район от предния край може да бъде:

- за 105-мм дивизиони — 2 - 4км;
- за 155-мм и смесените дивизиони — 4-6км.;
- за 203,2-мм дивизиони — 8-12км.
- за РСЗО — 5-15км;
- за корпусната артилерия — 6-12км за Турция и 4-8км за Гърция При извършване на марш дължината на колоната на дивизиона може да бъде от 5-6км за 105-мм дивизиони до 6-7км за 155-мм, смесените и 203,2-мм дивизиони. Дължината на колоната на всяка батарея може да бъде 800-1000м, а дистанцията между самите батареи - до 500м.

Що се отнася до схващанията за бойното използване на РСЗО (MLRS) в Турските сухопътни сили, можем да отбележим, че батареята е оптималната организационна единица за използване на MLRS. При изпълнение на огневи задачи огневите взводове заемат позиционен район с размери 3 на 3 км., на отдалечение 5 - 15км от предния край, а пункта за управление на огъня на батареята се развръща в район с радиус 500м на отдалечение 15-25км от него.

В позиционния район на огневите взводове, на всяка пускова установка се назначават една основна и две запасни позиции (на разстояние 500 - 800м една от друга) и пунктове за снабдяване и зареждане с боеприпаси на пусковите установки на отдалечение до 800м от огневата позиция.

Времето за изпълнение на огневата задача в зависимост от обема й варира от 5 до 10 мин., след което огневите позиции незабавно се сменят. Смяната и подготовката за пуск (в т.ч. презареждането на пусковата установка за 7 - 8 мин.) се извършва за 20 - 45 мин.

Друг значителен фактор за новия военен баланс на Балканите идва от **Сърбия.** Според анализа, сръбският арсенал остава непроменен от времето на бивша Югославия. По данни от неназовани източници военният производителен сектор е бил възстановен от пораженията нанесени от бомбардировките на НАТО през 1999 г. Смята се, че Сърбия отново е в състояние да произвежда различни видове амуниции, електроника, и ракети с различно предназначение.

Сръбската армия наброява 36000 военнослужещи. След провеждане на военната реформа, сръбската армия се състои от 12 бригади: - 4-ри пехотни, 1-на сме-

сена артилерийска, 1-на специална бригада, 2 авиационни, 1-на ракетна, 1-на артилерийска бригада, 1-на логистично-свързочна бригада и отделен батальон на военна полиция.

Артилерийски системи на въоръжение в сръбската армия: 128-мм РСЗО М-63 „Plamen" - 18бр.; 128-мм РСЗО М-77 „Огань" - 60бр; 262-мм РСЗО М-87 „Оркан" - 3бр.; 122-мм САУ 2С1 - 67бр.; 130-мм оръдие М-46 - 18бр.; 122-мм гаубица Д-30 78бр.; 152-мм оръдие-гаубица М84 „НОРА" 36бр.; 155-мм буксирна гаубица М1 - 66бр.; 155-мм гаубица М65 - 6бр.; 120-мм миномет М-74 – 57бр.

Сръбската армия разполага с уникална и крайно ефективна мобилизационна схема, като войниците от запаса държат оръжията и униформите си у дома. Тази схема е изключително гъвкава, не е централизирана и е подобна на армиите на Швейцария и Кипър. Не е ясно каква ще е нейната съдба. Но намаляването на въоръжените сили ще намали традиционния геостратегически капацитет на Сърбия, което е може би най-важната регионална тенденция на Балканите. Намаляването на историческата роля на Сърбия като военна сила на Балканите ще има дългосрочен ефект за регионалния баланс на военните сили. Едновременно с това отслабване на Сърбия, косовските албанци са все по-добре въоръжени и военен конфликт с Косово не е изключен. Черна гора пък може да се окаже без каквито и да било реалистични средства за отбрана, ако има проблеми със собствените си албански граждани.

Румънската армия включва 90000 военнослужещи. Около 75000 от тях са военният персонал, а 15000 са цивилните. 60000 ще бъдат действащите сили, докато 30000 ще образуват териториалните сили. От 75000 войници, 45800 съставят Румънските Сухопътни сили, 13250 — Румънските Военновъздушни сили, 6800 са в Румънските Военноморски сили, а останалите 8800 служат в други сектори.

Въоръжение на Румъния: Танкове 1098 бр.; бойни бронирани машини на пехотата 122 бр.; артилерия и МХ 1359 бр.; РСЗО 188 бр.

В румънската и сръбската армии е възприето при настъпление 2/3 от силите и средствата на артилерийските формирования да се разполагат по-близо до фронтовата линия, а 1/3 от тях - в дълбочина, като при отбрана това положение е равно противоположно.

Разсредоточаването по фронта може да бъде просто (чрез увеличаване на интервалите между артилерийските системи) и двойно (чрез увеличаване на интервалите между тях и артилерийските формирования). Счита се за целесъобразно увеличените интервали между оръдията (от 50 на 60м и повече, при което фронта на батареята ще бъде над 300 м. вместо 200 м.) да се използват, когато двете страни разполагат с приблизително еднакво количество артилерия. По-големи интервали между артилерийските системи и артилерийските формирования ще се прилагат и при недостиг на артилерия. В този случай интервалът между дивизионите е не помалко от 3000 м., а между батареите - 1500м (при нормални условия той е 500 - 1000м), като командният пункт на батареята е разположен на огневите позиции, а интервалът между него и огневите взводове трябва да бъде над 500м.

Препоръчва се разстоянието между противотанковите батареи в дивизиона да бъде най-малко 1500м., а между батареите - 500м. Счита се, че разсредоточаването в дълбочина е характерно за артилерията с калибър 100-мм. и повече и за РСЗО, и следва така да се планира, че да осигурява максимални възможности за водене на огън в участъка с дълбочина до 7 -10 км. от предния край (т.н. зона на масовия

огън), в който възможностите за наблюдение и коригиране на огъня със собствени средства са оптимални.

При извършване на марш от артилерийските подразделения дистанциите между батареите трябва да бъдат 600м., а между артилерийските системи над 100м.

От схващанията за бойното използване на артилерия от балканския регион следва да се отчете, че както Турция и Гърция, така и Румъния и в известна степен и Сърбия възприемат все повече постановките на концепциите за използване на войските на НАТО.

В заключение мога да отбележа, че "Всеки, който се интересува от сигурността в Европа трябва да анализира Балканите". Не само поради геополитическото им значение, но и защото в по-нови времена това е единственото място в Европа, което има опит с война. Освен всичко, много от напреженията в региона са невидими и е невъзможно да се каже със сигурност, че през 21 век на Балканите ще има мир.

ЛИТЕРАТУРА:

1. http://rusevik.ru/politika/, (28.02.2015).
2. http://topwar.ru/, (02.03.2015).
3. http://dic.academic.ru/, (02.03.2015).
4. http://commi.narod.ru/,(10.03.2015).
5. http://militpogony.do.am/,(10.03.2015).
6. http://www.senica.ru/,(10.03.2015).

ФАКТОРИ И ПРИНЦИПИ НА ВОЕННОТО ЛИДЕРСТВО

Станчо Г. Станчев

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

FACTORS AND PRINCIPLES OF MILITARY LEADERSHIP

Stancho G. Stanchev

Abstract: *This article examines some basis factors and principles of the military leadership in the context of the idea for combining the performance of the army mission with care for the soldiers.*

Keywords: *leader, led, leadership, situation.*

Проблемът за военното лидерство не е нов. През цялата човешка история военните лидери са се сблъсквали с въпроса как да водят своите войски. Опита от войните, които България води показва, че личността на командира е от изключително значение за дадено военно формирование. Едни и същи формирования, ко-

мандвани от командири с различни професионални, нравствени и интелектуални качества, имат различни резултати в мирно и военно време.

Под лидерството в армията се разбира преди всичко процеса на влияние върху военнослужещите, с цел те да изпълнят определена задача, като им се дава ясна цел, посока на действие и необходима мотивация.

Целта дава на военнослужещите смисъла защо трябва да правят трудни неща, например, като изпълнение на бойна задача, при опасни и стресови обстоятелства. Това изисква установяване приоритетите в изпълнението на задачата, обяснение значението й и насочване вниманието на войниците върху нея така, че тя да бъде изпълнена така както е необходимо.

Посоката подпомага военнослужещите с необходимата ориентация при изпълнение на задачи базирани на приоритетите, които се установяват от лидера. Тук са необходими стандарти, които след като бъдат възприети или наложени ще доведат до създаването на порядък, увереност в себе си и в лидерите.

Мотивацията дава на военнослужещите воля да направят всичко, на което са способни за изпълнение на задачата. Тя позволява л.с. да прояви инициатива, особено когато вижда необходимост да се действа незабавно. Целесъобразно е военнослужещите да се мотивират чрез осигуряване на пълноценен тренировъчен процес и посредством изграждане на екип в подразделението(екипажа, разчета) в посока на съвместната хармонична дейност, чрез поощряване на успехите и делегиране на пълномощия.

Ефективните лидери влияят, както по пряк, така и по непряк начин в процеса на осъществяваното от тях ръководство. Една част от командирите въздействате на войниците си като използват прекият начин, но други, особено от по-висшите командни звена, обикновено използват индиректният подход на влияние.

В наръчника FM 22-100 се отбелязва, че оперативната доктрина на американската армия е подчертано лидерска, а лидерството се разглежда като най-важният елемент от бойната мощ. Така ефективното лидерство се разглежда не като мистерия, а нещо, което може да се усвои чрез самоподготовка, образование, тренировки и упражнения. Успешните лидери се подготвят за война, като тренират и командват като за война, една идея трайно въплътена в използваният от много време у нас дидактически принцип – „да се учат войските на това, което е необходимо на война".

За да се подготвят войниците да действат ефективно в цялото многообразие на един конфликт има определени неща, към които наръчника препоръчва лидера стриктно да се придържа, т.е. той, лидера, командира на подразделение, трябва да знае и да прави точно определени неща.

В наръчника се разглеждат и четирите главни фактора на лидерството в армията, които винаги са актуални и влияят силно на предприеманите действия. Това са - последователите, лидерът, ситуацията и комуникациите.

Първият основен фактор на лидерството естествено са военнослужещите, за чието предвождане лидерът отговаря. В наръчника се подчертава идеята, че не всички трябва да бъдат предвождани по един и същи начин. Например, редник с нова за него работа или задание обикновено се нуждае от наставления по-близко от това на редник, който има опит със същото задание. Редник, който не е достатъчно уверен задължително се нуждае от подкрепа и насърчаване от страна на лидера. Редникът, който работи упорито и прави нужните неща, заслужава похвала, но този, който не отговаря на ясните стандарти (изисквания), може би трябва да бъде

наказан. В крайна сметка лидерът е този, който трябва правилно да използва компетентността, мотивацията и себеотдаването на военнослужещите, така че те да предприемат правилните действия в подходящото време.

Практиката показва, че в групата (екипа) е полезно да бъде изграден такъв климат, който насърчава подчинените да участват активно и да желаят да помогнат на лидера в изпълнението на задачата. Ключовите съставки за развиване на такава връзка са взаимното доверие, уважението и увереността в правилността на решението.

Вторият главен фактор на лидерството е самият лидер. Той трябва да е честен пред себе си за това какво знае и какво може. Изисква се той да е наясно със силните си страни, със слабостите, способностите и предела им така, че да може да се контролира и да командва подчинените си ефективно. В тази връзка той задължен да зачита достойнството им и да се отнася към тях с уважение.

Ситуацията е третият главен лидерски фактор. Всички ситуации са различни. Действията на лидера в дадена ситуация могат да се окажат неудачни в друга. За да се намери най-добрият начин на действие първо необходимо е да се проучи наличната информация и след това т. нар. четири основни фактора - mission enemy terrain, troops and time available (METT-T).

След това се взема под внимание равнището на компетентност на подчинените, мотивацията и решителността им за изпълнение на дадената задача или мисия. В една ситуация може да се наложи отблизо да се надзирава и насочва работата на подчинените. В друга може да се наложи да се дава кураж или да се изслушват идеи. Или пък всичко това заедно.

Комуникациите, четвъртият главен фактор в лидерството, представляват обмяна на идеи и информация. Осъществяването на ефективни комуникации става, когато другите разбират какво точно се опитва лидерът да им каже и след получаването на адекватна обратна информация от тях. Лидерът може да комуникира с другите писмено, устно или чрез жестикулации, както и чрез комбинация на посочените подходи. Той трябва да се осъзнае, че именно от лидера произтичат стандартите на поведение на основата на личния пример, поощрението или наказанието на определени постъпки. Начинът му на комуникиране в различни ситуации е много важен. Изборът на думи, тон и жестове въздействат по неповторим начин на войниците. Отбелязва се, че лидерството е нещо повече от това да служим за пример със смелостта си в дадена ситуация. Способността да кажем нещо правилно в точно необходимият момент по най-подходящия начин също е от значение за лидерството.

В мирно време лидерът следва да отработи начини на свръзка между военнослужещите така, че те да следват командите му, а също така и да взаимодействат добре в бойна обстановка. Изисква се той непременно да печели доверието им. По този въпрос С. Казанджиев преди повече от половин столетие на основата на командирският си опит от няколко войни дава много ценни препоръки в своята „Военна психология (психология на боеца)", и обяснява как, доверието, може да се използва като средство против страха в боя. За да спечели доверието на бойците от началника или лидера се изисква:

- да разбира отлично работата си;
- да е напълно убеден в целесъобразността на разпорежданията си;
- да държи за пълното и неизменно провеждане на тия разпореждания;
- да има вяра в хората си;

- да е спокоен, но твърд и решителен;
- да е хладнокръвен и със самообладание;
- да държи безусловно на дисциплината, да наказва но без това да влияе на човешките му отношения към подчинените;
- да се грижи като баща за подчинените - първо за тях, че после за себе си;
- да се поставя при същите условия както подчинените си;
- да иска най-първо от себе си това, което изисква от подчинените си;
- да бъде винаги готов да даде пример за достойно държание при страдания и лишения или при тежки моменти в боя.

Ефективните комуникации предполагат лидерът да се изслушва с внимание и да се разбира какво казва. И след като военнослужещите слушат своят лидер, то трябва да се направи нещо, за да се разбере какво точно подчинените се опитват да му кажат. Доброто слушане се постига с помощта на много усилия чрез системно учене и подходящ тренинг. На първо време бихме могли да се придържаме към няколко прости правила в поведението си, например да не прекъсваме другите, когато говорят; да гледаме в очите този, който говори; да слушаме активно, т.е. да следим какво е казал и как го е казал и пр. От съществено значение е да се отчита влиянието на емоциите, проектирани основно в невербалните послания (мимики, жестове, интонация) и възможността това да бъде „съзнателно" контролирано. Някои съвременни изследвания доказват, че те са важна съставна част на комуникациите. С внимателното изслушване на подчинените си ние изграждаме нагласа и умение и те да ни изслушват с внимание.

Четирите главни фактора на лидерството са налице винаги, при всяка една ситуация, но е важно да се знае, че те си влияят взаимно по твърде различен начин. И най-важният фактор в една ситуация може да се окаже маловажен в друга. Необходимо е постоянно да се имат пред вид тези основни положения в лидерството и да се избира най-верният начин на действие.

В наръчника са дадени някои много съществени правила или принципи на лидерството, които могат да бъдат отличен стълб за ефективната работа на командира. Те са универсални и могат да се разглеждат като фундаментални положения, издържали проверката на времето.

1. Създаване на условия, които да позволяват курсантите да опознайте самите себе си и да се стремят към самоусъвършенстване: За да познаваме себе си е необходимо да разбираме своята мисия и да познаваме предимствата, силните си черти, както и нашите недостатъци. Сам по себе си факта, че познаваме себе си ни гарантира възможността умело да използваме силните си черти и да преодоляваме слабостите си. Стремежа към самоусъвършенстване означава непрестанно обогатяване на силните качества и полагане на усилия за отстраняване на слабостите. Това ще повиши нашата компетентност и вярата ма войниците в умението ни да ги обучаваме и командваме.

2. Гарантиране качеството на тактическа и техническа ни компетентност: от нас се очаква да сме тактически и технически компетентни за длъжността, която заемаме. Това означава, че ние бихте могли да изпълним задачи според стандартите, характерни за военно време. Ние развиваме тактическата и техническата си компетентност посредством съчетаването на тактики, техники и различни процедури, които усвояваме в процеса на образованието ни във съответните учебни заведения (институционално обучение), посредством изпълнението на всекидневните

си задължения (оперативни задачи) и посредством самоусъвършенстване в съответната професионална област чрез четене и тренинг.

3. Насърчаване в търсенето и поемането на отговорност за действията си: лидерството винаги предполага отговорност. Ние бихте желали да имаме подчинени, които могат да поемат отговорност и да помогнат в изпълнение на съответните задачи. Когато установим проблем или нещо нередно, не трябва да чакаме да ни се каже да действаме. Примерът ни, независимо дали е положителен или отрицателен, ще помогне за развитието на нашите подчинени. Бойната доктрина се нуждае от смели лидери на всички нива, когато са склонни към инициатива и се възползват от всяка възможност на бойното поле, за да се осигури победата. Когато правим грешки, редно е да приемаме справедливата критика и да се коригираме. Не трябва да бягаме от отговорност като прехвърляте вината върху друг. Целта ни трябва да бъде постигането на доверие между нас и нашите непосредствени началници, както и между нас и подчинените ни като търсим и поемате отговорност.

4. Усвояване на изкуството да се вземат навременни и твърди решения: ние трябва да можем бързо да оценим дадена ситуация и да вземем навременно решение. Ако отложим или забавим вземането на решение ние може да предизвикаме нежелани последици и да провалим осъществяването на задачата. Нерешителните лидери проявяват колебание, загуба на увереност и объркване. Ние трябва да можем да разсъждаваме и при най-тежки условия и бързо да предприемаме необходимите действия. Ето няколко съвета, от Наръчника по военно лидерство - РМ 22-100, който ще ни помогнат да се проявим като ефективни лидери:

- събирайте важна информация преди да вземете решение;

- съобщавайте решението си навреме, така че войниците да могат да реагират адекватно;

- доброто решение взето навреме е по-полезно от най-доброто решение, което обаче е взето твърде късно;

- преценявайте ефекта от решенията си в близка и далечна перспектива.

5. Създаване на нагласа да бъдат винаги за пример на бъдещите си подчинените: нашите подчинени искат и се нуждаят от това да сме пример за тях. Това е тежка отговорност, но ние нямаме друг избор. Нито един друг аспект на лидерството не е толкова силен, колкото правилото за личния пример на командира. Ако очакваме решителност и компетентност от подчинените си, то ние трябва също да можем да ги демонстрираме. Ние трябва да поставим високи, но постижими изисквания, да сме склонни да правим това, което изискваме от подчинените си, да споделяме опасностите и несгодите заедно с тях.

6. Формиране на умения за опознаване войниците и полагане на грижи за тяхното добруване: ние трябва да познаваме и да се грижим за подчинените си. Необходимо е да разбираме вътрешната им мотивация и да разберем какво ги вълнува. Трябва да отделим време и усилия за да ги опознаем като индивидуалности. Когато показваме искрена загриженост за тях, те ще ни отвърнат с доверие и уважение.

Ако подчинените ни имат доверие те ще работят с желание и ще ни помогнат да изпълним задачите. Необходимо е да осигуряваме удовлетворяването на техните желания, да държим на дисциплината и честно да ги награждаваме. Връзките, които грижовното отношение формира, ще сплотят нашия колектив.

7. Изграждане на умения за информиране на подчинените си, особено за нещата, които пряко ги касаят: военнослужещите се справят най-добре когато

знаят защо правят дадено нещо. Информирането на подчинените ни ще им помогне да вземат решения, да изпълняват планове, ще окуражи инициативните, ще подобри работата в екип и ще вдигне морала. Нашите подчинени търсят логика в заповедите ни, подлагат на съмнение нещата, които нямат смисъл. Те очакват от нас да ги информираме и когато е възможно да обясняваме заповедите.

8. Развиване чувството за отговорност у военнослужещите и на способност за формирането на такава у техните подчинените: подчинените ни трябва да знаят и да разбират какво очакваме от тях. Те имат нужда да знаят какво искате да се свърши, какви са стандартите и кога искаме да бъде свършено. Контролът показва заинтересоваността ни от изпълнението на задачата. Все пак добре е да знаем, че прекомерното наблюдение се приема с неодобрение от подчинените.

9. Развиване на умения да се контролира доколко поставената задача е осъзната от подчинените и има ли условия за ефективното й реализиране: когато на военнослужещите се поставят нови задачи необходимо е да им бъдат обяснени изискванията за изпълнение. Необходимо е да ги оставим да опитат, да наблюдаваме действието им, както и да приемем изпълненията, които отговарят на стандартите ни. Да коригираме изпълнения, които не отговарят на изискванията. Трябва да обясним причината защо едно изпълнение е лошо и да предприемем необходимите действия. Когато държим сметка на подчинените си за техните действия, те ще осъзнаят, че са отговорили за изпълнението на задачи, като отделни личности и като екипи.

10. Формиране на умения за изграждането на екип за изпълнението на задачата: боят (операцията) е колективно действие. Ние трябва да развиваме колективен дух у военнослужещите, който да ги мотивира с увереност да изпълняват бойни задачи. Подчинените имат нужда да са уверени в способността ни да ги предвождаме, както и в собствената им способност да действат като екип. Ние трябва да тренираме отново и отново подчинените си, докато постигнем увереност в техническите и тактическите качества на екипа. Нашето подразделение ще се превърне в екип само тогава, когато подчинените ни изпитват уважение към нас, когато се чувстват като добре обучени професионалисти и виждат значението на това, което допринася за формированието.

Познаването на факторите и принципите на лидерството ще ни помогнат да осъществим задачите успоредно с осигуряване необходимата грижа за подчинените. Факторите на лидерството са винаги налице и въздействат на това какво и кога трябва да се направи. Имайки в предвид факта, че всяка ситуация в лидерството е различна ние трябва да можем да отчитаме спецификата на обстоятелствата и да решим какво да предприемем. Силно е въздействието чрез казаното, написаното и най-важното, чрез направеното от нас. Начина и предмета на нашата комуникация с останалите или ще подсили или отслаби взаимовръзките ни с тях.

Литература:

1. Ангелов А., Организационно поведение. С., 2002.

2. Евтиков, О. В., Стратегии и приемы лидерства – теория и практика. СПб., 2007.

3. Казанджиев С., Военна психология. МО, София 1995.

4. John Wileey & Sons. Personally Factors in Military Psychology. Handbook of Military Psychology, 1991.

5. Military Leadership. FM 22-10. July, 1990.

МОРАЛНИ, ЕТИЧНИ И ПСИХОЛОГИЧЕСКИ ГРАНИЦИ НА ПРЕВЕНЦИИТЕ СРЕЩУ ТОТАЛНИЯ КОНТРОЛ ВЪРХУ ЛИЧНАТА ИНФОРМАЦИЯ В КАЧЕСТВОТО Й НА ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ.

Младен Д. Тонев, Пламен Ц. Цонев

Варненски свободен университет „Черноризец Храбър”, Факултет „Международна икономика и администрация”,
катедра „Международна икономика и политика“ – гр. Варна, к.к. „Чайка”, Р. България

Национален военен университет „Васил Левски” – Факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи”, катедра „Информационна сигурност” – гр. Шумен, Р. България

MORAL, ETHICAL AND PSYCHOLOGICAL LIMITS OF THE PREVENTIONS AGAINST THE TOTAL CONTROL OF THE PERSONAL INFORMATION AS THE INTELLECTUAL PROPERTY

Mladen D. Tonev, Plamen Ts. Tsonev

ABSTRACT: *In a principled plan modern technical means actually increase the level of reliability of information security. However, that is state of the art technology allows and not very ethical practices in the control information such as tracking, wiretapping, hacking and other aspects of abuse and a breakthrough in information security systems.In today's technological possibilities - satellite communications, the Internet, global mobile communications networks of the third and fourth generation, etc. The struggle for control and protection of information as an object of intellectual property becomes a priority. If these moral and ethical issues in handling information resources in the systems of the new information technologies ikomunikatsionni not find an adequate and relatively quick decision is a risk of multiple negative practices. On those aspects of the problem and focus this publication.*

KEY WORDS: *communications, new informations and communications technologies, information resources, ethical practices, intellectual property.*

Защитата на интелектуалната собственост е важен момент от комплексната система на изграждане, поддържане и усъвършенстване на информационната сигурност в териториалните граници на даден регион или държава или в рамките дори на отделна стопанска микроединица. Използването на термина „граници“ в озаглавяването на темата на доклада предполага необходимостта от допълнително уточнение и тълкуване. Границата е винаги ограничение. В субективен план тя е едностранно ограничение. Даден субект може да се намира само от едната страна на дадена граница. Няма как даден индивид да бъде едновременно от двете страни на границата (главно като интелектуална, мисловна) позиция. Във физически смисъл една граница, маркирана по някакъв начин, може да се прекрачи от даден ин-

дивид и той да е заел позиция от двете страни едновременно. Това може да се случи с физическа граница. В случая границите, за които се говори в настоящото изложение – морални, етични, психологически имат премуществено условен, виртуален, импилицитен характер. Те не се усещат и възприемат като физически видими, осезаеми и с точни измерения рамки, маркери, ограничители, както при физическите граници на територия, на предмет, на сфера на обхват, на мащаби на дейност или други подобни аспекти на ограничаване и локализиране на даден процес или явление. Това ги прави по-особен обект на изследване и анализ. В морален, етичен и психологически аспект границата е условно разделение на две страни, две позиции, два подхода или мирогледа, които тя диференцира. В този смисъл тя е ограничение вече не за конкретен субект, както е физическата, материализираната граница, а е ограничение на периметъра на действие и влияние и за двете страни. Двете различни позиции срещат тази морална граница или своеобразната оценъчна скала, критерия, който ги позиционира в накакви различими парадигми, които много трудно могат да се обединят в някъкъв конкретен субект. Трудността е в това, че няма как едновременно субектът да е морален и неморален, да е етичен и неетичен, да е психологически манипулиран и едновременно да манипулира тези, които го манипулират. В случая с моралните и етични граници те разделят субектите. В този смисъл те са двойно проектирани граници – и за двете подгрупи разграничавани субекти – моралните и неморалните, етичните и неетичните.

Когато говорим за граници на защита на даден вид собственост тези граници се предполага, че определят полето на защитеност, гарантираност, сигурност, надеждностпри реализацията на базовите функции на собствеността – владеене, разпореждане и ползване. В случая - при настоящата цел на доклада – когато визираме границата на сигурност и защита на интелектуалната собственост „границите“ (морални, етични и психологически) разделят субектите собственици на интелектуални блага на две подмножества – първото е това подмножество от собственици на интелектуална собственост, чиито интелектуални продукти са защитени сигурно и надеждно от тези собственици на интелектуална собственост, която е относително лесно достъпна за посегателство от страна на хакери, информационни „пирати“ и дори от страна на редови ползватели на информационните и комуникционните съвременни технологии.

След разкритията на Едуард Сноудън и организацията „Уйкилийкс става ясно, че проблемът със защита на информацията отдавна е надхвърлил тесните граници на законовата и компютърната защита на информацията в качеството ѝ на обект на интелектуална собственост. Този проблем вече има глобални и главно геостратегически измерения. Да си спомним само коя страна предостави политическо убежище на Сноудън и отказа репатрирането му в САЩ. Руските власти, заеха тази подкрепяща позиция не толкова от желание да се доберат до стратегически тайни на геополитическия си съперник – САЩ, колкото с идеята да заемат моралната позиция на съдник и ментор по отношение на скандала с подслушванията и да извлекат предимно морални дивиденти. Това, което разтърси световните обществени медии и предизвика високо напрежение по управляващите върхове в Западна Европа и още по на запад - отвъд Атлантика – изтеклата информация за подслушване на високопоставени западни политици от съюзнически и приятелски на САЩ държави, още веднъж повдига сериозно въпроса за моралните граници на деянието „под-

слушване на политици“ и „използване на специални разузнавателни средства“ по един безогледен, и в разрез с добрия тон и с добрия етикет начин. Паралелно с това на преден план излиза и проблемът за контрола върху информацията. Кой има права да събира подобна информация и кой и как може да я използва и в името на какви цели?

В един принципен план съвременните технически средства действително повишават степента на надеждност на информационната сигурност. Същевременно обаче именно развитите съвременни технологии позволяват и неособено етични практики в контрола върху информацията като проследяване, подслушване, хакване и други аспекти на злоупотреби и пробив в системите за информационна сигурност. Нещо повече, понякога интервенцията по отношение на манипулациите с информационни продукти, води до блокиране на работата на информационните системи и мрежи или на отделни възли от тези мрежи (сървъри, компютри, централи, локални мрежи и др.) Интервенционните възможности се подобряват в дуалистичен план – както на глобално и национално равнище, така и на равнище микроединици и дори индивиди. Ето малко статистика за САЩ, като страна, която се оказа главна мишена на разобличенията и от там главен виновник в злоупотребите с контрола върху информацията и главен поръчител на пробивите в системите на информационна сигурност на западните държави. Освен правителствените структури като Национална агенция по сигурността, ЦРУ, ФБР и прочее агенции в разузнаването на САЩ са ангажирани още и 3200 частни организации. В книгата си „Изповедта на един икономически килър“ Джон Пъркинс директно заявява, че Националната агенция по сигурността директно обслужва интересите на големите американски корпорации както на теротирията на САЩ, така и зад граница. Казано с други думи правителстнети разузнавателни централи на САЩ действат главно в интерес на едрия американски бизнес. С още по-голяма сила това твърдение може да се преадресира и за 3200 частни организации занимаващи се с разузнаване в САЩ. Също така по официални данни в САЩ работят 10 000 съоръжения за разузнаване. Това са главно съоръжения които селектират, филтрират и обработват информация от различен характер. Въпросът е кой има достъп до тази информация и за какви цели се използва тя. Ако се вярва на Джон Пъркинс, най-вероятният адресат на разузнавателна информация от различен характер е крупният американски бизнес – гиганските транснационални корпорации, които имат интереси почти във всеки район на света като достъп до суровини, енергоизточници, пазари, капитали, информация. САЩ са страната, която харчи най-много пари за разузнаване, в това числро и за подслушване, както става ясно от последните разкрития. Средствата, които САЩ отделят за разузнаване са повече във финансово изражение, отколокото средствата, които харчат като пари останалите страни в света взети заедно. В САЩ 854 000 имат достъп до секретна информация. На този фон звучат крайно неубедително оправданията на членовете на Комисията за контрол на разузнаването, че не са знаели за мащабното и тотално подслушване организирано и осъществявано от структури на Националната агенция по сигурността (В някои източници тя се нарича още АНС - агенция по национална сигурност). Противно на твърдението на контролните органи, които искат да излязат „невинни“ от скандалното положение, шефът на АНС в прав текст заявява пред медиите в САЩ, че Комисията за контрол на разузнаването е информирана подробно и надлежно за

всички операции и дейности по подслушването на политически лидери от приятелски и съюзни държави.

Факт е, че през последното десетилетие под прикритието на борбата със световния тероризъм законодателния орган на САЩ – Конгресът приема редица закони, с които се дават на практика неограничени права на разузнавателните институции на САЩ да имат достъп и да разузнават „всяко нещо“, както е регламентирано в Патриотичния закон гласуван от Конгреса през 2004 г. Правомощията на разузнавателните институции са разширени с приетия през 2007 година Закон за защита на САЩ и с поправките към този Закон от периода 2008 – 2012 година. Достъпът до това да се разузнава „всяко нещо“ по преценка на самите институции се гарантира от конкретния законодателен акт, който премахва границите – морални, етични и психологически на това, което е допустимо и резонно в разузнавателната дейност и това, което надхвърля добрите норми и елементарната политическа и бизнес етика. Не може да се вменява във вина на разузнавателните централи каквото и да е действие, при такава нормативно гарантирана свобода на избора на обект и начин на разузнаване. Всяка разузнавателна институция би действала по подобен начин, при условие, че се окаже на практика в ситуация на гарантирана безконтролност и тотална свобода на действие. По тази причина най-вероятно не наблюдавахме оставки на низови ръководители в разузнаването на САЩ след скандалните разкрития на Едуард Сноудън. Тези служители и експерти не се чувстват длъжни в морален план да носят отговорност за нормативно гарантираната им тотална свобода в разузнавателната дейност. Какво подсказва логиката – моралната отговорност следва да се понесе от конгресмените, гласували правната регламентация на безконтролната тотална разузнавателна дейност. Но хората в законодателните органи на САЩ не са константна величина, както не е константно и множинството в Конгреса. Съставът на днешния Конгрес сигурно е доста различен в сравнение с Конгреса от началото на Милениума, когато се обсъжда и гласува Патриотичния закон.

При днешните технологични възможности – спътникови комуникации, Интернет, глобални мобилни комуникации, мрежи от трето и четвърто поколение и пр. борбата за контрол и защита на информацията в качеството й на обект на интелектуална собственост става приоритетна. Ако пак се върнем на логиката на Джон Пъркинс можем да обобщим, че резонната крайна цел на геоикономическото и геополитическото съперничество между водещите в развитието си държави е борбата за пазари – стокови, суровинни, финансови, кредитни и пр. В тази борба за пазари първостепенно е значението на контрола и достъпа до информация и и тук е главната роля на разузнаването като важна институция, осигуряваща необходимия информационен ресурс за пазарно и бизнес надмощие. Именно този цел и тази логика най-добре обясняват защо на фокуса на внимание на операциите по подслушване и шпиониране попадат лидерите на водещи икономически и същевременно политически и военно приятелски държави. Те са приятелски държави на САЩ в геополитически план, но на практика са конкуренти и са застрашаващи американския едър бизнес в качеството им на икономически центрове от един или друг калибър. Независимо от тази логика въпросът за морално-етичните аспекти на подобна политика на тотално подслушване остава открит. В този смисъл част от световната общественост подкрепя Едуард Сноудън в борбата му срещу тоталния контрол върху информацията. В подкрепа на Сноудън в редица западни градове и

столици преминаха протестни митинги и демонстрации. Не случайно той се оказа на второ място в класацията „Личност на годината“ за настоящата 2013 година.

Като контрапозиция на политиката на разузнавателните централи, насочена към тотален контрол върху движението на информацията от различен характер – политически, стопански, финансов, военен и дори битов – швейцарското списание „Вохен цайтунг“ (WOZ) в редакционна статия обявява, че в продължение на 24 часа е следило шпионин № 1 на страната – Маркус Зайлер[35]. Според АФП журналистите от списанието се добират до куп лична информация за Зайлер, която е поместена в специално издание на швейцарския седмичник.Успоредно със събраната за Маркус Зайлер информация се описват и методит,е по които тя е събирана – разговори със съседите и дори с учителката му от началното училище. Публикувани са данни за заплатата му, за личното му имущество, за платените данъци и пр. подробности. Идеята е наред с осъждането на повсеместния информационен контрол да се осъдят и методите, с които си служат разузнавачите. Като се има предвид как журналистите са успели да се доберат до информация, част от която би следвало да е конфиденциална, лесно е да си представим колко по-лесно и безпроблемно е това за всяко едно разузнаване, което по-принцип използва далеч по-рафинирани методи за набиране на разнообразна разузнавателна информация. В този история тип „ирония на съдбата“ има и комерсиален момент. Преди публикацията ръководството на списание WOZ предлага на шпионшна Зайлер да изкупи целия тираж от 20 000 бройки срещу сумата от 120 000 швейцарски франка (97 690 евро), но той не е реагирал до крайния срок на „ултиматума“ и броевете са пуснати на пазара. Паралелно с това списанието пуска и специален сайт в Интернет, посветен на „пробиването“ на шпионина – markusseiler.ch.

Главният редактор на „Вохен цайтунг“ - Щефан Ховалд обяснява действията на редакционния екип на списанието с пасивността на разузнавателната агенция на Швейцария, която обединява няколко служби по повод на кражбата на информация от WOZ през 2012 г. По този начин екипът на списание „Вохен цайтунг“ по своеобразен начин повдига въпроса за защитата на информацията като вид интелектуална собственост. Цената, която е предявена към г-н Маркус Зайлер може да се погледне и като един вид стойностна оценка на загубите на списанието от кражбата на информация, която явно е била важна за самото списание, и от бездействието или пасивността на разузнавателната агенция.

В Република България в пресата[36] излезе друг тип информация този път, свързана с посегателството върху личното пространство на гражданите. Отскоро нов вид жалби засипват Комисията за защита на личните данни. Жители на кооперации се оплакват от камерите за видеонаблюдение пред входа на кооперациите. Оказва се, че средствата за набиране на видеоинформация нарушават личното пространство на живеещите в непосредствена близост и представляват своеобразна кражба на лични данни. Възниква за пореден път проблемът за баланса между сигурността и личното пространство и личния живот на хората и опазването на частната собственост, отбелязва като коментар на жалбите председателят на Комисията по защита на личните данни – Венета Шопова.

Борбата за контрола върху информацията в различните страни и региони и в различните „частни случаи“ има различни подбуди и цел. Конкретно за САЩ и

35 „Списание шпионира топ шпионин“, в „Труд“, събота 07.12.2013 г., с.50.
36 „Комшии се жалват от камери“, в. Днес, 07.12.2013 г. , с.13

тяхната позиция на „Биг Брадър“ в подредбата на световния геополитически и геоикономически пъзел целите и мотивацията им са показани много добре от Джон Пъркинс н неговата „Изповед...“: Та кохортите мъже и жени за които става въпрос, напускат луксозните си офиси в Манхатън, Сан Франциско или Чикаго, кръстосват континенти и океани в луксозни самолети, отсядат в първокласни хотели и се хранят в най-шикозните ресторанти, които съответната страна може да предложи. След което тръгват на лов за отчаяние....Тези мъже и жени считат себе си за почтени. Те се връщат по домовете си със снимки на исторически места и древни руини и ги показват на децата си. Присъстват на семинари, където се потупват едни други по гърбовете и си разменят по някои и друг съвет за справяне със странностите и обичаите по далечните земи. Босовете им наемат адвокати, които да гарантират, че всичко извършено от тях е напълно легално. На свое разположение имат и състав от психотерапевти, както и други експерти по човешки ресурси, чиято цел е да ги убеждават, че всъщност помагат на отчаяните хора в различните точки на света...Съвременният търговец на роби се самоубеждава, че за обезверените хора е по-добре да изкарват по един долар на ден, отколкото да не изкарват нищо, и че така те получават възможността да се интегрират към по-голямата световна общност. Той също разбира че тези клетници са от ключово значение за оцеляване на компанията, че на тях се крепи начинът му на живот.“[37] Този дълъг цитат представя в резюме действията на кохортата „икономически килъри“, които имат за цел да впримчат и впрегнат в общия ярем на международната задлъжнялост поредната жертва – страна, регион, локална общност или друга обществена група. В тази им нелека дейност по корумпиране на администратори и политци от различни страни „икономическите килъри“ са подпомагани от „бойците на тихия фронт“. Нерядко битността на „икономически килър“ се съчетава и припокрива с позицията на резидент на определена разузнавателна централа. Такава двойна роля конкретно за себе си признава и в „Изповедта...“ самият автор – Джон Пъркинс. От една страна той официално присъства зад граница като служител на определена корпорация, от друга той е агент на Националната агенция по сигурността. Крайната цел на двете привидно независими структури – едната държавна, другата – част от корпоративния бизнес-сектор, всъщност е една и съща – финансово и икономическо обвързване на изостаналите страни и територии с икономически водещите държави в света и най-вече със САЩ.

Идеята за контрол върху глобалната мрежа не е нова. Още по времето на президента Клинтън в САЩ по законодателен път се опитват да наложат контрол върху Интернет-мрежата с приемането на Communication Decency Act[38]. Опитът за контрол върху Мрежата от страна на администрацията на президента Бил Клинтън става причина за появата на Декларацията за независимостта на киберпространството на Джон-Пери Барлоу - „Declaration of the Independence of Cyberspase – 1996“[39]Брожени часове след появата на протеста на Барлоу в Интернет-пространството той е копиран хиляди пъти и разпространен буквално със скоростта на светиланата. По този начин е формирана една неунищожима информационна среда. С тази си акция Барлоу доказва още в началните години на Интернет-

37 Пъркинс, Дж. Изповедта на един икономически килър. - София: Издателство Световна библиотека, 2012, с. 254-256.

38 Barlow, J.-P. A Declaration of the Independence of Cyberspase. 1996, http://www.eff.org/Publications/John_Perry_Barlow_0296.declaration

39 Пак там.

експанзията, че нито една власт не може да посегне на виртуалния свят понеже в него няма реални обекти и предмени, липсва ординарния, конвменционален материалин свят, с които оперират правовата държава и традиционните статусни общества.

