MODELING OF CYBERSECURITY IN THE ARMED FORCES

Yana E. Kolegova-Delcheva

kolegova@abv.bg

Abstract: *The topic of cybersecurity is becoming increasingly important. The advent of computer technologies in the military sphere poses a number of challenges for cybersecurity. Modeling is a process that helps to detect vulnerabilities in the system with the purpose of preventing unauthorized access to information. The accurate definition of the terms "model" and "modeling", the classification of models, as well as the description of the stages in modeling help to create effective and adequate models guaranteeing the cybersecurity. The creation of that sort of a model and its implementation in the structures of the armed forces contributes to the normal functioning of the systems and protects the information from unauthorized access*

Keywords*:model, modeling, definitions, classification, cybersecurity, armed forces*

МОДЕЛИРАНЕ НА КИБЕРСИГУРНОСТТА ВЪВ ВЪОРЪЖЕНИТЕ СИЛИ

Яна Е. Колегова-Делчева

1. Увод

Непрестанното използване на киберпространството означава, че разтушаването му може да доведе до намаляването на способностите на въоръжените сили да функционират ефективно, както в мирно време, така и по време на криза. Случващото се в киберпространството се развива с изключителна скорост и традиционните отговори за защитата на критичната инфраструктура могат да се окажат недостатъчни. Засилването на зависимостта от използването на компютърните системи и мрежи носи, както ползи, така и нови заплахи за опазване на информацията. Днес всички области на военната способност (оръжейни системи, насочване и т.н.) са свързани с информационните технологии и приложенията [7]. Това налага създаването и прилагането на адекватни модели гарантиращи киберсигурността.

2. Моделиране

2.1. Общи дефиниции

Когато се говори за създаването на модели трябва да се дефинират и основните понятия. В речника MerriamWebster понятието модел е дефинирано най общо, като „обикновено, миниатюрно представяне на нещо“, когато се касае за компютърно моделиране, моделът е представен като „система от постулати, данни и изводи, представени като математическо описание на образуване или състояние на нещата[10]“. От друга страна моделът представлява „нов обект (реален, информационен или въображаем), различен от изходния, който притежава съществени за реализиране на поставените цели свойства и в рамките на тези цели напълно заменя изходния обект[4]“. В книгата на акад. Кирил Боянов „Цифрово моделиране“ терминът „модел се използва като синоним на структура, описание, начин на използване на език, граматика, теория, схема, стил, аналог, предложен метод за изследване, абстракция, формализиране или частично формализирана теория, психологическо спомагателно средство за теория, възможна реализация на теория, образец, конкретна система, физически обект, реалност и т.н.[1]“. Понятието „модел“ в научната литература „се използва за означаването на различни по смисъл неща. По-детайлно изучаване на неговата употреба показва, че в него се влагат предимно две коренно различаващи се противоположни значения: 1. на някаква теория и 2. на нещо, към което се отнася дадена теория, т.е. това което тя описва или отразява[1]“. При различните науки в понятието модел се влага различен смисъл, така при математическите науки моделът в смисъла на „изоморфна теория се определя от спецификата на абстрактните математически обекти и характера на математическите методи[1]“. Понятието модел, като теория се използва и в редица други случаи:

1. Когато теорията е началото на своето създаване;
2. Като синоним на количествена теория, математическа схема или като цяло математическо описание;
3. В употреба близка до теорията (логиката), терминът „модел“ се употребява в смисъла на формална или формализирана система. Формализирана система е система, в която началните елементи, правилата за построяване от тях на сложни съвкупности и правилата за преобразуване са точно фиксирани и ясно формулирани. Тази формализация и абстрактните отношения се реализира посредством формализиран език[1].

Теорията и моделът носят общи характеристики. И двете представляват форми на опростяване, на схематизация, на абстрахиране, но в моделът се проявяват законите съответстващи и извадени от теорията в чист вид, т.е. някакво конкретно построение, нагледно до каквато степен е възможно и достъпно за наблюдение и практическа дейност. Най-пълно и точно определение за „модел“ дава В.А. Штоф, а именно „под модел се разбира такава мислено представена или материално реализирана система, която отразявайки или възпроизвеждайки обекта на изследването е в състояние да го замести, така че нейното изучаване да ни дава нова информация за този модел[5]“.

Основни характеристики на модела са:

1. Моделът винаги изобразява определени части от действителността;
2. Основна цел, при създаването на модела е да се получи нова информация за обекта на изследването;
3. Моделът е конкретно създаден и трябва да бъде достъпен за наблюдение, изследване и практически действия.
4. Моделите могат да бъдат, както материални, така и идеални;
5. За всеки модел съществуват конкретни параметри, спомагащи за различаването на информацията на модела от тази на обекта[1].