В най-общия случай независимостта на киберпространството обикновено се артикулира като проблем за свободата на комуникацията в Интернет. Днес този проблем намира нови проекции в практиките на превенция и защита на информацията в Интернет-пространството от посегателство и и от манипулация с цел постигане на користни цели и в частност на корпоративните цели на гигантските корпорации, които доминират съвременното глобализирано стопанство. Синята лента (Blue Ribbon) е едно от влиятилните обществени движения за свобода на словото в Мрежата от времето преди появата на социалните мрежи като Туитър, Фейсбук и др. подобни. Още през ноември 1997 г. по време на международна конференция в Брюксел, организирана от Фондацията за човешки права и и Регионалната програма за Интернет на Института „Отворено обчщество“, група научни работници и юристи от САЩ и Европа разработват един важен документ, какъвто са „Принципите на политиката за открит Интернет (Open Internet Polici Principles). Този документ е насочен към създването на модел на законодателна власт и управление, които могат да се използват от правителства и други правозащитни оргжанизации, които по един или друг начин са принудени да взимат решения относно използването и развитието на Интернет-мрежата. Тези принципи акцентират върху особеностите на Интернет-мрежата като социален феномен. Най-общо тези принципи включват следните моменти:

- Свобода на изказваните мнения;
- Възможност за достъп до инфраструктурата на Интернет (независимо дали срещу заплащане или безплатно);
- Запазване на тайната при обмена на информация от страна на структурите осъществаващи мениджмънта на информационния обмен в мрежата;
- Анонимност на комуникаторите в мрежата;
- Свободно използване на криптографията;
- Достъп до държавна информация, която няма секретен характер.

Както се отбелязва в специализираната литература „принципите за открит Интернет са пример за прогресивно политическо мислене.“[40] Според тези принципи правителствата би следвало да се въздържат от контрол върху съдържанието на информацията в Интернет-мрежата, най-вече затова защото „достъпът да глобалната мрежа и другите интерактивни комуникационни инфраструктури е изключително важен за всички граждани по света.“[41] Същевременно в този документ се обръща внимание на това, че принципите за свободен достъп до Интернет следва да се съгласуват със съществуващото национално законодтелство на отделните страни, което е израз на една балансирана позиция на авторите. Това е разбиране, че виртуалното пространство, макар да е в известна степен фикция е е неразделна част от социума и в някаква степен преставлява нещо като негово виртуално разширение и своеобразен допълнителен обхват като „правна територия“. Както отбелязва Р. Гинев: „Свободата на всяка социална субсистема, каквато е и Киберпрост-

40 Гинев, Р. Информация и Интернет. - Вектори на социалната трансформация. - Варна: Изд-во на ВСУ, 2005, с. 137.

41 Скиллингз, Дж. Кр. Эссик. Какими быть „Принципам политики открытого Internet“. - Computerworld, #15, 1997, http://www.osp.ru/cw/1997/15/022.htm.

ранството на Мрежата не може да се разбира к8ато крайна партикуларизация.“[42] Същевременно не е корлектно и определянето на своеобразния „обществен договор“ в Интернет-пространството единствено като технически компютърен протокол, каквито опити има от страна на автори като Док Сиърлъс и Дейвид Уайнбъргър[43]. Според последните двама автори като антитеза на политическата власт и бизнеса трите най-важни достойнства на Интернет са:

1./ Никой не владее мрежата;

2./ Интернет може да се ползва свободно от всеки;

3./ Всеки, който има желание може да усъвършенства Интернет.

Независимо как ще се интерпретират превенционалните аспекти на достъпа и ползването на Интернет и на другите комуникационни технологии, дали като част от принципи, които ще се приемат като база за действие и разработване напроцедури и алгоритми, или като част от технически протокол, подобно на крайния подход на Сиърлъс и Уайнбъргър, добре е те да станап постепенно част от неписаните правила, които всички ползватели на комуникационните и информационни технолгии спазват.

Защо хората, в качеството им главно на ползватели на новите информационни и комуникационни технолгии, се стремят да защитят информацията, която разменят и обработват в киберпространството? Главно за да защитят възможността си да извличат изгода от предоставянето на тази информация с комерсиални цели. Разбира се най-добре би било ако цялата Интернет информация както и информационния обмен в контеста на мобилната телефония са безплатни и напълно свободни за ползване, но това на този етап не е възможно, защото би унищожило стимулите да се разработва актуално и все по-иновативно Интернет-съдържание. Резонно е да има защита на авторските права по отношение на даден тип информация, независимо дали е текст, видео, музика, комбинация или вариант на презентиране на даден проблем. Кое би ограничило неетичното ползване на информация, кражбата на информация, направата на пиратски копия на различни информационни „обекти“ - филми, видеоклипове, книги, музикални записи и др. подобни? Едно от нещата е криптографията и създаването на информацинни продукти с високо качество на защитата. Доколкото всяка защита е доста условна и не представлява препятствие за компютърните експерти, възниква въпросат дали в етичен план не е подобре да се определи някаква много малка, почти символична такса за позване на даден тип информационен обект, която символична такса ще позволи масово ползване, ще направи пиратските копия, значително по-скъпи от платения но изключително евтин достъп до съответния вид информация. Друг подход, който също би могъл да се прилага в един етичен аспект като превенция срещу кражби и пиратство е този да се създаде фонд, в който да постъпва много малък процент от всяка платена транзакция в пространството на глобалния информационен обмен. Когато се появят информацинни обекти с особена ценност, към които има голям обществен интерес, а същевременно тяхната цена, определена от създателите им е висока за масовия ползвател, тогава от този специализиран акумулационен фонд да се отделят средства за закупуване на съответния информационен обект, като се заплаща толкова, голяма цена на създаделите на такъв тип информация, че те вече да

42 Гинев, Р. Цит. Съч. , с. 138.

43 Сирлз, Д., Д. Уайнбергер. Свет с окраин или что такое Интернет и как его ни с чем не путать. - Руский журнал, март 2003, http://www.russ.ru/netcult/20030316.html.

не се интересуват кой и в каква степен в последствие ще разполага с тази информация и как ще я използва. Високият хонорар следва да ги мотивира да се откажат от авторски права и да предоставят съответния информационен обект за свободно ползване. Понякога има такива авторови решения и без да се заплаща каквато и да е сума, но това са обикновено редки случаи на „информационна благотворителност“. Безплатния достъп до информационната система „Линокс“ е един от тези примери за информационна благотворителност от страна на разработчиците на конкурентната на Майкрософт система.

Какво ще спечелим в етично отношение при такива подходи – първо няма да има злоупотреби с авторските права, второ част от хакерските атаки и усилия ще се обезсмислят, ако до ценни информационни обекти има един по-свободен и олекотен достъп, второ ще се спести огромен труд на криптолози и специалисти по защита на информация, които ще могат да насочат усилията си към защита на информационни обекти които представляват по същество класифицирана информация и не са предназначени за масово ползване, трето ще се мотивират подействгвено разработчиците на ценно информационно съдържание, защото ще знаят, че почти гарантирано ще получат адекватно на труда им високо заплащане на техните усилия и креативни изяви, макар и еднократно. Последващите заплатени моменти могат да бъдат тези свързани с усъвършенстването и актуализацията на информационните продукти.

В един морален аспект раелизацията на тези подходи за стимулиране – или като много евтин, но много масов достъп до информация или високо еднократно заплащане на ценни информационни продукти би следвало да се съпътства от една по-морална позиция на авторите за отказ от плагиатство. Предлаганите за оценка и хоноруване от специалните фондове продукти следва да минават проверка за автентичност. Подобни проверки ще доведат постепенно до отказ от масовата практика на информационно пиратсво на дребно на принципа „копи/пейст“.

Ако тези морално-етични проблеми при боравенето с информационните ресурси в системите на новите информационни икомуникационни технологии не намерят адекватно и относително бързо решение има опасност от появата на множество негативни практики. Най-крайната е отказът от „публикация“ на информацията във виртуалното пространство. Друго следствие би било минимизирането на информацията от индвидуален характер в Интернет-пространството. Публична тайна е, че при обменът на информация между различните криминално проявени личности от ъндърграунда на отделните страни по светау отдавна се използват специфични кодировки на привидно явната информация, за да се предават съобщения по официалните канали, за които се знае, че се подслушват и контролират. Няма да е учудващо, ако подобен подход на специфично кодиране на обменяната информация се възприеме постепенно и от хората, които не са криминално проявени, но не желаят да имат външен контрол върху споделяните идеи и проблеми. Другият момент с контролът е сворзан с проследяването, къде е позициониран даден източник на информация. Техническите възможности в тази посока са изключително напреднали. За момента подслушвателните техники могат да работят при изключени и неактивни технически средства и да проследяват самите чипове, които управляват информационния обмен. Днес вече и свалянето на батерията на телефона не гарантира, че той няма да се използва за подслушване и контрол върху информацията от индивидуално естество. Затова и някои секретни съвещания се провеждат

при депозиране на телефони и други мобилни устройства далеч, извън залата, където се водят конфиденциални разговори. Нерядко за такъв тип разговори се избират пусти места, без мобилно покритие, навън сред природата, където се предполага, че различни подслушвателни устройства биха били лесно откриваеми и забележими. И въпреки тези мерки никога няма сигурна гаранция, че конфиденциалността на разговорите е защитена в подобаваща степен.

Рамките на едно такова изложение не позволяват да се презентира цялата палитра от проблеми, които възникват в резултат на опитите за контрол и следене на информацията от индивидуално естество в информационните и комуникационни мрежи в съвременната глобализирана икономика. Няколкото аспекта, на проблемите на превенция срещу тоталния контрол на информацията и произтичащите от това проблеми по защита на личните данни на гражданите и на личната информация в качеството й на интелектуална собственост все пак са добра илюстрация, че отлагането на решенията в тази посока и пренебрегването на тези проблеми заплашват с подкопаване на доверието в надеждността и защитеността на информационните и комуникационни мрежи, а от там липсата на доверие снижава мащабите и обхвата на този социален капитал, който се генерира на база на общностите, създавани и поддържани благодарение на новите информационни и комуникационни технологии.

Търсенето на оптимални и перспективни решения на морално-етичните и психологически аспекти на оперирането на информация от мрежов тип е своеобразна инвестиция в социален капитал от нов тип, който се базира на технологичните достижения на човечеството и позволява преноса на социалните взаимодействия, социалната подкрепа и взаимопомощта от реалното във виртуалното пространство, където няма граници за човешката креативност и изобретателност. Тези нови орбити и радиуси на обхват на социалния капитал все още не са достатъчно добре изследвани и анализирани и представляват реално научно предизвикателство пред младите хора, на които предстои да бъдат граждани на бъдещото информационно общество, на чийто праг днес стои човечеството.

Използвана литература:

1. Гинев, Р. Информация и Интернет. - Вектори на социалната трансформация. - Варна: Изд-во на ВСУ, 2005, с. 137.

2. Пъркинс, Дж. Изповедта на един икономически килър. - София: Издателство Световна библиотека, 2012, с. 254-256.

3. Скиллингз, Дж. Кр. Эссик. Какими быть „Принципам политики открытого Internet“. - Computerworld, #15, 1997, http://www.osp.ru/cw/1997/15/022.htm.

4. Сирлз, Д., Д. Уайнбергер. Свет с окраин или что такое Интернет и как его ни с чем не путать. - Руский журнал, март 2003, http://www.russ.ru/netcult/20030316.html.

5. Barlow, J.-P. A Declaration of the Independence of Cyberspase. 1996, http://www.eff.org/Publications/John_Perry_Barlow_0296.declaration.

6. Стоянова-Тонева, Й. Международни конфликти и икономически деструктивизъм. - Годишник на ВСУ, том XII, 2007.

РЕГИОНАЛНИ И ЛОКАЛНИ КОНФЛИКТИ И ОТРАЖЕНИЕТО ИМ ВЪРХУ ДЪРЖАВНОСТТА

Пламен Ц. Цонев, Младен Д. Тонев

Национален военен университет „Васил Левски" – Факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи", катедра „Информационна сигурност" – гр. Шумен, Р. България

Варненски свободен университет „Черноризец Храбър", Факултет „Международна икономика и администрация",
катедра „Международна икономика и политика" – гр. Варна, к.к. „Чайка", Р. България

REGIONAL AND LOCAL CONFLICTS AND THEIR IMPACT ON STATEHOOD

Plamen Ts. Tsonev, Mladen D. Tonev

ABSTRACT: *The present report deals with the regional and local conflicts and their impact on the statehood. Advocates argue that this impact can't be assessed uniquely. Much of the conflicts and undermine past and present are leading to erosion of the state. While a significant part of the conflicts - mostly separatist and irredentist - have state-creative nature and effects.*

The effects of conflicts on statehood interpreted as a set of processes and phenomena of political, economic, military and cultural character in both aspects of impact: state-erosion and state-creative.

KEY WORDS: *conflicts; security; state-erosion; state-creative; separatism; irredentism; centralized state power.*

Стереотипните нагласи и възприятия формират усещането за своего рода обратно-пропорционална връзка между конфликтността (в национално-обществен и международен план) и държавността. Инерцията на мисленето ни води по логиката на деструктивните последици на конфликтните ситуации. Обикновено щом се разрази конфликт от по-малък мащаб – локален или регионален – то той действа ерозийно, разрушително по отношение на държавността. Най-малко се приема, че даден конфликт, който ангажира дадена държава или се разразява на нейна територия подкопава устоите ѝ и намалява центростремителните и центро-удържащи сили. Нещо повече – Жак Атали в книгата си „Речник та XXI век" прогнозира, че през новия век на големи територии на планетата в резултат на конфликти ще липсва познатата ни държавност с охранявани граници, централно определяни закони и централно-регулиран обществен ред и порядък. Накратко – големи територии от Африка, Азия и дори Латинска Америка ще останат извън обхвата на държавността. В останалите части на планетата, където атрибутите на държавата успеят да се съхранят ще се установи според него „комунитарно общество". Жак Атали си представя това общество като море от маргинализирани индивиди, в което са потопени малките градски общности, обитавани от високо-образован и

високо-заплатен елит, който ще си купува социалния мир, чрез „откупуване“ спрямо маргинализираното множество.

Истината е, че стереотипната представа губи смисъл ако само обърнем поглед назад към историята и констатираме, че повечето държави в света са резултат на конфликти – граждански и антиколониални войни, сепаратистки и иредентистки движения, междудържавни конфликти и дори световни войни. Само в Европа след Първата световна война възникват повече от 10 държави – Унгария, Чехословакия, Полша, Югославия, Финландия, Литва, Латвия, Естония, Грузия, Армения, Азербайджан, (последните три за кратко, преди да влязат в състава на СССР). Подобни държавно-творчески процеси поражда и краят на „Студената война“.

Тези две привидно противоположни следствия от локалните и регионални войни, всъщност се допълват и взаимообуславят. Нерядко разрушаването и унищожаването на дадена държава, ражда нови държави чрез процеса на „творческо разрушаване“. Като цяло не можем еднозначно да определим един конфликт като държавно-ерозионен /подкопаващ/. По същия начин не можем категорично да го определим и като държавно-творчески. Тези констатации налагат извода, че всеки конфликтен процес е двуяк – едновременно той руши и подкопава държавността или най-малко подрива силата на централната власт, от друга страна той съдържа потенциала нерядко да даде старт на нов държавен субект на политическия небосклон.

Всеки регионален или локален конфликт е уникален и неповторим като характеристики, фактори, причини и условия, които го пораждат, поддържат и финализират, както и като последици и разрушителни или конструктивни сили. Това обаче, не е препятствие пред различните опити за класификация и типологизация на този тип конфликти и последиците им в специализираната литература.

Съвременната конфликтология предлага сравнително широк набор от дефиниции на конфликтите на различни равнища и от различно естество. В принципен план М. Дойч дефинира конфликта като „ ситуация на антагонистични (противоположни) отношения между хората, които възникват и се развиват в следствие на непримирими техни позиции”. Конкретно регионалните и локални конфликти също са многоаспектно дефинирани и прегледа и анализа на различните дефиниции може да бъде предмет на отделно изследване. За да не навлизаме в „лабиринта” на подобен анализ предлагам една по-широка визия за това, което ще разглеждаме като „регионален и локален конфликт”, а именно всяка ситуация на сблъсък на интереси между общности (политически и партизански движения, сепаратистки движения, терористични групи, частни армии, етнически кланове, господстващи клики, групи за натиск, протестни движения, ситуационни групи за гражданско неподчинение и др.) и държави, между самите държави и между държави и наддържавни и международни институции и организации с идеална цел, която се развива в регионални или вътрешно-държавни граници.

Това, което е общото между „регионалните вътрешно-държавни и международни конфликти” и другите конфликтни реалности от различен характер е това, че и при тях са налице трите важни характеристики на всеки конфликт:

- налице е *противопоставяне на хора*;
- налице е процес или резултат на *сблъсък и налагане на интереси*;
- реализацията или разрешаването на конфликта предполага някакъв мащаб и някакво ниво на *„материализация”на надделелите интереси, во-*

деща до изгода и печалби за някоя от участващите в конфликта страни..

Спецификата при регионалните и локални конфликти се изразява в следните няколко аспекта:

Първо: Както и при другите видове конфликти и при местните конфликти (включително и при тези с международен характер) имаме противопоставяне на хора, но в битността им не на личности, граждани, индивиди, а в качеството им на оторизирани представители на различни държавни институции на законодателната, изпълнителната и съдебната власт от една страна и на представители на претендиращата за власт и права или за територии общност /държава/ наднационална институция.

Второ: Налагането на интереси има други мащаби и измерения и се отнася до аспекти на държавния суверенитет, независимост и териториална цялост на дадена страна, както и до накърняване на аспекти от конституционното устройство на конкретно държавно образувание. Това е валидно за голяма част от конфликтните ситуации. При друга част от конфликтите налагането на интереси има или укрепващ ефект върху централизацията на държавната власт или води до появата на нови държавни структури.

Трето: Материализацията на надделелите интереси има също други мащаби и най-вече друго равнище – микро- и макроикономическо. Особеното при регионалните и локални конфликти е, че пораженията (чисто военните) се локализират в относително ограничен географски ареал. При глобалните международни конфликти мащабите са мегаикономически и пораженията от материално и морално естество в социален, стопански, политически, културен и религиозен план са много по-мащабни, както и последствията от глобалните конфликти са много подълготрайни и обременяващи историческата памет на народите.

Тези особености на регионалните и локални конфликти предполагат изследването им като самостоятелни процеси и най-вече типологизирането им от различни гледни точки и в различни контекстни интерпретации. При условие, че обикновено най-малко една от страните в подобни конфликти има държавнически характер и статут, то най-ниското равнище на проявление на тези конфликти е макроикономическото и по-високото мегаикономическо равнище. Резултатите от развитието на конфликтните ситуации също имат подобно измерение – макро и мегаикономическо, но това не им пречи да имат същевременно и микроикономически проекции, т.е. да рефлектират върху статуса и функционирането на отделните фирми и домакинства в рамките на дадена държава.

1.2. Типологизация на регионалните и локални конфликти.

Една относително по-пълна класификация на регионалните и локални международни конфликти предполага систематизирането на един комплексен набор от типологизации на този тип конфликти, които типологизации се основават на различни признаци и критерии.

Според **равнището на проявление** регионалните а и някои локални конфликти могат да се реализират главно на макро и на мега равнище, но като последствия и резонанс те могат да имат рефлексия на всички равнища:

- микроикономическо;
- макроикономическо;

- мезоикономическо;
- мегаикономическо.

Като **исторически резултат в оценките и нагласите на хората** регионалните и локални конфликти могат да имат като следствие:

а) историческа гордост (например Сръбско-българската война от 1885 г. или Балканската война от 1912 г. за нас българите);

б) историческа обремененост – (Междусъюзническата война и загубата на Беломорска Тракия и Вардарска Македония);

в) исторически комплекс, който може да бъде или комплекс за превъзходство или комплекс за малоценност – (такъв комплекс на обремененост и малоценност се формира у подрастващите, поради дефекти в начина на поднасяне на историческата познавателна материя, спрямо Османска Турция, който прераства и в комплекс спрямо съвременната Република Турция).

Като **статусен резултат** регионалните и локални конфликти могат да бъдат:

- *държавно конституиращи (държавно-творчески),* при които се създават нови държави, най-често като **разпад на съществували държавни структури** като Съветския съюз, Титова Югославия, Чехословакия и др. или чрез **отделяне на части от съществуващи и исторически утвърдени държави** като Панама, която се отделя от Колумбия; Бангладеш, която се отделя от Пакистан, Косово, което се отделя от Сърбия, Еритрея, която се отделя от Етиопия както и като **обединение на исторически разделени или териториално близки държави** като присъединяването на щата Тексас към другите Съединени американски щати в общата федерация САЩ; обединението на Северен и Южен Виетнам в резултат на победата на Северен Виетнам във войната със САЩ в района на Индокитай, обединението на Германия в резултат на разпадането на бившата Световна социалистическа система.;
- *държавно деструктивни конфликти,* при които се разпадат и дори ликвидират дадени държавни образувания – разпадането на Съветския съюз в резултат на загубата на Студената война, разпада на Югославия в резултат на същия процес, арабско-израелския конфликт от 1948 г. в резултат, на който се възпрепятства създаването на независима Палестинска държава; отделянето на Северна Осетия и Абхазия от Грузия; отделянето на Приднестровската република от Молдова или на Косово от Сърбия (*т.е. един и същ конфликт може да бъде различно позициониран и като държавно творчески и като държавно деструктивен в рамките на една и съща типологизация в зависимост от оценката и тълкуването на съответния резултат от конфликтния процес.*). Аналогични конфликти, имащи за следствие разрушение на държавността в резултат на сепаратистки движения или като следствие на вътрешноплеменни и междукланови (граждански) войни са процесите на ерозия на държавността в Судан, Сомалия, Руанда, Бурунди, Конго и др.;
- *неутрални по отношение на държавното структуриране регионални и локални конфликти* – конфликтът между САЩ и Куба, конфликтите между Китай и Виетнам в началото на 80-те години на XX век; Фолклендският конфликт между Великобритания и Аржентина и др.

Според **обхвата** на даден конфликт може да се диференцират три различни равнища на обхват (Виж Таблица 1.1.):

а) *локални международни конфликти* – Кипър със Севернокипърската турска република; конфликта между Израел и Палестинската автономия, спорът за името „Македония" между Република Гърция и БЮР Македония; граничния териториален спор между Хърватия и Словения в началото на лятото на 2009 г., който застрашава бързото приемане на Хърватия в ЕС в близко бъдеще;

б) *регионални международни конфликти* – тук се визират по-комплексно и по-обобщаващо конфликтите в даден географски регион – Балканите (войната в Босна, войната между Сърбия и Хърватия, Косовския конфликт), Прикавказието (войната в Чечня, отделянето на Абхазия и Северна Осетия от Грузия, някогашните конфликти между Армения и Азърбейджан по повод събитията в Нагорни Карабах, противопоставянето между Русия и Грузия в Северен Кавказ и др.); конфликтите в Близкия Изток – Израел и Сирия, Израел-Иран, Израел-Палестина и т.н..

в) *глобални международни конфликти* – това са глобално проявяващи се противопоставяния – Първата и Втората световни войни; Студената война; Войната с международния тероризъм, която водят САЩ и някои от европейските държави с различни терористични групировки като „Ал Кайда", „Мюсюлмански братя", „Джамии исламия", както и войната с различните кланове в Сомалия и срещу талибаните в Афганистан и срещу някои сунитски родове в Ирак, близки до свалените и публично обесен иракски диктатор – Саддам Хюсеин.

Противопоставянето между ислямския фундаментализъм в различните му разновидности, /олицетворяван преди всичко от Ислямска република Иран и някои консервативни арабски монархии и от най-новата терористична структура – Ислямска държава (Бивша Ислямска държава в Сирия и Ирак)/ и западните държави, начело със САЩ, олицетворяващи ценностите на западната представителна демокрация може също да се интерпретира като конфликт с глобални измерения, ако използваме алюзията на С. Хънтингтън, който е автор на бестселър със заглавие „Сблъсъкът на цивилизациите". Въпросното заглавие много точно илюстрира сблъсъкът между исляма и християнството (без значение дали говорим за католици, протестанти или православни християни, или за сунити и шиити сред изповядващите исляма).

Според **продължителността** на регионалните и локални конфликти те могат да се подразделят на (виж Таблица 1.1.):

- *еднократни инциденти* – ситуации на сблъсък на интереси, на дипломатически реакции, дори и на военни акции, интервенции и диверсии за кратко време, еднократно, най-често като реакция или ответно действие и респективно контра-действие на даден политически, икономически или дипломатически акт. Арестът на група студенти от САЩ в карибската държава Гранада през 1985 г. служи за повод за нахлуването на американската морска пехота на малкия карибски остров. Подобна е акцията на САЩ в Панама през 90-те години на XX век под предтекст, че президентът на Панама - Даниел Ортега препятства борбата срещу трафика на дрога в района на Централна Америка. Нахлуването в Иран през 1979 от страна на САЩ, което търпи военен неуспех, е аргументирано като акция за спасяване на заложниците в посолството на САЩ в Техеран. Служителите от посолството на САЩ в Техеран са блокирани и държани в обсада като заложници от иранските

ислямисти след революцията на аятоласите, превърнали Централноазиатската монархия в Ислямска република.

- *кратки като времева продържителност конфликти* – границата между инцидентните и кратките конфликти е условна. Като относително краткотрайни военни сблъсъци могат да се визират боевете между Съветската армия и японската Квантунска армия при езерото Хасан и при височините Халхин гол през 1939 г. Сравнително краткотраен е конфликтът между Аржентина и Великобритания известен като Фолкленската криза през 1981 г. Като краткотраен военен сблъсък може да се определи и Сръбско-българската война от 1885 г. след Съединението на Княжество България с Източна Румелия на 6 септември същата година.

- *продължителни като времетраене конфликти* – обикновено това са конфликти, развиващи в продължение на години с променлив интензитет в различните периоди на протичането им. Типични в това отношение са Наполеоновите войни в Европа, които продължават повече от десетилетие. Гражданската война в САЩ между Севера и Юга за отмяна на робството е първият конфликт, който се характеризира както с продължителност така и с гигантските мащаби на човешки жертви и поражения на инфраструктурата. Първата и Втората световни войни също са много продължителни като времетраене и съответно се характеризират с мащабни деструктивни процеси във всички аспекти – демографски, социални, инфраструктурни, стопански, морални, здравно-медицински и т.н. Студената война е също продължителен конфликт, макар и без явни военни сблъсъци тя също има деструктивен ефект, доколкото форсира надпреварата във въоръжаването между двете суперсили – САЩ и СССР и техните сателити и въвлича огромни ресурси в трупането на оръжейни и ядрени арсенали.

- *перманентни конфликти* – тяхното диференциране също е условно. От дистанцията на времето, в едно близко бъдеще, някои от тези конфликти може да се определи просто като продължителен, след като вече е прекратен или загубил смисъл. Партизанските движения в някои страни на Латинска Америка – Перу, Колумбия, Боливия отдавна са изгубили своята лява, промарксистка идейна основа. Те съществуват по-скоро по силата на някаква историческа инерция. На практика те са се изродили във фракции и групировки, които отвличат чужденци и богаташи с цел откуп, за да финансират базите и начинанията си. В такъв един аспект може да се припише характеристиката „перманентност" на тези движения, които имат своите исторически корени още в борбата за национално освобождение и независимост на страните от района на Латинска Америка. Множество противопоставяния между някои консервативни леви и ислямистки диктатури и Запада също могат да се позиционират като перманентни конфликти, генериращи едно постоянно напрежение в международните отношения. Например, противопоставянето на Куба на САЩ от периода на Карибската криза в началото на 60-те години на XX век почти до наши дни, напрежението между Северна и Южна Корея и обтегнатите отношения между Северна Корея и САЩ, между САЩ и Либия до неотдавна, както и между Иран и Западните държави.

Таблица 1.1.

Кростаблица на видовете конфликти като мащаби и продължителност

Мащаби Продължителност	Локални / местни /	Регионални	Глобални
Инцидентни/ еднократни	1929 г. Събитията по Източнокитайската железница	1939-1940 г. Германския блицкриг и окупацията на Европа от хитлеристка Германия	Нахлуването на американската морска пехота в Гренада през 1985 г. като момент от глобалната Студена война, за да не допуснат създаването на съветско-кубинска военна база
Кратковременни	1979 г. Военни сблъсъци между Китай и Виетнам; 1981 г. Фолкландската криза	1939 г. Събитията при езерото Хасан и боевете при Халхин гол	Нападението при Пърл Харбър на 07.12.1941 г., което става начало на войната между САЩ и милитаризираната Японска империя и провокира включването на САЩ в световната война.
Продължителни	100 годишната война между Англия и Франция; Селската война в Германия в първата половина на XVII век.	Антифашистката съпротива в Европа в годините на Втората световна война. Войната на САЩ срещу индокитайските държави Ветнам, лаос и Камбоджа.	Студената война 1946-1989 г.
Перманентни	Вековни родови вражди в някои средиземноморски страни и области.	Партизанските движения в Латинска Америка	САЩ и Зап. Европа срещу опитите на Иран да развива ядрени технологии с военно предназначение; Войната на САЩ със световния тероризъм.

Според **интензитета** на един регионален или локален конфликт можем да говорим за:

А) *латентни (дремещи), (потенциално възможни) регионални и местни конфликти*. Жак Атали в „Кратка история на бъдещето" предполага бъдещ конфликт между Китай и Русия по повод демографската експанзия на китайски граждани в Югоизточен Сибир и Приморския край. Конфликтът между албанското „малцинство" и славомакедонците в Северозападната част на БЮР Македония също може да се определи като „латентен" на настоящия етап. Неговото активиране зависи от комплекс от фактори, сред които като определящи могат да се посочат демографската експанзия на албанския етнос в този политически невралгичен район на младата македонска държава и външната намеса (по линия или на САЩ или на различни групировки на ислямските фундаменталисти, които биха потърсили реванш в противопоставянето със Запада на самата територия на континента Европа).

Б) *явни (изразени), експлицитни регионални и локални конфликти* – те на свой ред могат да се подразделят на няколко подвида:

- явни конфликти с нисък интензитет – типична в това отношение е неотдавнашната „Студена война" между САЩ и Съветския съюз и техните сателити, (в случая Студената война има повече глобални измерения, но не липсват и локални противопоставяния – САЩ – Куба; Източен и Западен Берлин; Северен и Южен Виетнам и др.) Кипър и Севернокипърската турска република; споровете и проти-

вопоставянето между Турция и Гърция; енергийните и газови „войни" между Русия и Украйна в близкото минало (днес заменени от явен конфликт между двете страни и производна от него анексия първо на Крим, а вероятно и на Донецка и Луганска области от страна на Руската Федерация); противопоставянето между САЩ и Куба, което отслабва с всеки изминат ден; Северна и Южна Корея, споровете между САЩ и Иран по повод на контрола върху иранските ядрени програми и технологии и др.;

- явни международни конфликти със среден интензитет – тук диференциацията налага известни условности и уговорки. Трудно е де се разграничат точно кои конфликти са тези, които могат да се дефинират като „конфликти със среден интензитет". Ако приемем, че такива са конфликтите, които периодично „припламват" и се активизират по различни причини, в различно време то такива са гражданските войни в Южен Судан, в Сомалия, в Конго по границата с Руанда и Бурунди, донякъде Израелскоо-Палестинския конфликт, войната в Чечня и Ингушетия и др.;

- явни международни конфликти с висок интензитет – в по-ново време това определено са двете световни войни през първата половина на XX век, войната на САЩ в Индокитай през 60 и 70-те години на XX век, Първата и втората война на САЩ и съюзниците им срещу Ирак. В миналото такива конфликти са били Гражданската война в САЩ в периода 1861-1865 г., Наполеоновите войни, Руско-японската война 1904-1905 г. и много други.

Според **характера и факторите**, които ги обуславят регионалните и локални конфликти могат да се подразделят на (Виж Таблица 1.2.):

А*) политически;*
Б*) военни*;
В) *социални;*
Г) *икономически;*
Д) *религиозни;*
Е) *културни;*
Ж) *екологични.*

Политическите конфликти най-често са резултат от опита за защита на интересите на определена политическа сила от външни фактори. Факт е, че редица политически събития като въстания, граждански войни в по-новата история са подтиквани и инспирирани от политическа намеса на външни сили. Днес, например, се признава, че опитът за разпалване на гражданска война през септември 1923 г. в Царство България е резултат от намесата на току що създадения Съюз на съветските социалистически републики. Самата революция на партията на Болшевиките от октомври 1917 г. е инспирирана и финансирана косвено от Великобритания (Империята на Ротшилдови) и пряко от Германия (Германският генерален щаб, чрез немският агент Парвус). Първата (Великобритания) цели да елиминира Русия като геостратегически конкурент. Втората (Кайзерова Германия) цели да я извади от участие във войната и да избегне война на два фронта.

По подобен начин фашистка Германия инспирира преследвания на судетските немци в Чехословакия, за да аргументира необходимостта от окупация и анексия на Судетската област и в последствие на самата Чехословакия.

Военните конфликти не се нуждаят от особен коментар. Най-семплата им типологизация може да ги диференцира като ***военни регионални и локални конф-***

ликти с международен характер и ***такива които са ограничени до територията на една държава.*** Последните се определят като граждански войни с присъщите им преки военни сблъсъци между противопоставящите се страни, вътрешни смутове, размирици, терористични актове, диверсии, саботажи и др. Те от своя страна могат да се разграничат като *сепаратистки войни* – военните стълкновения между Етиопия и Еритрея, между Грузия и Абхазия, терористичната война на Ирландската републиканска армия срещу Великобритания през 70 и 80-те години на XX век и *политически или религиозни граждански войни* – Гражданската война в САЩ за отмяната на робството, Хугенотските войни във Франция – XV – XVI век, продължилата близо 75 години гражданска война в Испания през XIX век, известна като Карлистките войни.

Социалните конфликти са по-трудно диференцируеми, доколкото в основата на много от военните стълкновения стоят социални проблеми и процеси. Като се започне от въстанията на робите в античността, премине се през антифеодалните въстания – Жакерията във Франция, селските войни на Стенка Разин и на Емелян Пугачов в Русия и се стигне до съвременните революции в Русия, Китай, Гражданската война в Испания 1936-1939 г. и др. При всеки от тези военни конфликти водещият мотив е социалният. Повечето от тези конфликти се разразяват на територията на една държава, но доколкото имат широк международен резонанс може да се разглеждат като част от международните конфликти. Най-малко те са придружени с мащабни миграционни процеси – бежанци, бегълци, изгнанници, които пренасят напрежението на вътрешния, локален конфликт извън граница.

Икономическите конфликти /"войни"/ са свързани главно със сблъсък на икономическите интереси на отделни страни и дори на групи държави. Най-често това са външно-търговски интереси и претенции, произтичащи от несъразмерността на търгуваните обеми, пораждащи значителни дефицити във външнотърговските баланси на отделни страни. Класически в това отношение са противоречията между САЩ и Западна Европа по отношение на евтиния внос на аграрна продукция, която разорява европейските фермери и е причина за мащабни излишъци при добива на мляко в Западна Европа. През 80-те години на XX век тези противоречия са известни като „млечната война" между САЩ и Западна Европа. Аналогично в Северния Атлантик през същия период съществува сблъсък между интересите на Исландия, Великобритания и Норвегия относно параметрите на зоните за риболов.

Религиозните войни като вид международни, междуетнически и междуобщностни конфликти присъстват в цялата история на човечеството. Още в древността религиозните различия се използват за аргументиране на насилието и на воденето на военни действия. В по-ново време класически в това отношение са Хугенотските войни във Франция завършили със Нантския едикт от 1599 г., Селската война в Германия, Хусистките войни в Чехия и Бохемия и много други.

Културните конфликти са най-безобидни и не пораждат преки държавно-ерозионни или държавно-творчески процеси. На практика културните различия много рядко са използвани са обосновка и за предтекст на държавно обособяване, отделяне и конституиране. Обикновено в този случай става дума за сблъсък на културни влияния или за субкултурни процеси, които са посрещани критично от по-консервативно мислещото множество. Изключително агресивна в културен план е Франция. Неслучайно френският колониализъм от края на XIX и началото на XX век се определя като „културен" колониализъм, чиято главна същност е

културната и езикова инвазия на метрополията – Френската република спрямо покорените племена и народи. И днес Франция е държавата, която най-силно се съпротивлява на налагането на чужди културни образци сред французите и най-вече на влиянието на американската масова култура. Сблъсъкът между исляма и християнството също може да се интерпретира като културен сблъсък. Действията на австралийските аборигени и на новозеландските маори за запазване на тяхната автентична култура също се вписват в идеята за сблъсък на култури и ценностни системи.

Таблица 1.2.

Таблица на съвременните конфликти като видове и локализация

Видове/ Локализация	Между национални	Между етнически	Религиозни	Социални
Европа	Русия-Грузия Сърбия-Хърватия	Косово Босна Абхазия Приднестровието	Северна Ирландия Чечня Ингушетия Дагестан	Вълненията в гетата на Париж, Амстердам и др. европейски Градове в лятото на 2005 г.
Латинска Америка	Перу-Еквадор Венецуела-Колумбия	Индиански движения.	-	Сендеро Луминосо в Колумбия; .
Северна Америка	-	Движението за автономия на Квебек в Канада	-	Сапатисткото движение в Юкатан, Мексико.
Азия	Индия- Пакистан Израел-Палестина	Палестина Ливан Белуджистан Кюрдистан	Ирак –сблъсък между шиити и сунити. Афганистан – войната с талибаните. Войната с Ислямска държава.	Вълненията на мюсюлманските общности и на тибетците в Китай, поради икономическата изостаналост и подтискането на гражданските им свободи.
Африка	Мароко-Западна Сахара	Войната за освобождение на Южен Судан. Сблъсъците между тутси и хуту в Руанда и Бурунди и Източно Конго.	Войната между ислямските и прозападните военни милиции и групировки (кланове) в Сомалия	Отвличанията за откуп в Нигерия и нападенията на сомалийските пирати, които са възможни предвид масовата бедност в тези райони.
Австралия и Океания	-	Претенциите на аборигените в Австралия и на маорите в Нова Зеландия за запазване на тяхната автентична култура и самобитност.	Партизанската война на ислямската групировка Абу Саяф във Филипините, които са католическа страна	-

Екологичните движения, които са генератор на множество конфликти в съвременния свят също допринасят за някои дестабилизиращи държавността процеси. Като цяло обаче общественото мнение е настроено позитивно спрямо тях, доколкото те преследват запазване на природата, съхранение на съществуващите екосистеми, подобряване на условията за работа и живот на хората. Една типологизация, която предлага Мануел Кастелс в мащабния си труд „Информационната епоха". - том II – „Силата на идентичността" достатъчно добре илюстрира опасенията и визиите на еколозите от различните течения и групировки за деструктивното развитие на определени страни и региони. (Виж Таблица 1.3.)

Таблица 1.3.

Типология на екологичните движения

Тип (Пример)	**Идентичност**	**Противници на: (визии за деструктивно развитие)**	**Цел**
Запазване на природата (Групата на 10-те САЩ)	Любители на природата	Неконтролираното развитие	Дивата природа
Защита на собственото ни пространство („не в моя заден двор")	Местната общност	Замърсителите (фирми, ТНК, държавни органи, военни)	Качество на живота/здраве
Контракултура Крайна екология (радикална) („Първо земята" е кофеминизъм)	Зеленият „Аз"	Индустриализма, технократията и патриархализма	Екотопия (от екология и утопия)
Спасете планетата	Интернационалисти Екобойци „Гринпийс"	Безразборното глобално развитие	Устойчивост, стабилност. Запазване на статуквото.
Зелена политика	Защитени граждани	Политическата система	Контрасила

Източник: Кастелс, М. Информационната епоха. – II том, „Силата на идентичността". –София: ЛиК, 2006, с. 106.

В цитирания по-горе втори том на трилогията на М. Кастелс са изведени и принципите на „дълбоката екология", които са в основата на противопоставянето на различните национални и интернационални екологични движения на съществуващия глобален порядък[44]:

„1/ Добруването и процъфтяването на човека и човешкия живот на Земята имат смисъл сами по себе си.

2/ Богатството и разнообразието от форми на живот допринася за реализацията на такава ценност като живота и сами по себе си са ценност.

3/ Хората нямат право да намаляват това богатство и разнообразие освен за животоспасяващи цели.

[44] Кастелс, М. Информационната епоха. – II том, „Силата на идентичността". –София: ЛиК, 2006, с. 106-107.

4/ Процъфтяването на човешкия живот е съвместимо с намаляването на човешката популация. Нечовешкия живот дори изисква такова намаляване.

5/ Настоящата човешка намеса в нечовешкия живот е прекомерна.

6/ Следователно политиката трябва да се промени.

7/ Идеологическата промяна е промяна в оценката на качеството на живота."

Представените принципи на „дълбоката екология" дават основание да се заключи, че екологическите движения са антидеструктивни като нагласа и цели, но конфликтите, които те пораждат с гражданската си активност и претенции не винаги се вписват в тази логика на прокламирана деструктивност. Дейвид Рокфелер в своята автобиография много добре илюстрира деструктивните последици от претенциите и съдебния натиск на едно гражданско екологично движение за защита на морската фауна, което възпрепятства строителството на автомагистрала и мост между два района на град Ню Йорк. Дългогодишните съдебни дела между инвеститори и еколози оскъпяват и обезсмислят проекта за въпросните инфраструктурни строежи независимо, че се доказва екологическата му безопасност. От позициите на радикалния екологизъм група граждани стават причина за задълбочаването на депресията в крайбрежната зона на Ню Йорк. Вместо добра инфраструктура и добри условия за бизнес развитие и просперитет, които планира градската администрация на Ню Йорк в края на 80-те години на XX век, въпросните райони днес са едни от най-проблемните нюйоркски гета с всичките им негативни характеристики.

Според **начина на разрешаване** на конфликтите те могат да се подразделят на:

- ***конфликти разрешавани с мирни средства*** - главно чрез преговори, които могат да бъдат двустранни и многостранни, с посредник или без посредник. Обикновено такива преговори приключват с *договор, споразумение, съвместно комюнике* или друг дипломатически документ, който може да бъде таен или явен или смесен – т. е. явен, но включващ тайни клаузи. „Намирането на формула за решаване на конфликта, която евентуално се превръща в привлекателна възможност и за двете страни е ключът към приключването на всеки едни преговори"[45], отбелязва в една своя студия Даниела Фридл;
- ***конфликти разрешавани с немирни*** /военни/ средства. В крайна сметка тези конфликти също завършват с някакъв вид политическа и дипломатическа договореност под формата на мирен договор или най-малко с временно примирие.

Според **резултатите** от конфликта можем да говорим за няколко дихотомни двойки характеристики:

А) *държавно-разрушителни конфликти / държавно-творчески конфликти*;

Б) *контрактни* /разрешени с договор/ и *неконтрактни* /конфликти, които не приключват с договор/;

В) *конфликти, които водят до чужда намеса във вътрешните работи на дадена страна* и такива които се характеризират с *ненамеса във вътрешните работи на съответната държава*.

В по-новата история на човечеството двете световни войни ще останат в историческата памет на народите именно с огромните разрушения в Европа и в Близкия и Далечен Изток. Същевременно икономическите и културни „войни" на практика не предполагат никакви разрушения и материални щети, освен промяна в размер-

ността на държавния дълг при големите външно-търговски дефицити или в някои законодателни промени за защита на даден национален език или други национални културни достижения.

Войната на САЩ в Индокитай приключва с подписването на мирен договор между САЩ и Северен Виетнам в резултат на мирните преговори в Париж през 1975 г. Съветската инвазия в Афганистан през 80-те години на XX век приключва с изтегляне на съветските войски от афганска територия, но на практика не приключва нито с мирен договор, нито с каквото и да е друго споразумение, доколкото „легитимността" на афганско правителство се крепи единствено на съветското военно присъствие. Останалите групировки, които водят война със съветския военен контингент в Афганистан са политически разединени и не могат да представляват страната като цяло.

Конфликтът между косовските албанци и сръбското малцинство в Косово и опита за етническо прочистване от страна на сръбски военни формирования през 1999 г. довежда до *външна намеса*, а именно намесата на САЩ и някои техни съюзници от НАТО като Италия и Великобритания. В резултат на бомбардировките на американската авиация, излитаща от летища в Италия и от самолетоносачи в Средиземно море се стига до промяна в политическата обстановка в Република Сърбия и падането на режима на Слободан Милошевич. Като следваща стъпка стартира процес на отделяне на Косово от Сърбия, който акт все още се оспорва от сръбска страна.

Същевременно в Чеченския конфликт „външната намеса" се свежда само до политически и дипломатически обструкции от страна на Запада по адрес на Русия за нарушаване на човешките права в Чечения и Ингушетия. Респектът, който имат западните държави от военната и отбранителна способност на Русия изключва каквато и да е идея за намеса в конфликтите, които се разразяват перманентно на нейна територия и в приграничните й райони – Северна Осетия и Абхазия или районите на Източна Украйна - от началото на 90-те години на XX век насам.

В специализираната литература съществуват множество други класификации на регионалните и локални конфликти от различни гледни точки – форма на провление, факторите, които ги пораждат, причини за възникването, състав на страните-участнички в даден конфликт и т.н. Например, М. Дойч разглежда конфликтите от гл.т. на тяхната обективна причинност. Той диференцира „конфликти, съответстващи на действителността", „случайни конфликти", „неясни конфликти", „неправилно съотнесени конфликти", „скрити конфликти", „лъжливи конфликти" и пр. Руската авторка О. Громова от своя страна разграничава антагонистични (насилствени) и компромисни (ненасилствени) конфликти.

Посочените класификации на М. Дойч, О. Громова и др. автори обслужват друг тип изследователски цели и трудно могат да се използват за анализ и разкриване на конструктивните/деструктивните процеси от държавно-творчаски или държавно-ерозионен характер, пораждани от различните конфликти.

Самото категоризиране на конфликтите пък като „държавно-творчески" и „държавно-разрушителни" не е уместно, защото почти всеки конфликт има потенциала да бъде и едното и другото. По-скоро може да се търсят нюанси, степени в процеса на създаване на държавност в резултат на даден конфликт. Някои войни водят само до право на национално самоопределение или до повече етнически права – религиозни, културни и др. Други пораждат автономии – като например

Руско-Турската война от 1877-1878 г., в резултат на която за кратко съществува автономната област „Източна Румелия“. Част от конфликтите директно пораждат независими държави. Някои държави възникват като изкуствени – буферни образования – например Далекоизточната република, която възниква в хода на Гражданската война в Русия от 1918-1921 г. По късно тя, както и Тувимската република са включени в състава на СССР.

По аналогичен начин има нюанси и степени в държавно-разрушителните процеси, породени от даден конфликт. Има конфликти които само леко разклащат устоите на дадена държава като Парижката комуна от 1871 г. в резултат на Френско-Пруската война. Същата война обаче способства за обединението на Германия под скиптъра на пруския крал и възраждането на Германската империя. Други конфликти сериозно ерозират държавността и са необходими десетилетия, за да се излезе от затрудненията, които те пораждат - например Гражданската война в Испания от 1936-1939 г. Има конфликти, които пък не позволяват установяването на силна централна власт, като най-висш израз на държавността. Такива са междукланови войни в Сомалия. Най-деструктивни са конфликтите, които са разрушителни по отношение на дадена държавност. Например окупацията на Тибет от Китай през 1958 г.

Тези градации на ерозията и на конструктивността в релацията „държава-конфликт“ могат да се обосноват и подкрепят с примери и фактология в едно бъдещо самостоятелно изследване.

Литература:

1. Fridl, Daniella D. , Kosovo Negotiations: Re-visiting the Role of Mediation, Center for International Development and Conflict Management, University of Maryland, USA, 2008., p. 27.

2. Кастелс, М. Информационната епоха. – II том, „Силата на идентичността”. –София: ЛиК, 2006, с. 106.

3. Кастелс, М. Информационната епоха. – II том, „Силата на идентичността”. –София: ЛиК, 2006, с. 106-107.

ТЕРОРИЗЪМ И ИКОНОМИЧЕСКИ ДЕСТРУКТИВИЗЪМ

Младен Д. Тонев, Пламен Ц. Цонев

Варненски свободен университет „Черноризец Храбър”, Факултет „Международна икономика и администрация”,
катедра „Международна икономика и политика“ – гр. Варна, к.к. „Чайка”, Р. България

Национален военен университет „Васил Левски” – Факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи”, катедра „Информационна сигурност” – гр. Шумен, Р. България

TERRORISM AND ECONOMIC DESTRUCTION.

Mladen D. Tonev, Plamen Ts. Tsonev

ABSTRACT: *The report examines the destructive role of terrorism in terms of business processes in a country. It is proposed multiple typologisations of the economic destruction. In the first, introductory part of the exhibition is a brief overview of terrorism guidelines and scale of impact on the economic and political system of a country. In the second part of the study has presented economic destruction as a set of processes and phenomena in the economic nature that occur as a result of terrorist activities and attacks.*

KEY WORDS: *act of terrorism; security, economic destruction; terrorist network; international terrorism.*

Всеки терористичен акт е уникален и неповторим като характеристики, фактори, причини и условия, които го пораждат, поддържат и финализират, както и като последици и и деструктивни резултати. Това обаче, не е препятствие пред различните опити за класификация и типологизация на този тип актове, както и за изследване на деструктивните им последици в специализираната литература. Идеята на настоящото изложение е да прибави още една гледна точка, още една версия на този тип класификации и типологизации в пъстрата „мозайка” на исторически проявилите се, съществуващите в момента и потенциално възможните терористични актове (в това число и актовете на международен тероризъм) и деструктивните процеси, които те пораждат.

Тероризмът, като практика на унищожение на вражески и враждебни групи от хора (обикновено по-силни във военно отношение), в различните му форми и измерения съществува от дълбока древност. Това, което го отличава от другите практики на водене на война и на силово противопоставяне на множества от индивиди, привърженици на противоборстващи каузи, е обстоятелството, че при тероризма принципът „целта оправдава средствата“ е доведен до крайност. Става дума за това, че терористичните актове целят като правило „максимум жертви“, в това число (ако е необходимо или неизбежно) и жертва на собствения живот на атентатора-терорист.

Безспорен факт е, че актовете на тероризъм застрашават живота и здравето на невинни и неангажирани с политически, военни, религиозни и културни каузи мирни граждани.

По дефиниция тероризмът е "политически мотивирано престъпно насилие извършено срещу невоенни цели от субнационални групи или нелегални агенти"[46] Днес тероризмът еволюира, издигайки се на нови равнища и придобивайки планетарни мащаби до „международен тероризъм". Последният е по същността си „тероризъм, който засяга граждани или собственост на повече от една държава"[47] След 11.09.2001 г стана едва ли не традиция да се обвинява за международния тероризъм ислямският фундаментализъм. Нещо повече по линия на религиозното противопоставяне всички мюсюлмани започват да се възприемат от западните християнски общности като потенциални врагове. Това е много краен извод, но това не значи, че той не се споделя и от учени от световна величина. Например, тезата на Самюъл Хънтингтън за „сблъсъка на цивилизациите", според която сблъсъкът между западното християнство и исляма е неизбежен и с непредвидим край.

Има доста по-конкретни дефиниции на тероризма. Робърт Харви в книгата си „В капана на глобалния хаос" определя тероризма „като метод на извършване на атаки, които не са били предизвикани, срещу цивилно население, далеч от военни театри, като извършителите на са свързани с нито една политическа сила, обявила война на атакуваната страна"[48]. Тази дефиниция напълно пасва на терористите, чиито самолетни атаки довеждат до срутването на кулите-близнаци на Световния търговски център в Ню Йорк на 11.09.2001 г. Атаките са неочаквани, не са предизвикани от някаква военна намеса на САЩ, врязването на самолетите в кулите е далеч от каквито е да е театри на военни действия, жертвите са предимно от цивилното население и пожарникарите, мобилизирани в спасителните операции, извършителите са от Саудитска арабия – страна, която не само не е обявила война на САЩ, но е и стратегически съюзник на САЩ в района на Персийския залив. Самата терористична структура „ал Кайда", която се счита, че е стои зад този акт, е по-скоро виртуална политическа сила, отколкото реална групировка, общност или въобще субект, който не се свързва с конкретна страна, а е по-скоро мрежа от явни и скрити „клетки", които се активират в зависимост от конюнктурата.

Всеизвестно е, че почти всички терористи се самоопределят и се изживяват като борци за свобода, справедливост, национална или религиозна идея. Последната дефиниция на понятието „тероризъм", която дава Робърт Харви изключва възможността един терорист да се счита за борец за свобода и за социална справедливост. Няма такива политически мотиви, които да оправдаят смъртта дори на един човек, а още по-малко гибелта на над три хиляди души за време по-малко от 40 минути.

Това, че и до ден днешен понятието „тероризъм" не е добре определено и не улавя границата между „добро" и „зло" предполага при една по-широка трактовка към терористичните актове да отнесем както бомбардировката на Дрезден в края на ВСВ, така и бомбардировките на Токио, Хирошима и Нагасаки.

Съвременният тероризъм – издигнал се до нивото на „международен тероризъм" има една слаба страна в моралното основание за съществуването си – за раз-

---

ru/cw/1997/15/022.htm.

46 Гинев, Р. Цит. Съч. , с. 138.

46 Сирлз, Д., Д. Уайнбергер. Свет с окраин или что такое Интернет и как его ни с чем не путать.

- Руский журнал, март 2003, http://www.russ.ru/netcult/20030316.html.

лика от обикновения тероризъм, който неглижира както терористите, така и действията им, международния тероризъм ги „легитимира“ и ги прави „субекти“ както на международните отношения, така и на международното право с всички произтичащи от това права на демократична защита и съдебна справедливост. Подобна трактовка работи в полза на „международните“ терористи вместо да подпомага борбата с тях.

Според Румен Гюров „тероризмът е непростимо и безпощадно насилие, насилие, което не може да бъде простено от поразената жертва, насилие което не може да прости и затова иска да накаже безпощадно другия.“[49] В съвременни условия тероризмът все по често е резултат на структурно насилие. Една от догадките в посока към деструктивната роля на тероризма наблюдаваме в тезите на Джей Ан Тикнър. Последният приема, че преживяванията в субективен план при терористичните актове преминават отвъд физическото и включва непряко насилие върху лица в резултат от въздействие върху политически и икономически фактори и структури „които отнемат достъпа до основни материални блага и намаляват качеството и продължителността на живота.“[50] Друга теза, която също кореспондира с идеята за връзка между тероризма и икономическия деструктивизъм на индивидуално ниво и която отново има за източник Джей Ан Тикнър е, че „ в контекста на мотивационната теория може да се каже , че структурното насилие е възпрепятстване на себереализацията“.[51]

На едно равнище на масови представи съществува заблудата, че тероризмът няма като последици някакви сериозни деструктивни следствия, поради факта, че обикновено терористичните атаки са свързани с ограничено използване на оръжие, бойни и взривни вещества или с други някакви средства за физическо и психическо въздействие върху хората-жертви на терористични атаки. В действителност почти всеки акт нанася материални щети, а също така води до човешки жертви и до инвалидизиране на част от жертвите на терора. Взривяват се сгради (най-често места на съсредоточаване големи маси от хора) – атентатът в църквата „Св Неделя“ в София през 1924 г., атентата в берлинската дискотека, атентати в молове, търговски центрове, училища, театри и др. , атентата на летище Домодедово, в Москва, Руската федерация, атентатът в центъра на гр. Чешме, Република Турция, атентатът срещу търговския център „Арднал“ в Манчестър, Великобритания от страна на ИРА-извънаредни и мн.др. При всички тези атентати освен множеството жертви са нанесени и немалки стопански щети, включително и отказ от туристически и бизнес пътувания и отказ от потенциални инвестиции в местата обект на терористични атаки.

Другият тип обекти от материално естество, които често са жертва на терористични атаки са транспортните средства от сферата на масовия транспорт – атентатите в метрото в Мадрид, атентатите в Лондонското метро, атентатите в Московското метро, взривяването на автобуси (например в Израел, на летище Сарафово у нас, в Чечня и др.), взривяването на автомобили, самолети, кораби (взривяването на американския военен кораб в Аденския залив в Йемен). При всеки такъв теро-

---

[49] Кастелс, М. Информационната епоха. – II том, „Силата на идентичността”. –София: ЛиК, 2006, с. 106-107.

49 Fridl, Daniel

la D. , Kosovo Negotiations: Re-visiting the Role of Mediation, Center for International Development and Conflict Management, University of Maryland, USA, 200

8., p. 27.

ристичен акт има унищожени изцяло или частично транспортни средства, а нерядко и транспортна инфраструктура.

Много често обект на терористични атаки са стопански съоръжения – фабрики, заводи, пристанища, летища, логистични центрове и др. Те са желан обект на терористични атаки в случаите, когато се цели подкопаване на стопанските устои на една страна чрез терористична заплаха и терористичен натиск.

Нерядко цел на терористите са и инфраструктурни системи и съоръжения – газопроводи и петролопроводи – Чечня, Нигерия, Ирак, Сирия и др.; транспортни артерии – шосейни и ж.п. пътища, въжени линии, мостове, язовирни стени и др.

Най-съществения деструктивен аспект на тероризма е обаче унищожаването на човешкия живот. Човешките жертви не могат да се компенсират. Те трудно се поддават на някаква количествена оценка. Стопанските щети от материален характер могат да се компенсират или възстановят след време (например в Русия е възстановена по снимки и чертежи т.нар. „Кехлибарена стая“, унищожена от немските обсадни войски при обсадата на Ленинград по време на Втората световна война.) Човешкият живот е уникален и веднъж загубен не може да се „възстанови“. Именно в този смисъл деструктивизмът, породен от тероризъм е съотносим, съпоставим и идентичен като обхват с деструктивизмът породен от всеки един друг вид конфликти – войни, конфликти, гранични сблъсъци, агресии, диверсии, саботажи и др.

Деструктивизмът не е само и единствено следствие от катаклизми, бедствия, стихии, конфликти, военни сблъсъци и прочее колизии, обществени сривове и провали. Той има много проявления, различни форми, разностранни и специфични измерения, както и количествени и качествени характеристики. Историческите факти и събития ни дават голяма доза основание да говорим за множество аспекти на деструктивно развитие на човешката цивилизация. Още в епохата на европейското просвещение Жан Жак Русо прокламира девиза „Назад към природата”. В средата на XIX век вече съвсем отчетливо Кропоткин формулира своята идея за защита на природата като реакция на настъпващата индустриална революция в страните от Западна Европа.

Много племена и народи – американските индианци, австралийските аборигени, маорите в Нова Зеландия, както и множество малки племена и народи, населяващи някои от тихоокеанските острови не могат да приемат технологичния начин на живот, налаган им от европейските заселници в резултат на процеса на колонизация, характерен за предходните векове. Те се опитват да съхранят традиционния си природо-съобразен начин на живот, но това все по-трудно им се удава поради „цивилизационното” преобразяване на планетата от страна на развитите нации и държави.

Колкото и парадоксално да звучи, но именно относително по-бедните държави и общности от хора са тези, които настояват за мащабни промени, за бързо индустриално и технологично развитие с идеята, че така ще подобрят положението си. С тези си цели те усилват деструктивните процеси, включително и такива от стопанско естество – изсичането на горите, изтощаването и ерозията на почвите, пресъхването на изворите и реките, изчерпването на невъзстановимите запаси от суровини и енергоносители, унищожаването на обработваеми земи за индустриални и урбанистични цели и т.н.

В един екологичен план противоположна позиция на множеството бедни държави и човешки общности заемат относително по-богатите страни и по-заможните

статусни групи от хора. Имотните, богатите се опитват да ограничат мащабните и интензивни процеси на „преобразяване" на природата за утилитарни нужди – храна, отопление, битови потребности и доколкото могат да я съхранят.

Не е трудно да се представят акцентите на една **„технология" на деструктивното развитие:**

- развитието на съзидателната дейност при хората – появата и развитието на уседнали земеделски общества постепенно преобразява природата, за жалост не винаги в позитивен план. Днес на мястото, където според Джерълд Даймънд възниква човешката цивилизация преди около 10-11 хиляди години – района на т. нар. „Златен полумесец" – имаме главно пустини и полупустини и с изключение на Израел и отчасти Турция всички страни и населващите ги племена и народи са относително бедни и изостанали, независимо, че на територията на някои от тях са открити и се експлоатират значителни природни богатства – нефт, фосфати, руди и пр.;

- урбанизацията – появата и развитието, разпространението и нарастването на инфраструктурните и демографски мащаби на градските центрове, които днес се обитават от преобладаващия брой на населението в глобален план;

- акцентът върху развитието на технологиите, който поставят в стопанското си развитие, първоначално страни като Индия и Китай, а впоследствие и западните държави в Европа и Северна Америка;

- териториалната експанзия на хората, породена от демографския взрив като следствие на комплекс от социални иновации. Развитието на медицината и здравната помощ, създаването на болничната мрежа, масовизирането на образованието и повишаване на културата и хигиената на хората в много страни водят съответно до намаляването на детската смъртност, до повишаване на средната продължителност на живота и оттам до бърз демографски ръст. Нарасналата численост на населението е в основата на колониалната експанзия на европейските държави през XVIII и XIX век и постепенно води до проникване на капиталистическия начин на производство до всяко кътче на планетата. Преследването на изгоди и печалби е безогледно. Унищожават се множество животински и растителни видове и дори цели екосистеми в резултат на хищническата експлоатация на природните дадености и ресурси.

- краткият, нисък планов хоризонт на капитализма като предприемаческа и цивилизационна система. Масата от предприемачите нямат визия за дългосрочните последици от експлоатацията на природните ресурси. Нерядко за да компенсира щетите от разработването на дадено рудно находище на дадена човешка общност й се налага да инвестира огромни средства за рекултивация и утилизация, многократно превишаващи размера на капиталистическата печалба от експлоатацията на съответното находище. Същевременно компанията /фирмата/, нанесла щетите в резултат на експлоатацията на визираното находище е прекратила съществуването си и трудно може да бъде съдена за нанесените екопоражения. Дори и да заплати компенсации, те не могат да върнат чистотата на водите, унищожените биологични видове или да изчистят почвите и водоизточниците от тежки метали и вредни химикали – главно цианиди, нитрати и нитрити;

- гигантските транснационални и многонационални компании, които имат икономическа сила и мощ, многократно надвишаващи мощта и силата на отделни държави. Контролът на такива мезоикономически структури е труден и не винаги

достатъчно ефективен. Най-често такива структури изнасят екологически вредните и опасните за здравето на хората производства и технологии в икономически изостанали страни, възползвайки се от несъвършенствата в екологическото законодателство на тези страни. С тази си политика те определено подсилват деструктивните в екологичен и стопански аспект процеси във въпросните страни. Същевременно те акцентират върху конструктивните аспекти на международната си дейност – достъп до нови технологии за слаборазвитите държави, осигуряване на работни места, създаване на транспортна, комуникационна и производствена инфраструктура и т.н.

Тези няколко акцента в „технологията" на деструктивното развитие на човечеството са достатъчни да илюстрират аспектите и тенденциите на този негативен процес. Терористичните актове и инциденти определено подсилват тези акценти и форсират интензитета и мащабите на стопанския деструктивизъм.

Същност на стопанския деструктивизъм, предизвикан от терористични актове и инциденти.

Като икономически деструктивизъм в следствие от някакъв инцидент или сблъсък, диверсия, погранични сблъсъци, военен саботаж, терористичен акт и др. можем да определим всеки акт, който води до нарастване на икономическите разходи (до извънредни, допълнителни разходи на суровини, материали, енергия, финансови и трудови ресурси, за да може след въпросния терористичен инцидент или акт дадено национално или регионално стопанство да възстанови нормалния ритъм на икономически живот), както и до негативни промени в живота на жителите на дадена страна и дори до човешки жертви.

Ако трябва да акцентираме главно върху **икономическите аспекти** на деструктивизма, породен от локален, регионален или международен тероризъм, то те са следните:

- извънредни разходи за защита и сигурност на хората, обществените групи и обществото като цяло;
- материални и морални загуби в индивидуален и обществен план при терористични действия;
- преки разрушения на материални обекти – жилищна, индустриална, транспортна, комуникационна, здравна и образователна инфраструктури при много от терористичните актове;
- рязко свиване на външнотърговския обмен, поради полицейски и военни блокади в борбата с тероризма, както и пряка терористична заплаха за традиционните търговски пътища и канали (типични са действията на сомалийските пирати, които нападат кораби движещи се по установените морски пътища);
- драстични промени и обрати в съдбата на отделни индивиди за голяма част от населението на дадена страна – жертви, невинно пострадали, преки свидетели и пр. при много от терористичните актове;
- значителни загуби на хора като загинали, ранени, осакатени и психически травмирани. Дори един неуспешен атентат като този на летище Сарафово, Бургас довежда до 6 жертви, плюс няколко тежко ранени и инвалидизирани за цял живот хора;

- като цяло терористичните актове имат слабо отражение върху тенденцията към спадане на средната продължителност на човешкия живот, така или иначе имат своя принос и в тази посока;

- деморализация и криминализация на част от населението, поради разстройването на контролните и защитни функции на държавните институции в борбата с тероризма;

- негативно въздействие върху природата (замърсяване на въздуха, водите, почвите, унищожаване на биологичното богатство на планетата) в случаите на екотероризъм, а нерядко и при ординарния тероризъм.

Видове икономически деструктивизъм, породен от локален, регионален и международен тероризъм.

В специализираната литература има сравнително малко информация по тези въроси. В публикации от 70-80 години на XX век се разглеждат проблеми, главно и единствено, на коалиционната война в контекста на тогавашното противопоставяне между двата големи военни блока – Североатлантическия пакт НАТО и Варшавския договор. Повечето оценки и очаквания са една потенциална война между двете големи военни коалиции да се води с различни оръжия, но предимно с такива за масово унищожение – ядрено, химическо, биологично и бактериологично, като в този арсенал присъстват и терористичните актове, диверсиите и саботажът. В този план са представени и деструктивните процеси. Оценката е, че те в преобладаваща степен ще се дължат на конвенционалните форми на военен сблъсък и в минимална степен ще се обуславят от терористични прояви. Дори от гледна точка дали поразяват материалните средства или живата сила на противника оръжията се подразделят на хуманни и нехуманни. Например, ядрените ракети с неутронен заряд се характеризират като нехуманни, доколкото унищожават живата сила на противника с висока доза първична и остатъчна радиация, почти без да засягат материалната база и инфраструктурата.

В съвременни условия на преден план в контекста на силов сблъсък между западната цивилизация и регресивните структури излиза борбата с тероризма. Начина на разразяване, протичане на терористичните сблъсъци и инциденти днес е коренно различен от ситуацията на междукоалиционна ядрена война. В такъв един аспект има множество „бели полета" в изследванията и публикациите с подобна насоченост.

В този смисъл тук ще представим нашата авторска визия за деструктивните промени от стопанско естество в резултат на разгръщането на борбата с международния тероризъм. Презентацията на въпросната визия е един от възможните варианти на ранжиране и групиране на деструктивните промени в принципен план. Логично е тя да бъде изложена като набор от типологизации в зависимост от един по-пълен набор от критерии, фактори, обстоятелства и оценки.

Ето един възможен набор от типологизации на деструктивните изменения в резултат на зараждането, разразяването и колуминацията на различни по мащаби и обхват терористични действия:

Според **равнището на проявление** можем да диференцираме стопанския деструктивизъм като:

а/ ***деструктивизъм на индивидуално ниво***, който се проявява като:

- загуба на лично и домашно имущество и нерядко, повреда и разрушаване на жилища и стопански постройки в резултат на обстрел, бомбени и терористични атентати и др.;

- загуба на източници на доходи, в резултат на унищожени средства за производство, транспортни средства, инфраструктура и пр. при подобни актове;

- структурна безработица, вследствие на структурни промени в стопанството, наложени от мащабни терористични актове. Например в Ирак след последната война в Залива, която се води под мотото за борба с международния тероризъм, рязко нараства безработицата в резултат на раздържавяването на множество стопански предприятия и драстичните съкращения, с които е съпроводена тази приватизация и резкия преход към пазарно стопанство;

- промяна на социалния статус. Нерядко инцидентите с терористичен характер водят до разоряване на хора, преживявали с някакъв дребен бизнес. От уважавани и почтени стопани и занаятчии те стават бедняци, парии заради невъзможността да възстановят бизнеса си. Такива ситуации има немалко в Палестина, в резултат на миналите арабско-израелски войни, както и в Ирак след окупацията на страната от САЩ и съюзниците им;

- легална и нелегална емиграция в индивидуален план. Почти всеки помащабен терористичен акт, както и междуетническите напрежения и противопоставяния, пораждат вълни от бежанци и емигранти, включително и такива, които могат да се определят като „вътрешни емигранти";

Компенсаторните действия от страна на потърпевшите от деструктивните промени в стопанството субекти могат да се разграничат на априорни /предситуационни/ и апостериорни /постситуационни/. Превантивно е добре хората да застраховат имуществото си и да акумулират спестявания. Не случайно старите хора казват „Бели пари за черни дни". Историческия опит показва, че финансовите акумулации в предконфликтните и предситуационни периоди дават възможност по-леко да се понесат деструктивните процеси и резултати при разразяването на даден сблъсък като момент от борбата на демократичните държави с международния тероризъм.

Постситуационните компенсаторни действия са по-разнообразни. Най-често срещаното действие е адаптацията към ситуацията на увреждане и разстройване на стопанството. Тя обаче означава на практика драстично влошаване на качеството на живот на гражданите, преживяли терористичен инцидент. Друго компенсаторно средство е спазването на традициите, които осигуряват приемственост в историческия опит на всеки народ, в това число и опит по справяне с посттерористични деструктивни състояния на личното и обществено стопанство. Най-често това са исторически доказали се добри семейни и обществени практики, изразяващи се в мобилизация на социалния капитал на дадена етническа, национална или племенна общност – сдружаване за прагматични цели, колективизъм, взаимопомощ, благотворителност и пр.

б/ ***деструктивизъм на групово ниво*** – този аспект на деструктивизма се проявява като:

- смяна на местообитаване и местоживеене на големи групи от хора – бежанци, емигранти. Балканската, Междусъюзническата и Първата световна войни стават причина за изселването на хиляди български домакинства от Одринска Тракия и Вардарска Македония в пределите на Царство България. В такъв един контекст

тази форма на деструктивизъм по-слабо кореспондира с проблемите породени от борбата с международния тероризъм;

- геноцид – за жалост, често срещано явление в проявите на международен тероризъм. Типични в това отношение са Холокоста, клането между хуту и тутси в Руанда и Бурунди в началото на 90-те години на XX век и редица други междуетнически сблъсъци в миналото. В новата военна лексика като по-приемлива и не толкова стресираща се налага конструкцията „етническо прочистване", което е просто евфемизъм на понятието „геноцид";

- в много случаи при някои от актовете на международен тероризъм са налице практики на изолация, ограничаване на гражданските права и свободи, ограничаване свободата на придвижване за цели етноси, нации, религиозни общности и др.;

- нерядко тероризмът и опитите за ограничаването му водят до затягане на режима, до свръх-регулации, до централизация на стопанството, до реквизиции на стоки, суровини, енергоизточници. Нерядко такива крути мерки, които лишават някои обществени групи от препитание и условия на живот предизвикват реакции като протести, стачки, влошават като цяло кримогенната обстановка в дадена държава, въвлечена в международен конфликт.

в/ ***деструктивизъм на ниво социум*** – той от своя страна намира изражение в следните процеси и явления:

- разрушаване на ценностната система на преобладаващата част от населението на дадена страна, въвлечена в борбата с тероризма, или напрежение, генерирано по политически, религиозен или дипломатически път. Чувството на несигурност, на незащитеност, на безпомощност у масата от хората, в страна, където има конфликтна обстановка от някакъв характер, ги деморализира и демотивира по отношение на множество градивни действия и процеси;

- загуба на социален капитал поради разкъсване на родовите и землячески връзки, при мащабните разместванията на хора и дори на цели народи, наложени от някакви военни, терористични и въобще конфликтни действия. Показателно в такъв аспект е изселването на немците от Поволжието във Ферганската долина в Узбекистан при настъплението на 6-та германска армия под командването на генерал-фелдмаршал Паулус към Сталинград през Втората световна война;

- загуба на политически рейтинг и още повече на кредитен и инвестиционен рейтинг. Когато опасността за дадена страна да бъде въвлечена в борбата с международния тероризъм нарасне, това води до бягство на капитали и до отказ и стопиране на различни инвестиционни проекти. Кредитните институции изискват посигурни гаранции, за да отпускат кредити на подобни застрашени от тероризъм държави. Още по-малко се „котират" държавите, които се определят от САЩ, Съвета за сигурност при ООН и други международни институции като „терористични държави";

- нарастване на престъпността и влошаване на кримогенната обстановка съпътстват всяко едно терористично нападение, особено ако то е относително попродължително;

- увеличените разходи за въоръжение и отбрана и за обществена защита, също се отразяват негативно в обществен план. Тези нараснали разходи означават, че съответната страна мобилизира средства и ресурси не за съзидание и изграждане на по-добри условия за бизнес и живот, за по-добра инфраструктура, а за разруше-

ние, противодействие на тероризма и за сдържане и защита от последния. Разходите за въоръжение и въобще за борба с тероризма са за сметка на данъкоплатците и те означават по малко средства за здравеопазване, за социални нужди, за образование, за подрастващите и за възрастните и болни хора.

Според **резултатите** от даден акт на тероризъм деструктивните процеси от стопански характер биват следните:

а/ процеси, форсиращи нарастването на разходите в личен, групов и обществен план, като извънредни разходи, породени от обстоятелството, че повечето терористични актове ако и да не са свързани с унищожение на хора, материални ценности, исторически паметници, инфраструктура, екосистеми и пр. най-малкото предизвикват затруднения от инвестиционен, търговски, кредитен, управленски и пр. характер;

б/ процеси, водещи до разрушения и унищожаване на материални ценности. Това са типични последствия за военни стълкновения, терористични актове, разпад на държавността в някой от случаите на международни конфликти. Понякога небрежност, нихилизъм и деморализация при част от хората в резултат на тези конфликти стават причина за разрушения и материални загуби от различен характер;

в/ процеси, водещи до териториални загуби. Те са чест резултат от загуба на военни кампании, сепаратистки процеси, процеси на разпад на държавността. Обикновено такива действия са следствие от някаква форма на международен тероризъм пораждащ сепаратистки процеси и откъсване на територии – Косово, Южна Осетия, Приднестровието, Абхазия, Източен Тимур, Еритрея и др. При този тип терористични действия има дуалистична трактовка на ситуацията. От страна на терористите и групите, които ерозират държавността и утвърдените по някакви договори граници техните действия се оценяват като борба за национална, религиозна или етническа свобода. От страна на поддържниците на статуквото, действията на „борците за свобода“ се приемат и интерпретират като акт на международен или междуетнически тероризъм;

г/ процеси, водещи до преки икономически загуби – унищожение на предприятия, ферми, племенни животни, култивирани растителни видове. Просто това е аспект на конкретизация на деструктивните процеси, свързани с унищожението на материални ценности. Обикновено се приема, че при терористичните актове пораженията няма как да са толкова мащабни, но практиката нерядко показва точно обратното. Само цената на кулите близнаци на Световния търговски без обзавеждането и съпътстващите системи е 500 млн. долара по първоначален проект;

д/ процеси, нанасящи поражения на природата. Не само оръжията за масово унищожение, но и голяма част от конвенционалните бойни средства, както при военното им използване, така и при конверсията и утилизацията им нанасят сериозни щети на околната среда, както и здравето на хората. При един от актовете на международен тероризъм – окупацията на Кувейт от страна на иракската армия на диктатора Саддам Хюсеин – запалването на десетки петролни кладенци предизвиква мащабна екокатастрофа в района на Персийския залив;

е/ процеси, водещи до промени в климата. Те са по-скоро резултат от индустриалните методи на производство – повишаване на средногодишните температури /глобално затопляне/, разширяване на озоновата „дупка”, изтъняване на озоновия слой, ефекта „Ел Ниньо”, бързото топене на полярните ледени шапки и пр. В една голяма степен индустриалните производства са пряко и косвено свързани с произ-

водства, осигуряващи националната и регионална сигурност, в това число и борбата с регионалния и международен тероризъм. В такъв смисъл противодействието на тероризма може да има и такъв тип деструктивни последици;

ж/ поражения върху живота и здравето на хората. Тези поражения не се нуждаят от коментар, особено що се отнася до разразяването и ескалацията на терористичните конфликти.

Според **инициаторите и подбудителите** икономическият деструктивизъм може да бъде следствие от следните ситуации и обстоятелства в системата на терористичните актове и въздействия:

а/ небрежност и атипично поведение на индивиди и групи от индивиди при борбата с тероризма:

- неуместно спазване на традиции в чужда културологична среда;
- предизвикване на форсмажорни обстоятелства чрез диверсия, саботаж или небрежност – пожари, наводнения, взривяване на обекти и др.;
- нехайство по отношение на опазване на природата и човешкия живот от страна на чужди граждани, което води до дипломатически усложнения и конфликти /типичен случай имаме с обвинението на българските медицински сестри и д-р Здравков в Либийската джамахирия/;
- хулигански прояви и посегателство върху живота на хора от страна на групи чуждестранни граждани /типични в това отношение са изявите на английските запалянковци в чужбина и произтичащите от това усложнения – случаят Майкъл Шийлдс и обвиненията към българското правосъдие от страна на британската правораздавателна система;

б/ небрежност и некомпетентност от страна на управленските елити и структури на отделни страни:

- поведението на либийският ръководител – полк. Муамар Кадафи често става повод за нагнетяване на напрежението между Либия и други страни, както от Западна Европа и Северна Америка, така и със страни от самия африкански континент. Либийската джамахирия при управлението на полк. Муамар Кадафи нерядко е обвинявана като страна, която поддържа международния тероризъм;
- липсата на държавност в страни като Сомалия, Судан, Конго и др. в резултат, на което се развихрят престъпност и анархия с всички произтичащи от това негативи и заплаха за живота на гражданите на тези страни и на чужденците, които по една или друга причина са принудени да ги посещават и да пребивават на тяхна територия;

в/ насилствени международно-правни действия – война, окупация, аншлус, диверсия на една държава срещу друга или срещу други държави.

Според **субектите, инициращи и генериращи деструктивни действия** могат да се диференцират няколко нива на индивидуалности и общности:

- отделни индивиди, които действат по самоинициатива;
- индивиди в качеството им на представители на управленските и политически елити;
- сепаратистки партии и движения – тук примерите са многобройни като се започне със сапатистите в Мексико и се свърши с партизанската групировка Абу Саяф във Филипините;
- терористични групи и организации – групировката Хамас, мрежата „Ал Кайда" и мн. др.;

Предложеният вариант на типологизация и класификация на деструктивните явления в резултат на международен и междуетнически тероризъм няма претенции за изчерпателност и на практика е отворена система, която предполага доразвитие и дообогатяване. Ценността му е в това че дава възможност за един относително пълен анализ на деструктивните процеси, предизвикани от даден терористичен акт.

Разглежданите в доклада релации „тероризъм – икономически деструктивизъм“ може да се използват като методическа система за анализ и изследване на различните терористични актове и последиците от тях в стопанско и социално отношение. Това е разбира се само един препоръчителен вариант на анализ на конфликтни ситуации проявяващи се като терористични реакции и на пораженията, които те нанасят в стопански план, без претенции за универсална валидност, поради комплексността и многообразието на процесите на терористични въздействия и натиск спрямо общности и групи от хора, и дори спрямо цели държави в системата на международните отношения.

Литература:

1. Perl Raphael Terrorism and National Security: Issues and Trends. Washington: CRS, 2006, p. 8 PDF, http// fpc.state.gov, 20.04.2010.

2. Пак там, p. 7

3. Харви, Р. В капана на глобалния хаос. –София: ИК „Анимар“, с. 28.

4. Гюров, Р. Към анализа на сигурността. – София: Фондация „Национална и международна сигурност“, 2011, с. 104.

5. Цитирано по Sachs, Stephen The Changing Definition of Security. – Oxford 2003. HTML, www.stevesachs.com 22.12.2009.

6. Пак там.

ИНФОРМАЦИОННА СИГУРНОСТ

КРИПТОГРАФИЯ И СТЕГАНОГРАФИЯ В УЧЕБНОМ ПРОЦЕССЕ

Александр П. Алексеев, Максим И. Макаров, Владимир В. Орлов

apa2008@rambler.ru,moox700@gmail.com, crypter@mail.ru

CRYPTOGRAPHY AND STEGANOGRAPHY IN THE LEARNING PROCESS

Aleksandr P. Alekseev, Maxim I. Makarov , Vladimir V. Orlov

ABSTRACT: *The report deals withs the requirements for textbooks on cryptography and steganography for students and principles of modern security systems. The idea of time-space spreading of hidden information is underlined.*

KEYWORDS*: cryptography, steganography, containers, space-time spraying.*

Число публикаций, посвящённых криптографии и стеганографии, растёт экспоненциально. По криптографии издано большое число учебников, задачников, пособий для проведения лабораторных работ и практических занятий [1, 2, 12, 13], а также проводятся онлайн курсы [10, 11]. Применительно к стеганографии заметен дефицит учебной литературы, содержащей описание лабораторных работ и практических задач. Компенсировать это пробел пытаются преподаватели и учёные в различных высших учебных заведениях, в том числе России и Болгарии. В России такими работами являются [3, 4, 5], а в Болгарии - книги, написанные профессором С. Станевым и его учениками [6, 14, 15].

Авторы этой статьи придерживаются мнения, что современная учебная литература по защите информации должна строиться на основе комплексного многоуровневого подхода. Это означает, в частности, что методы стеганографии невозможно рассматривать изолированно от криптографии. В свою очередь, рассмотрение только лишь криптографических алгоритмов защиты данных не раскрывает для студентов всей полноты современных методов обеспечения информационной безопасности. Несмотря на то, что исторически стеганография появилась раньше, чем криптография, изложение материала в учебных пособиях целесообразно начинать именно с методов криптозащиты, поскольку теория криптографии разработана значительно глубже по сравнению со стеганографией.

Теоретическая часть учебного пособия должна содержать описание используемого математического аппарата. На наш взгляд, наибольшее внимание следует уделить модульной арифметике, булевой алгебре, математической статистике, теории вероятностей, спектральным преобразованиям (Фурье, DCT) и теории искусственных нейронных сетей. Особое внимание нужно уделить Китайской теореме об остатках, теореме Байеса и алгоритму Евклида.

При изложении криптографических методов должны быть описаны методы замены, перестановок, гаммирования, алгоритмы шифрования с помощью открытых ключей. Здесь же целесообразно описать алгоритм цифровой подписи, хэш-функции и протоколы обмена ключами.

Специалистам по защите информации приходится использовать случайные числа. Например, для псевдослучайного выбора адреса стеганографического внедрения или генерирования криптографического ключа. По этой причине в учебном пособии необходимо дать представление о достоинствах и недостатках различных алгоритмов формирования псевдослучайных чисел.