Моделите притежават и редица свойства[3]:

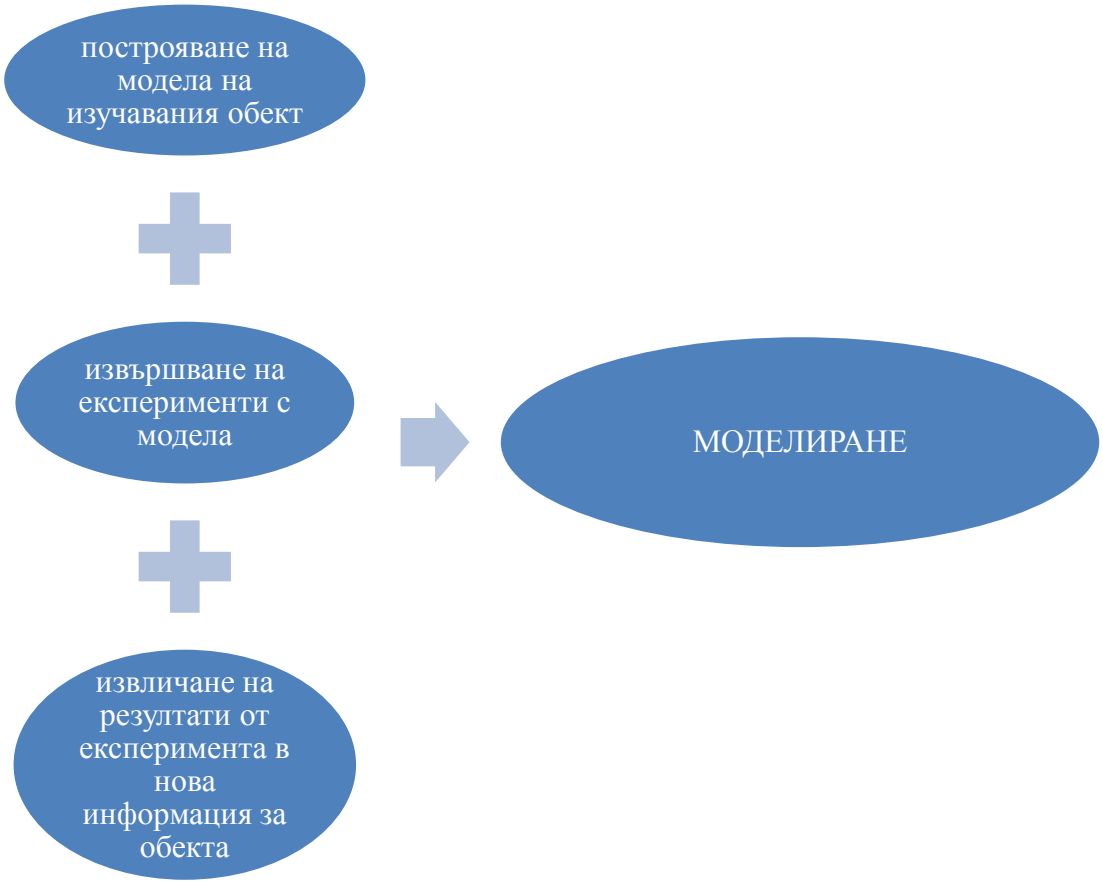
Фиг. 1. Свойства на моделите - http://tuj.asenevtsi.com/APIS/APIS04.htm

1. Крайност на модела – свойствата на абстрактните модели са фиксирани и могат да се използват само определени от множеството свойства на обекта, които ни интересуват;
2. Опростеност-за целите на моделирането се оказва достатъчно, не пълното, опростено изобразяване на действителността.
3. Приближеност – свързва се с количествените различия между модела и оригинала.
4. Адекватност- адекватен е онзи модел,с който се стига до поставената цел.

В съвременните условия на високо технологичен процес с цел постигане на ефективни резултати във всяка област, включително и военната от особено значение е моделирането. Изготвянето на адекватни модели може да доведе до ограничаване на уязвимостите в КИС, до ограничаване на пораженията при евентуална атака и до осигуряване на защитени военни КИС. На всяка една система могат да бъдат създадени собствени модели, чрез които да се предвиди необходимостта от изграждане на защитни, технически механизми за осигуряване на киберсигурността в мрежите. Счита се, че моделирането е станало основна и неизменна част от всички КИС.