Так как нередко сокрытие данных происходит в мультимедийных контейнерах, то в теоретических разделах учебных пособий безусловно должны быть рассмотрены форматы контейнеров: графических, звуковых, текстовых, архивных, видео, Web-приложений. Скрывать передаваемые данные можно в любом электронном контейнере, обладающим избыточностью. Важно, чтобы студенты изучали материал по первоисточникам. Для этого в учебном пособии должны быть соответствующие литературные ссылки (на патенты, стандарты и технические спецификации). Студенты должны научиться количественно оценивать и сопоставлять различные стеганографические и криптографические методы защиты информации.

Учебные пособия должны содержать материал, который многократно используется во многих алгоритмах защиты данных. Например, использование наименее значащих бит контейнера для сокрытия информации (метод LSB). В то же время студенты должны понимать, что рассматриваемые классические методы защиты информации не являются догмой и порой возможна их существенная модернизация. Так внедрять информацию в звуковой файл формата WAV можно не только в младшие разряды цифровых отсчётов, но и в старшие разряды [7].

По нашему мнению, учебная литература должна содержать большое число примеров, которые позволят обучаемым понять идею метода защиты. Должны быть приведены программы, с помощью которых можно исследовать нюансы алгоритмов сокрытия информации. Для иллюстрации рассматриваемых идей можно использовать любой язык программирования или популярные математические системы. Предпочтение можно отдать языкам программирования C#, JavaScript, Java, Python и математическим системам Mathcad и MATLAB.

Не менее важным является развитие практических навыков. На лабораторных работах студенты должны познакомиться с современными достижениями криптографии и стеганографии (с опубликованными программами для сокрытия данных в мультимедийных файлах, например, S-Tools). Работа с подобными программами позволяет обучаемым наглядно увидеть результаты сокрытия данных, невозможность органолептически (визуально или на слух) выявить секретное вложение. Очевидно, что обучаемые должны познакомиться с программами стеганоанализа (например, Stegdetect, Stego Suite, StirMark, Wireshark). Необходимо довести до сознания обучаемых, что возможна скрытая передача не только текста, но и произвольных данных (изображений, звуков).

Наилучший способ освоения стеганографии – это выполнение лабораторных, курсовых работ, дипломных проектов и решение практических задач по извлечению скрытой в контейнерах информации. В этом случае необходимо познакомиться с редакторами памяти и сетевыми анализаторами.

Объёмные задачи по извлечению данных из электронных контейнеров вырабатывают у студентов пунктуальность и понимание того, что ошибка в одном бите часто приводит к катастрофическим последствиям. Сложные задачи приучают к длительному, напряжённому, кропотливому труду, вырабатывают профессиональные навыки, необходимые будущим аналитикам. Сложные задачи создают убеждённость в необходимости обязательного использования вычислительной техники, зачастую подталкивают к самостоятельному нахождению оригинальных способов решения задач.

Понятно, что наибольшее совершенствование своих навыков профессионалы могут получить, упражняясь в решении нестандартных задач стеганоанализа. В частности, для эффективного изучения стеганоанализа необходима тренировка в применении уже известных статистических распределений в мультимедийных файлах, так и практика по формированию математических моделей контейнеров.

Каждая книга пишется с учётом индивидуальных пристрастий авторов, она должна содержать оригинальные идеи, разработанные авторами. Тогда материал, полученный из первоисточника, представляет для обучаемых наибольший интерес.

Авторы длительное время разрабатывают идею пространственно-временного распределения скрываемой информации. Предлагается использовать метод скрытого распределения информации по множеству каналов телекоммуникационной сети, что позволяет использовать идеи множества различных алгоритмов защиты информации. Следуя принципу многоуровневой защиты, распределяемая информация шифруется, стеганографически скрывается в контейнерах различной природы, применяется алгоритмический барьер в виде полного сцепления блоков защищаемых данных. Кроме того, информация распыляется не только в пространстве, но и во времени. Рассмотрим данный метод подробнее.

Корреспонденты связаны телекоммуникационной сетью. В их распоряжении имеется множество каналов связи. В текущем сеансе связи используются не все доступные каналы, а только их часть. Остальные каналы имитируют активность (передают служебную информацию, шум, дезинформацию). Камуфлирующие сообщения передаются по всем каналам. По каналам связи передаются стеганоконтейнеры. Такие каналы можно создать, например, с помощью протокола HTTP, FTP, электронной почты, ICQ, социальных сетей, интернет-радиостанций, интернет TV и т.д. Для связи могут быть использованы локальные и глобальные сети. Сообщения целесообразно передавать не напрямую абоненту, а через промежуточные узлы и меняя на них протоколы.

Корреспонденты обмениваются ключевой информацией и выбирают шифры *A* и *B*. Отправитель разбивает защищаемую информацию на блоки, зашифровывает их шифром *A* в режиме сцепления блоков. Затем полученная криптограмма разбивается на блоки большей длины и подвергается шифрованию по алгоритму *B*. Таким образом, получается криптограмма, каждый блок которой содержит несколько блоков криптограммы шифра *A*. Блоки криптограммы шифра *B* скрытно нумеруют и внедряют в них фрагменты ключа шифра *A*. С помощью стеганографического ключа определяют тип контейнера, параметры сокрытия и осуществляют внедрение битов криптограммы шифра *B*. Сформированные стего в соответствии со схемой организации и расписанием связи, определяемыми ключом распределения, передаются получателю.

На приёмной стороне получатель накапливает поступающие контейнеры и в соответствии с ключом распределения извлекает информацию, применяя стеганографический ключ. Извлечённая криптограмма шифра *B* расшифровывается, при этом из её блоков извлекаются фрагменты ключа шифра *A*. Наконец, расшифровав криптограмму шифра *A* с помощью составленного ключа, получают секретные данные.

Достоинством многоуровневой защиты является возросшая сложность дешифрования криптограммы в случае отсутствия у криптоаналитика хотя бы одного блока криптограммы. Это происходит из-за необходимости многократного увеличения мощности вычислительных средств криптоаналитика. В данном методе, если злоумышленник не смог перехватить блок криптограммы минимальной величины, то трудоёмкость его вычислений увеличится в 264 раза [8].

Ещё одна область интересов авторов – это сетевая стеганография. При рассмотрении этого направления защиты информации следует описывать не только привычные способы размещения бит секретной информации в специфичных для протокола полях заголовка, но и более современные способы защиты. Важным требованием является сокрытие данных при помощи ключа, определяющего позиции и порядок размещения бит секретной информации в контейнере. Одним из таких методов сетевой стеганографии является сокрытие информации в значении длины сетевого пакета.

Алгоритм сокрытия данных заключается в следующем. Для обмена информацией абоненты выбирают симметричный ключ (одинаковый для сокрытия и извлечения). Отправитель вырабатывает на основании ключа двоичную криптографическую гамму. Используя двоичную гамму в качестве маски, отправитель располагает биты секретной информации в тех позициях (разрядах) значений длины сетевых пакетов, в которых биты маски равны единице, а на прочих местах, которым соответствуют нулевые биты маски, размещает случайные биты. Таким образом, формируется последовательность длин сетевых пакетов (точнее, длин данных, передаваемых в сетевых пакетах). Далее отправитель выбирает камуфлирующий текст, не несущий секретной информации, и посылает его в сеть пакетами в соответствии со сгенерированными длинами, включающими в себя биты секретной информации. В итоге в заголовках сетевых пакетов всех уровней отсутствуют сами биты секретной информации, однако, опосредованно через фактическое значение длины камуфлирующих данных скрытно осуществляется передача секретных данных.

На приёме получатель действует симметрично: он накапливает камуфлирующий текст, поступающий из сети, одновременно запоминая длины пакетов. Формирует на основании ключа двоичную криптографическую гамму. Используя гамму в качестве маски, накладывает её на значения длины поступивших сетевых пакетов и из позиций, соответствующих единичным битам гаммы, извлекает секретную информацию.

Такой алгоритм может серьёзно повлиять на эффективность использования канального ресурса и стать демаскирующим признаком для скрытого канала связи. Поэтому, договорившись заранее, абоненты могут принять несколько старших разрядов двоичного значения длины равными единице. Это решение позволяет передавать камуфлирующие данные на большей скорости, эффективнее используя канальный ресурс и снизить вероятность обнаружения скрытого канала связи.

Важным требованием описанного алгоритма сокрытия данных является поддержание необходимой последовательности поступления пакетов на приёмную сторону. При передаче пакетов по протоколу UDP может возникнуть ситуация, когда требующийся порядок поступления пакетов будет нарушен, что приведёт к неверному извлечению скрытой информации. Для исключения этого недостатка отправитель и получатель должны разработать алгоритм восстановления последовательности пакетов, либо применить протокол передачи, поддерживающий её изначально, например, TCP. Сложности технического характера могут возникнуть и при использовании протокола TCP, так как он предназначен для передачи потока информации без сохранения границ, то есть длин отдельных пакетов. Для решения этой проблемы может потребоваться собственная низкоуровневая реализация протокола TCP, работающая в обход средств операционной системы. Эти особенности позволяют сформулировать задачи для их проработки в рамках смежных дисциплин [9].

Сформированное таким образом учебное пособие позволяет получить теоретические сведения и практические навыки применения современных методов защиты информации. Погружение в методы криптографического и стеганографического анализа даёт наглядное представление о сложности задач защиты информации, стимулирует итерационное развитие методов защиты данных.

ЛИТЕРАТУРА

1. Осипян В.О., Осипян К.В. Криптография в задачах и упражнениях. – М.: Гелиос АРВ, 2004. – 144 с.
2. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. – СПб: БХВ-Петербург, 2007. 304 с.
3. Алексеев А.П., Орлов В.В. Стеганографические и криптографические методы защиты информации: учебное пособие. - Самара: ИУНЛ ПГУТИ, 2010. – 330 с.
4. Алексеев А.П. Информатика для криптоаналитиков: учебное пособие/ Алексеев А.П. – Самара: ИУНЛ ПГУТИ, 2015. – 376 с.
5. Алексеев А.П. Информатика 2015. - М.: СОЛОН-Пресс, 2015. – 400 с.
6. Станев С. С. Стеганологична защита на информацията. Университетско издателство „Епископ Константин Преславски”. Шумен, 2013. – 320 с. ISBN 978-954-577-825-4.
7. Аленини А.А., Алексеев А.П. Помехоустойчивое стеганографическое внедрение информации в звуковые файлы//Вопросы защиты информации, №1, 2013. Стр. 15 – 19.
8. Макаров М. И. Разработка и исследование методов скрытой распределённой передачи сеансовых данных в телекоммуникационных сетях: дис. … канд. техн. наук. ПГУТИ, Самара, 2013.
9. Орлов В. В. Методы скрытой передачи информации в телекоммуникационных сетях: дис. … канд. техн. наук. ПГУТИ, Самара, 2011.
10. URL: https://www.coursera.org/course/crypto
11. URL: https://www.udacity.com/course/cs387
12. Paar. C., Pelzl, J. Understanding Cryptography – Springer, 2010 - 372c.

13. Junod, P. A Classical Introduction to Cryptography Exercise Book - Springer Science & Business Media, 2005 – 254 с.

14. Станев,С., С. Железов, Х.Параскевов. Обучението по компютърна стеганография в Шуменския университет „Епископ Константин Преславски”. В: Наука, образование, сигурност. София: Издателство на НБУ, 2013. стр.445-451. ISBN:978-954-535-796-1.

15. Станев,С., С. Железов. Первые результаты внедрения курса „Компютерная стеганография” в Шуменском университете. В: Трудове на международната научно-практическа конференция на ВДПУ „Коцюбински”, Виница, Украйна, 2012, стр. 205-207.

ПРОБЛЕМИ НА СИГУРНОСТТА В МОБИЛНИТЕ САМООРГАНИЗИРАЩИ СЕ МРЕЖИ

Григор Р. Велев

ИНСТИТУТ ПО ОТБРАНА “ПРОФ. ЦВ. ЛАЗАРОВ” – МИНИСТЕРСТВО НА ОТБРАНАТА СОФИЯ, 1592, БУЛ. „ПРОФЕСОР ЦВЕТАН ЛАЗАРОВ” № 2

SECURITY ISSUES IN MOBILE AD HOC NETWORKS

Grigor R. Velev

DEFENCE INSTITUTE “PROFESSOR CVETAN LAZAROV” – MINISTRY OF DEFENCE, SOFIA, 1592, BLVD. “PROFESSOR CVETAN LAZAROV” 2

***ABSTRACT**: Mobile ad hoc network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. The provision of security services in the MANET is related to a set of challenges specific to this new technology. In this report security issues, vulnerable nature of the mobile ad hoc network and the main attack types that exist in it are discussed.*

***KEY WORDS:** MANET, Information security, Vulnerability of MANETs*

1. ВЪВЕДЕНИЕ

Навлизането на безжичните мобилни устройства в съвременния живот и непрекъснатото им усъвършенстване, налагат задълбочаване на изследванията и търсене на нови решения за сигурни комуникации в мобилните самоорганизиращи се мрежи (Mobile Ad hoc NETworks – MANETs). Един от основните проблеми, свързани с използването на MANETs за оказване на помощ при бедствия, при извънредни ситуации и за военни цели е осигуряване на сигурността им.

MANET е система от мобилни безжични устройства, които динамично се самоорганизират във временна и случайна мрежова топология. Динамичната структура на MANETs позволява да се използват мрежови услуги в области, в които няма предварително изградена комуникационна инфраструктура. Мобилни самоорганизиращи се мрежи, могат да се използват по време на кризи, спасителни операции, военни действия. Отличителна тяхна характеристика е функционалната еквивалентност на устройствата, които формират мрежата. Честата промяна на мрежовата топология, предполага адекватни механизми за управление на маршрутизацията и същевременно малка консумация на енергийна мощност, изчислителни ресурси и комуникационен трафик. Специфичните свойства на самоорганизиращите се мрежи изискват прилагане на подходящи механизми и подходи за осигуряване на защитени комуникации и цялостност на данните.

Мобилните самоорганизиращи се мрежи са автономна съвкупност от устройства, които са в състояние самостоятелно да се организират в безжични мрежи. Позицията на устройствата не е предварително детерминирана. Това дава възможност за произволното им разполагане в труднодостъпни местности или за наблюдение при опасни операции. Мрежата е децентрализирана и доставянето на съобщенията трябва да бъде извършвано от самите устройства, т. е. маршрутизиращата функционалност се извършва от самите устройства. Следователно мобилните самоорганизиращи се мрежи се характеризират с 2:

- липса на предварително изградена инфраструктура;
- радиокомуникации – съвместно използвана комуникационна среда;
- всяко крайно устройство (възел) от мрежата е и маршрутизатор;
- мобилност – динамична топология;
- автономност на крайните устройства;
- ограничена енергийна мощност и изчислителни ресурси.

2. АСПЕКТИ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В МОБИЛНИТЕ САМООРГАНИЗИРАЩИ СЕ МРЕЖИ

Подобно на кабелните мрежи, сигурността на MANETs е свързана с осигуряване на защита на информацията и ресурсите от атаки. Сигурността на мобилните самоорганизиращи се мрежи, трябва да се разглежда в контекста на основните аспекти на информационната сигурност:

- Наличност (Availability)

Осигурява достъпност на заявените мрежови услуги, т.е. винаги, когато е необходимо, независимо от наличието на атаки. За да се постигне висока наличност трябва да се неутрализират DoS атаките, атаките, свързани с изчерпване на енергията, както и поведението на компрометираните възли.

- Автентификация (Authentication)

Осигурява автентична комуникация на един възел с друг възел в мрежата, с други думи, компрометиран възел не може да се представи като сигурен възел от мрежата.

- Конфиденциалност (Data confidentiality)

Осигурява тайната на изпращаните съобщения, т.е. едно съобщение не може да бъде разбрано от възел, различен от този, за който е предназначено. Обикновено се прилага симетричен или асиметричен криптографски алгоритъм, за да се постигне конфиденциалност (тайна) на данните.

- Цялостност (Integrity)

Осигурява интегритета (целостта) на съобщението, изпратено от един възел до друг възел, т. е. не е възможно модифициране на съобщението от някой компрометиран възел по време на предаването. Ако се използва сигурен механизъм за запазване на тайната, осигуряването на целостта може да постигне просто чрез добавяне на хеш-стойност, преди криптиране на съобщението.

- Невъзможност за отказ от авторство (Non-repudiation)

Осигурява невъзможност даден възел да откаже авторство на съобщение, което е изпратил. Цифровият подпис може да бъде приложен за осигуряване на този аспект.

3. УЯЗВИМОСТИ НА МОБИЛНИТЕ САМООРГАНИЗИРАЩИ СЕ МРЕЖИ

Мобилните самоорганизиращи се мрежи са едни от най-трудните за управление безжични мрежи, което се дължи на характеристиките им и на функционалността, която трябва да предоставят. Уязвимостите на мобилните самоорганизиращи се мрежи, представляват слабости в сигурността на системата. Поради същността си, MANETs са по-уязвими в сравнение с останалите безжични и кабелни мрежи. Някои от уязвимостите са свързани с 1:

- Липса на централизирано управление

MANETs нямат централен сървер за наблюдение. Отсъствието на управление, прави откриването на атаки трудно, защото не е възможно наблюдение на трафика в динамично променяща се мрежа.

- Наличност (достъпност) на ресурси

Достъпността на ресурсите е основен проблем в MANETs. Осигуряването на сигурни комуникации в променлива среда, както и защита срещу специфични заплахи и атаки, води до разработване на различни схеми и архитектури за сигурност. Съвместната ad hoc среда позволява и интегриране на механизъм за сигурност в протокола за самоорганизация на мрежата.

- Мащабируемост

Поради мобилността на устройствата от мрежата, размерът на мобилната мрежа се променя непрекъснато. Механизмът за сигурност би трябвало да може да управлява тази динамика на размера на мрежата, т.е. да управлява и голяма и малка мрежа.

- Кооперииране на устройствата

Маршрутизиращият алгоритъм за MANETs, обикновено предполага, че устройствата се кооперират и не са компрометирани. В резултат на това, компрометирано устройство може лесно да стане маршрутизиращ агент и да разруши мрежовите операции, нарушавайки спецификацията на протокола.

- Динамична топология

Динамична топология и променящото се членство на устройствата може да наруши отношението на доверие сред тях. Доверието може да бъде разрушено също, ако част от устройствата са определени като компрометирани. Динамичното поведение, може да бъде по-добре защитено с разпределни и адаптивни механизми за сигурност.

- Ограничена енергийна мощност

Устройствата в MANETs са с ограничена енергийна мощност, което поражда някои проблеми. Устройство в мрежата, може да започне да се държи по начин, който да му пести мощност, когато разбере, че енергийната му мощност се е изчерпила. До това състояние може да доведат и атаки от тип отказ от услуга (Denial-of-service).

- Ограничена пропускателна способност

Комуникациите в MANETs са променливи и с нисък капацитет, като в сравнение с безжичните мрежи са по-податливи на външен шум, интерференция и ефектите от затихване на сигнала.

- Възможност за вътрешна атака

Мобилните устройства в MANETs могат свободно да се присъединяват и да напускат мрежата. Възможно е някое от устройствата да е компрометирано. Трудно е да се открие, че поведението на такова устройство е зловредно, следователно тази атака е по-опасна от външна атака.

- Липса на предварително дефинирана физическа граница на мрежата

За MANETs не може прецизно да се дефинира физическа граница на мрежата. В такъв смисъл, ако компрометирано устройство се присъедини към радиообхвата на друго устройство от мрежата, то ще е в състояние да комуникира с него и да компрометира мрежата.

3. ТИПОВЕ АТАКИ В МОБИЛНИТЕ САМООРГАНИЗИРАЩИ СЕ МРЕЖИ

Осигуряването на сигурността на мобилните самоорганизиращи се мрежи е трудна задача и е предизвикателство за изследователи и работещите в областта на киберсигурността. Идентифицирането и класифицирането на възможните форми на атака е първата стъпка в разработването на решения за сигурност на MANETs.

Съществуват различни типове атаки в MANETs, но почти всички могат да се класифицират в следните групи 4:

- Външни атаки – атакуващият цели да причини натоварване на мрежата, разпространяване на фалшива маршрутизираща информация, или да затрудни възлите да предоставят услуги.

- Вътрешни атаки – атакуващият желае да получи достъп до мрежата и да участва в мрежовата активност, или като злонамерено се представи за нов възел, или чрез директно компрометиране на възел и използвайки го като основа за провеждане на зловредни действия.

- Пасивни атаки – пасивната атака е непрекъснато събиране на информация, която може да се използва по-късно, когато се провежда активна атака. За тази цел атакуващият подслушва пакетите и ги анализира, за да извлече необходимата информация.

- Активни атаки – включва почти всички други атаки, провеждащи се чрез активно взаимодействие с жертвата, такива като отвличане (hijacking), при което атакуващият взема контрола върху комуникацията между два възела и се маскира за един от тях; заглушаване (jamming), което причинява недостъпност на канала, чрез претоварването му; лишаване от „спящ“ режим на устройството, което води до изчерпване на батерията.

Най-често реализираните атаки основно включват подслушване, представяне от чуждо име, DoS (Denial of Service) атака 3.

Атаките с военни цели се разделят на два вида – стратегически маршрутизиращи атаки и тактически маршрутизиращи атаки 3. Целта на стратегическите атаки е събиране на разузнавателна информация, докато тактическите атаки, главно имат задача да направят някоя важна част от мрежата неработоспособна, чрез DoS атака.

4. ЗАКЛЮЧЕНИЕ

Мобилните самоорганизиращи се мрежи са нова технология, която позволява на потребителите да комуникират без предварително изградена физическа структура. Характерните свойства на MANETs поставят сериозни проблеми пред сигурността им, която е един от основните фактори за успешното им използване.

В доклада се анализирани аспектите на сигурността в контекста на MANETs, някои типични уязвимости в тях и типовете атаки, които дефинират насоките за изследвания, свързани със сигурността им. За да могат ефективно да се използват е необходимо да се търсят конкретни решения, чрез които MANETs да преодолеят разгледаните уязвимости.

ЛИТЕРАТУРА

1. Goyal P., V. Parmar, R. Rishi „MANET: Vulnerabilities, Challenges, Attacks”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011, ISSN (Online): 2230-7893, www.IJCEM.org

2. Ilyas M. (editor), The Handbook of Ad Hoc Wireless Networks, CRC Press LLC, 2003

3. Mishra A., K. M. Nadkarmi “Security in Wireless Ad Hoc Networks — A Survey”, in the book M. Ilyas (ed.), “The handbook of ad hoc wireless networks”, CRC press LLC, 2003

4. http://www.cs.ucsb.edu/~koc/ns/projects/12Abstracts/JiahongWeng.pdf

ЗАСЕКРЕТЯВАНЕ ПРЕДАВАНЕТО НА ДАННИ В CDMA2000 1XEV-DO

Линко Г. Николов

Национален военен университет „Васил Левски“
Факултет „Артилерия, ПВО и КИС“- гр. Шумен

SECURE DATA TRANSFER IN CDMA2000 1XEV-DO

Linko G. Nikolov

***ABSTRACT**: Security layer in CDMA2000 is utilized to provide private data processing in the multiple access environment. The Diffie-Helman algorithm and Advanced Encryption Standard (AES) are applied, but cryptographic security is hardly to be assumed. The complexity of the algorithms is presented in this paper and some further details about data transfer are discussed as well.*

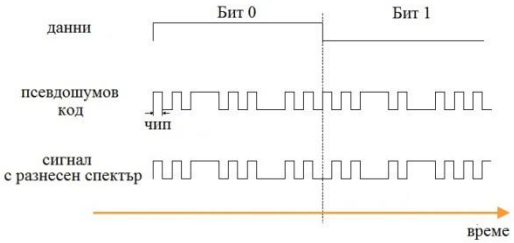
***KEYWORDS**: encryption, security protocols, cryptography, Gallois Field.*

1. Въведение

Клетъчната система с кодово разделяне на каналите CDMA2000 има няколко реализирани стандарта. Единият от тях е с изцяло пакетна обработка на данните – 1XEV-DO. Означението 1X определя първа скорост, която е възможна за разнасяне на спектъра на биполярните импулси – 1,2288 Мбит/с [3]. Абревиатурата „EV“ идва от „еволюционно развитие“, а DO от „оптимизирано предаване на данни“. Възможностите, които предоставя точно този стандарт на клетъчни комуникации, са много, но най-важното предимство е повишаването на шумоустойчивостта чрез разнасянето на спектъра на сигналите от и към терминалите и базовата станция. И в тази система, както и във всички останали клетъчни системи, данните биват засекретявани (криптирани). Засекретяването става на няколко етапа посредством протоколи, работещи в обособен слой за сигурност от мрежовия модел.

2. Предаване на данни чрез 1xEV-DO

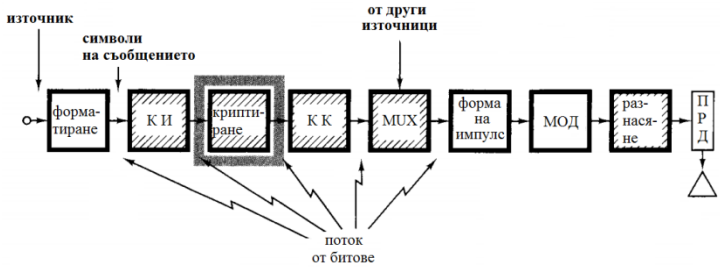
Системата с кодово разделяне на каналите осигурява защитеност на данните на първо място посредством самите кодове, използвани за осъществяване на комуникация между абонатите и базовата станция. Тези кодове „маскират“ информационния поток, при което се получава разнасяне на спектъра на сигнала. Скоростта 1,2288 Мбит/сек, използвана за разнасяне на спектъра, се явява точно 512 пъти по-висока от първоначално определената скорост на дискретизация за един цифров комуникационен канал – 2400 отчета/сек. В момента, скоростта, която е максимално възможна в новия стандарт на CDMA - 3XEV-DO, е трикратно увеличена, или 3,68 Мбит/с. Намаленото времетраене на един чип от кода води до разширяване на спектъра на сигнала, изграждащ този код. Разнасянето на спектъра се извършва посредством т. нар. „псевдошумови“ кодове за отделните абонати (вж. Фиг. 1). Това означава, че достъп до информация, ще има само този потребител, за когото е предназначена информацията, тъй като предварително знае използвания от предавателя код. Никой друг няма да може да „подслушва“ предаваните данни.



Фиг. 1. *„Маскиране“ на данните с код.*

3. Криптиране на данните

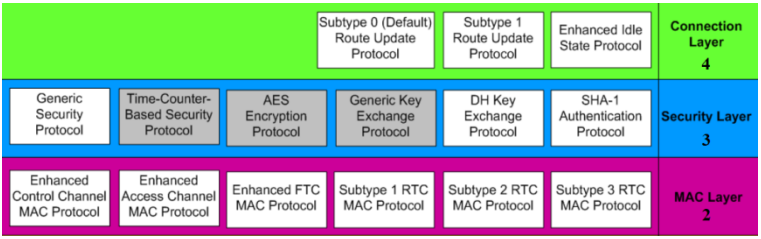
За осигуряване на защита на потребителските данни е необходимо те да бъдат засекретени и разпознати само от потребителя, за когото са предназначени. Това се осъществява посредством специализирани протоколи. Наред с кодовото разделяне на абонатните канали, за предоставяне на конфиденциалност е предвиден специален комуникационен слой за сигурност (Security layer) в мрежовия модел на системата CDMA2000 [3]. Този слой се явява трети в йерархията.



Фиг. 2. *Система за предаване на данни с криптиране.*

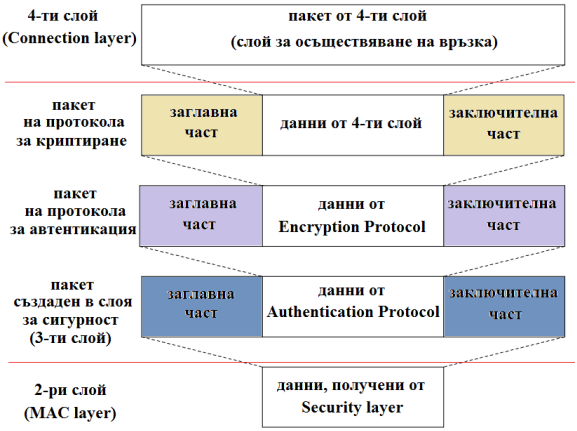
Слоят за сигурност извършва следните функции:

- **обмен на ключове;**
- **автентикация;**
- **криптиране.**



Фиг. 3. *Слой за сигурност в йерархията на мрежовия модел на CDMA.*

Обмяната на ключове за засекретяване и автентикация се извършва от терминалите и БС по процедури, определени от протокола “Key Exchange Protocol”. Автентикацията е необходима за разпознаване на трафика от собствената мрежа, като се извършва според процедурите на “Authentication Protocol”. Криптирането се извършва по процедурите както на “Default Encryption Protocol”, така и на “AES Encryption Protocol”. Общият брой протоколи от този слой са шест (вж. Фиг. 3) – “Generic Security”, “Time-Counter Based Security”, “AES Encryption”, “Generic Key Exchange”, “DH Key Exchange” и “SHA-1 Authentication”. Три от протоколите се явяват като допълнителни възможности и не се използват за всяка сесия. Те ще се използват само ако е изрично указано от по-горен протокол. Основните три протокола спазват поредността, представена на фиг. 4:



Фиг. 4. *Йерархия на протоколите за засекретяване в 1XEV-DO.*

Особеност в протоколите от слоя за сигурност е, че всички добавят и заключителна част (trailer) към поднесените данни. При първоначално установяване на свръзка между устройствата обаче, протоколите от слоя за сигурност отсъстват. След като свръзката е установена (извършена е конвергенция между устройствата) и сесията започне, слоят за осъществяване на свръзка указва кой протокол от слоя за сигурност ще се използва. Протоколът за криптиране „Encryption Protocol“ добавя заключителна част или т. нар. „*опашка*“ с цел да прикрие точното количество битове, пристигащи от горния слой, т. е. скрива реалния размер на пакета. Една от променливите, съдържащи се в заглавната част (header) на този протокол, е инициализиращ вектор – *IV*. Протоколът за автентикация „Authentication Protocol“ съдържа цифров подпис, който осигурява автентичност на пакета. Важен момент тук е, че декриптирането в получаващата страна се извършва единствено при успешна автентикация. Протоколът за сигурност „Security protocol“ съдържа параметри за крипто синхронизация, времеотметки, използвани протоколи от слоя и др.

Не винаги пакетите, преминаващи през слоя за сигурност, трябва да бъдат криптирани. В такива случаи се използва *Нулев протокол за сигурност* „Default Security Protocol“ [4]. В останалите случаи, протоколите от слоя се използват.

При организирането на сесия, в протоколите от слоя за сигурност се наблюдават два режима на опериране:

- режим на конфигурация „InConfiguration Instance“;
- режим на сесийна експлоатация „InUse Instance“.

В случаите, когато се извършва криптиране, първият възможен протокол е т. нар. Основен протокол за сигурност - „Generic Security Protocol“. В предавателната част той е отговорен за вмъкването на *cryptosync* променлива. В приемната част, този протокол изчислява *cryptosync* стойността, позовавайки се на променливите, представени в заглавната част.

В системата CDMA2000 се използва асиметрично засекретяване [4]. Асиметричното засекретяване използва два различни ключа – публичен „public“ за криптиране, и частен „private“ за декриптиране [1, 2]. За да се осъществи засекретяването, тези ключове трябва да бъдат генерирани (изчислени) и предадени по канала за свръзка. Протоколът „Diffie-Helman Key Exchange Protocol“ има задача да пренася тези ключове. Той използва два вида съобщения за публичен ключ в заглавната си част - заявка за получаване на ключ „KeyRequest“ и отговор на заявката „KeyResponse“. За потвърждение, че частните ключове са генерирани, използва съобщенията: *Готовност на ключа в базовата станция* „ANKeyComplete“, и *Готовност на ключа в мобилния терминал* „ATKeyComplete“. Мобилния терминал, при получаване на заявка за ключ, избира случайно число *ATRand* и извършва математическо изчисление на публичния ключ по формулата:

$$ATPubKey = g^{ATRand} mod\ p \qquad (1),$$

където g и p са взаимно прости над предварително определено крайно алгебрично поле $GF(2^n)$, определящо дължината на ключа. Случайното число *ATRand* е със стойност между 1 и *p-2*. Дължината на ключа се знае предварително, като информацията е обменена чрез сесия в режим InConfiguration. Секретния ключ (*private key, secret key, SKey*) се изчислява по формулата:

$$SKey = ANPubKey^{ATRand} mod\ p \qquad (2)$$

Така изчислен, частния ключ се предава по засекретен от протокола „DH KeyExchange“ канал и истинското засекретяване на данни може да започне.

4. Заключение

В системата CDMA2000 слоят за сигурност осигурява засекретяване на данните на необходимото ниво на конфиденциалност. Използваните протоколи са надеждни, като процесорната им обработка не усложнява в голяма тежест потока от инструкции. Не се получава ненужно забавяне на пакетите, а латентността е в границите на приемливото за потребителя.

Недостатък се явява ниската криптографска устойчивост на засекретените данни. С цел да не бъдат натоварвани процесорите в БС и терминалите, протоколите за криптиране не генерират ключове с достатъчна дължина и криптографски свойства. Това се явява уязвимост в сигурността на системата, но тя се открива само при специализирани преднамерени атаки и криптоанализ.

ЛИТЕРАТУРА:

1. Bernard Sklar, “Digital Communications”, второ издание, Глава 14, Prentice Hall, 2007, ISBN 0-13-084788-7.

2. Bruce Schneier, “Applied Cryptography”, John Wiley&Sons, NY, 1996.
3. Rohde & Schwarz, “1xEV-DO Revision A+B”, White paper, October 2013, Интернет адрес: www.rohdeschwarz.com.
4. Техническа спецификация на системата CDMA2000 1XEV-DO, 3GPP2 C.S0024-B, Версия 3.0, Септември 2009.

КИБЕРСИГУРНОСТТА – ОСНОВЕН ПРИОРИТЕТ В ОТБРАНАТА

Добрин Д. Петров

1000 София, ул. „Дякон Игнатий“ 9, e-mail: dpetrov@mtitc.government.bg

CYBERSECURITY – BASIC PRIORITY IN DEFENCE

Dobrin D. Petrov

ABSTRACT: *The report presents NATO's development in cybersecurity, the current threats operating in cyberspace, and the different ways for protecting against cyberattacks.*

KEY WORDS: *Information security, Malware, Firewall, Cyberspace*

Въведение

През последните години се наблюдава тенденция на увеличаване на броя и разнообразието на констатираните кибератаки като обхват, използвани технологии и преследвани цели. Поради тази причина е необходимо да се проследяват, изследват и анализират различните случаи на кибернападения в световната мрежа и методите за защита от тях. За изминалата 2014 г. в България бяха констатирани близо 3000 кибератаки [1].

Организации на НАТО, свързани с киберсигурност

НАТО има опит с киберзаплахите още от 1999 г. когато сървъри на организацията са атакувани и блокирани за няколко дни от IP адреси, базирани в Сърбия, Русия и Китай. Като резултат от това (2005 г.) е основан НАТО център за реакция при компютърни инциденти (NCIRC) [2]. Случаят с атаките срещу члена на алианса – Естония през 2007 г. също е добре известен и един от отговорите на тази атака е основаването на Център за киберзащита в Талин, Естония (NATO Cooperative Cyber Defence Centre of Excellence) [3]. NATO CCDCOE е създаден на 14 май 2008 г. и постига статута на международна военна организация на 28 октомври 2008 г. Центърът се ръководи и координира от полковник Артур Сузик и началника на Генералния щаб Дженс ван Лаак. В момента страните участващи в рамките на центъра са Естония, Германия, Италия, Латвия, Литва, Полша, Словакия, Испания, Унгария, САЩ, Холандия, Франция, Великобритания, Чехия и Австрия. Членството в CCDCOE е отворена за всички страни от НАТО и също така може да се установи сътрудничество със страни извън НАТО, университети, изследователски

институти и бизнес организации. Структурата се състои от пет отдела: „Стратегически“, „Правен и политически“, „Технически“, „Поддръжка“ и „Обучение и тренировки“. През 2010 г. НАТО създава ESCD (Emerging Security Challenge Division) и под нейно ръководство е NATO CDMA [4]. На 1 юли 2012 г. като резултат от сливането на NC3A, NACMA и NCSA започва да функционира NCIA (NATO Communications and Information Agency) [5]. NCI агенцията осигурява:

- Непрекъсната (24/7) връзка с Алианса;
- Защита на своите компютърни и комуникационни мрежи;
- Управление и контрол на технологията за балистична противоракетна отбрана на НАТО и въздушна командна и контролна система (ACCS) в подкрепа за съвместни възможности за наблюдение и разузнаване (JISR) и федерални мисии свързани с компютърните мрежи (FMN);
- Разработване на оперативно съвместими и рентабилни възможности в областта на C4ISR;
- Сигурни и икономически ефективни комуникационни и информационни системи и услуги.

Агенцията се ръководи от генерал-майор Коен Гисберс.

Международна правна рамка и сътрудничество за киберсигурност

Всички релевантни участници в киберпространството изразяват убеденост за неотложно изработване на международноправен документ, регулиращ тази сфера и гарантиращ сигурността и ефективното противодействие на кибертероризма, киберпрестъпността и недопускане на кибервойна. Позициите на основните играчи засега, обаче, са принципно трудно съвместими. В тази ситуация са възможни два прагматични подхода. Първият, се прилага от Великобритания, като възможна реална първа крачка за изработване на международна правна рамка чрез сключване на двустранни договори/споразумения за кризисни комуникации между държави, които най-често са обект на кибератаки. През 2012г. Обединеното кралство активно развива такава двустранна политика с Китай и Русия. Идеята е, в случай на криза, предизвикана от зловредни действия в киберсферата, държавите да споделят информация по механизма, по който това се прави в областта на контрола на въоръженията. Вторият подход се базира на концепцията за регулиране на киберпространството чрез т.нар. „меко право“ – изработване на кодекс за поведение в киберпространстовото, който държавите съблюдават на доброволна основа [6].

Заплахи в киберпространството

Атаките се осъществяват чрез различен вид софтуер, който се използва, за да се проникне в дадена система – като adware, spyware, malware, оогромна вариация от вируси, като за операционната система Windows са над 100 000.

Stuxnet е първият образец за зловреден вирус/софтуер (разкрит е през юни 2010 г.). 60 % от заразените компютри са в Иран, но има и в Индия, Русия, Индонезия. Stuxnet е обявен за първия вирус, специално създаден да поразява реални физически инфраструктури, промишлени обекти, атакувайки SCADA (Supervisory Control and Data Acquisition) системите, които са едни от най-широко използваните типове системи за контрол на индустриални обекти (ICS).

Вторият, известен от този порядък зловреден вирус е Flame (разкрит през май 2012 г.) Flame определят като инструмент на кибершпионажа, който събира мно-

жество информация от компютрите-жертви (картинки, натиснат клавиш, пароли и информация за местоположение). Най-пострадали страни са Иран, Израел, Судан, Сирия, Ливан, Саудитска Арабия и Египет.

Компютърните специалисти доказват, че и двата вируса са циркулирали няколко години, преди някой да ги забележи. Според тях, създаването на толкова съвършени продукти предполага огромни инвестиции и държавна ангажираност в проекта. Според характеристиките и поставените цели, Stuxnet е кибероръжие. Неговата поява доказва, че правителствата ще продължат да развиват злонамерен софтуер, за да саботират информационно-технологичните системи на противниците си и тяхната критична инфраструктура. То показва също така, че враждебни правителства могат лесно да превърнат SCADA системите, от които зависи функционирането на системите за електричество, газ, петрол, вода и т.н.т в цел, побеждавайки по този начин защитата, на която разчитат повечето компании.

През юни 2012 г. вестник Washington Post [7] съобщи, че шпионския вирус Flame е разработван от специалисти на САЩ и Израел за получаване на информация, която би могла да бъде полезна за проваляне на иранската ядрена програма.

Тези два случая са много опасни, защото отварят кутията на Пандора и различни страни по света, позовавайки се на прецизното право, вече могат да твърдят, че е законно да използват зловреден софтуер превантивно срещу индустриални обекти и критична инфраструктура на враговете си. Друга опасност произтича от възможността зловредните вируси, които вече са заразили хиляди компютри (предполага се, че Stuxnet е заразил около 50 000) да бъдат копирани, адаптирани и използвани от хакерски групи, киберпрестъпници и разузнавателни агенции. Клонингите, обаче могат да не са толкова съвършени, колкото оригинала, което означава, че те биха могли да заразяват и повреждат обекти, извън пределите на своите цели.

Създаването и атакуването с двата от този порядък (засега) разкрити зловредни вируса не оставя съмнение за наличието на надпревара във въоръжаването в киберпространството. Може да се допусне, че в информационното пространство „се разхождат“ и други такива вируси, чието създаване е спонсорирано от други държави. До разкриването на Stuxnet и Flame даже говоренето за такива оръжия беше недопустимо. Днес те са част от реалността и става очевидно, че тяхното притежание и развиване ще е неотменен елемент от военния капацитет на държавите.

Кибероръжието има безспорни предимства: ефективно е, значително по-евтино от конвенционалното, сложно може да бъде приписано на конкретния нападател, от него е много трудно да се защитиш, репликира се с нулеви загуби, привидната му безобидност намалява прага на прилагането му. По своята разрушителна сила то е сравнимо с ядреното, химическото и биологичното, но за разлика от тях не се контролира по никакъв начин и се смята, че кибероръжието сериозно превъзхожда останалите оръжия за масово поразяване със своята точност, невидимост и всеобхватност.

През 2013 г. изтече информация за част от действията на САЩ в тази област. Оказва се, че американските военни са сред основните движещи сили на черен пазар за т.нар. zero-day слабости в сигурността на софтуерни разработки. С термина zero-day се означават новооткрити пропуски в сигурността, които започват да се разпространяват сред хакерите, преди компанията да е имала време да разработи обновление, което да реши проблема или дори преди да е разбрала за неговото наличие.

Дълго време подобни открития се обявяваха по време на хакерски конференции, като обикновено наградите бяха дребни суми, по-висок престиж и от време на време някое и друго предложение за работа. Постепенно zero-day пробивите в сигурността на софтуерите привличат вниманието на големите компании и правителства, което създава своеобразен черен пазар за търговия с тях, твърди онлайн изданието TechnologyReview [8]. Според негова информация администрацията на САЩ е готова да плати стотици хиляди долари за определени zero-day открития.

През есента на миналата година САЩ дори са приели специфични директиви, които изваждат използването на zero-day пробивите в сигурността от регулацията, която се занимава с кибероръжията. Така правителството отказва да носи отговорност, когато се възползва от тях и практически може да ги използва неограничено. Според действащата американска регулация за кибероръжие се приема само специален код, който е използван за нанасяне на щети. Кодът, който е използван за проникване в системата и практически дава възможност за последващо нанасяне на щети, обаче не се смята за такова.

Софтуерен инженер разкрива част от тарифите при търговията с подобна информация. Zero-day хак за Android например варира между $30 000 и $60 000. Слабост в Windows се котира между $60 000 и $120 000. Интересът към интернет браузърите Chrome и Internet Explorer, както и към мобилната платформа iOS на Apple, е най-голям. Там цените започват от $80 000 и достигат $250 000. В зависимост от важността на софтуера понякога откривателят на проблема получава и месечно възнаграждение, докато дупката не бъде открита от компанията и поправена [9].

Съвременни информационни системи за сигурност и отбрана (C4I)

C4I (Command, Control, Communications, Computers, and Intelligence) системите са основните градивни елементи на системите за информационен обмен и за подпомагане вземането на решение [10]. При кризи C4I се използват за осигуряване на постоянен поток от данни, който трябва да дава информация в реално време за обстановката в района на кризата. Тази информация трябва да може да бъде получавана при поискване от ръководителите навсякъде и по всяко време. Все по бързото развитие на ИТ и очакването, че C4I технологиите могат значително да повишат ефективността на различните операции ги правят ключов елемент в модернизацията на въоръжените сили и страната като цяло. Очаква се и интерфейса човек-машина да е доста по-различен, включващ разпознаване на команди чрез говор, монитори с висока разделителна способност монтирани върху каските на войниците или вградени в защитните очила и всичко това с размери подходящи за носене във всякаква ситуация. Ключови елементи за развитието на комуникационните системи като част от C4I системата са: внедряването на нови методи за компресиране на видео и данни и предаването на тази информация по линии с малка пропускателна способност; създаването на безжични глобални и локални мрежи с пакетна комутация чрез използването на мобилни базови станции; намаляване цената на оптичните преносни среди и увеличаване на разстоянието за предаване на сигналите; разработването на нови методи за модулация с цел по-ефективно използване на честотните ленти; въвеждане на т.нар. „софтуерно радио”; разработването на нов тип антени-многофункционални и работещи в множество честоти които да се използват (антените) както в комуникационните технологии така и в

сензорните системи. Бъдещите оръжия ще имат интегрирана цифрова информационна подсистема (не само цифрова комуникационна система) която ще е напълно интегрирана с всички системи изграждащи C4I. Тази функционалност ще доведе до това, информацията, която има един отделен елемент (войник, сензор и т.н.) да бъде автоматично споделена с всички елементи на C4I (на всяко едно от нивата – тактическо, оперативно и стратегическо). Целите засечени от сензорните системи ще бъдат указвани на различни типове оръжия (ракети, самолети, кораби войници на бойното поле). С времето използването на сензорите, комуникационните и информационните технологии ще даде възможност да се изгради единна система за мониторинг и контрол на всички елементи от бойното поле (войници, въоръжение и техника) даваща ни всичката необходима информация в точното време и на точното място. Например количеството снаряди, гориво, процента щети и др. за всеки танк, самолет и т.н.

Поради важността на C4I-системите за осигуряване на информационни способности на въоръжените сили, в Инвестиционният план-програма на Министерството на отбраната до 2020 г. са включени три важни проекта [11]:

- Проект 7 „Придобиване на модул за комуникационно-информационна поддръжка на контингент", с което ще се осигурят в комуникационно и информационно отношение българските военни контингенти при участието им в операции и ще се създадат способности за действие в мрежова среда при осъществяване на националното управление.
- Проект 12 "Кибернетична защита", с който се осигуряват способности за повишаване на кибернетичната сигурност на съществуващи, изграждани и предстоящи за изграждане военни системи и мрежи, като се поддържа и развива център за наблюдение и анализ, и център за реагиране и възстановяване.
- Проект 13 „Развитие на автоматизирана информационна система на Министерството на отбраната, Българската армия, оперативните и тактически щабове", като се изгражда единна мрежова информационна среда за функциониране на системата за командване и управление на всички нива – стратегическо, оперативно и тактическо и подпомагане на дейността на структурите от Министерството на отбраната за успешно изпълнение на мисиите и задачите, чрез непрекъснат, бърз и надежден електронен обмен и достъп до общи информационни масиви.

Мерки за защита в киберпространството

Когато става на въпрос за армия, се имаме предвид корпорация, при която ако нещо не се купува с пари, то се купува с много пари [12]. Финансовите възможности, с които разполагат армиите и често срещаната фраза "строго секретно" върху по-голямата част от информацията, са причина за изграждането на възможно най-сигурната информационна мрежа. Най-силните армии разполагат със сигурна собствена мрежа чрез сателитни връзки за отдалечен достъп и не използват несигурни мрежи. За да се осигури още по-добра защита е добре да има и биометрична система за сигурност. Най-общо казано биометрията е модерен, скъп, автоматизиран метод за разпознаване на даден човек въз основа на физическите и поведенческите му характеристики. Точно по тези два показателя може да се направи едно условно деление на биометрията: физическа и поведенческа. Физическата биомет-

рия включва: пръстови отпечатъци, форма на ръката, дланта, ухото, пръстите, ириса на окото и лицева характеристика. Поведенческата биометрия се изразява в: подпис, почерк, походка или глас (който се отнася и за физическата). Тези технологии най-често се използват, за да провери и идентифицира даден потребител и да му се предостави достъп до даден компютър (информация), стая, сграда… Биометричните системи за сигурност намират своето приложение най-вече в държавните структури (като армия, правителство, полиция), банките и други мащабни организации изискващи високо ниво на сигурност. Най-голямото предимство на тези технологии е, че се осигурява сигурност от чисто физическа гледна точка. Всеки потребител, който използва някаква биометрична система, може да се оторизира, че наистина е той, а не някой друг човек, който му използва компютъра, кредитната карта или пропуска. Разбира се, изключваме случаите в които "силата е над правото" и има отрязани пръсти, ръце, глави и извадени очи. Но дори и тогава има начин да се създаде сигурна оторизация на дадено лице. На въпроса "Ти ли си човекът за който се представяш?" ние можем да се идентифицираме, използвайки едновременно три различни начина:

- доказваме физически, че наистина ние сме въпросният човек – биометрично;
- с нещо което само ние знаем – парола или ПИН код;
- с нещо което само ние имаме – ключ, пропуск.

Комбинирайки едновременно тези три начина, ние получаваме тройно по-голяма защита при разпознаването от дадена машина или софтуерна програма (примерно военният сървър, на който имаме акаунт). Заедно с осигуряването на сигурна отдалечена връзка през виртуална частна мрежа, ние можем да постигнем една висока степен на сигурност подходяща за организация от типа на армията. Проблеми при биометричните технологии са, че всяка една от тях има малко или много недостатъци свързани най-вече с чисто физиологични фактори. При поведенческата биометрия подписа, почерка, гласа могат да бъдат подправени, което не е добре решение за сигурността. При физическата има далеч по голяма сигурност. Така например, при лицева характеристика, пръстови отпечатъци, сканиране на ириса се постига изключително добра точност. Недостатъците са , че при стареенето си хората доста се променят, което налага често обновяване на информацията в базата данни за даден потребител. Честите промени правят тези системи по-трудни за поддръжка и използване, но и далеч по-сигурни благодарение на актуалната информация, с която работят. Може да се обобщи, че в киберпространството стопроцентова защита няма, но когато става въпрос за организации разполагащи с огромни средства (като армията например), тогава се

използват най-модерните, скъпи и надеждни продукти на пазара, което гарантира за възможно най-високото ниво на защитеност.

Изводи:

- Кибервойната дава непропорционална мощ на малките държави, не изисква голям финансов ресурс (само компютър и достъп до интернет), може да се започне отвсякъде;
- Съществува огромно разнообразие от видове кибератаки и методи за кибершпионаж;
- Извършването на киберпрестъпление не е сложно и е много трудно да се разкрие извършителя;

- Нито една отделна мярка за сигурност не е достатъчна за да осигури надеждна защита в кибернетичното пространството;
- Ефективна сигурност в киберпространството се постига чрез използване на стратегия за сигурност, която обединява множество практики, политики и технологии за сигурност (Република България все още няма разработена стратегия за киберсигурност, на фона на това, държави като Кения и Руанда имат от 2014 година.);
- Гарантирането на отстраняването на киберзаплахите е ключово за постигането на националната сигурност.

ЛИТЕРАТУРА:

1. http://www.dnes.bg/technology/2015/01/23/blizo-3000-kiberataki-e-imalo-v-bylgariia-prez-2014-g.252258
2. http://itlaw.wikia.com/wiki/NATO_Computer_Incident_Response_Capability
3. https://ccdcoe.org/
4. http://itlaw.wikia.com/wiki/Cyber_Defence_Management_Authority
5. https://www.ncia.nato.int/About/Pages/About-the-NCI-Agency.aspx
6. Милина В., Предизвикателства пред международната сигурност, сп. Военен журнал, бр 3-4, 2012
7. http://www.washingtonpost.com/
8. http://www.technologyreview.com/
9. http://www.capital.bg/biznes/tehnologii_i_nauka/2013/02/22/2007653_bit-pazar_za_kiberorujiia/
10. http://cio.bg/3279_analiza_na_riska_za_informacionnata_sigurnost__osnova_za_it_proektite_v_ba
11. Симеонов, С., Реформите във въоръжените сили на република България, Пролетна сесия на Парламентарната асамблея на НАТО, 27-30 май 2011 г., Варна
12. http://www.iseca.org/downloads/2004_2005 1/papers/43599_43695_43697_RAS.pdf

ВЛИЯНИЕТО НА РАЗДЕЛИТЕЛНАТА СПОСОБНОСТ, КОНТРАСТА И ЯРКОСТА НА МОНИТОРА ВЪРХУ ДОСТОВЕРНОСТТА НА ОЦЕНКАТА ЗА КАЧЕСТВОТО НА ИЗОБРАЖЕНИЕТО

Николай Ж. Кулев

НВУ „ Васил Левски“ , Факултет „ Артилерия, ПВО и КИС“
nz_kulev@abv.bg

INFLUENCE OF RESOLUTION, CONTRAST AND BRIGHTNESS OF THE MONITOR ON THE CREDIBILITY OF THE EVALUATION OF IMAGE QUALITY

Nikolay Zh. Kulev

***ABSTRACT**: Analyzed are the conditions for viewing visual assessment tailored to the variety of available devices for visualizing information. Were examined relationships between terms of monitoring and evaluation criteria of the criticality of the monitored video sequences.*

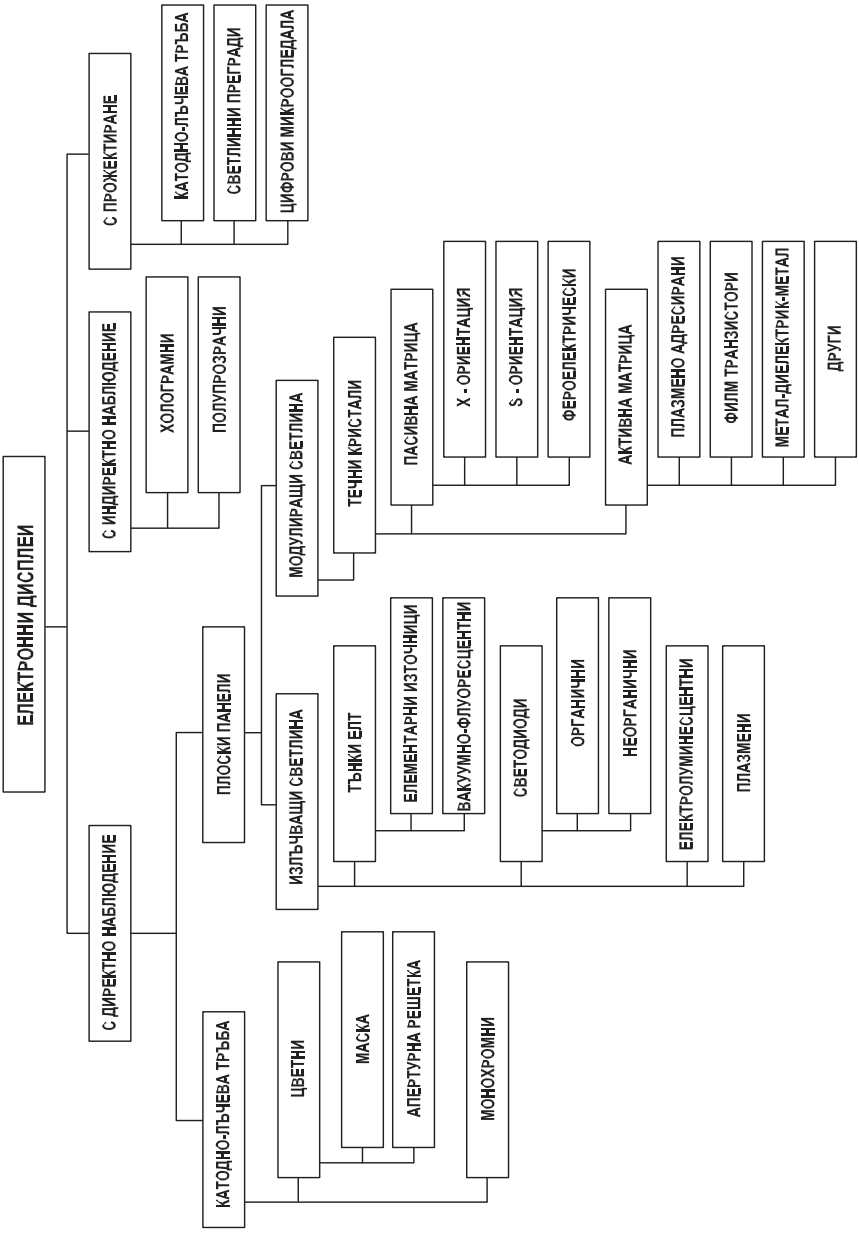
За извършване на субективна анализ за достоверността на оценката за качество на изображението се използват множество устройства за визуализация на графична информация. Тяхното разнообразие е показано на фиг.1. Все още най-широко приложение за оценка на качеството на телевизионни системи намират мониторите с катодно-лъчева тръба и мониторите с течно-кристални дисплеи. Дефинират се два типа условия за наблюдение с различно предназначение – лабораторни и домашни. Първите са предназначени да осигурят критични условия за проверка на дадена система. Целта на вторите е да осигурят средства за оценка на качеството на системата от потребителския край на телевизионната верига. Трябва да бъдат подбрани като малко по-критични от типичната домашна обстановка.

Таблица 1. Общи условия за наблюдение при провеждане на визуална оценка на качеството

Отношение на максималната осветеност към осветеността на угасен монитор	$\leq 0{,}02$
Отношение на осветеността при ниво бяло към осветеността при ниво черно в напълно тъмна стая (за лаборатория)	$\approx 0{,}01$
Максимален допустим ъгъл на наблюдение спрямо нормалния (важи за CRT монитори, за други е все още в изследване)	30°

Цветова температура на екрана	D_{65}
Цифрова обработка на изображението в монитора	не
Пиково количество светлина, излъчена от монитора	200 cd/m^2
Ниво на околната светлина в помещението	ниско
Ниво на осветеността на монитора от околни източници	200 lux
Разделителна способност на монитора (резолюция)	
Яркост и контраст на монитора	
Диагонал на екрана	
Разстояние на наблюдение	

Върховото количество светлина, излъчена от монитора, е тази при 100 % ниво на амплитудата на видеосигнала. Монитори със стойност, по-голяма от 100 cd/m^2, е допустимо да се използват, докато посоченото в таблицата ниво стане технически изпълнимо за всички устройства. Отношението на максималната осветеност към осветеността на угасен монитор може да бъде повлияно от осветлението в стаята, както и от диапазона на контраст на монитора. Ниво черно съответства на количеството светлина, излъчено от монитора при 0 % амплитуда на видеосигнала. То не бива да се бърка с осветеността при угасен монитор. Нивото на околната светлина не се измерва специално, а трябва да е с ниска стойност, така че да се осигури изпълнението на първите две условия.



Фиг. 1. Типове видеодисплеи, използвани за визуална оценка на качеството на видеоизображения

Резолюцията на професионалните монитори, оборудвани с катодно-лъчеви тръби, обикновено покрива изискванията за приложимост за визуални тестове при работните си нива на светлинно излъчване [1]. При течно- кристалните и плазмените дисплеи обикновено резолюцията е фиксирана и се определя от броя елементи, изграждащи светлинната матрица на устройството. Не всички монитори обаче могат да достигнат 200 cd/m^2 пиково количество светлина. В потребителски телевизионен приемник е възможно резолюцията да бъде неадекватна, зависима от нивото на излъчване. В този случай е необходимо да се установят минималната и максималната разделителна способност за съответното ниво. Внимание трябва да се обърне на факта, че както резолюцията, така и яркостта в центъра на екрана и по краищата може да се различават. Този проблем касае по-скоро CRT мониторите, докато при LCD са налични еднакви яркост и резолюция по площта на екрана.

За момента най-практично за оценка на разделителната способност на мониторите се оказва използването на електронно генерирани тестови таблици. В тяхно отсъствие резолюцията може да бъде проверена и с помощта на визуален анализ. Визуалният праг е определен като -12/-20dB. Главният недостатък при CRT мониторите е разделителната способност, която се определя от маската на тръбата, което затруднява визуалната оценка. Но от друга страна, наличието на изкривявания, предизвикани от маската, е признак, че видеосигналите надвишават честотно ограниченията на съответния монитор.

Прието е за визуална оценка на една система да се използват качествени устройства, позволяващи прецизна регулировка на параметрите. Контрастът на един монитор може да бъде силно повлиян от околното осветление. Професионалните монитори обикновено разполагат с техники за подобряване на контраста си в зависимост от светлината в обкръжаващата среда, така че е възможно да не отговарят напълно на изискванията към контраста на системи за визуална оценка. За определяне контраста на даден монитор е необходимо да се знае коефициентът на отражение на екрана *K*. Добрите дисплеи с CRT имат *K* = 5-6 %, при LCD мониторите този коефициент е още по-малък, около 1%. Отразеното количество светлина от неактивен монитор се определя по формулата.

$$\boldsymbol{L}\mathbf{ref} = \frac{\mathbf{1}}{\pi}.\boldsymbol{K} \qquad (1)$$

при ниво на разсеяната околна светлина *I* = 200 lux и *K* = 6%, *Lr* = 3,82 cd/m^2 или около 2%. Контрастът на монитора се изчислява според израза

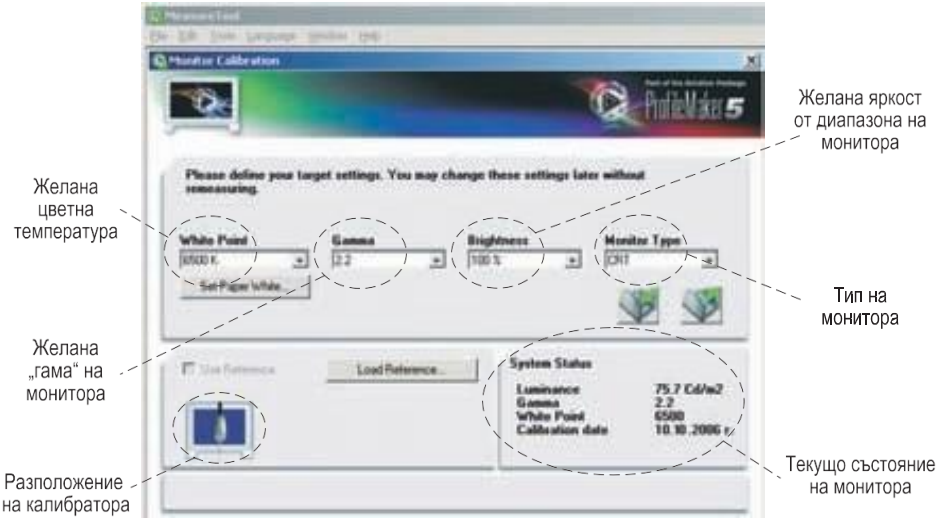
$$\boldsymbol{CR} = \boldsymbol{L_{min}} \;/\; \boldsymbol{L_{max}}\;, \qquad (2)$$

където L_{min} е яркостта на неактивните области при стандартна околна осветеност, а L_{max} е яркостта на бяло поле при стандартна околна осветеност.

За настройка на яркостта и контраста на мониторите се използват тестови образци, наречени PLUGE. Те са приложими както за конвенционалната телевизия, така и за цифровата, и за телевизията с висока резолюция. Разликите са в тяхната конструкция, но като цяло съдържат бели, черни и сиви полета, като от сивите има такива, които са много близки до бялото или

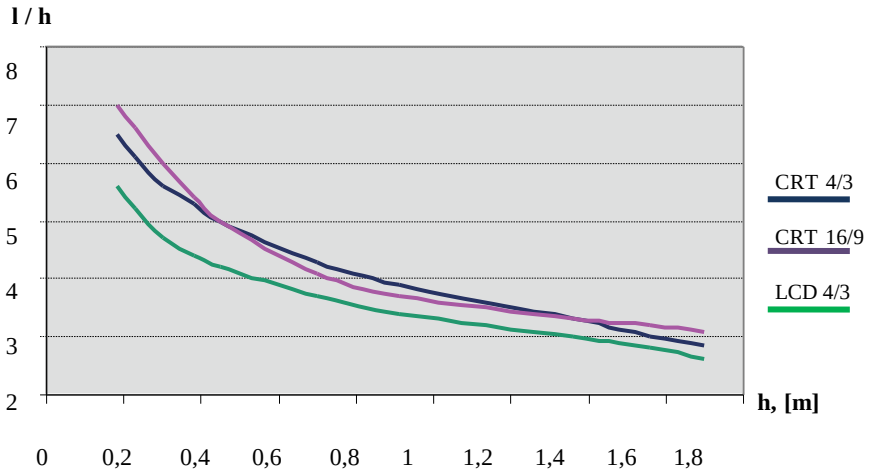
черното. Спецификацията на тестовите изображения и процедурата за настройка на яркостта и контраста на един дисплей са описани подробно в Препоръка ITU-R BT.814 [2]. Тя е съпроводена и от Препоръка ITU-R BT.815 [2], описваща детайлно процедурата по измерване контраста на мониторите.

За измерване на яркостта, контраста, гамата, цветовата температура и други параметри на устройствата за визуализация, както и за калибрирането им (настройването им да отговарят на единен стандарт или препоръка), се използва спектрофотометър GretagMacbeth Spectrolino и на софтуерното приложение GretagMacbeth GM Measure Tool [3].



Фиг. 2. Екран на приложението за калибриране на монитори и дисплеи GretagMacbeth Profile Maker - Measure Tool

Понастоящем няма ограничения за големината на диагонала на използваните устройства за субективна оценка на телевизионни системи. В различни лаборатории са използвани дисплеи с диагонал от 10 до 100 инча. Единственото условие е да бъдат спазени препоръките за оптимално разстояние на наблюдение. На фиг.3 е показана зависимостта на предпочитаното разстояние за наблюдение от размера на екрана при най-широко разпространените монитори и отношения на размера на изображението.



Фиг. 3. Зависимост на отношението на предпочитаното разстояние за наблюдение към височината на екрана *l* / *h* от височината на екрана *h*

Както се оказа от проведените тестове, диагоналът на екрана за наблюдение е пряко свързан с предпочитаното разстояние за наблюдение от потребителите. Тази зависимост не е линейна – с увеличаване на размера на екрана намалява отношението разстояние на оптимално виждане / височина на екрана. За аналогова телевизия с висока разделителна способност разстоянието на оптимално наблюдение е по-малко в сравнение с това при стандартната телевизия. Това се дължи на по-високата детайлност на предаваната картина, както и на по-фината структура на повърхността, върху която се изобразява картината. Същото е в сила и за мониторите с течни кристали пред тези с катодно-лъчева тръба – при тях изображението е по-детайлно и затова предпочитаното разстояние за наблюдение е по-малко. В зависимост от целта на визуалната оценка – дали на качеството, или на изкривяванията, при втората разстоянието на наблюдение е допустимо да се намали, като резултатите трябва да се дадат отделно. Важно е да се има предвид, че форматът на монитора (4:3, 16:9) и типът му (CRT, LCD, plasma) влияе върху предпочитаното разстояние за наблюдение от субектите и респективно на получените резултати и затова при упоменаването им те трябва да се покажат отделно за различните формати на картината.

Оказва се, че и критичността на видеопоследователностите влияе на предпочитаното разстояние за наблюдение. В таблица 2. са показани коефициентите на корелация между предпочитаното разстояние за наблюдение от субектите и оценки на критичноста на тестовите последователности.

Таблица 2. Коефициенти на корелация между разстоянието за наблюдение и критичността на последователностите

Характеристики на последователностите	Коефициент на корелация
Разстояние на наблюдение – вектор на движението	0,57
Разстояние на наблюдение – брой преместващи се детайли	0,82
Разстояние на наблюдение – компресия с „RAR“	-0,49
Разстояние на наблюдение – компресия с „Huffman“	0,11
Разстояние на наблюдение – компресия с „MSU-LS“	-0,65

От таблицата следва изводът, че броят преместващи се детайли в изображението може да се използва за ориентировъчно определяне на коректното разстояние за наблюдение при субективните тестове. Тези с по-голям брой преместващи се детайли изискват наблюдение от малко по-голямо разстояние.

ЛИТЕРАТУРА:

1. Делийски А. , Телевизията в света на високите технологии, Сиена, 2002
2. TV приемници с цифрова обработка на сигнала, Тютюнджиев Н. , Техника, 2006
3. Цифрова телевизия, Конов К., Сдиос, 2004
4. Бекярски Ал. Телевизионни системи. Издателство на ТУ-София, 2009
5. В.А. Серов – Сфирнос цифрове телевидение DVB-T/H-спб БХВ – Петербург, 2010

АНАЛИЗ НА ВЛИЯНИЕТО НА ЧЕСТОТАТА НА КАДРИТЕ, ФОРМАТА НА ГРУПАТА КАДРИ, СТЕПЕНТА НА КОМПРЕСИЯ И РАЗМЕРА НА ИЗОБРАЖЕНИЕТО ВЪРХУ КАЧЕСТВОТО ПРИ СТАНДАРТА MPEG-2

Николай Ж. Кулев

НВУ „ Васил Левски“ , Факултет „ Артилерия, ПВО и КИС“
nz_kulev@abv.bg

ANALYSIS OF THE INFLUENCE OF THE FRAME RATE, THE SHAPE OF THE GROUP FRAMES, THE COMPRESSION RATIO AND THE SIZE OF THE IMAGE QUALITY IN THE STANDARD MPEG - 2

Nikolay Zh. Kulev

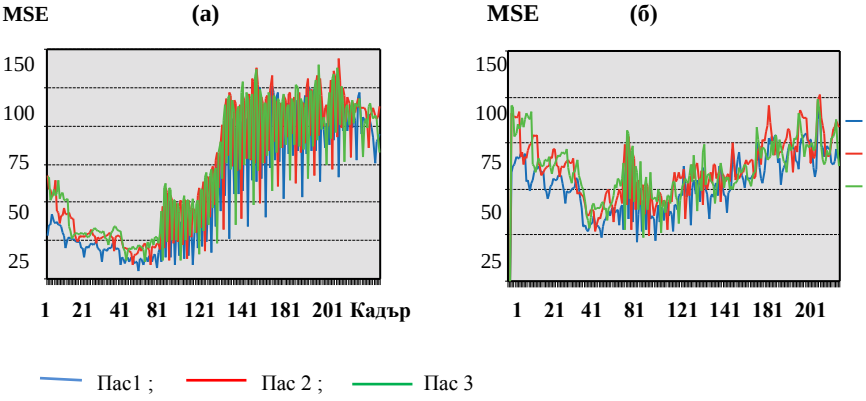
ABSTRACT*: There has been a study and analyze the impact of the main parameters of the standard, video compression MPEG - 2 on image quality - stability of the algorithm for compression, speed of work, degree of compression, the image size.*

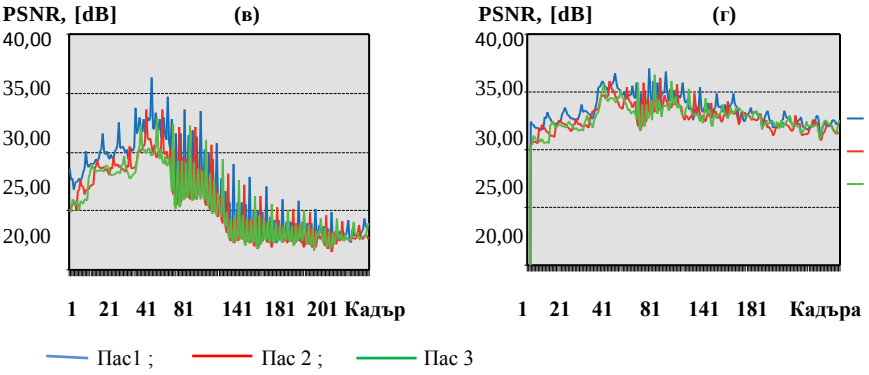
В работата е изследвана стабилността на компресиращия алгоритъм. За целта две последователности са компресирани с еднакви битови скорости последователно по три пъти. Оценките на отношението сигнал/шум и средноквадратичната грешка на яркостта и цветността са показани на фиг. 1. и фиг. 2. От покадровото сравнение се вижда, че при MPEG-2 има известна нестабилност при повтарящо се компресиране на един и същ видеоматериал. При първото повторение резултатът винаги е по-оптимистичен от реалния (по-ниска MSE, по-високо пиково отношение сигнал/шум - PSNR), а едва след второто повторение кодерът започва да дава стабилен резултат. Осреднените за цялата продължителност на тестовите последователности резултати са показани в табл. 1.

От резултатите в таблицата се открояват няколко особености. Първо, разликите в качеството при различните пасове са по-силни за яркостта, отколкото за цветността. Второ, големината на разликите в качеството при различните повторения зависи от контекстуалното съдържание на тестовото видеоизображение, и особено от степента на движение в него. Трето, разликите са по-големи при ниски скорости на битовия поток, поради по-критичната работа на алгоритъма за компресия при този стандарт.

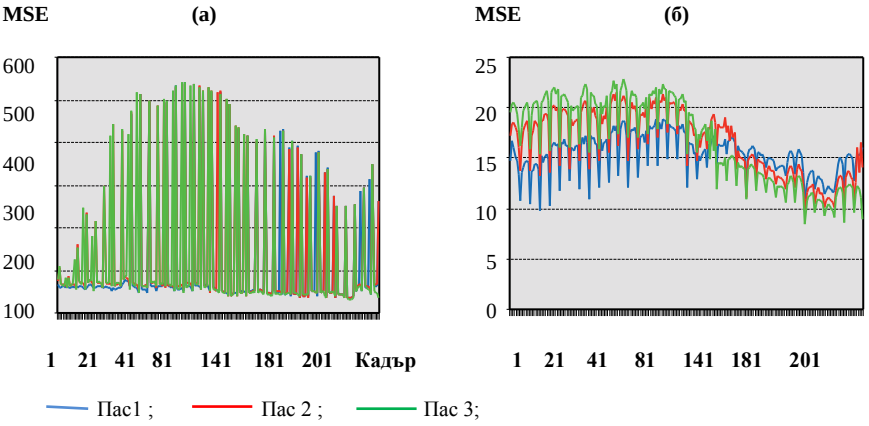
Таблица 1. Стойности на грешката и отношението сигнал/шум при тройно повторение на процеса на компресиране за MPEG-2

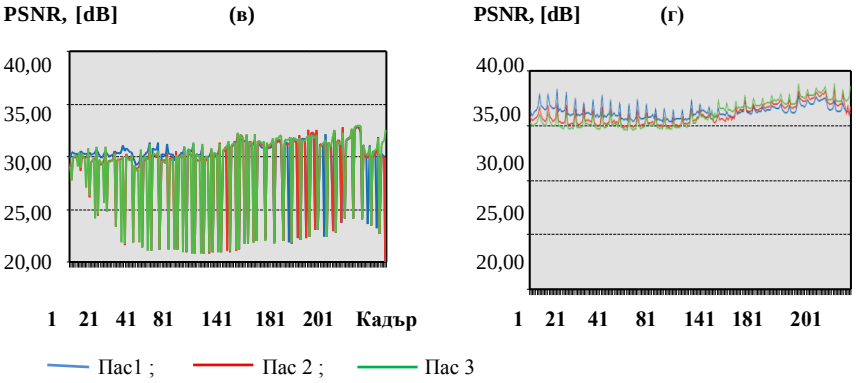
Тестова последователност	Компонент / битова скорост	Номер на повторението (паса)	MSE	PSNR [dB]
„Schumacher“	яркост / 1000 kbps	1	60,8	31,6
		2	69,9	30,6
		3	69,8	30,5
	цветност / 1000 kbps	1	10,6	38,4
		2	12,2	37,8
		3	12,2	37,8
„Concert“	яркост / 1000 kbps	1	113,5	29,3
		2	133,4	28,7
		3	135,6	28,8
	яркост / 4000 kbps	1	15,4	36,3
		2	16,6	36,0
		3	16,7	36,0





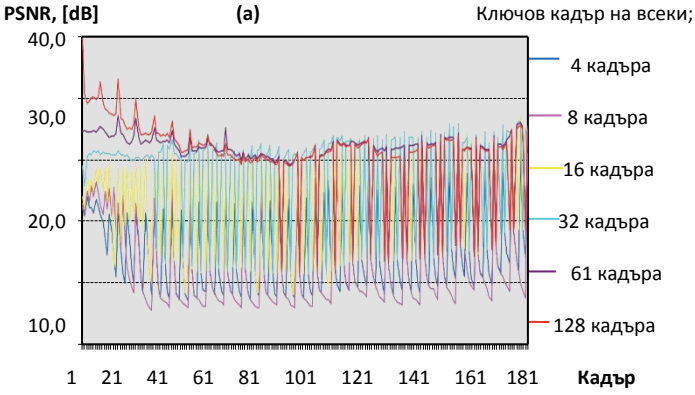
Фиг. 1. Стабилност на MPEG-2 кодера за тестово изображение „Schumacher“ при 1000 kbps и три последователни паса: (а) MSE на яркостта; (б) MSE на цветността; (в) PSNR на яркостта; (г) PSNR на цветността.

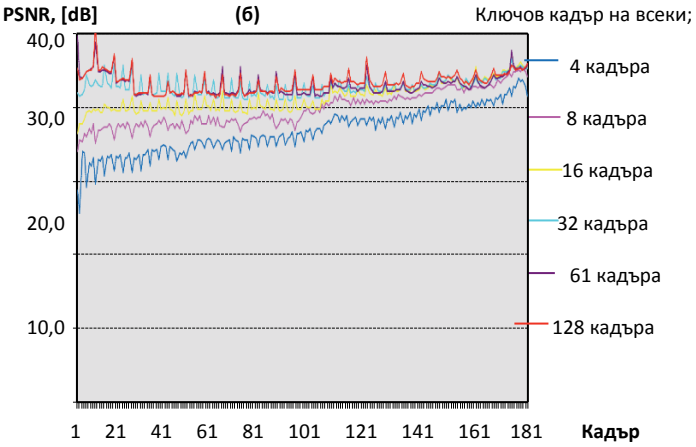


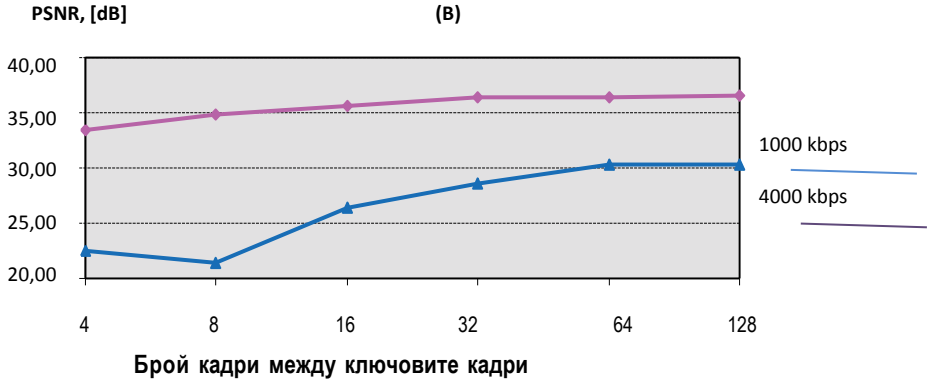


Фиг. 2. Стабилност на MPEG-2 кодера за тестово изображение „Concert“ и три последователни паса: Покадрова оценка на яркостта: (а) MSE при 1000 kbps; (б) MSE при 4000 kbps; (в) PSNR при 1000 kbps; (г) PSNR при 4000 kbps.

На следващо място, е изследвано качеството на компресираното изображение в зависимост от показателя на MPEG-2 – организацията на групата от кадри или честотата на разположение на ключовите кадри във видеопоследователностите. За тази цел две тестови последователности – „Concert“ и „Schumacher“, са компресирани при две различни битови скорости – 1000 kbps и 4000 kbps. Получените експериментални резултати са изобразени графически на фиг.3. и фиг.4. Показано е както покадровото им сравнение при различните битови скорости, така и обобщените резултати за цялата продължителност на тестовите последователности.

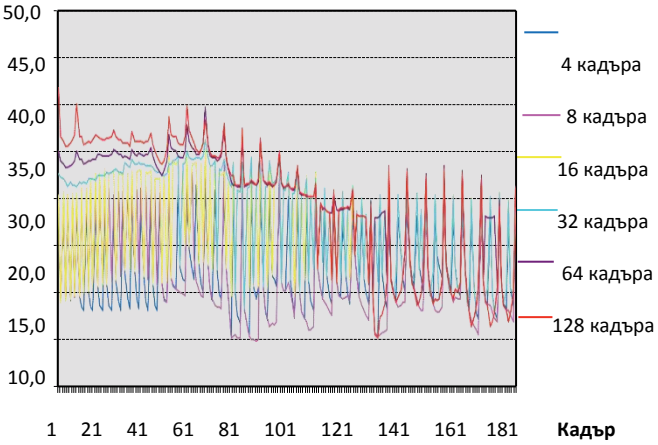




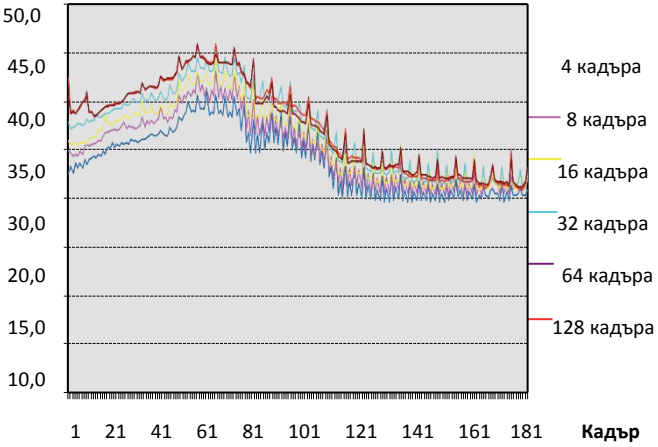


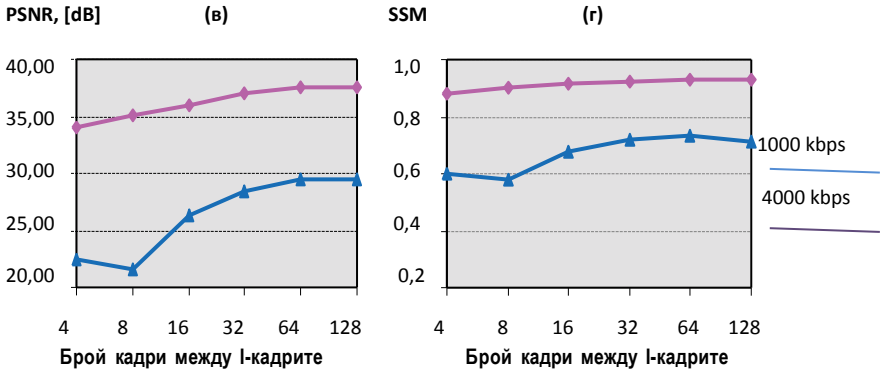
Фиг. 3. Зависимост на качеството на изображението от броя ключови кадри за тестово изображение „Concert“: (а) покадрово при 1000 kbps; (б) покадрово при 4000 kbps; (в) осреднено за цяла видеопоследователност

PSNR, [dB] **(а)** Ключов кадър на всеки;



PSNR, [dB] **(б)** Ключов кадър на всеки;





Фиг. 4. Зависимост на качеството на изображението от броя I-кадри за последователност „Schumacher“: (а) покадрово 1000 kbps; (б) покадрово 4000 kbps; (в) средно за последова- телността, измерено с PSNR; (г) средно за последователността, измерено със SSM.