Понятието „модел“ е тясно свързано с понятието „моделиране“. Моделирането представлява „метод за изследване на обекти, посредством техния модел [5]“.

Моделирането обединява три основни дейности [1]:



Фиг. 2 . Основни дейности при моделирането.

Моделирането има няколко характеристики [4]:

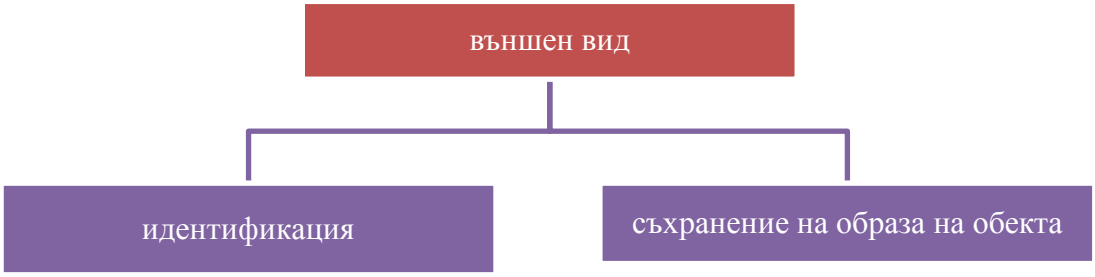
1. Структура - структура на обекта се нарича съвкупността от елементи и съществуващите между тях връзки.Структурата се използва за четири основни дейности (фиг.3).

2. Външен вид - под външен вид се разбира съвкупност от признаци, които характеризират външността на обекта и се използва за две основни действия (фиг. 4).

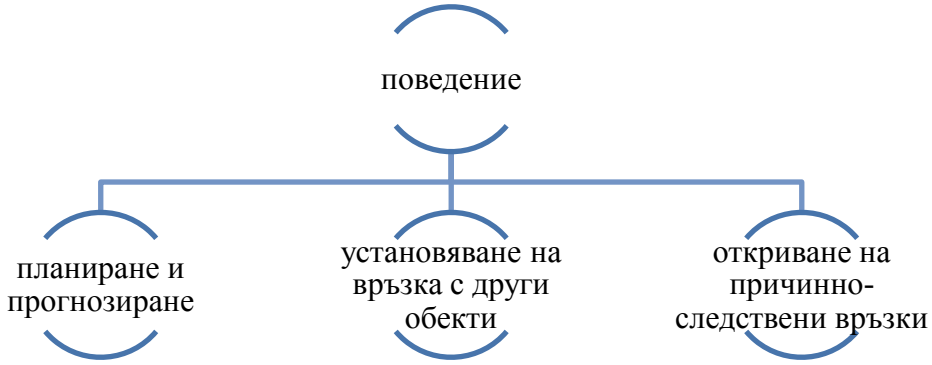
3. Поведение - поведение на обекта представлява измененията на неговия външен вид и структура при взаимодействие с външни обекти, протичащо във течение на времето.(фиг.5)

4. Управление - конструиране на технически устройства т.н.

Фиг. 3. Дейности изобразяващи структурата на моделите.



Фиг. 4. Действия изобразяващи структурата на моделите



Фиг. 5. Дейности характеризиращи поведението на моделите

2.2. Класификация на моделите

Когато говорим за модели и моделиране е необходимо да бъде направена класификация на самите модели. В книгата на акад. Кирил Боянов [1] моделите като за начало са разделени в три основни групи, по признаци, които ги характеризира (табл. 1).

Група модели	Обобщаващ класифициращ признак
Първа група	Начина на отражение или възпроизвеждане на действителността посредством моделите
Втора група	Начин на функциониране на моделите
Трета група	Характерът на онези страни на оригинала, които се възпроизвеждат или изследват в модела.

Табл. 1. Класификация на моделите по общи признаци

2.3. Етапи за създаване на модела

Когато се създава моделът той преминава през три основни етапа:

1-ви етап - създаване на концепция за модела- представлява етап на формулиране на замисъла на модела. Концептуалният модел представлява „описание и определяна на модела в абстрактни термини и понятия“.