От показаните графики могат да се направят следните изводи:

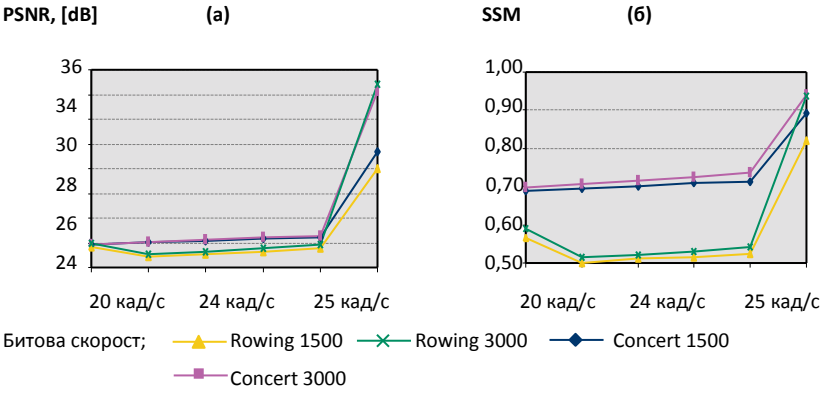
Първо, разликите в качеството между ключовите, предсказаните и двупосочните кадри се увеличава с увеличаване на компресията (намаляване на битовата скорост) и с увеличаване честотата на ключовите кадри (намаляване броя на кадрите между два ключови кадъра

Второ, нарастването на качеството на картината при занижаване броя на ключовите кадри е по-силно изразено при малките битови скорости.

Трето, поради факта, че MPEG-2 е създаден, от една страна, като стандарт за цифрово съхранение на видеоданни при сравнително високи битови скорости и много добро визуално качество, а от друга страна - като стандарт за компресия на видеопоток при разпространение на цифрова телевизия, увеличаването на периода на I-кадрите не може да става неограничено.

Последният извод, който може да се направи, е, че съществува определено разстояние между ключовите кадри, което осигурява максимално качество за тази конкретна видеопоследователност.

Следващият проведен експеримент е с цел оценка на влиянието на честотата на кадрите в една видеопоследователност върху качеството на изображението. Оценката на качеството е направена със статистическата метрика PSNR и метрика SSM (Structural Similarity Metric). Получените графически зависимости са демонстрирани на фиг.5.



Фиг. 5. Зависимост на качеството на изображението от честотата на кадрите за две битови скорости, измерено чрез: (а) PSNR; (б) SSM

От резултатите на фиг. 5. следват няколко извода.

На първо място, това е слабата зависимост на качеството от изходната битова скорост. Основният тип артефакти, възникващи в случай на редуциране на честотата на кадрите, е накъсването на движението, което маскира деградацията на качеството от по-високата степен на компресия. По тази причина следва вторият извод - дори при 24 кад./с следва неточно възстановяване на оригиналната последователност и загубата на качество според използваните метрики. Качеството на изображението почти не зависи от това, с колко е редуцирана кадровата честота в рамките на изследваната такава. Най-важният резултат е в разликата между показанията на двете метрики за видеопоследователността „Concert“ – въпреки неточното възстановяване след редуцирането на честотата на кадрите, измерено от PSNR, поради малката стойност на вектора на движението в тази последователност, самото движение остава плавно, с едва забележими накъсвания. Това е отчетено от SSM, която измерва по-слаба деградация в качеството спрямо последователността „Rowing“, където поради високата стойност на вектора на движение, след понижаване честотата на кадрите движението става силно насечено и дразнещо наблюдателите.

ЛИТЕРАТУРА:

1. Претт, У. Цифрова обработка изображений т.Л., М., Мир 1998
2. Беноа, Е. „Цифрова телевизия & MPEG-1, MPEG-2. Принципи на системата DVB. С., Лик 2001.
3. Бекярски, Ал. Телевизионни системи. Издателство на ТУ-София, 2009
4. J. De Lamellieure and R. Schater, “MPEG-2 Image Coding for Digital TV” Frenseh and Kino Techinik, K. Jahrgang, pp. 99-107, March 1994 German
5. Peter, D. Symes – Video Compression McGraw – Hill Professional 1998

СТУДЕНТСКО-ДОКТОРАНТСКА СЕКЦИЯ

АДМИНИСТРАТИВНОПРАВЕН РЕЖИМ НА ДОСТЪПА ДО ОБЩЕСТВЕНА ИНФОРМАЦИЯ

Е. Ю. Кузманова, З. Ю. Кузманов

Национален военен университет „Васил Левски“,
Факултет „Артилерия, ПВО и КИС“, Шумен

ADMINISTRATIVE MODE OF ACCESS TO PUBLIC INFORMATION

Elitsa Y. Kuzmanova, Zdravko Y. Kuzmanov

ABSTRACT: *The report addressed issues of information resources in the context of national security, the principles of access to information and their influence in the national security system, legislation on access to information and specific administrative law regime of access to information legislation and its application.*

KEYWORDS: *national security, information, information resources, access to information, administrative law regime*

Правото на достъп до информация е признато като основно човешко право от Интерамериканския съд за човешки права, от Европейския съд за правата на човека, Комитета по човешки права на Обединените нации и редица други международни организации. Към момента 97 държави имат действащи закони, според рейтинга на законите за достъп до информация.

Прилагането на тези закони в Република България също има богата практика. Първото заявление за достъп е подадено само седмица след влизането на закона в сила. За тези години са подадени 336 603 заявление, от които средно 11 660 писмени на година. Списъкът на съдебните актове на Върховния административен съд по Закона за достъпа до обществена информация е впечатляващ – 1616 акта.

През годините се променят и административните практики, променят се заявителите, променило се е отношението и познаването на правото на достъп до информация от гражданите.

Хората от протестите в България от 2013 година искаха прозрачност и отчетност на управляващите и ясни механизми за гражданско участие във формирането на политики.

В доклада са разгледани въпросите за информационните ресурси в контекста на националната сигурност, принципите на достъпа до информация и тяхното влияние в системата за национална сигурност, законодателството в областта на достъпа до

информация и конкретния административноправен режим на достъпа до информация с неговото законодателство и приложение.

В края на XX и началото на XXI век на преден план в развитието на държавите и тяхната национална сигурност излиза една нова категория ресурси, възникнала от древни времена и преминала през шест фази докато достигне днешния си облик - информационните ресурси (ИР). На практика до последната четвърт на XX век ИР не се разглеждат от позицията на социално значима икономическа или друга категория, оказващи влияние върху състоянието и развитието на страните, а се обръща внимание предимно на културното наследство на една или друга нация или държава. Към настоящия момент, в ера на пост-индустриалното развитие на обществото. По своята ефективност на използване, значение, полезност и степен на значимост ИР играят все по-важна роля и се разглеждат като приоритетни стратегически ресурси, съизмерими с материалните и енергийни ресурси.

Информационните ресурси представляват индивидуални и колективни експертни знания, отделни документи, отделни масиви документи, както и документи и техните масиви, които изграждат бази данни, бази знания, библиотеки, архиви, фондове, информационни системи и други системи в определена предметна и тематична област, които удовлетворяват функционалните потребности и изисквания на потребителите на информация.

В случай, че информацията пресича държавните граници и се използва на международно и междунационално ниво, се говори за световни информационни ресурси.

За класификацията на ИР и тяхното разбиване на видове и категории, могат да се използват множество разнообразни признаци. Най-общия от тях, който не изисква анализ на семантичени, синтактични и прагматични образуващи е форма или запис на информацията, според който информационните ресурси се делят на документирани и недокументирани. По признак на тематична принадлежност, ИР могат да се разделят на множество тематични области и подобласти на знанието.

Фиг. 1. Класификация на информационните ресурси.

В основата на информационните ресурси стои информацията. Понятието „информация“ произхожда от латинското „informatio“ и означава опознаване, разсяснение, представяне. В науката няма общо приета дефиниция на понятоето инфор-

мация, тъй като то се използва във почти всички науки и всяка от тях го използва в контекста на своята тематика. Реално погледнато информацията е отражение на обективната реалност.

В контекста на националната сигурност, тя се проявява при функционирането на високоорганизираната система, която е способна самостоятелно да развива и запазва своята дейност. Тя представлява съдържанието на сигналите, носещи сведения за външната среда и вътрешното състояние на системата, и на тези, необходими на системата при избора на поведение, осигуряващо нейното съществуване и развитие. От тук става ясно защо е необходим контрол над достъпа на информация и над съответните информационни ресурси.

Една от основните цели на системата за национална сигурност е да се постигне състояние, при което не съществуват заплахи за жизненоважните интереси на нацията и правата на гражданите. Съгласно Конституцията едно от основните права на гражданите е правото на достъп до информация. [1]

Правото на информация е гарантирано от Конституцията, Закона за достъп до обществена информация, Закона за опазване на околната среда, Закона за защита на класифицираната информация и редица други специални закони:

- Закон за достъп до обществена информация;
- Заповед ЗМФ № 1472 от 29 ноември 2011 г. за актуализация на нормативите за разходите по предоставяне на обществена информация;
- Конвенция за достъп до информация, участие на обществеността в процеса на взимане на решения и достъп до правосъдие по екологични въпроси (Орхуска конвенция), ратифицирана от България със закон, приет от Народното събрание на 2 октомври 2003 г. и в сила от 16 март 2004 г.;
- Закон за защита на личните данни;
- Закон за защита на класифицираната информация;
- Списък на категориите информация, подлежаща на класификация като държавна тайна приложение 1 към чл. 25 от ЗЗКИ;
- Служебна тайна Извлечение от нормативни актове, в които се споменава института на служебната тайна в Република България;
- Наредба за общите изисквания за гарантиране на индустриалната сигурност приета с ПМС 51/4.03.2003 г.;
- Наредба за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване приета с ПМС 52/4.03.2003 г.;
- Наредба за реда за извършване на проверките за осъществяване на пряк контрол по защита на класифицираната информация приета с ПМС 44/21.02.2003 г. и др.

Законът за достъп до обществена информация (ЗДОИ) е обнародван в брой 55 на Държавен вестник от 7 юли 2000 г. Такъв закон се приема за първи път в България. Дотогава гражданите имат регламентиран достъп само до информацията, която се съдържа в публичните регистри и до информацията, свързана с околната среда. Подобни закони съществуват в повечето демократични държави. Те улесняват всеки гражданин или юридическо лице в търсенето на информация, тъй като с тях се дава достъп до най-богатата съществуваща база данни - тази на държавата.

Последните съществени изменения в ЗДОИ са обнародвани в бр. 104 на Държавен вестник от 5 декември 2008 г.

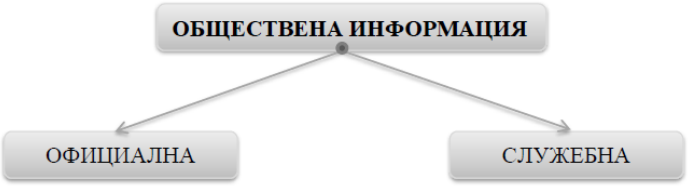
Промените са консултирани с ПДИ (Програма за достъп до информация) и са в съответствие с нейния анализ, представян няколко години поред в годишните доклади за състоянието на достъпа до информация в България. Измененията са резултат от обединение на два законопроекта за изменение и допълнение на ЗДОИ. Като цяло те отговарят както на проблемите, срещани в реалното прилагане на закона, така и на международните стандарти в тази област.

Нормативите за разходите по предоставяне на обществена информация са определени със Заповед ЗМФ № 1472 от 29 ноември 2011 г. за актуализация на нормативите за разходите по предоставяне на обществена информация, обнародвана в ДВ бр. 98 от 13.12.2011 г., която отменя Заповед № 10 на МФ от 10.01.2001 г. за определяне нормативи за разходите при предоставяне на обществена информация по Закона за достъп до обществената информация според вида на носителя публикувана в Държавен вестник на 07.07.2000 г., обнародвана в ДВ бр. 98 от 13.12.2011 г.

Целта на Закона за достъп до обществена информация (ЗДОИ) е регламентиране на условията и реда за осъществяване на конституционното право на гражданите да търсят и получават информация относно обществения живот в Република България. Ефективното упражняване на това право дава възможност на членовете на обществото да си съставят собствено мнение за дейността както на органите на държавната власт, така и на други субекти, чиято дейност има обществен характер. Регламентацията на достъпа до информация е елемент от общата уредба на информационните права на гражданите и създава нормативна основа за регламентиране и на редица свързани с него обществени отношения - защита на личната информация, определяне на съдържанието, обхвата, условията и реда за създаване и за работата със защитена информация. [1]

Обществената информация представлява всяка информация, свързана с обществения живот в Република България и даваща възможност на гражданите да си съставят собствено мнение относно дейността на задължените по закона субекти, независимо от вида на нейния материален носител. Тя може да бъде обективирана върху хартиен, електронен или друг носител, включително съхранена като звукозапис или видеозапис, и събрана или създадена от организация от обществения сектор. [1]

Съгласно ЗДОИ се съществуват два вида обществена информация: официална и служебна.



Фиг. 2. Видове обществена информация.

Официална е информацията, която се съдържа в актовете на държавните органи и на органите на местното самоуправление при осъществяване на техните правомощия. [1]

Официална обществена информация представляват нормативните актове на държавните органи като Конституцията, различни кодекси и закони, постановления на МС, правилници, наредби и инструкции, както и ненормативни актове като заповеди и решения.

Служебна е информацията, която се събира, създава и съхранява във връзка с официалната информация, както и по повод дейността на органите и на техните администрации. Достъпът до служебна обществена информация може да бъде ограничен, когато тя е свързана с оперативната подготовка на актовете на органите и няма самостоятелно значение (мнения и препоръки, изготвени от или за органа, становища и консултации). [1]

Служебната информация може да представлява такава информация, която е създавана и съхранявана във връзка с официалната информация или такава по повод дейността на органите и техните администрации.

ЗДОИ дава право на достъп до обществена информация на всеки български или чужд гражданин, както и на лица без гражданство и юридически лица, регистрирани на или извън територията на Република България. Конкретното лице може да поиска и получи достъп до информация, без да е необходимо да доказва конкретен интерес. [1]

Законът не поставя никакви ограничения по отношение на заявителите. Това положение е напълно съобразено с международните стандарти за достъпа до информация/достъпа до документи, в които е залегнал принципът, че информацията, създавана и съхранявана от държавата, е достъпна за всеки.

Осъществяването на това право не може да бъде насочено срещу правата и доброто име на другите граждани, както и срещу националната сигурност, обществения ред, народното здраве и морала.

Право на достъп до обществена информация имат дори неправносубектни организации на граждани. Те могат да търсят и искат информация без да е необходимо да доказват своята правосубектност.

Обществената информация се създава и/или съхранява от държавните органи от трите власти, техните териториални звена и органите на местно самоуправление в Република България. Също така тя може да бъде създадена и съхранена от публичноправни субекти, различни от официалните, включително публичноправните организации и физически и юридически лица само относно извършваната от тях дейност, финансирана със средства от консолидирания държавен бюджет и средства от фондовете на Европейския съюз или предоставени от Европейския съюз по проекти и програми. [1]

Организациите от обществения сектор са длъжни да предоставят обществена информация, когато тя е поискана по установения законен ред, както и да я предоставят за нейното повторно използване. Осъществяването на правото на достъп до обществена информация и на повторно използване на информация от обществения сектор не може да бъде насочено срещу правата и доброто име на други лица, както и срещу националната сигурност, обществения ред, здравето на гражданите и морала.

Публичноправните организации са юридически лица, създадени за задоволяване на обществените интереси. За тях характерното е че над 50% от приходите им са от публичен източник (30% лечебни заведения), над 50% от управителния/контролен орган е определен от възложител на обществена поръчка и самата организация е обект на управленски контрол от възложител на обществена поръчка.

При предоставянето на обществена информация, органите се ръководят от редица основни принципи. Основните принципи при осъществяване правото на достъп до обществена информация са: [1]

- откритост - правото е принцип, ограничението - изключение (РКС номер 7 от 4 юни 1996 г.);
- достоверност - достъп до оригинални документи;
- пълнота на информацията - ограничение е допустимо само при засягане на права или законни интереси;
- осигуряване на еднакви условия за достъп до обществена информация;
- осигуряване на законност при търсенето и получаването на обществена информация;
- защита на правото на информация;
- защита на личната информация;
- гарантиране на сигурността на обществото и държавата.

Основните принципи при предоставяне на информация от обществения сектор за повторно използване са:

- осигуряване на възможност за многократно повторно използване на информация от обществения сектор;
- прозрачност при предоставяне на информация от обществения сектор;
- забрана за дискриминация при предоставяне на информация от обществения сектор;
- забрана за ограничаване на свободната конкуренция.

Органите информират за своята дейност чрез публикуване или съобщаване в друга форма. Те са длъжни да съобщават информация, събрана или станала им известна при осъществяване на тяхната дейност, когато тази информация може да предотврати заплаха за живота, здравето и безопасността на гражданите или на тяхното имущество, опровергава разпространена недостоверна информация, засягаща значими обществени интереси; представлява или би представлявала обществен интерес или следва да бъде изготвена или предоставена по силата на закон. [1]

С цел осигуряване на прозрачност в дейността на администрацията и за максимално улесняване на достъпа до обществена информация всеки ръководител на административна структура в системата на изпълнителната власт периодично публикува актуална информация, съдържаща:

- описание на неговите правомощия и данни за организацията, функциите и отговорностите на ръководената от него администрация;
- списък на издадените актове в изпълнение на неговите правомощия;
- описание на информационните масиви и ресурси, използвани от съответната администрация;

- наименованието, адреса, телефона и работното време на звеното в съответната администрация, което отговаря за приемането на заявленията за предоставяне на достъп до информация.

Всеки ръководител изготвя годишен отчет за постъпилите заявления за достъп до обществена информация, който включва и данни за направените откази и причините за това. Годишният отчет е част от ежегодните доклади по чл. 62, ал. 1 от Закона за администрацията.

Информацията се публикува на интернет страниците на административните структури в системата на изпълнителната власт, както и се включва в доклада за състоянието на администрацията, който се приема от Министерския съвет, като по този начин звеното се отчита.

Осъществяването на правото на достъп до обществена информация и на повторно използване на информация от обществения сектор не може да бъде насочено срещу правата и доброто име на други лица, както и срещу националната сигурност, обществения ред, здравето на гражданите и морала. Поради тази причина съществуват определени ограничения, които са свързани със защитени интереси в областта на националната сигурност. [1]

Не се дава достъп до информация, която засяга националната сигурност, отбраната, външната политика и конституционния ред. Такива са държавните и служебни тайни (по Закон за защита на обществената информация), консултативните процеси или преговори (по ЗДОИ), следствените тайни (Наказателнопроцесуален кодекс), текущи преговори или информация за трето лице - търговски тайни, защита на частна собственост или лична информация (Закон за защита на личната информация).

Дори когато съществува основание за отказ, информация трябва да се предостави, ако е налице т.нар. „надделяващ обществен интерес“ от узнаването ѝ. Според закона надделяващият обществен интерес трябва да се преценява при следните ограничения: защита на трети лица - лични данни; защита на трети лица - търговска тайна; защита на оперативната подготовка на актовете - чл. 13, ал. 2, т. 1 от ЗДОИ; защита на текущи или предстоящи преговори.

Надделяващ обществен интерес е винаги налице, когато чрез исканата информация се цели разкриване на корупция и на злоупотреба с власт, повишаване на прозрачността и отчетността на институциите и лицата, длъжни да предоставят обществена информация.

Информация от надделяващ обществен интерес може да бъде публикувана от самите институции без поискване – например така са публикувани в интернет декларациите по Закона за публичност на имуществото на лицата, заемащи висши държавни длъжности, и по Закона за предотвратяване и разкриване на конфликт на интереси. В други случаи балансът трябва да се извършва от администрацията при подадено заявление - това са най-често случаите на обществени дебати, разкриване на случаи на лошо управление и корупция и др.

Понякога исканите документи или папки с документи могат да съдържат части, достъпът до които е ограничен.

В тези случаи се предоставя т.нар. „частичен достъп до информация“, което означава, че ограничените за достъп части се заличават, а останалата част от документа се предоставя. Типичен пример е достъпът до документи, в които се съдър-

жат и лични данни. В този случай думите или пасажите, които разкриват лични данни се зачернят и се предоставя копие от документа без тези данни. [1]

Искането за информация може да бъде устно запитване или писмено заявление. Могат да се използват и двата начина.

Съгласно закона в рамките на всяка институция трябва да са определени длъжностни лица, които да отговарят пряко за предоставянето на обществена информация. Най-често информация за наименованието, адреса, телефона и работното време на приемащите заявления за достъп до информация може да се открие на интернет страницата на институцията.

Друг вариант за това е да се осъществи контакт с пресцентъра, деловодство или приемната на институцията, с цел установяване към кой служител да се отправи искането за информация. [4]

Служителят трябва да разгледа въпроса, от който се интересува лицето, което иска достъпа до информация в конкретна форма: устна справка; преглед и прочит на търсената информация; копия на хартиен или технически носител.

Служителят е длъжен да предостави информацията веднага, ако това е възможно. В случай на отказ информацията се иска в писмен вид. [4]

Писменото искане на достъп до информация е във вид на заявление. То може да бъде в свободен текст, написано на ръка или компютър. Задължително трябва да съдържа: [1]

- трите имена на лицето (за юридически лица - наименование и седалище);
- каква информация иска да получи лицето;
- точните документи, от които се интересува лицето, вид, номер и дата на издаване;
- описание по адресата на заповедтта и органа, който я е издал (не е нужно да се знаят подробности за документа, достатъчно е да се знае, че документът се идентифицира недвусмислено);
- адрес на кореспонденция;
- телефонен номер и/или адрес;
- предпочитана форма, в която да се предостави информацията (не е задължително).

Не е законно да се искат:

- ЕГН на физическите лице;
- Номер, дата на издаване на документ за самоличност за физически лица;
- Представяне на документ за самоличност;
- Актуално състояние за юридически лица;
- Данъчен номер и БУЛСТАТ за юридически лица;
- В качеството си на какъв лицето иска информацията;
- За какво ще се използва исканата информация;
- Има ли лицето правен интерес да получи исканата информация.

Съгласно ЗДОИ достъп до информация може да се получи в няколко различни форми. [1] Лицето само определя в какво форма може да му бъде предоставена исканата информация и съответната институция е длъжна да се съобрази с предпочитанието. Може да се поиска:

- устна справка;
- на място да се прегледа цялата налична информация;
- да се направи копие на хартия или технически носител.

Лицето може да иска информацията да му бъде представена в няколко форми. За да се спестят средства, лицето може да се поиска първо да прегледа и прочете информацията, а след това да избере на кои документи точно да поиска копие.

Съгласно ЗДОИ във всяка една институция следва да има подходящо място за четене на предоставената информация. Служителите са длъжни да предоставят информация в желаната форма, освен в случаите, когато за това няма техническа възможност, свързано е с необосновано увеличаване на разходите или води до възможност за неправомерна обработка на тази информация/нарушаване на авторски права.

Заявлението може да се подаде на място в съответната институция или да се изпрати по пощата с обратна разписка. [3]

Отговор на заявлението за информация трябва да се получи задължително до 14 календарни дни от неговото подаване. Исканата информация се предоставя с решение на съответната институция. [4]

Възможно е преди институцията да вземе решение по заявлението лицето да получи някое от следните уведомления:

- Уведомление за уточняване на искането. Възможно е този, от когото се търси информация, да поиска уточните каква точно информация е нужна. Това може да се случи, когато е описано прекалено общо исканата информация - напр. „Искам информация относно задграничните командировки във вашата институция“. Получаването на подобно уведомление, не означава, че трябва да се посочи конкретна заповед за командировки. Необходимо е конкретизиране на питането, като се посочи определен/и служител/и, за чиито пътувания се интересува лицето. Може да се фиксира и период от време, за който се търси тази информация.

Уточняването трябва да се направи до 30 календарни дни, след като се получи уведомлението за това. Ако лицето пропусне да го направи, заявлението за достъп до информация се оставя без разглеждане.

След уточняване на точно каква информация се иска, трябва да се изчака нови 14 дни за отговор. [4]

- Уведомление за удължаване на срока. Причината за това може да бъде:

1. За предоставяне на исканата от информация е необходимо съгласието на трето лице. Такова съгласие не следва да се иска , ако третото лице също е задължен по закона субект (чл. 31, ал. 5). Удължаването на този срок не може да е повече от 14 календарни дни (или общо 28 календарни дни от подаване на заявлението).
2. Исканата информация е в голямо количество и е необходимо повече време за нейното събиране и подготвяне. Удължаването на срока не може да е повече от 10 дни (или общо 24 дни от подаване на заявлението).

В уведомлението за удължаване на срока непременно трябва да са посочени причините за удължаването и крайният срок, в който ще бъде предоставена информацията. [4]

- Уведомление за препращане на искането. Възможно е този, от когото се търси информация, да не разполага с нея, но да има данни за нейното местонахождение. В този случай той е задължен да препрати заявлението към институцията, в която се намира исканата информация. Няма нужда да се подава ново заявление. Срокът за получаване на решение тече от датата, на която е получено уведомлението за препращане. В уведомлението за препращане задължително трябва да са посочени наименованието и адресът на съответната институция. [4]

В случаите, когато няма пречки за предоставяне на исканата информация, следва да се получи решение за предоставяне на достъп до информация. [3]

В решението съответната институция трябва да е посочила:

- до каква информация се предоставя достъп;
- в какъв период от време може да се получи достъп до информацията (не може да бъде по-кратък от 30 дни);
- къде се предоставя достъп до информацията;
- формата, в която се предоставя достъп;
- каква сума трябва да се заплати.

Ако се пропусне определения в решението 30-дневен срок за достъп или не се заплати определената сума, може да се загуби правото на достъп, предоставен със съответното решение. В такъв случай е възможно да се подаде отново заявление за същата информация, но може да бъде отказано нейното предоставяне до изтичането на 6 месеца. [3]

Съгласно закона се заплащат само разходите по копиране на документацията върху хартиен или технически носител. Това става по нормативи, определени от Министъра на финансите. [3]

За да се получи информацията, предоставена с решението за достъп, следва да се заплати посочената в него сума и да представите съответния платежен документ.

При получаване на исканата информация се подписва протокол, който съдържа описание на предоставените документи. Понякога, ако информацията е малка по обем, тя се изпраща по пощата, заедно с решението за нейното предоставяне.

В случай, че исканата информация или част от нея следва да бъде ограничена за достъп, се изготвя решение за отказ на достъп до информация.

Отказът трябва да се направи с решение, което се изпраща по пощата или се предоставя срещу подпис. В решението трябва да е посочено:

- фактическото основание за отказа - то представлява описание на това кой, кога, каква информация е поискал, какви действия е предприела институцията и до какви заключения по случая е достигнала относно защитените права и интереси;
- правното основание - това е разпоредбата от съответния нормативен акт, в която е посочено основанието за отказ;
- датата на приемане на решението;
- пред кого и в какъв срок се обжалва решението.

Възможно е също така да се получи решение, в което се предоставя достъп до част от поисканата информация, така наречения частичен достъп.

Всяко решение по заявлението за достъп до информация може да се обжалва пред компетентния съд, тъй като законът не предвижда обжалване пред по- висшестоящ орган.

Трябва да се провери посочени ли са в решението мотиви за отказа. Задължително е да са посочени причините, както и законовата разпоредба, въз основа на които е взето решението за отказ. В противен случай решението е незаконосъобразно.

При отказ от достъп до информация лицето може да обжалва. [3]

Достъпът до информация е основно човешко право, легитимирано както от редица Европейски органи и организации, така и от българското законодателство. То се защитава от системата за национална сигурност (СНС) в лицето на органите за управление от трите власти. С оглед опазването на националната сигурност и поддържане и регулиране на вътрешния държавен ред се налага контролиране на достъпа до информация. За тази цел е създадена система от законодателство, което е активно и действа вече над 15 години. Предоставянето на информация от обществения сектор се извършва по строго определен от закона (ЗДОИ) ред, който се спазва както от задължителните субекти - органите на управление и техните териториални звена и администрации, така и от гражданите и физическите лица.

Чрез закона се регламентират условията и реда за осъществяване на конституционното право на гражданите да търсят и получават информация относно обществения живот в Република България. Ефективното упражняване на това право дава възможност на членовете на обществото да си съставят собствено мнение за дейността както на органите на държавната власт, така и на други субекти, чиято дейност има обществен характер.

Към днешна дата е необходимо да се стартира един необходим дебат за промени в регулацията на правото на достъп до информация. Необходимо е ясно разбиране, че това не е само право на административна услуга по подадени заявления, а основно конституционно право на човека. Гражданинът в демократичното общество трябва да знае как бива управляван, как се взимат решения, как се разходват обществени средства, кой носи отговорност за случващото се. Само при тези условия гражданите могат равнопоставено да участват в дебата за обществените политики.

ЛИТЕРАТУРА:

1. Закон за достъп до обществената информация. Обн. ДВ. бр.55 от 7 Юли 2000 г., изм. ДВ. бр.39 от 20 Май 2011 г.

2. Жулева, Г. и колетив. Състоянието на достъпа до информация през 2013 г. София : Програма достъп до информация, 2014.

3. Жулева, Г. Новите стандарти в достъпа до информация. София : Програма достъп до информация, 2010.

4. Как да получим достъп до информация? Програма за достъп до информация. [Online] [Cited: Април 20, 2015.] http://www.aip-bg.org.

ЗА РАЗУЗНАВАТЕЛНАТА И ОПЕРАТИВНО-ИЗДИРВАТЕЛНАТА ДЕЙНОСТ В КОНТЕКСТА НА СИСТЕМАТА ЗА НАЦИОНАЛНА СИГУРНОСТ

Елица Ю. Кузманова, Здравко Ю. Кузманов

Национален военен университет „Васил Левски“,
Факултет „Артилерия, ПВО и КИС“, Шумен

INTELLIGENCE AND OPERATIONAL TECHNIQUES IN THE CONTEXT OF THE SYSTEM OF NATIONAL SECURITY

Elitsa Y. Kuzmanova, Zdravko Y. Kuzmanov

ABSTRACT: *The report deals with issues of intelligence and operational-search activities in the context of the system of national security, intelligence and its place in national security, legal regulation and control of operational-search activities.*

KEYWORDS: *national security, intelligence, operational techniques*

Понятието „национална сигурност“ е легално дефинирано в Република България през 2002 г. с §1, т. 13 от Допълнителните разпоредби на Закона за защита на класифицираната информация като „състояние на обществото и държавата, при което са защитени основните права и свободи на човека и гражданина, териториалната цялост, независимостта и суверенитетът на страната и е гарантирано демократичното функциониране на държавата и гражданските институции, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива“. Възможно е това да е една добра юридическа дефиниция. Но съдържателно тя фиксира националната сигурност като състояние, т.е. нещо статично и моментно, при това недефинирано и неутрално по отношение на субекта на сигурността и затова на практика не може да бъде база за разкриване на причинно-следствените връзки, т.е. за анализ. [2]

Националната сигурност най-кратко може да се определи чрез способността на държавата да реализира националните интереси или да ги защити ефективно. В този смисъл тя е баланс на дефинираните национални интереси и ресурсния потенциал, който ги обслужва и защитава.

С цел постигането на националната сигурност освен общата политическа и нормативна рамка се организира съвкупност от институции и служби, които да извършват необходимите действия и дейности за гарантирането и. Тя съставлява системата за националната сигурност (СНС). СНС се изгражда на четири нива на компетентност, със също толкова нива на структуриране на институциите и службите.

Развитието на държавността (респективно усложняването и бюрократизирането на административните дейности), увеличаването на броя на субектите и активизирането на международните отношения, както и усъвършенстването на комуника-

циите, транспорта и международния обмен налагат създаването на държавни органи със специални компетенции в областта на:

- добиването на информация в интерес на националната сигурност;
- анализа на информацията с цел оптималност (или поне адекватност) на политическите действия на държавата спрямо външните и вътрешните условия;
- защита на собствените тайни;
- извършването на действия за реализация на националния интерес, без да се разкрива причастността на държавата.

Тази последна група държавни органи за стратегическа информация в сферата на националната сигурност, използващи тайни методи и средства (обособени или не в самостоятелната подсистема информационен сегмент на СНС), в отделните страни са с различно родово наименование – специални, секретни, тайни, разузнавателни служби, които в настоящия доклад ще бъдат използвани като синоними. [2]

Защитата на националната сигурност е основна функция на държавата. Като цяло тя се осъществява от нейните законодателни, изпълнително-разпоредителни и съдебни органи в рамките на тяхната компетентност и в съответствие с възложените им функции и предоставените им сили, средства и методи на дейност.

Разузнавателните и контраразузнавателните служби са част от държавния механизъм, които са специално създадени и предназначени за опазване на националната сигурност. Подчинени на тази обща цел – да защитават националната сигурност и не допускат нанасянето и на вреди, те имат своите особености в конкретните задачи и дейност, които ги отличават и обособяват във функционално, структурно, организационно и тактическо отношение. [3]

Както често (особено у нас) се случва с темите и проблемите – обект на активен медиен и обществен интерес, разузнавателните дейности, осъществяващите ги органи, организацията и мястото им в СНС са обект на интерпретации и спекулации в широк диапазон. Принос за това имат и бившите, и действащите професионалисти и изкривените понятия (привнесената и адаптираната лексика и жаргон, жертва на некоректен превод или стремеж за оригиналност). На дневен ред са уточняването и стандартизирането на понятийния апарат в областта на специалните служби и оперативните разузнавателни дисциплини.

Под разузнавателни (специални, секретни) служби се разбира на първо място държавни органи със стратегическа функция и специална оторизация за дейност в информационната сфера на защитата на националната сигурност. Следователно първият диференциращ признак на разузнавателните органи са стратегическата насоченост, обхватът на дейността и особено – ценностите и интересите (вече определени като национална сигурност), за реализацията и защитата на които те са създадени. Втората разграничителна линия преминава през обекта и изпълняваните задачи. Всяко правителство се нуждае от информация за чуждите интереси, които в даден момент могат пряко или косвено да повлияят по някакъв начин или да попречат за реализацията на националния интерес, както и на плановете за постигането му. В този смисъл разузнавателната дейност в сферата на сигурността има за цел да постигне стратегическо превъзходство над обектите на наблюдение и въздействие. Става дума за особен вид дейност, стояща по много свои елементи някъде

между дипломацията и войната. За извършването и правителството се нуждае от органи, специализирани в придобиването на чужда информация и в опазването на собствената, узнаването на която поради спецификата и може да увреди националния интерес. Следователно то се нуждае от разузнаване, чиито функции са: [3]

- добиване на информация със специални методи и средства;
- дезинформиране на противника, неутрализиране на неговите агенти;
- дискредитиране или унищожаване на негови ключови лица;
- действия по „стимулиране“ на промени във властта в дадена страна.

В науката съществуват множество понятия за разузнаване. Според „Речник на американските военни термини“ разузнаването е процесът на придобиване, интегриране, интерпретиране и анализ на цялата актуална и потенциално интересна информация, необходима за процеса на планирането на отношението към чужди държави, обекти и области на действие. Съществуват още хиляди дефиниции за разузнаването, част от които принадлежат на български специалисти в областта. Според Българския тълковен речник (С., 1963) разузнаването представлява „проучването на определен обект, най-вече неприятелски фронт“. Пак според него да разузнаваш значи да разучаваш какво има наоколо. Според Българската енциклопедия (С., 2002) разузнаването е военно понятие, което означава „вид бойно, оперативно и стратегическо осигуряване на войските чрез събиране на сведения за въоръжените сили на противника, местността и други за успешното водене на боя и операцията. Бива стратегическо, оперативно и тактическо, въздушно, морско техническо специално, агентурно и космическо“. Реално е това понятие, което се използва в почти всяка сфера на обществено-политическия, икономическия, социалния, научния и личния живот на хората. Това е така, защото неговото обяснение ще зависи от това кой и защо го извършва. [3]

Изхождайки от позициите на държавното разузнаване, в понятието разузнаване могат да се включат два основни елемента.

Първият, това са специализираните служби, които са създадени от всяка държава за събиране и анализиране на политическа, военна, икономическа и научно-техническа информация за чужди страни, организации и граждани и за провеждане на тайни операции. Това са т.нар. сили на разузнаването, които включват кадровите служители, а също и извънщатни такива. Всички те имат определени права и задължения, определени от законите.

Вторият елемент на това понятие обхваща специфичната дейност на тези служби, наричана разузнавателна, чиято цел е да се защитава националната сигурност. Тя има три основни функции:

- Да събира информация от политически, военен, икономически и научно-технически характер, касаеща чужда страна, организация, група, конкретно лице;
- Да обработва и анализира събраната от различни секретни и открити източници информация;
- Да извършва тайни операции в чужди страни.

Изпълнението на тези три основни функции се осъществява чрез използването на специфични средства (агенти, технически средства) и методи (комбинация,

проникване, дезинформиране), а самата дейност се извършва в рамките на работа по обекти за оперативно проникване и организиране на тайни операции.

Тази кратка характеристика на разузнаването показва, че неговата същност може да бъда разкрита като един процес (цикъл), обхващащ в себе си пет основни момента: получаване на задачата, събиране на първична информация, обработка на първична информация, анализ на обработената информация и разпространение на анализираната информация. Една от основните функции на разузнавателната дейност е оперативно-издирвателната дейност. [4]

Оперативно-издирвателната дейност представлява дейност, която цели да се защити националната сигурност и общественият ред в Република България от престъпни посегателства. [4]

Контраразузнавателните и полицейските служби в България са основните субекти, имащи право да извършват оперативно-издирвателна дейност. Основната цел на тази дейност е опазване на националната сигурност и обществения ред, създаден в Република България въз основа на Конституцията и съответните закони, като не се допусне извършването на престъпления и нарушения срещу тях. Особеното, специфичното в дейността на оперативно-издирвателните служби е, че те имат правомощията да използват специфичните средства, методи и форми на тази дейност за постигането на горната цел. В рамките на тази дейност , както вече се бе споменато, оперативно-издирвателните служби разкриват, предотвратяват и пресичат престъпления и нарушения, извършвани срещу националната сигурност и обществения ред, а също подпомагат наказателното и административното производство.

Организацията на оперативно-издирвателната дейност е различна в отделните страни. Като цяло има два варианта – контраразузнавателните и полицейските служби да бъдат в рамките на едно ведомство (например ФБР в САЩ), или пък да бъдат в рамките на отделни ведомства (Федерална служба за сигурност в Русия). В България, в различни периоди от нейното развитие, са използвани и двата варианта на организация. Понастоящем в нашата страна съществуват три държавни служби, които извършват оперативно-издирвателна дейност. Едната е Държавна агенция „Национална сигурност“, която има за основна задача да разкрива, предотвратява и пресича престъпления и нарушения, нанасящи вреди на националната сигурност. Другата е Министерството на вътрешните работи (МВР), което има за основна задача да разкрива, предотвратява и пресича престъпления и нарушения, засягащи установения обществен ред в страната. И третата служба е „Военна полиция“ към Министерството на отбраната, която има за основна задача да разкрива, предотвратява и пресича престъпления от общ характер, нанасящи вреда на реда и сигурността, установени на територията на военните поделения и обекти на Министерството на отбраната, Българската армия и структурите на подчинение на министъра на отбраната. Организацията на тяхната дейност може да се разглежда на три нива – национално, регионално и индивидуално. Всяка от службите изпълнява своята дейност с помощта на отделни дирекции. [4]

Оперативно-издирвателата дейност на контраразузнаването и полицията се извършва в пълно съответствие с действащата Конституция на Република България и законите на страната. В своята дейност оперативно-издирвателните органи се съобразяват преди всичко с постановките на Конституцията.

Наред с този основен закон оперативно-издирвателната дейност на контраразузнаването и полицията се регулира с разпоредбите на Закона за МВР, Закона за ДАНС, Закона за отбраната и въоръжените сили, Закона за специалните разузнавателни средства, Наказателния кодекс, Наказателно-процесуалния кодекс, Закона за административните нарушения и наказания и с други действащи закони. По този начин гражданското общество чрез законодателната власт в посочило основните принципи, цели и задачи на тези служби.