2-ри етап – създаване на логическата блокова схема на модела – „представлява ясно, еднозначно, крайно и конкретно реализиране на абстрактната идея, описана в концептуалния модел.“

3-ти етап - програмиране на модела – представлява „запис на логическата блокова схема в термините на някой език за програмиране“. Езикът за програмиране представлява програмно средство за цифрово моделиране. Езиците за моделиране са „проблемно-ориентирани езици за програмиране, специално предназначени за описание на цифрови модели.“.[1]

При изграждането и създаването на модели за киберсигурност се заснема поведението и/или структурата на системата, свързана със сигурността. Моделът представлява абстракция на реалната система, от гледна точка на сигурността и понякога може да бъдат пропуснати други важни аспекти, които не засягат нейните свойства на защити. Модел, базиран на приложения, може да дефинира и се отнася до субекти, видими за потребителите (потребители, съобщения, файлове,

устройства за въвеждане и изход), докато базиран на механизъм модел може да се съсредоточи върху процеси, блокове за съхранение, заключване на файлове и т.н. Трудности възникват, когато изискванията за сигурност на ниво приложение са трудни за изпълнение с механизмите, налични на по-ниски нива. Тъй като компютрите са все по-взаимосвързани, заплахите за сигурността и уязвимостите, произтичащи от тези взаимовръзки, нарастват. Намирането на полезни, комбинируеми свойства за защита, които биха дали основа за свързване на системи, без да се въвеждат нови уязвимости, е актуална изследователска тема [9].

2.4. Формални модели

За да се създаде качествен обектно -ориентиран софтуер се използват моделите за анализ и дизайн. Моделите, касаещи въпросите за сигурността се присъединяват към обширните знания за сигурността и чрез тяхна помощ се изграждат по-сигурни и надеждни системи за киберсигурност. Изграждането на модели спомага за откриване на уязвимости в ранен етап, премахване на грешки в системата и предотвратяване на евентуални атаки[6]. За да бъде сигурна една система първо трябва да бъде уточнено, какво означава „сигурно“ спрямо нуждите на организацията. Киберсигурността при въоръжените сили е част от националната система за киберсигурност и се отнася о защита на класифицирана информация. Основната цел на създаването на формални (официални) модели за киберсигурност е да се убедят експертите в сигурността на определена системата [8]. Именно чрез изграждането на формални модели сигурност се демонстрира, че дизайнът на реалната система притежава надеждни механизми за защита. Всички модели за сигурност имат една обща цел, а именно да определят разрешените и неразрешените състояния на конкретната система и съответно да ограничат преминаването й към неразрешено състояние [2].

Когато говорим за киберсигурността във въоръжените сили трябва да се има в предвид, че моделите на сигурност, механизмите за защита, откриването на уязвимости в системите, както и предотвратяването на атаките произтича от наличието на информация, която попаднала в ръцете на врага може да навреди на националната сигурност. В Българската армия се разграничават различни нива на класификация на информацията:

- Некласифицирана (явна) информация;
- Информация класифицирана като служебна тайна - За служебно ползване;
- Информация класифицирана, като държавна тайна:

✓ Поверително;
✓ Секретно;
✓ Строго секретно.

Идеята за създаване на тази система за класификация на информацията е да се предотврати неконтролируемо разпространение на чувствителната информация. Чрез определени процедури за разрешение се определя нивото на достъп до информацията за всеки индивид, който работи в структурите на БА. Така при евентуални изтичане на информацията, отговорност ще носят лицата, които са имали достъп до нея.Освен това разделение на информацията в структурите на БА могат да се обособят и специални отделения, в които се борави с конкретна информация (документи касаещи НАТО, ЕС). За тях също се изисква определен документ за достъп, като непречи човек да притежава разрешения за достъп до информация на всички нива и отделения. Използването на комуникационни и информационни системи улеснява комуникацията между структурите и индивидите, редактирането, разпространениетои четенето на текстове става по опростено. Разбира се използването на компютърни системи има както своите ползи, така и своите недостатъци. От една страна голяма част от устройствата се използват от няколко потребителя. Когато един от тях няма необходимото разрешение за достъп до определена информация, това води до нерегламентираното й използване. От друга страна незащитените системи се превръщат в основен обект на атака от трети лица. В статията си „FormalModelsforComputerSecurity“, Carl E. Landwehr казва,

че информацията, която се съдържа в автоматизираните системи трябва да бъде защитена от три вида заплахи:

1. Неразрешено разкриване на информацията;

2. Неразрешено изменение на информацията;

3. Нерегламентирано отказване на информацията (обикновено наричано отказ от предоставяне на услуга) [8].

Официалните модели се използват за моделиране на военната сигурност и за основа „за определяне на програми, които карат компютъра да симулира контрола на сигурността във военна среда[8]“. Въпреки, че методът на моделиране представлява огледален образ на реалните системи, улавянето на сложностите от действителността във формална структура водят до отклонения в някой отношения. „По принцип моделите налагат контроли, които са по-твърди от тези в реалната среда. Всички компютърни операции, които се подчиняват на структурите на модела, са позащитени спрямо конвенционалните дефиниции[8]“. Някои от основните формални модели са:

- решетъчен модел на достъпа (LatticeModelof Access Security).
- модел на Bell-LaPadula за гарантиране на конфиденциалност на информацията;
- модел на Biba за контрол на достъпа;
- модел на Кларк-Уилсън.

За проверка на теоретичните ограничения на конкретна архитектура на система управление на сигурността се използват следните модели:

- модел на Graham-Denning;
- модел на Jones (take-grant) [2].

Те са създадени в различен период от време, съответно разрешават различни проблеми за сигурността и представят различни нива на детайлност в спецификациите си.

ИЗВОДИ:

1. Създаването на модели на вече съществуващи системи, спомага за тяхното развитие и усъвършенстване.
2. Осигуряването на ефективна система за киберсигурност е от съществено значение за функционирането на въоръжените сили.
3. С помощта на моделирането могат да се открият редица уязвимости в системите и най-вече да се създадат и приемат методи за тяхното предотвратяване.
4. Моделите спомагат за изграждането на ефективни и ефикасни механизми за предотвратяване на атаки в киберпространството.
5. Чрез изграждането на модели могат да се проверят различни средства за киберзащита, и да се избере подходящото такова, което да гарантира адекватната превенция срещу кибератаки.
6. Внедряването на формални модели, приспособяването им към спецификите на военната сфера, спомага за намаляването на уязвимостите и гарантира нормалното функциониране на системите.

Заключение:

Компютърните системи и мрежи обхващат все повече сфери от човешкия живот. Нарастващият им размер и сложността на мрежите води до нарастване на сложността на изготвяне на анализ за тяхната сигурност. Въпросът за защита на комуникациите излиза на преден план. Като част от изготвянето на адекватни политики за киберсигурност е създаването на модели, които имат за цел да намалят уязвимостите и да предоставят ефективни и ефикасни решения, осигуряващи защита на системите. Съчетаването на опит и добри практики води до разработването на ефективни модели за сигурност. Разработени са множество различни модели за сигурност за изграждане на адекватни и надеждни защитни системи. Такива например включват удостоверяване, контрол на достъпа(базиран на роли), авторизация, защитни стени и др. Така моделите предоставят храни-

лище от решения за настъпили проблеми. Моделът решава конкретен проблем в даден контекст и може да бъде пригоден да отговаря на различни ситуации. Моделите за сигурност описват точен общ модел за механизъм за защита.

References:

1. Боянов К., Н. Синягина, Р. Киркова, В. Лазаров, Г. Георгиев, С. Сребрев. „Цифрово моделиране.“- Техника, София, 1975
2. Дойчинов Д. „Модели за контрол на достъпа до информация“, сборник научни трудове „Облачните структури и защитата на информацията“, Шумен 2016 - http://www.aadcf.nvu.bg/scientific_events/papers_is/IS_2016.pdf
3. Туджаров, Хр. „Модел“, 2008 http://tuj.asenevtsi.com/APIS/APIS04.htm
4. Туджаров, Хр. „Моделиране“, 2008 - http://tuj.asenevtsi.com/APIS/APIS03.htm
5. Шнипа(Барнаул) Н.Г. „Модель формирования готовности студентов к дидактическому исследованию:“ -https://www.sibran.ru/upload/iblock/be3/be3cfee4ead8f5bb5c967419df34a05e.pdf
6. Fernández Eduardo B. „Security Patterns and Secure Systems Design“ - https://www.researchgate.net/publication/220996345_Security_Patterns_and_Secure_Systems_Design
7. KärkkäinenAnssi„Cyber security architecture for military networks using a cognitive network approach, 2013- https://www.doria.fi/bitstream/handle/10024/92640/Y2642_K%c3%a4rkk%c3%a4inenAP_YEK56.pdf?sequence=2&isAllowed=y
8. Landwehr C., „Formal models for computer security“ - http://crypto.stanford.edu/~ninghui/courses/Fall03/papers/landwehr_survey.pdf
9. Landwehr C., „Protection (security) models &policy“ - https://pdfs.semanticscholar.org/cc4c/0c2168bb9291d607053d6eb1022870f9e3dd.pdf
10. https://www.merriam-webster.com/dictionary/model