Освен със законите оперативно-издирвателната дейност на контраразузнаването и полицията се регулира и с правилници за прилагане на Закона за МВР и Закона за ДАНС, с Правилника за структурата и организацията на дейността на служба „Военна полиция“, които са приети от Министерския съвет, а също така и наредби, касаещи тази дейност. Сред тези наредби могат да се посочат Наредбата за организиране сътрудничеството с граждани и осъществяване на функциите на МВР, Наредбата за организацията на дейността по използване на служители под прикритие в МВР и ДАНС и т.н.

Основни моменти и проблеми, свързани с оперативно-издирвателната дейност, които представляват класифицирана информация и имат секретен характер, се регламентират с инструкции и заповеди, издавани от Министъра на вътрешните работи, Председателя на ДАНС и Директора на служба „Военна полиция“.

В своята дейност оперативно-издирвателните служби се съобразяват и с принципите и нормите на международното право и на международните договори, сключени от нашата страна. България се явява участник в редица между държави, междуправителствени и междуведомствени договори, съглашения, конвенции и решения, някои от които имат отношение към оперативно-издирвателната дейност. Такива са например Конвенцията на ООН за борба против незаконния оборот на наркотични средства и психотропни вещества, приета през 1988 г, регулира провеждането на контролираните доставки и т.н.

Както вече бе споменато, оперативно-издирвателните служби имат правомощията да използват специфичните средства, методи и форми на тази дейност за постигането на вече посочените цели. Едно от тези средства за специалните разузнавателни средства (СРС). [4]

Понятието специални разузнавателни средства обхваща два основни елемента. В него се включват както техническите средства в тяхното многообразие и специфични свойства и възможности, така и различните оперативни способи за тяхното прилагане. То е както гражданско, така и правно понятие.

Специални разузнавателни средства са техническите средства и оперативните способи за тяхното прилагане, които се използват за изготвяне на веществени и доказателствени средства – кино записи, видеозаписи, звукозаписи, фотоснимки и белязани предмети. [1]

Тук се налагат две терминологични уточнения. Техническите средства са електронните и механични съоръжения и вещества, които служат за документиране на дейността на контролираните лица и обекти. Това са например радиоапаратура, радиопредаватели, радиоприемници, микрофони, звукозаписваща апаратура, фото- и видеоапаратура, оптически прибори, приспособления за отваряне на заключващи устройства и др. Техническите средства в разузнаването може да се разделят на две основни групи. Първата са технически средства, които се използват за целите на агентурното разузнаване. Популярно е наименованието оперативно – технически

средства. Втората група технически средства са тези, които се използват в техническото разузнаване като самостоятелно направление в разузнаването.

Основните способи, които се прилагат при използването на техническите средства включват: [1]

Наблюдение и проследяване. Зрително и чрез технически средства се разкрива поведението на контролираните лица по време на тяхното движение и пребиваване на различни места.

Подслушване. Слухово или чрез използване на технически средства се установяват и записват устни или телефонни разговори, а също и електронни комуникации по контролираното лице.

Проникване. Чрез използване на технически средства се прониква в помещения, ползвани от контролираните лица, с оглед да се установят фактически данни и вещи, свързани с тяхната престъпност.

Белязване. Чрез технически средства и вещества се поставят белези на предмети и вещи с цел да се установява тяхното движение и мястото на съхранение.

Проверка на кореспонденцията. Чрез използване на химически вещества и технически средства се извършва проверка на кореспонденцията на контролирани лица.

Проверка на компютърна информация. Прониква се в даден компютър с цел изясняване характера на информацията в него.

Контролирана доставка. Контролираното лице се допуска да пренесе вещ, която е доказателство за престъпление.

Доверителна сделка. Служител под прикритие купува или продава вещ, която може да се използва като доказателство за престъпление.

Информацията, която се получава от СРС, дава възможност при професионален анализ да се открият причините и условията, които благоприятстват извършването на престъпления против националната сигурност. С това тя подпомага процеса на разработване и прилагане на профилактични и други мерки за неутрализиране на престъпленията в страната.

Използването на СРС става по строго установен от закона ред. Инстанциите, имащи правомощия да ползват тези средства в своята дейност, могат да правят това само с разрешение на съдебните органи. То се дава от председателя на Софийски градски съд, съответно от председателите на окръжните съдилища или от изрично упълномощени от тях зам.-председатели. За военнослужещите решението се дава също предварително от председателя на съответния окръжен военен съд.

Един от основните оперативни способи за прилагането на СРС е подслушването. [1] То, заедно с наблюдението (те са от един и същи род – наблюдението може да е визуално или акустично) са едни от най-старите и използвани разузнавателно-контраразузнавателни способи. Тяхната древност и използваемост се дължат на това, че основният организационен и операционен елемент е човекът и неговите сетива – зрение, слух, обоняние и т.н. [7]

При подслушването чрез използване на технически средства, слухово или по друг начин, се усвоява устна, телефонна или електронна комуникация на контролирани лица. [1, чл.6]

Реализацията на подслушването предполага много и различни както от оперативна, така и от техническа гледна точка варианти. Съществено е, че се използва наличието на следните физически явления:

Акустичен сигнал. Подслушването може да се осъществи от оперативен работник или агент (секретен сътрудник, осведомител) чрез запис със съответно записващо устройство – скрито, миниатюрно или камуфлирано; с помощта на монтирано специално техническо средство, предаващо информацията по съществуващи комуникации (вериги за сигнализация, захранваща мрежа 220 V, телефонни линии и т.н.), по специално положени кабели (жични, оптични), по радио или инфрачервен (ИЧ) канал, чрез насочен микрофон. Това означава, че независимо от голямото разнообразия на методи, почти винаги първоначално се извършва преобразуване на акустичния сигнал в електрически с помощта на микрофон и в последствие обратното – до ясен говор.

Виброакустичен канал. Може да се използва стетоскоп, радиостетоскоп – вибродатчик (контактен микрофон) с предаване на информацията по кабел, радио или ИЧ канал, оптически лазерен микрофон. Извършва се преобразуване на вибрациите на повърхнини и предмети в електрически сигнал.

Хидроакустичен сигнал. Преобразуването на трептенията на течност в електрически сигнал се осъществява чрез хидроакустичен датчик. Тази техника се използва в разузнаването и контраразузнаването, свързани с издирване и защита на подводници и идентифициране на чужда разузнавателна техника в собствени на субекта води.

По движение на устните. Получаване на информацията може да се осъществи визуално, в това число чрез оптически прибори, последващо изучаване на запаси, с помощта на специално обучени да четат по устните на обекта хора.

В крана сметка есенцията се съдържа в необходимостта да бъдат подслушани, фиксирани, записани разговори на лица, подозирани в извършване на тежка престъпна дейност, които да дадат на субекта на подслушването информация, довеждаща до разкриване, предотвратяване и пресичане на престъпленията, както и на създаване на доказателствени средства, валидни в един наказателен процес.

ЛИТЕРАТУРА:

1. Закон за специалните разузнавателни средства. Обн. ДВ. бр.95 от 21 октомври 1997 г., изм. ДВ. бр. 107 от 24 декември 2014 г.
2. Асенов, Б. Теория на разузнаването. София : Албатрос, 2005.
3. —. Теория на разузнаването и контраразузнаването. София : ВСУ „Черноризец храбър“, 2009.
4. —. Основи на оперативно-издирвателната дейност. София : ВСУ „Черноризец Храбър“, 2009.
5. Бояджиев, Т. Шпионажът като занаят. София : Захарий Стоянов, 2002.
6. Василев-Чангов, М. Секретни операции. Разузнаване. Национална сигурност. София : Военно издателство, 2009.
7. Способи за подслушване. Специални разузнавателни средства. [Online] [Cited: май 1, 2015.] http://www.srs.bg.

СИГУРНОСТ НА СЪВРЕМЕННИТЕ ИНФОРМАЦИОННИ СИСТЕМИ

Николай Ю. Марков

SECURITY OF TODAY'S INFORMATION SYSTEMS

Nikolai Y. Markov

ABSTRACT: *The issue of the threats to modern information systems is described in this paper. Cyber attacks define recent vulnerability in communication and information systems. Security problems and objects are reviewed with classification. A conclusion of security precautions is proposed.*

KEY WORDS: *computer threats, hackers, cyber-security, malware, spyware.*

Въпросът, свързан със заплахите, отправяни към съвременните информационни системи, никога не е представлявал по-голямо предизвикателство за държавните служби. Правителствените агенции са изправени пред голям поток от кибератаки, които стават все по-сложни, усъвършенствани, невидими и опасни. Използваните в момента решения с използване на цифрови подписи и анализи, базирани на файлове, не могат да открият усъвършенстваните атаки и своевременно да ги спрат.

1. Технологични аспекти на киберсигурността

В технологично-информационен план киберсигурността се изправя пред необходимостта да се намери адекватен отговор на атаките, на които са подложени комютърните системи и интернет пространството. Голяма част то тях идват от т.нар. кракери. Той анализира нивото на сигурност на системата, за да формулира необходимите изисквания и условия за повишаване нивото на нейната защита. Кракерът осъществява несанкциониран достъп до системата с цел лична изгода - подмяна, кражба, унищожаване на информация или обявяване факти на достъпа.

Кракерите биват няколко типа: вандали, шегаджии и разбивачи. Поради наличието на много вируси, „вандалите" са най-известната и най-многобройна част от кракерите. Основната им цел е да получат достъп до системата чрез нейното разрушаване. Вандалите се делят на „любители", които използват обикновени команди, и „специалисти", които създават вируси или троянски коне. Вторият тип кракери - „шегаджиите" - представляват най-безобидната част. Те имат за цел известност, която постигат чрез влизане в компютърни системи и вмъкване на различни ефекти. Третите биват „разбивачите"- професионалисти, които реализират собствени или чужди цели. Постигат това чрез влизане „взлом" в системата, за да осъществят кражба или подмяна на съхраняваната там информация. Разбивачите са най-опасните киберпрестъпници, защото крадат лична информация или средства на други и след това се възползват от нея. При техните атаки се оставят възможно най-малко следи, за да не разбере атакуваният сайт, че информацията в него е разбита и компроментирана с цел клиентите да не бъдат уведомени.

Атаките на хакерите се осъществявят чрез различен вид софтуер, който се използва, за да се проникне в дадена система - като адуер (adware), спайуер (spyware), малуер (malware), огромна вариация от вируси, като за операционна система Windows са над 100 000 [1] и различни хакерски програми като Brutus. Адуера, спайуера и малуера биват програми, малки по размер, но сложни, съдейки по начина им на действие - инсталират се и се вплитат в софтуера на Windows. Те могат да нанесат от малки до огромни щети, заплашващи сигурността на идентичността и финансите на потребителя, ползващ интернет. Най-лошото, което могат да постигнат програмите, е да записват всяко натискане на клавиш и да направят поредица от снимки на случващото се на монитора. Впоследствие те изпращат информацията до указано предварително от създателя на програмата място.

Огромен проблем, за който специалистите все още търсят най-правилното решение, е "бот-нет". “Бот-нет”-ите представляват съвкупност от заразени (зомбирани) компютри, които разпространяват зловреден софтуер, червеи и троянски коне. “Бот-нет”-ите най-често са управлявани от т.нар. "бот-мастър". Ботмастърът от своя страна често си сътрудничи с експерт по сигурността, който следи най-вече уеб приложенията, десктоп софтуера и операционните системи, като търси слаби места. Ботмастъра използва информацията, набавена от експерта по сигурността и създава вируси или троянски коне, като ги маскира като приложение, което интернет потребителя сваля от уеб сайт, получава по пощата, или инсталира на компютъра си от преносима памет. След това маскираното приложение се свързва към определен сървър за управление. Дадено лице се свързва с ботмастъра и закупува неговите услуги, като най-често това е спамър, желаещ да изпраща нежелани съобщения до определен брой адреси. Процесът се финализира, когато ботмастърът инструктира вируса в заразения компютър да препраща спам съобщения на всички контакти от мейл-клиента на жертвата. При случай на среща със заразен, заразеният отново препраща спам мейла до всичките си контакти. Съществуват ботнети, които препращат десетки милиарди писма на ден. Ботът (заразеният компютър) обикновено се стартира в невидим за обикновения потребител режим и без да подозира, той става част от ботнета.

Чрез бот-нет мрежите се осъществяват DoS (Denial-of-Service) атаки и изключително опустошителните DDoS (Distributed-Denial-of-Service) атаки. При DoS атаките се изпраща чрез ботмастъра голямо количество информация, което би спряло достъпа до сайта, при условие, че машината, чрез която функционира сайта, е слаба. DDoS атаките са от същия тип като DoS, но са по-мощни. При тях едновременно се включват хиляди, понякога милиони потребители. Така инфомацията, която пристига към сайта е огромна и той блокира. Потребителите са заразени и не разбират какво се случва, тъй като компютърът им бива заразен и включен в ботмрежа. В редки случаи, DDoS атаките са доста печеливши за кибер престъпниците, тъй като могат да държат блокадата над сайта с дни и да искат откуп, за да спрат атаката. Сайтът и при двата типа атаки не е хакнат, а претрупан от входяща информация, на която не може да издържи.

Ботнетите заемат голям процент от заплахите за сигурността в киберпространството. Най-опустошаващата ботнет мрежа е Zeus, заразила над 3,6 милиона и нанесла поражения за милиарди. Тя действа чрез троянски кон и технологията keyloggin, чрез която краде имена, пароли, номера на кредитни карти и номера на акаунти. Втората по мощ бот-нет мрежа е Koobface, атакувала успешно над 1,5

милиона компютъра. Тя се развива чрез социалните мрежи My Space и Facebook с фалшиви съобщения и коментари от приятели. Когато някои се подлъже да откликне на съобщението, най-често да види видеото, получава съобщение, че трябва да обнови своите кодеци, за да го изгледа. Това всъщност не са кодеци или ъпдейт на програмата, а злонамерен софтуер, който взема контрол върху компютъра на интернет потребителя.

За постигне на кибер сигурност е нужна най-вече базова защита на виртуалните машини. Един от начините за постигане на сигурността е Core Protection for Virtual Machines на Trend Micro. Този продукт използва софтуер, който предпазва виртуалните машини онлайн и офлайн от различни уеб-заплахи, вируси, троянски коне и червеи. Постига се известно ниво на защита, но на виртуалните машини, не на кибер мрежите. За предпазване на сървърите в частност се използват програмни решения, създадени изключително за използване във виртуални и „облачни" (cloud) среди (технологии и услуги, достъпни чрез интернет). Продуктите от този вид включват средства за откриване и предотвратяване на атаки, защита на уеб приложения и други. Според експертите, те представляват добър начин за преодоляване на известни и неизвестни атаки, най-вече поради факта, че съдържат в себе си така наречените "Smart rules" (умни правила), подход, чрез които зловредният код се разпознава въз основа на необичайни данни.

Съществуват различни архитектури за киберзащита, а именно комплекс от мерки, които обхващат тактическото, стратегическото и оперативното ниво. Една от тях е архитектурата на SANS [2], известна още като „20 критични контроли на сигурността". В нея са посочени начини за измерване и тестване на приложените мерки и средства и примерна схема за взаимовръзките между страните, които имат отношение към използването на този тип уязвимости. Тези начини са формулирани в двайсетте контроли на сигурността. Архитектурата на Northrop Grumman Corp от своя страна включва в себе си 5 слоя на сигурност, които биват:

1. Сигурност на периметъра.
2. Мрежова сигурност.
3. Сигурност в крайните точки.
4. Сигурност на приложенията.
5. Сигурност на данните.

Като извод за това ниво може да се каже, че с увеличаването броя на опасностите, застрашаващи киберсигурността, се оправдава настоящата градация на изработване на система от технологии, които да я постигнат. За да се достигне добро ниво на защита трябва да се отделят значително количество ресурси и внимание на всеки детайл от основата на сайта до най-новите новини, свързани с виртуалната сигурност. Технологията на гарантирането й все още не е изобретена в достатъчно добър вариант. В бъдеще, с модернизацията и глобализацията, този проблем ще стане още по-належащ за решаване.

Технологическа сигурност представлява също така и държавната регулация. Гарантирането на остраняването на киберпрестъпленията е ключово за постигането на националната сигурност. Киберпространството представлява критична инфраструктура, поради факта, че едно разрушаване на статуквото може да афектира трайно живота на отделния индивид и обществото като цяло, поради което съвременните държави, и особено най-развитите в технологично-информационно отно-

шение предприемат специални комплексни мерки за регулацията на неговото функциониране.

2. Проблеми на киберсигурността

Прилаганият сега традиционен модел за информационна сигурност не успява да открива и предотвратява някои от съвременните сложни и усъвършенствани атаки. Основна причина за това забавяне при откриване на атаките е сложността на съвременния усъвършенстван зловреден софтуер, който лесно заобикаля традиционните защити, базирани на подписи. Усъвършенстваният зловреден софтуер може да се раздели на следните основни групи:

- Социален (Social). Усъвършенстваните атаки се насочват към специфични обекти чрез използване на социално инженерство и някои дупки в уеб сайтове, които привличат посетители от целевата група на съответната индустрия.
- Усложнен (Sophisticated). Днес зловредният софтуер използва недостатъци от типа нулев ден и техники с усъвършенствана полиморфна мутация на кода или писане на неразбираем объркващ код, за да се заобиколят традиционните защити, базирани на антивирусни списъци и доверие.
- Скрит (Stealthy). Съвременният зловреден софтуер често след първоначалното компрометиране на информационната система, скрива следващите си етапи на нападение и криптира съобщенията до сървъри чрез комуникации за командване и управление CnC (Command-and-Control).
- Режисиран (Orchestrated). Усъвършенстваният зловреден софтуер изпълнява атаките в серия от ниско-профилни ходове или потоци чрез множество вектори.

3. Обекти на кибер атаките

Интересен е въпросът, към кои области от индустрията са насочени най-много от новите усъвършенствани атаки? Отговор ни дава изследването на Fire Eye за извършените кибер атаки през 2013 г. То представя следните основни резултати:

- Анализирани са 39 504 уникални инциденти в кибер сигурността (средно повече от 100 на ден);
- 4 192 от тези атаки са асоциирани с усъвършенствани устойчиви заплахи (APT) (средно повече от 11 на ден);
- Открити са 17 995 уникални инфекции със зловреден софтуер, дължащи се на APT дейности (средно почти 50 на ден);
- Активирани са над 22 милиона комуникации за командване и контрол CnC (средно повече от една на всеки 1,5 секунди);
- Установено е, че към САЩ, Канада и Германия са били насочени най-голям брой зловредни програми.

Установено е, че правителствените организации са областта, която е най-атакувана през 2013 г., с 84 от 159 зловредни кодове документирани от Fire Eye.

Същевременно, днес мобилните компютри са мястото, където компромисите между изискванията на потребителя за ефективност и сигурност са най-разпространени. От една страна, клиентите искат удобство и ефективност, които се предоставят от безжичния достъп чрез мобилни приложения. От друга страна, най-големите рискове в сигурността понастоящем са открити в мобилните приложения. В момента, мобилният зловреден софтуер е най-бързо разпространяващ се в информационните мрежи и системи.

За съжаление, тенденциите в развитието на зловредния софтуер се очаква да продължат и през 2015-а год. Хакерите и кибер крадците ще доразвият своите техники. Това, от своя страна, ще отправи ново по-голямо предизвикателство към правителствените агенции и компании за защита на техните информационни системи и данни.

4. Тенденции в развитието на зловредния софтуер

Основните 5 тенденции в развитието на зловредния софтуер през 2015 г. са :

1) Увеличаване на уеб-базирания зловреден софтуер

Голям процент от заразите със зловреден софтуер днес са резултат от сваляне на данни от уеб страници. Когато потребителите сърфират в компрометиран сайт или сайт измамник, зловредният софтуер автоматично се инсталира на тяхното устройство.

Някои от техниките, използвани от компрометираните сайтове включват атаки чрез инжектиране, които се възползват от пропуски в SQL бази данни и библиотеки, както и атаки чрез скриптове между кръстосани сайтове (Подмяна на код) XSS (Cross-site scripting). XSS позволява на атакуващите да инжектират скриптове от страната на клиента в уеб страници, разглеждани от други потребители. Основната цел на тези атаки е компрометирането на легитимни уеб сайтове. В много случаи, когато сайтове са изложени на риск, с тези техники, хакерите използват слабости в уеб браузърите и техните плъгини чрез HTML или JavaScript кодове на експлойти. През 2015 г., хакерите ще продължават да се възползват от новооткрити в мрежата уязвимости в сървъри и приложения, за да заразяват търговски и правителствени уеб сайтове. Все по-често, започват да се прилагат и други форми на атаки чрез уеб-базиран зловреден софтуер.

2) Продължаващо разрастване на бот мрежите

Заразените със зловреден софтуер компютри и сървъри често принудително се присвояват за ползване в масивни бот мрежи. През последните няколко години такива мрежи все повече са били използвани за извършване на клик измами (с ботове симулиращи кликванията върху реклами на уеб сайт, където действията генерират приходи на клик основа). Някои бот мрежи са били използвани за Bitcoin mining (процес на добавяне на записи по транзакции в главната счетоводна книга на последните сделки в системата за плащания Bitcoin). Най-много бот мрежи са използвани за мащабни разпределени атаки от вида отказ от услуги DDoS (Distributed Denial of Service).

В продължение на години, бот мрежите са привлекателни за злонамерени лица и групи, защото те предоставят евтина процесорна мощ и така осигуряват платформа за реализиране на атаки и разпространение на спам. Експертите очакват

хакерският интерес към бот мрежите да нарасне през следващата година, защото DDoS атаките са се доказали като ефективни при нарушаване целостта и работоспособността на бизнеса. През 2015 г. на пазара ще са достъпни все повече IP-съвместими мобилни устройства, които могат да бъдат компрометирани и включени в бот мрежи за разпределени атаки.

3) Все по-сложни фишинг атаки от типа социално инженерство

Фишинг атаките отдавна се използват от хакери, за да компрометират системи чрез заразени прикачени файлове или да насочат потребителите към измамнически сайтове. Такива сайтове или са готови да доставят зловреден софтуер или се представят като легитимни сайтове, като се опитват да откраднат пароли и друга лична информация, която да се използва при кражба на самоличност и измами.

Фишинг атаките са във възход през 2013 г. и се очаква да продължат да нарастват. Една от най-последните тревожни тенденции при фишинга е неговата повишена сложност чрез използване на техники на социално инженерство. Например, социалните мрежи често се обект за откриване на множество полезна информация, като определяне на имена и имейли на приятели или колеги, използвани в персонализираните фишинг атаки. В много случаи, пристигането на съобщение от приятел или колега може да намали бдителността на потребителя и той да отвори прикачения файл или да кликне върху предложения лъжлив линк. Друг подход, използван при персонализирате атаки е възползване от новини базирани на интересни събития, скандали в живота на обществени знаменитости или голямо бедствие.

Още една тревожна тенденция, за която трябва да се следи, е увеличението на фишинга чрез така наречените атаки от типа "носене на гръб" (piggyback attacks). При такива атаки, хакерите се възползват от объркването на клиентите след някакво нарушаване в работата на информационната система и предлагат възможност да помогнат за разрешаване на проблема. При това те целят да получат допълнителна информация от потребителя, като го приканват да отвори прикачен файл или да отиде на фалшив сайт.

4) Атаки използващи дупки в изходния код и целенасочени атаки, които незабелязано се вмъкват в изходния код

Хакерите често използват новооткрити уязвимости, разработвайки зловреден софтуер, насочен към най-новите слабости, които са идентифицирани. В миналото този подход обикновено разчиташе на нормалното развитие на бизнеса и съобщаването за поява на дадена уязвимост. Но през миналата година се е увеличил проактивния подход към намирането на уязвимости. Оповестени са случаи, когато са извършени целенасочени атаки, за да се открадне сорс код. Пример за това беше разбиването на Adobe Systems Inc., при което хакери са откраднали пароли на потребители и изходния сорс код на Adobe Acrobat, ColdFusion и други продукти. Изтичането на изходния код потенциално може да доведе до откриването на нови уязвимости, които да се използват за атаки.

5) Увеличаване на зловредния софтуер чрез препращане на мобилни съобщения

Зловредният софтуер, насочен към мобилни устройства ще се увеличи и усъвършенства през следващата година. Това ще направи по-трудна защитата на самоличността на потребителите и данните, особено ако компаниите и правителствените агенции прилагат политиката „Донеси своето собствено устройство" BYOD (Bring Your Own Device).

Една особено тревожна мобилна заплаха, която се очаква да донесе нови и по-големи проблеми е разпространяването на зловреден софтуер чрез SMS съобщения. Този сравнително нов метод за извършване на престъпления е в състояние да прихваща и препраща SMS съобщения.

Кибер престъпниците демонстрират голяма креативност, когато става въпрос за неговото използване. Един подход, наречен измама фиксирана премия (Premium-Rate Fraud), компрометира мобилното устройство и изпраща SMS съобщения за услугите фиксирана премия. Такава услуги са все по-популярни сред клиентите, като позволяват на потребителите да извършват плащане за определени позиции или да направят дарение за благотворителни цели само чрез изпращането на текстово съобщение.

Друга схема използва по-традиционен подход, насочен към кредитните карти и банкови сметки на потребителите. Техниката се възползва от използването на текстови съобщения за предаване на информация за удостоверяване. Например, много банки изискват онлайн клиенти, ползващи обществени или нови компютри, да се удостоверят чрез въвеждане на код за достъп изпратен на техния мобилен телефон. Хакерите, прихванали тази информация за удостоверяване, могат да я използват за достъп до онлайн акаунти. През следващата година се очаква SMS-базираните техники да разширяват възможностите си за извършване на злонамерени действия от хакери и кибер крадци.

На основата на разгледаните по-горе състояние и тенденции в развитието на зловредния софтуер, може да се направи изводът, че откриването на атаките възможно най-рано е от решаващо значение, защото последиците, нанесени от усъвършенствания зловреден софтуер, са реалност. Правителствените агенции се нуждаят от по-бърз, по-добър начин за запазване на чувствителните данни и намаляване на потенциалните политически, финансови и физически щети, които могат да произтичат от новите усъвършенствани атаки.

5. Борба с усъвършенствания зловреден софтуер

Законът за управление на Федералната информационна сигурност FISMA [5] признава съществуващия риск в съвременните информационни системи и необходимостта от постоянно наблюдение на усъвършенстваните и упорити заплахи и атаки от типа нулев ден.

При разглеждане на технологичните решения за управление на бързо променящия се пейзаж на съвременни заплахи, държавните агенции се нуждаят от платформа за сигурност, която се определя от следните характеристики:

1. Откриване на зловреден софтуер в рамките на секунди или минути след инцидента.
2. Възможност за откриване на зловреден софтуер по време на критичната фаза на експлойта.
3. Видимост за страничното движение на зловредния софтуер.
4. Разузнаване в реално време и кибер криминалистика през целия жизнен цикъл на атаката.
5. По-голяма точност при откриване на атакатас цел намаляване на неверни положителни и фалшиви отрицателни грешки.

Насоките изискват държавните агенции да разработят процедури, за да се даде възможност за съгласувана промяна от статично откриване до осъзнаване на запла-

хите и атаките в реално време. Това включва непрекъснат мониторинг в кибернетичното пространство, активен анализ, диагностика на заплахите и блокирането им в реално време. Насоките също така препоръчват и способности за проследяване на заплахите обратно към източника на тяхната CnC инфраструктура. Тези нови възможности включват осигуряване на непрекъснати сензори за наблюдение, диагностика, инструменти за смекчаване, и непрекъснат контрол като услуга CMaaS (Continuous Monitoring as a Service)

6. Технологии

В основата на технологичните решения на проблема стои предложният от Lockheed Martin Corporation модел за неутрализиране на веригите зловреден софтуер (Malware Kill-Chain Model). Той описва координираните и свързани етапи на една типична усъвършенствана атака. Чрез разбиране на същността на цикъла на живот на една такава атака, организациите могат да конструират подходящи процеси и инструменти за откриване, забрана и разрушаване на нарушенията в сигурността на всеки етап от веригата за тяхното неутрализиране. Намаляването на щетите от атаките изисква тяхното по-ранно откриване и премахване на евентуалните фалшиви положителни резултати.Във всички атаки, бързото откриване на експлойта е от решаващо значение.

7. Практики

Усъвършенстваните атаки започват с разузнаване. Нападателите идентифицират и избират своите цели чрез придобиване на информация от всички налични източници, включително имейл списъци, участници в конференции, социални мрежи и т.н. При действителната атака, използваща зловреден софтуер, обикновено пакетът от експлойт и полезен товар се доставя в серия от стъпки чрез множество вектори. Експлойтът позволява на атакуващия да изпълни код на целевата машина. Кодът на този експлойт изтегля полезния товар на зловредния софтуер, който често е криптиран с нестандартни алгоритми. В този момент, нападателят установява канал за командване и управление CnC на целевата машина. С помощта на този цифров канал, нападателят въздейства върху крайните цели, които могат да включват преместване на външни елементи в рамките на околната среда на системата и нарушаване на поверителността, целостта или работоспособността на информационната система. Опасността се увеличава с всяка следваща фаза. Следователно, ефективното смекчаване на щетите изисква разрушаване на началните етапи от веригата на зловредния софтуер. Колкото по-скоро продуктите за защита могат да открият, блокират и изолират атаката, толкова по-малки ще бъдат нанесените щети върху информационната система.

8. Заключение

Правителствените агенции се нуждаят от коренно нов подход за ситуационна информационна сигурност. Ефективното предотвратяване и реагиране за атаки изисква внедряването на нови технологии за защита и отговор при инциденти. Използването на непрекъснато наблюдение, диагностика и контрол като услуга ще спомогне за по-ранното откриване на атаките и оттам до намаляване на тяхното въздействие и изолиране на всички щети.

ЛИТЕРАТУРА:

1. FireEye Advanced Threat Report: 2013, FireEye Labs, February 2014, Интернет адрес: http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf
2. Top 5 Malware Trends for 2014 and How to Combat Them, A QuinStreet Executive Brief, 2014, Интернет адрес: https://www.ncbpinc.com/collateral/Webroot-Executive-Brief-01-22-14.aspx
3. Executive Summary, 2013 Data Breach Investigations Report, Verizon, 2014
4. Matusitz, Jonathan, "Cyberterrorism: American Foreign Policy Interests 2", страници 137–147, Април, 2005.
5. Markoff, John, "Before the Gunfire, Cyberattacks", The New York Times, 13 Август 2008.

ПОЛИТИКАТА ЗА УПРАВЛЕНИЕ НА ИНЦИДЕНТИТЕ КАТО ИНСТРУМЕНТ ЗА ПОВИШАВАНЕ НА НИВОТО НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Владимир П. Крумов

Национален военен университет „ Васил Левски ”
vladimirkr_vd@abv.bg

THE POLICY FOR THE MANAGEMENT OF INCIDENTS, AS A TOOL FOR ENHANCING THE LEVEL OF INFORMATION SECURITY

Vladimir P. Krumov

ABSTRACT: *This report is presented a model for the management of the incidents described are the processes and their sequence. Guidelines are given for improving incident management activities in information security*

KEY WORDS: *information security, incident, incident management*

През последните години, моделите на общуване които навлязоха в живота на хората и които се намесиха в средствата за масова комуникация, въведоха нов термин за същността и съдържанието на човешкия живот – информационно общество. Най – характерно за него е, че то разкрива нови връзки между хората и институциите на основата на споделянето на информацията.

През този период информацията се превърна в стратегически актив с все по – голямо значение. Като всички други активи които са особено ценни за дадената организация и информацията трябва да бъде добре защитена. Това е особено важ-

но и в днешната бързо променяща се среда, в която информацията е изложена на множество и разнообразни заплахи.

Анализа на съвременните отношения показва, че с нарастване на размерите на обмена на информация както между отделните структури на дадена организация, така и между партньорите в дадена сфера ще нарастват рисковете, свързани с опазване на добрата репутация и име, а също така и стабилността на организацията.

Развитието на процесите по обмен на информация води също така и до нарастване на рисковете от несанкциониран достъп до конфиденциална информация. Ефективен начин за намаляването на нивото на тези рискове е разработването на план за действие в извънредни ситуации като част от цялостната политика по сигурност на информацията, в резултат на което при възникване на нежелано събитие дейностите по реагиране да са последователни и достатъчни за отстраняване на неговото действие. Част от този план за действие при извънредни ситуации е и управлението на инцидентите в информационната сигурност.

За да се оцени едно събитие като инцидент, то трябва да отговаря на едно от следните определения:

- отделно събитие или серия от нежелани или неочаквани събития, свързани със сигурността на информацията, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията [1]

- Нарушение или непосредствена заплаха от нарушение на политиката за компютърна сигурност , използване на приемливи политики, както и стандартни практики за сигурност. [2]

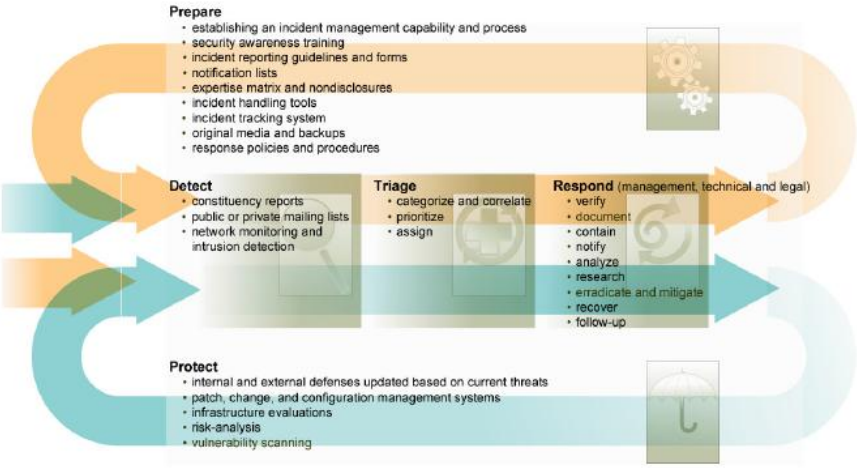
- Действително или потенциално събитие, което застрашава поверителността, цялостта или наличността на информационна система или информацията, която системата обработва, съхранява или предава, както и представлява нарушение или непосредствена заплаха от нарушение на политиките и процедурите за сигурност. [2]

От дадените определения може да се направи извода, че всяко действие или събитие което застрашава нормалното функциониране както и особено ценните активи на дадената организация може да се разглежда като инцидент в информационната сигурност и има нужда от съответния отговор и реакция.

Методът за управление на инцидентите, който ще разгледаме, е описан в „Defining Incident Management Processes for CSIRTs: A Work in Progress”. В него процесите за управление на инцидентите са:

- Подготовка
- Защита
- Откриване
- Разпределение
- Отговор

На фигура 2 са дадени връзките между отделните процеси и последователността на тяхното осъществяване.



Фигура 2. Последователност на процесите при управление на инцидентите

По време на процеса на подготовка се определя, какво трябва да включва управлението на инциденти, за да може то да се извърши по навременен и ефективен начин. Това може да включва:

- изисквания към обучението на персонала

- инструменти , оборудване и инфраструктура която ще може да предостави механизми за сигурни комуникации и мрежови връзки, база данни за проследяване на инциденти, отчетни форми, или инструменти за анализ

- политики и процедури, които ще регулират работата на способността за управление на произшествията и взаимодействията си с всяка друга част от организацията. Това може да включва политики за разкриване на информация както и стандартни оперативни процедури.

Една част от този процес включва изграждането на първоначален CSIRT или способности за управление на инциденти. Основните подпроцеси се разделят на две основни области:

- координиране на планирането и проектирането на способностите

- координиране на изпълнението

В процеса на планиране и проектиране се прави анализ на нуждите и определяне на изискванията, което се извършва с цел да се определи какви способностти ще има CSIRT . Те могат да включват интервюта и дискусии със заинтересованите страни, съществуващи политикити, бизнес нужди и наредби и закони, свързани с установяването на капацитет за управление на инциденти.

Определението на изискванията се използва за очертаване на визията на CSIRT, като се определя мисията, видовете услуги, организационен модел, както и ресурси които са необходими, писмени процедури, които са налице и в състояние да осигурят организационно - специфични насоки за извършването на тези процеси Процеса на подготовка включва подпроцеси за поддържане и подобряване на съществуващите възможности.

Подобряването на възможностите може да са в резултат на :

- препоръки за подобрение, произтичащи от наблюдения на това къде процеса има слабости или кога процесът е бил успешен по време на обработката на инцидент. Този тип на препоръка може да дойде от всяка дейност, в рамките на процеса на управление на инциденти. Препоръки също могат да бъдат предавани директно от процеса на реагиране. Това се случва, когато се взема решение за провеждане на преглед на предприетите действия на управлението на инцидентите.
- модифициране режисирано от управлението на дадена организация (например, бюджетните изменения, решение да се изнесе част от процеса, или други подобни промени). В този случай, ръководството може да реши да промени даден процес и тези промени да са предадат на лицата, отговорни за вземане на решенията за подобрения в процесите за управлението на инциденти.

Следващия процес е този на защита, която съдържа подпроцеси, които описват дейностите

- оценка на инфраструктурата или получаване на подобрения за защита на инфраструктурата. Тези действия могат да включват добавяне или изменение на защитата като защитни стени, мониторинг на мрежи, както и IDS; промени в конфигурацията на сървъри, рутери, защитни стени, както и други компоненти на инфраструктурата;
- промени в политиките и процедурите, свързани с приемливо използване, управление на сметки, физическа сигурност, човешки ресурси, или други подобни зони.

Част от процеса на защита включва подпроцес за извършване на оценка на инфраструктурата. Тази оценка може да включва проактивни оценки на сигурността, като например анализ на риска, тестване за проникване или сканиране за уязвимости.

Като цяло, подобренията в защитата на инфраструктурата са средства за повишаване на сигурността на компютърна инфраструктура. Тези подобрения са от различни източници, включително :

- пряко наблюдение на проблем, недостатък, или дупка в изчислителна инфраструктура, която поставя инфраструктура в риск на заплахи и атаки за компютърна сигурност. Възможно е това наблюдение да се случи в рамките на всеки процес по всяко време и да се предостави на хората отговорни за съответната част от инфраструктурата. В този случай не е необходимо да чакаме да се направи преглед на събитието, за да се вземат необходимите мерки. Така например, в процеса на разпределяне, съобщение може да дойде от друга част от организацията, което е забелязана злонамерената активност в инфраструктурата. Въпреки, че това съобщение трябва да се отнесе към хората които се занимават с проверка, оценка и ответна реакция, тя може да се предава и на лицата, отговорни за поддръжката на защитната стена, които може да оценят необходимостта за изпълнение на препоръките, докато тези, участвали в инцидента все пак ще направят преглед на съобщението за всяко доказателство за дадения инцидент.
- най-добри практики, както и правилата, които определят мрежови и системни конфигурации или методи за мониторинг на мрежи, които подобряват сигурността на инфраструктурата и могат да предотвратят или смекчат злонамерена дейност и експлоатация на известни уязвимости. Тези видове най-добри практики и стандарти може да дойдат от органи по стандартизация, компютърни експерти

по сигурността външни за организацията, или дори от управителя на предприятието.

Процеса на откриване често се свързва само на дейностите, свързани с откриване на проникване или мрежов мониторинг. Откриването по отношение на управлението на инциденти всъщност включва всички наблюдения на злонамерени или подозрителни дейности и всяко събиране на информация, която дава представа за текущите заплахи за сигурността или рискове.

В процеса на откриване, информация за потенциални инциденти, уязвимости за управление на произшествията е събрана или реактивно (получен от вътрешни или външни източници под формата на доклади или уведомления) или активно (мониторинг показатели на възможни последващи инциденти или експлоатацията на уязвимости чрез механизми за мониторинг на мрежи или IDS). Дейността или информацията, след като се открие се предава на процеса на разпределение под формата на доклад, сигнал или подробно уведомление.

В зависимост от политиките и процедурите в дадена организация, откриването може да се случи за минути или дни-това е мярка за ефективността на екипа и надеждността на политиките и процедурите. Ако същите служители изпълняват и процеса на разпределение който е следващия процес , тези два процеса може да се случат почти едновременно.

В зависимост от начина на откриване на събитията те биват два вида:

Косвено откриване

В косвено откриване, информация може да бъде открита и докладвани от два основни източника:

- тези, които използват компютърни съоръжения на организацията могат да забележат някои необичайни или злонамерени действия и да докладват за това на служителя определен за това. Докладването може да включва подаване на форма за докладване на инциденти или извикване на съответния човек за контакт, като например бюрото за помощ или гореща линия CSIRT;
- Други експерти за компютърна сигурност, като например външен CSIRT, координиращ CSIRT, или организация по сигурността.

Пряко откриване

Вторият път изисква проактивни действия от страна на определения служител за идентифициране на подозрителни действия, като персонал активно осъществяващ мониторинг на различни данни и използване на софтуер за откриване на признаци за подозрителна дейност . Данните се анализират и всяко необичайно или подозрително информационно събитие се препраща към процеса на разпределение.

В такива случаи е важно да има установени процедури за предаване на тази информация и установени насоки и правила за определяне на това, какво представлява инцидент или потенциална заплаха. Тези насоки ще бъдат използвани, за да се реши какво ще бъде прехвърлено за разпределение, какво ще бъде затворено, както се изисква, като действие и това, което ще бъде прехвърлено в друга част на организацията за работа.

Процесът на разпределение е съществен елемент на всяка възможност за управлението на инциденти,. Разпределението дава възможност за първоначална оценка на входящ доклад и го реди на опашка за по-нататъшна обработка. Той също така извършва първоначалната документация на събитието ако това все още не е направено в процеса на откриване на процеса.

Разпределението е процес на сортиране, категоризиране, корелация, приоритизиране и възлагане на входящите събития, доклади за инциденти и доклади за уязвимости .

Разпределението може да се извърши от различен персонал. Кой изпълнява това зависи от рамките и функциите за управление на инцидента и в цялата организация. Той също така зависи от нивото на обслужване от страна на персонала. В много малки организации тази функция може да е изпълнява от служител по сигурността , който получава доклад за събитие и който изпълнява функциите на разпределение. В една голяма мултинационална организация, тази функция може да бъде изпълнявана от съответен отдел за разпределение.

Особено внимание трябва да се обърне на това как се прехвърля информацията и какъв тип обучение се предоставя за тези служители, извършващи сортировка, така че те да знаят каква информация трябва да се предаде и в какъв формат трябва да се пропуска. Това е много важно, тъй като ако се прави неправилно, може да доведе до забавяне на отговора, който може да увеличи размера на щетите и въздействието в резултат от инцидент или да забави допълнителното разследване на доклада, защото той не е получен своевременно.

Процесът на разпределение включва преглед на входящата информация, за да се определи неговата валидност и да се определи какъв тип събитие се съобщава и какво първоначално действие да предприеме.

Тя улеснява признаването и подходящо разделение на:

- Нови инциденти
- Нова информация за текущи инциденти
- Искания за информация
- Доклади за уязвимости
- Други заявки за услуги

Разпределението може да се извърши на две различни нива

- Тактическо – фокусира се върху сортирането и категоризацията, както и оценка на доклади и искания въз основа на предварително определени критерии

- Стратегическо - фокусира върху извършването на истински оценка на ситуацията и определяне на въздействието върху бизнеса.

Функцията за сортировка осигурява незабавен преглед на текущото състояние на всички дейности - какви доклади са отворени или затворени, какви действия са висящи и кой от всеки вид доклад е получен. Този процес може да помогне за идентифициране на потенциални проблеми със сигурността и степенуване на обема на работа. Информацията, събрана по време на разпределянето може да се използва за извличане на поуки на висшето ръководство.

Важна стъпка в процеса на разпределяне в този модел за управление на инциденти е категоризирането на събития, като се използва предварително определени критерии, ако е налична за класифициране на входящите събития.

Колкото по-бързо анализатора направи оценка на въздействието и ефекта на инцидента, толкова по-бързо може да бъде овладян и обработен

Следващия процес от управлението на инциденти е и най – важния от всички а той е отговора на съответното събитие или инцидент. Този процес включва стъпките, предприети за справяне, решаване, или смекчаване на дадено събитие или инцидент. Определени са три вида дейности по отговор на инцидента : технически, управленски и юридически. Тези три вида дейности могат да се случат едновре-

менно, но за най-ефективен отговор те трябва да се случат координирано съгласно предварително определени процедури. Когато това е възможно и целесъобразно, информация следва да бъде споделяна в тези подпроцеси.

Въпреки че всяка от трите подпроцеси включва различни хора с различни умения и експертиза, основните стъпки при всеки подпроцес са сходни.

Технически отговор

Този отговор се фокусира върху действията, предприети от техническия персонал, за да се анализира и реши събитието или инцидента. Технически персонал може да включва персонал вътрешен и външен за организацията, като системни и мрежови администратори, други членове на ИТ операциите,експерти по външната сигурност. Технически ответни действия, които трябва да се предприемат може да включват:

- анализиране на информацията за събитие или инцидент
- намиране на съответстваща стратегия за смекчаване и опции за възстановяване
- издаване на бюлетини, сигнали и други издания, които предоставят насоки и съвети за решаването или смекчаване на събитието или инцидента
- съдържание на всякакви текущи злонамерени дейности чрез технически промени в инфраструктурата, като изключване засегнати системи от мрежата, промяна конфигурации за сигурност, услуги, IP адреси или съдържание на пакети чрез защитни стени, сървъри, рутери, или други устройства.
- изтриване или почистване всякакви злонамерени процеси и файлове
- ремонтиране или възстановяване на засегнатите системи

Отговор свързан с управлението

Отговор по отношение на управлението включва административни или управленски дейности.

Такива са осигуряване на взаимодействието между различните части на организацията когато се наложи да работят заедно, за да се справят със събития и инциденти и разрешаването на всички проблеми.

Правен отговор

Правния отговор включва действия, които са свързани с разследване; преследване; гражданска отговорност; авторското право; тълкуване на правни решения, закони и подзаконови актове. Правният отговор може да се инициира само от управлението на организацията.

Дейности по координирането на подпроцесите на отговор

Този вид сътрудничество и координация би трябвало да възникне чрез установени канали за комуникация, които трябва да бъдат очертани в политиката, процедури, както и планове, свързани с процеса на реагиране. Действията трябва да бъдат координирани, за да се гарантира, че няма дублиране на усилия и че всички задачи са завършени в рамките на договорените срокове.

При разглеждането на този модел може да се направят следните насоки за по нататъшна работа и подобряване на процеса на управление на инцидентите:

- документиране на всички дейности и процеси при управлението на инцидентите;
- сравнителен анализ на съществуващите възможности за управление с такива които представят най – добри практики;

- планиране и проектиране на нови или подобрени възможности за управление на инцидентите
- оценяване на изпълнението на процеса на управление на инцидентите.

ЛИТЕРАТУРА:

1. ISO / IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary
2. Glossary of key information security terms, U.S. Department of commerce, 2011
3. Defining incident management processes for CSIRTs: A work in progress, Carnegie Mellon University, Pitsburgh, 2004
4. Creating and managing computer security incident handling teams (CSIRTs), Carnegie Mellon University, Pittsburgh, 2008

СТЕГАНОГРАФИЯ В МОБИЛНИТЕ ТЕЛЕФОНИ И PDA

Сунай А. Алиев

E-mail: sunay.aliev@yahoo.com

STEGANOGRAPHY IN MOBILE PHONES AND PDA

Sunay A. Aliev

***ABSTRACT**: The paper aims to present the application of steganography in modern mobile devices. Hiding and finding information through technology of SMS, MMS, Bluetooth. There are presented separate principles and algorithms realizing this process. There are listed mobile applications that use steganography for secret communication between users.*

***KEYWORDS:** Steganography in mobile devices, PDA devices, secret communication, SMS, MMS, Bluetooth*

I. Въведение

В последното десетилетие мобилните комуникационни устройства заемат все по-голяма част от нашето ежедневие и начин на живот, стават все по функционални и позволяват приложението на разнообразни услуги. Телефони, смартфони, таблети, фаблети, лед ръчни часовници, pda устройста и други, разполагат с нови разнотипни сензори, софтуер и апликации.

С увеличението на приложението на мобилните устройства нарастват и заплахите, свързани както със защитата и сигурността на данните в тях, така и на преноса на информация по време на комуникация. Търсенето на сигурност при обмена на данни между потребителите и устройствата прави възможно приложението на стеганографски методи за осигуряване на защита [1].

III. Анализ на стеганографски продукти за мобилни устройства

В таблица 1 са изброени най-разпространените стеганографските мобилни приложения, които могат да се изпозлват в настоящите мобилни устройства.

Таблица 1

Название на софтуер/апликация	Подходящо за следните устройсва	Операционна система	Размер
Concealment	смартфон, таблет, фаблет	iOS	-
Hide It In	смартфон, таблет, фаблет	Android OS	3.2MB
Acoustic Picture Transmitter	смартфон, таблет, фаблет	Android OS	1.5MB
Spy Pix	смартфон, таблет, фаблет	Android OS	1.1MB
Steg-O-Matic	смартфон, таблет, фаблет	Android OS	1.6MB
DeepSound	смартфон, таблет, фаблет	Android OS	842kB
Secret Tidings	смартфон, таблет, фаблет	Android OS	2.3MB
Stegais	смартфон, таблет, фаблет	Windows Phone 8/Android OS	459kB
Steganography+	смартфон, таблет, фаблет	Android OS	856kB
Magic Picture	смартфон, таблет, фаблет	Android OS	789kB
DaVinci Secret Message	смартфон, таблет, фаблет	Android OS	322kB
PixelKnot	смартфон, таблет, фаблет	Android OS	3.8MB
Steganografia	смартфон, таблет, фаблет	Android OS	2.3MB
Secret Letter	смартфон, таблет, фаблет	Android OS	1.8MB
Incognito	смартфон, таблет, фаблет	Android OS	6.5MB
Photo Hidden Data	смартфон, таблет, фаблет	Android OS	1.2MB
Barcode Steganography	смартфон, таблет, фаблет	Android OS	2.8MB
Pocket Stego	смартфон, таблет, фаблет	Android OS	989kB
MobiStego	смартфон, таблет, фаблет	Android OS	38kB
Crypsis Eye	смартфон, таблет, фаблет	Android OS	1.4MB

Stegosaurus	смартфон, таблет, фаблет	Android OS	1.7MB
Stegano Imessage	смартфон, таблет, фаблет	Android OS	496kB
Steganography Application	смартфон, таблет, фаблет	Android OS	139kB

При оценяването на стеганографските продукти се вземат в предвид удобен потребителски интерфейс, разнообразни функционалности за скриване, откриване и споделяне, висок потребителски рейтинг, възможност за използване на различни контейнери. След анализа на изброените в таблица 1 продукти в таблица 2 се посочват 5 от тях, които удовлетворяват в най-голяма степен посочените критерии.

Таблица 2

Название на софтуер/апликация	**Подходящо за следните устройсва**	**Операционна система**	**Размер**
Concealment	смартфон, таблет, фаблет	iOS	-
DaVinci Secret Image	смартфон, таблет, фаблет	Android OS	322kB
Steganografia	смартфон, таблет, фаблет	Android OS	2.3MB
Stegais	смартфон, таблет, фаблет	Windows Phone 8/Android OS	459kB
Incognito	смартфон, таблет, фаблет	Android OS	6.5MB

Concealment – софтуер, разработен от Lakeside LIama позволява скриването на информация в снимки, направени чрез самото устройство. Стего изображенията могат да се запазят в галерия от снимки или да се изпратят чрез електронна поща или друг тип комуникация. На фигура 1 е показан интерфесът на мобилното приложение Concealment.

Фиг. 1. Интерфейс на приложението Concealment

Stegais – приложение предназначено за потребители на операционни системи Windows Phone 8/Android OS. Потребителите могат да скрият текстова информация в снимка, която е направена с камерата на устройстовото или от библиотеката със изображения. Изображението може да се изпрати или съхранява по всички стандартни медоти за съхранение и комуникация или да се изпозлва за прикриване на информация в самото устройство. На фиг. 2 е показан интерфесът на мобилното приложение Stegais.

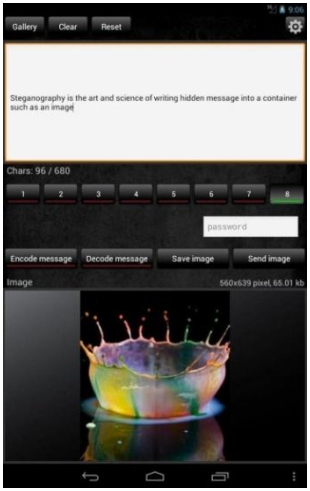
Фиг. 2. Интерфейс на приложението Stegais

DaVinci Secret Message – мобилно приложение за операционна система Android. Скриването на информация е отново в цифрово изображение с тази възможност, че

съобщението може да се защити предварително с парола, което е още едно по-високо ниво на сигурност. А специалната функционалност за допълнително задаване на размера на окончателното изображение, го прави по трудно за отркриване от анализаторите. На Фиг. 3 е показан интерфесът на мобилното приложение DaVinci Secret Message.

Фиг. 3. Интерфейс на приложението DaVinci Secret Message

Steganografia – тази мобилна апликация позволява няколко нива на сигурност при скриването на съобщение в изображение и използване на парола. Целта е скритата информация в изображението да се запази, при допълнителна обработка, например при компресия или преоразмеряване, използващи се в някои от социалните мрежи. На Фиг. 4 е показан интерфесът на мобилното приложение Steganographia.



Фиг. 4. Интерфейс на приложението Steganografia

Incognito – приложението е подходящо в случаите когато, конфиденциалността и сигурността са на първо място. Тази апликация позволява скриването на файлове от различен тип, като текстови, pdf файлове, изображения, аудио файлове в цифрово изображение. На фиг. 5 е показан интерфесът на мобилното приложение Incognito.

Фиг. 5. Интерфейс на приложението Incognito

IV. Стеганография чрез SMS, MMS и Bluetooth

Стеганографски техники могат да бъдат реализирани в мобилинте устройства и чрез други възможности за комуникация – SMS, MMS, Bluetooth.

Според [2,3] SMS (short message service) – стеганография има няколко вариации, чрез които да се реализира.

- Line Shifting: при този стеганографски метод, линиите на текста са вертикално променени до 1/300 инча нагоре или надолу. А информацията е скрита, чрез създаване на уникална форма на текста. Методът е подходящ за печатни текстове. Разбира се с подходящи инструменти и приложения за анализ на разстоянията между символи и редове, могат да бъдат въведени промени и скритата инфомация да се унищожи или замени с друга.
- Word Shifting: при този стеганографски метод, чрез изместване на въведения текст хоризонтално или чрез промяна на разстоянието между думите, желаната информация се скрива. Този метод може да се идентифицира по-трудно, защото промяната на разстоянието с цел запълване на ред или по прегледен запис е често срещан похват. Но, ако се приложи алгоритъм за презаписване на текстовото съобщение с поставен един интервал между всяка дума, а останалите интервали биват анализирани може да се открие търсената информация. За да се заобиколи едно анализиране с подобен алгоритъм е възможно създаването на изображение посредством символи.
- Semantic Methods: – метод, при който ключовите думи се заменят със синоними. По този метод откриването на скрито съобщение е почти невъзможно, но има опасност и от промяна на основния смисъл на първоначалното съобщение.
- Feature Coding: – при този подход някои от функциите на текста са променени. Крайната част на някои изпозлвани символи са удължени или намалени като стойност. По този начин може да се скрие голям обем информация без да прави

впечетление на потребителите, освен на потребителя, който го е създал с различна цел и ползваемост.

• Open Spaces – при този метод скриването на информация се осъществява, като се добавят допълнително бели празни пространства в текста. Поставените интервали могат да бъдат използвани във всеки един момент от записа на текста. Обемът на информация, който може да се скрие по този начин е много малък, но в различните ситуации е бързо решение за реализация на такъв стеганографски подход.

• Persian/Arabic Text – изключително добър според водещи специалисти метод за скриване на информация. За съжаление е подходящ само за персийски и арабски подобни езици. Причината е, че този метод използва точките, които са част от отделните букви и символи и чрез изместване на хоризонталните редове може да се получи графика от несвързани точки или малка карта, която да е скритата информация.

• Stealth – при този метод информацията се крие в текущото съобщение, като то е придружено с цифрово изображение, в което също може да има скрита информация. Информацията може да е кодирана с парола или не.

• Abbreviation: – скриването на информацията се осъществява, чрез използването на съкращения. Така много малко информация може да бъде скрита в текста. Например, само на няколко бита могат да се скрият в файл със съдържание няколко килобайта. На Таблица 3 са изведени акроними на често използваните абревиатури за бърза комуникация.

Таблица 3

Абревиатура/Акроним	Превод	Значение
ASAP	As soon as possible / Възможно най-бързо	Веднага
C	See / Да се видим	Нека се видим
CM	Call me / Обадими се	Звънни ми
F2F	Face to face / Лице в лице	На четири очи
NC	No comment / Без коментар	Нямам какво да кажа
DND	Do not disturb / Не ме безпокой	Не ме притеснявайте
SRY	Sorry / Извинявай	Съжалявам
T+	Think positive / Мисли позитивно	Бъди оптимист
zZzZ	Sleeping / Спя	Изморен съм, имам нужда от сън

Според [4] MMS (Multimedia Messaging System) – стеганография е технология, позволяваща изпращането на мултимедийни обекти. Мултимедийните обекти могат да съдържат скрита информация скрити чрез различни стеганографски алгоритми. Алгоритмите, които се прилагат в SMS (short message service) технологията са в сила и тук.

Bluetooth – стеганографията създава възможност за предаване на стегофайлове чрез безжично предаване на разнотипни мултимедийни файлове[5]. Има обсег на действие 50 метра в зависимост от условията, в които се използва.

V. Заключение

Според направеното изследване може да се направи извод, че стеганографските методи са приложими и в мобилните устройства. В следствие на това може да се повиши надеждността за провеждане на сигурна комуникация на потребителско или бизнес ниво.

ЛИТЕРАТУРА:

1. Параскевов, Хр., Ст. Станев, Е. Стефанова. Подход за мрежова стеганография на базата на протокол RDP. Международна научна конференция „Съвременни методи и технологии в научните изследвания", ВВМУ "Н. Й. Вапцаров"- Варна. Варна,2013
2. Badgaiyan, C., Ashish Kumar Dewangan, A., Pandey, B. A survey paper on SMS based steganography
3. Shirali-Shahreza, M., Shirali-Shahreza, M. H. Text Steganography in SMS
4. Papapanagiotou, K., Kellinis, K, Marias, G. F., Georgiadis, P. Alternatives for Multimedia Messaging System Steganography
5. Baker, S., Nori , Dr. A. Steganography in mobile phone over Bluetooth

АТАКИ КЪМ ИНФОРМАЦИОННАТА СИГУРНОСТ НА ИЗЧИСЛЕНИЯТА В ОБЛАК

Сунай А. Алиев
E-mail: sunay.aliev@yahoo.com

ATTACKS AGAINST INFORMATION SECURITY IN CLOUD COMPUTING

Sunay A. Aliev

***ABSTRACT**: This article aims to present classification on attacks aimed at security of cloud computing.Vulnerable zones of different infrastructures and ways of dealing with malicious interference in order tomaintain personal and confidential information from a consumer and business perspective.*

***KEYWORDS**: Cloud Computing, attacks, security, services, infrastructure, model*

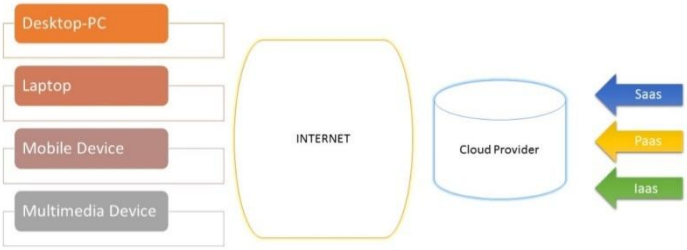
1. ВЪВЕДЕНИЕ

Облачните услуги са следващото поколение модерна технологична архитектура (фиг. 1), която се налага в съвременната ИТ индустрия. Чрез доставяне на потребителски и бизнес услуги през съвременните медийни среди в съчетание с надеждно физическо хранилище на данни, нисък финансов ресурс, екологична насоченост и гъвкавост при работа – моделът на облачните услуги заема водеща роля и ниша в

ИТ индустрията. Според [1, 2] пример за това са топ ИТ компании като: Microsoft, Apple, Amazon, Google, EBay, IBM, които мигрират към този работен модел.

С внедряването, използването и предлагането на тази услуга следват и редица проблеми и въпроси върху, които трябва да се обърне внимание. Сигурността и защитата на потребителските и фирмените данни са основен показател до колко може да се мигрира към облачните услуги.

Дори с новоконцептуалните въведения като споделяне на ресурси и аутсорсинг се създават още по-големи предизвикателства през сигурността и защитата от атаките върху облачната структура. Разработването и внедряването на защитни средства и системи налага детайлното анализиране на заплахите и атаките срещу сигурността на информацията в облачните услуги [3].



Фиг. 1. Облачни услуги

2. АТАКИ СРЕЩУ ИНФОРМАЦИОННАТА СИГУРНОСТ В ОБЛАЧНИТЕ УСЛУГИ

В табл. 1 са посочени основните специализирани зловредни атаки свързани и насочени към облачните структури и услуги, които носят опасност върху данните, които се съхранавят и оперират в тях [4, 5, 6, 7, 8].

DENIAL OF SERVICE – вид атака, според водещи специалитсти в областа, които твърдят, че тя е изключително мощен инструмент за зловредно влияние върху облачната структура и ресурсите, които тя ползва и предоставя за позлване. Тази атака разполага с много разновидности като (DDoS, Http-Based DDoS, REST-Based-DDoS, Shrew attack light traffic DoS).

С цел справяне на такъв тип атака Cloud Computing-ът ще използва по-вече изчислителен ресурс, който ще поеме натоварването от многобройния трафик, като го разпределя в още изчислителни машини, по този начин няма да се достигне до наводняване и претоварване на обслужващите услуги.

CLOUD MALWARE INJECTION – вид атата, при която атакуващият инжектира противника със зловредна услуга, софтуер или код, който се появява като валидно съобщение в апликациите, с които работят потребителите и самите ресурси. Ако атаката е успешна, облачната структурата може да бъде подслушвана – чрез

финни промени по функционалността, мъртви зони и т.н.. Атаката засяга IAAS и PAAS инфраструктурите. Защитните механизми не могат да различат виртуалната намеса като външна и я интерпретират като напълно нормално състояние в работния модел. По този начин нападателя може да осъществи достъп до желаните точки за зловредна атака и намеса с цел извличане на информация, манипулиране на информационното поле и движещите се в трафика заявки.

SIDE CHANNEL ATTACK – атака вид – страничен канал, атакуващият поставя зловреден софтуер и виртуална машина в непосредствена близост до целевия клауд сървър – атаката използва специфични криптографски алогоритми за извличане на информация от дейта центровете и сриване на слоевете в инфраструктурата.

Название на атаката	**Засегнати зони**
DENIAL OF SERVICE	Хардуер IAAS, PAAS структури
CLOUD MALWARE INJECTION	Облачниинфраструктури
SIDE CHANNEL ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
AUTOTHENTICATION ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
MAN IN THE MIDDLE	Облачни инфраструктури, мрежови достъп и комуникация
AUDIO STEGANOGRAPHY	Облачниинфраструктури и мрежови комуникационен достъп
TARGETED SHARED MEMORY	IAAS, PAAS структури
PHISHING	Облачниинфраструктури, мрежови достъп и комуникация
BOTNETS	Облачниинфраструктури, мрежови достъп и комуникация
BACKDOOR CHANNEL ATTACK	Хардуер, IAAS, PAAS структури
FLOODING ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
TRACEBACK	Облачни инфраструктури, мрежови достъп и комуникация
DATA STEALING PROBLEM	Облачни инфраструктури, мрежови достъп и комуникация
THEFT OF SERVICE	Облачни инфраструктури, мрежови достъп и комуникация
PORT SCANNING	Облачни инфраструктури, мрежови достъп и комуникация
ATTACK ON VIRTUALIZATION	Облачни инфраструктури, мрежови достъп и комуникация
STORAGE ALLOCATION AND MULTITENACY	Облачни инфраструктури, мрежови достъп и комуникация

Табл. 1. Атаки срещу информационната сигурност в облачните услуги

AUTOTHENTICATION ATTACK – вид атака, при която уязвимо място са хоствaните виртуални услуги. Чрез идентификация на това което потрибетилите използват и извличат от ресурсите, атакуващите регистрират автентичността-идентификацията. Така те засягат архитектурата на Saas, Iaas и Paas. Тъй като и към днешна дата най-разпространеният метод за автентчност-идентификация е

потребителско име и парола – атакуващите използват това за извличане на важна информация касаеща редица финансови институции, клавиши на уебсайт, виртуални клавиатури, споделени тайни въпроси и т.н.

MAN IN THE MIDDLE – вид атака, при която се изпозлват в основата критпографски модули и нападателя се поставя между конекцията на двама потребители като манипулира трафика на съобщенията между тях и може да достъпи с пълни права върху работещите устройства. Тук се включват разновидности на лъжливи ARP, DNS, рутер и др.

AUDIO STEGANOGRAPHY – вид атака сочена като една от най-опасните и сериозни за системите за съхранение на облака. Тази атака помага на потребителите да крият своите тайни данни в рамките на редовните аудио файлове. Хакерите използват този принцип и метод, за да заблудят настоящите механизми за сигурност. Атакуващите крият своя злонамерен код в аудио потоци и ги изпращат на потрбителите чрез сървърите под различна медийна форма – по този начин те осъществяват достъп до желаните точки за атака.

TARGETED SHARED MEMORY – целева, точкова атака, нарушаваща ресурсите за общо използване. Изтичане на системна информация и потребителска. Но най-вече е отворена врата за други канални атаки върхи инфраструктурата на облачната медийна среда.

PHISHING – високо скоростна атака за извличане на ключова информация – потребител, парола, кредитни данни. Заразяването се осъзществява чрез добре маскиран malware, spyware, bugware и airware.

BOTNETS – вид атака, при която се достига до неоторизиран достъп до системните дейта ресурси. Изкуствено карайки облачните системи да работят А-нормално, като извличането на системна и потребителска информация става плавно на порции.

BACKDOOR CHANNEL ATTACK – пасивна атака, която нарушава възли – точкови връзки в облачните комуникации. Присвоените възли се използват като троянски коне и други подобни структури в системата, като създава зомби клонинг на цялата структура и извличането става незабелязано от защитните системи.

FLOODING ATTACK – така наречените наводнени атаки, хакерите могат да изпращат големи количества пакети от експлоатираните информационни ресурси – зомби. Пакетите могат да бъдат от вид TCP/UDP/ICMP и комбинации. Тези видове атаки са най-вече реализирани над неоторизирани мрежови връзки.

TRACEBACK – атака, при която се създава контрол и комнадване на сървър, чрез стъпкови каменни виртуални пътеки.

DATA STEALING PROBLEM – традиционен вид атака за нарушаване работата на група потребителски акаути. Потребителските данни за откраднати, достига се до извличане на данни и дори унищожаване. Щетите са както клиентски така и върху ресурсите за съхранение на отделните засегнати структури.

THEFT OF SERVICE – атака, която прихваща услуги – краде услуги, използва уязвимост в графика на някои хипервайзъри. Атаката се реализира, чрез механизъм за график на услугите. Сливат се услуги, които централният процесор не засича и по този начин се позволява зловредна намеса. Атакуващият може да се възмолзва от облачни услуги за сметка на редовен с разрешени права за достъп потребител.

PORT SCANNING – атака сканираща портовите връзки – атаката анализира, филтрира и индентифицира състоятнията на сканираните портове (отворени и

затворени). При този вид атака, атакуващите се сдобиват с желаната информация, чрез използване на отворените портове, които работят като услуги на една система, IP и MAC адреси, които принадлежат към една връзка, рутер, шлюзове и защитни стени. TCP, UDP, SYN, FIN, ACK и Window са най-честите нападения със сканиране.

3. КЛАСИФИКАЦИЯ НА АТАКИТЕ СРЕЩУ ИНФОРМАЦИОННАТА СИГУРНОСТ НА ИЗЧИСЛЕНИЯТА В ОБЛАК

Множеството от видове атаки е систематизирано в табл. 2 с цел конкретизиране на йерархията, в която попада и типът атаки към които попада.

Раздел и тип на атаките	**Група**
Мрежови атаки	DENIAL OF SERVICE, FLOODING, BACKDOOR CHANNEL ATTACK, THEFT OF SERVICE, PORT SCANNING
Атаки – лъжлив клиент	MAN IN THE MIDDLE, SIDE CHANNEL ATTACK
Стеганографски атаки	AUDIO STEGANOGRAPHY
Атаки социално инженерство	PHISHING
Малуер атаки	CLOUD MALWARE INJECTION, TARGETED SHARED MEMORY, BACKDOOR CHANNEL ATTACK, BOTNETS

Табл. 2. Раздел, тип и група на атаките

В основата на облачните услуги са залегнали принципите на глобалните мрежи и комуникации и това е причината до голяма степен заплахите и атаките срещу тях да са аналогични. Въпреки това съществуват някои специфики, които не позволяват директното използване на стандартните средства за мрежова защита.

4. ЗАКЛЮЧЕНИЕ

Според анализираните атаки може да се направи извода, че моделът Cloud Computing ще продължава да заема водеща роля в работата от потребителска и бизнес страна. Това налага насочване на усилията към създаване все по-ефективни системи за защита, които да съчетават в себе си, както традиционните средства за защита, така и нови такива, свързани със спецификата на облачните услуги.

ЛИТЕРАТУРА:

6. URL: http://www.businessinsider.com/10-most-important-in-cloud-computing-2013-4?op=1 [10.04.2015, 18:23 h]
7. URL: http://smartdatacollective.com/gilallouche/145341/7-well-known-companies-have-moved-cloud [10.04.2015, 19:10 h]
8. Станев, С., С. Железов, Компютърна и мрежова сигурност, Шуменски университет, Шумен, 2005

9. Khalil ,I., Khreishah , A., Azeem, M. Cloud Computing Security: A Survey
10. Singh, A., Shrivastava, Dr. M. Overview of Attacks on Cloud Computing
11. Siva, T., Krishna, E.S. P. Controlling various network based ADoS Attacks in cloud computing environment: By Using Port Hopping Technique
12. Zunnurhain, K., Vrbsky, V. Security Attacks and Solutions in Clouds
13. Oktay, U., Sahingoz O. Attack Types and Intrusion Detection Systems in Cloud Computing

НАПРАВЛЕНИЯ ЗА ИНФОРМАЦИОННА ЗАЩИТА НА ОБЛАЧНИТЕ УСЛУГИ

Дениз А. Еминов **Селиме И. Хасанова**
Гюнер И. Зекерие **Синан Д. Ниязиев**

Шуменски университет „Епископ Константин Преславски”
denyodeniz@gmail.com
sellhasanowa@gmail.com
guner.zekerie@abv.bg

DIRECTIONS FOR INFORMATION SECURITY OF CLOUD SERVISES

Deniz A. Eminov **Selime I. Hasanova**
Guner I. Zekerie **Sinan D. Niyaziev**

Bishop Konstantin Preslavski University of Shumen
denyodeniz@gmail.com
sellhasanowa@gmail.com
guner.zekerie@abv.bg

ABSTRACT: *This work provides an overview of using cloud technology as a model that enables network access to shared resources such as internet networks, servers and software applications with little involvement or control of the service provider. The need to protect the clouds of attacks as cyber attacks, data leakage, data loss, exposure of confidential information to unauthorized access. Types of protection of the cloud, which are used as multiple encryption and protection software (antivirus), mechanisms for access control, and protection from malicious mobile code, etc.*

KEY WORDS: *information hiding, steganology, steganography,information security, cloud computing, protection, cloud security, insiders,encryrting.*

1. Въведение

В интернет пространството все повече започна да се откроява терминът „Cloud”. Тенденцията е все повече в посока на развитие на облачните структури в науката и услугите, които предоставят те на хората.Облачните услуги (ОУ) пестят

много време, пари и ресурси. „Облаците“ представляват място, където дадена услуга може да бъде достъпна на определени хора (частни лица) или на маса хора (публична видимост). В себе си услугите крият много данни от различен вид и произход, които имат своята нужда от запазване, съхранение и поддръжка на услугата, в която те се намират. Популярна дефиниция на националният институт по стандарти и технологии (NIST) определя характеристиките на облачната технология като собствена услуга при поискване, неограничен мрежов достъп, споделен и наличен ресурс, светкавична еластичност и заплащане само на използваният ресурс.

Бързината, с която се преминава към облачни технологии по естествен начин увеличи изискванията към създаване на повече и по-разнообразни технологични модели.

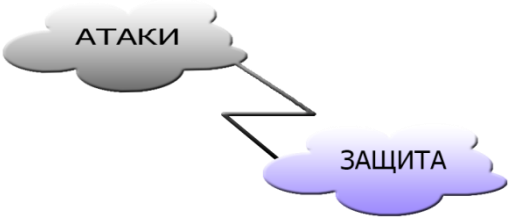
Изборът на тези модели зависи от вида на информацията и достъпа до нея както и от специфични изисквания по управлението.[1] Защитата им подлежи на много строг контрол под формата на логично ниво и на физическо ниво.

2. Специфика на защитата

Защитата е много важна за всички данни. ОУ са първа цел на хора атакуващи потребители, с цел кражба или заличаване на информация от тази среда. Данните са от първа важност и политиката на ОУ гарантира тяхната неприкосновеност и поверителност. Всяка такава услуга на различни доставчици гарантира запазването на данните в хранилището на „облака“ за дълъг период на време с гаранция на тяхната цялост и непокътнатост. Защитата в тези предоставени услуги трябва задължително да включва:

- По-висока надеждност на защита спрямо всички други структури от данни.
- Изискваща по вече данни за потребителят за да може да се идентифицира максимално при началната проверка.
- Задължително многослойно криптиране на данните получени от потребители ползващи услугата.
- Изискване към физическата подръжка да бъде максимално добре охранена и защита от злонамерен достъп към центъра на машината поддържаща тези услуги.

Спецификата на защита в себе си включва множество от методи, които препокривайки се успяват да гарантират максимална сила на защита. Сигурността в ОУ и Облачните структури от данни (ОСД) е един от най – важните критерии и цел на работа в тази сфера. Потребителят винаги трябва да знае, че ползваната услуга от него е максимално добре пазена и бранена.



Фиг. 1

3. Изисквания към потребителите

Потребителите не по-малко са отговорни за защита на собствената си информация. Тяхната лична защита и начин на предоставяне на личните си данни при регистрирането или ползването на такъв тип услуга трябва да е с максимална степен на сложност. При програмирането на такава платформа и услуга се изискват много добри познания по навиците на потребителите в интернет обществото така, че максимално добре да се усвоят пропуските на потребителите при самото попълване на поверителна и ценна информация. Пример за това може да бъде началната регистрация изискваща име/поща и парола за достъп. Ползващият услугата трябва да бъде много добре запознат, че неговите лични данни могат да бъдат повредени, заличени и дори откраднати при изтичане на информация за неговата ел. поща и парола.

4. Модели на облачните услуги:

- IaaS (Infrastructure as a Service) – Инфраструктурата като услуга
- SaaS (Software as a Service) – Софтуер като услуга
- PaaS (Platform as a Service) – Платформа като услуга

IaaS дава възможност да се използването на компютърната инфраструктура „под наем“. Вместо купуването на скъпи хардуерни сървъри, сървърен софтуер, дискови масиви за съхранение и др. компаниите имат възможност да използват това под формата на услуга - аутсорсиг продукт. Подобна услуга обичайно се заплаща на принципа на комуналните услуги. Цената зависи от обема на консумираните ресурси.

При **SaaS** модела софтуерът е инсталиран при доставчика и потребителите го достъпват чрез интернет. Моделът особено се разпространева с появата на Уеб услугите (Web Services). Разплащането е на абонаментен принцип.

PaaS моделът за доставяне на облачни услуги предоставя възможност на потреителя да разработва и редактира потребителски приложения и интерфейси върху облачната инфраструктура.

5. Видове облаци, уязвимост и защити

5.1 Видове облаци

-*частни облаци (private cloud)* – Инфраструктурата на облака се използва изключително за конкретната организация.Тя може да се управлява от организацията или от трета страна и може да съществува в помещения или извън помещенията на организацията.Трябва да се отбележе, че частният облак разчита като минимум на определени технологии, които са типични за публичните облаци – в това число, по специално, виртуализационни технологии, които подпомагат реорганизацията на архитектурата за обработка на данните.

-*публичен облак (public cloud)* – Инфраструктурата на облака се предоставя на широка общественост или на голяма отраслова група и собственост на организацията.

-*хибриден облак (hybrid cloud)* – Съставен е от два или повече облака

-*обществен облак (community cloud).* – Инфраструктурата на облака се споделя от няколко организации и служи за поддържането на специфична общност от потребители, които споделят обща мисия, обща политика, общи изисквания към информационната сигурност и други.

-вътрешен облак (облак в облаците)(Cloud of Clouds) – Инфраструктурата представлява, инфраструктура в друга себеподобна инфраструктура, която изпълнява определена функция.

5.2. Уязвимост

- *Динамични виртуални машини* – Виртуалните машини са доста гъвкави и бързо решение за много проблеми с физическите машини. Може да има една главна физическа машина и в нея да има множество виртуални машини, които работят в синхрон за процеси и подръжка на системата в стабилно ниво. Уязвимостта от атаки към виртуалните машини е висока, но въпреки това то е едно добро решение за да няма много физически достъпни машини към предлагата услуга. В облак компютърната среда е важно да се осигури статуса на заща на системата, докато тя не трябва да зависи от неговото състояние и местонахождение.

- *Уязвимост във Virutal Enviroment* – Облачните сървъри и локални сървъри използват същите операционни системи и приложения. За облаците заплахата от дистанционно хакване или зловреден софтуер инфекция е висока. Рискът за виртуални системи също е висока. Система за откриване на проникване и превенция трябва да бъде в състояние да открива злонамерени дейност на нивото на виртуални машини, независимо от тяхното местоположение в облака.

- *Защита в празех ход на виртуални машини* – Когато виртуалната машина е изключена е подложена риск, защото няма софтуер или програмен подход, който да я защитава успешно.

5.3. Защити

- *Запазване на данните.* Encryption – един от най-ефективните начини за защита на данните. Доставчик, който осигурява достъп до данните трябва да бъдат криптирани информация за клиента, съхранявани в информационния център, както и при липса на необходимостта да се заличава постоянно.

- *Защита на предаване на данни.* Encrypted – предаване на данни трябва да бъде на разположение само след удостоверяване. Данните няма да се четат или да се промени, дори в случай на достъп чрез ненадеждни възли. Тези техники са добре познати и надеждни алгоритми и протоколи AES, TLS, IPsec отдавна се използват от доставчиците.

- *Удостоверяване* – Различни методи за удостоверяване на ползващият услугата. Предимно човек се сертифицира чрез картинки, глас или образ за проверка.

- Потребителят Isolation – Използване на индивидуална виртуална машина и *виртуална мрежа.*

- *Защита от layer 3 и 4 атаки* – доставчиците на облачни услуги предоставят защита от този тип атаки чрез пренасочване на трафика към тяхната мрежа.Те пренасочват трафика вътрешно към техните центрове.По този начин големият брой пакети минава през различни пътища и атаката се акумулира от мрежата и крайният порт на клиента остава защитен.

- Защита на DnS усилваща се атака – при тази атак се използва същият метод като при layer 3 и 4 атаки.

- *Защита на Smurf атаки* – по голямата част от мрежовите оператори са конфигурирали техните маршрутизатори по такъв начин, че да забранят отговора ICMP към broadcast адреси.

- *Защита от атаки на седми слой* – този тип атаки са трудни за защита.Необходимо е филтриране на http трафика.Друг метод за защита, по който редица допълнителни проверки се извършват във фонов режим, междинна страница се представя на постителите на сайта в продължение на 5 секунди, докато проверките приключат.

ЛИТЕРАТУРА:

1. I. Piskov. Облачни технологични модели - видове облаци. [онлайн]. [прегледан 23.04.2015]. http://blog.icn.bg/новини-от-icn-bg/облачни-технологии-модели/.

2. Безопасност и защита при Cloud Computing. [онлайн]. [прегледан 23.04.2015]. http://www.slideshare.net/danielachudomirova/security-in-cloud-computing-17857629?related=1

3. Деница Петкова Петкова. Безопасност и защита при „Cloud Computing“. [онлайн]. [прегледан 23.04.2015]. http://www.slideshare.net/Exlanttia/ss-33475590

4. Найден Неделчев. Унифициране на критериите за информационна сигурност. [онлайн]. [прегледан 23.04.2015]. http://cio.bg/3221_unificirane_na_kriteriite_za_informacionna_sigurnost__zavrashtane_kam_izvora.1

5. D. Dobrev.”Trends in cloud security”. Научно-техническа конференция 2013. [онлайн]. [прегледан 25.04.2015].

6. Станев, С. Стеганологична защита на информацията. Университетско издателство „Епископ Константин Преславски”. Шумен, 2013.

7. Станев, С. Софтуерни продукти за стеганализ. В: Сборник научни трудове на Научна конференция 2013 ”Защита на личните данни в контекста на информационната сигурност. Факултет АПВОКИС на НВУ”В.Левски”. Шумен,2013.

8. Д. Еминов, С. Хасанова и Д. Тончев. Стеганография в он-лайн социални мрежи. В: Сборник научни трудове на международната научна конференция MATTEX14, Том 1, ISBN 1314-3921. Шумен, 2014. стр. 173-178.

9. Станев, С., С. Ниязиев, С.Железов, Х. Параскевов. Стеганологичен софтуерен пакет. В: Сборник научни трудове на Научна сесия на НВУ-факултет АПВОиКИС, Шумен, 2013. (под печат).

НАУЧНА КОНФЕРЕНЦИЯ 2015

НОВИТЕ ПРЕДИЗВИКАТЕЛСТВА ПРЕД СИСТЕМИТЕ ЗА ИНФОРМАЦИОННА СИГУРНОСТ

СБОРНИК НАУЧНИ ТРУДОВЕ

Българска. Издание първо. Тираж 30

Предпечатна подготовка - Факултет „Артилерия, ПВО и КИС“ - Шумен