PROBLEMS OF PREVENTION IN THE PROTECTION OF INFORMATION CRITICAL INFRASTRUCTURE

HRISTO A. DESEV

National Military University "V. Levski", Artillery, "Air Defense and CIS" Faculty
Shumen, "K. Scorpil"str. № 1

***Abstract**: After a series of natural disasters and terrorist acts in recent years, the world community has already recognized that it is not possible to prevent all threats to all assets at all times.Key words: disaster, management operations, good practices. The resilience model consists of a hierarchy of four dimensions of system resilience, which together realize the four resilience capacities of the system. The evaluation of sustainability indicators aims to improve the assessment when making decisions for a specific structure of sustainability at the lowest level of its implementation. The aim is to create optimal characteristics and increase the capacity of the system.*

***Key words**: disaste, sustainability, prevent, capacity of the system.*

ПРОБЛЕМИ НА ПРЕВЕНЦИЯТА ПРИ ЗАЩИТАТА НА ИНФОРМАЦИОННАТА КРИТИЧНА ИНФРАСТРУКТУРА

Христо А. Десев

Европейският съюз (ЕС) е изправен пред все по-сложна съвкупност от рискове, които са преплетени във всички аспекти на бизнеса, инфраструктурата и общността. Заплахата от природни бедствия, финансова нестабилност, пандемии, престъпления в кибернетичното пространство, социални безредици, терористични актове и други разрушителни събития, произтичащи от процеса на глобализация, вече са част от ежедневието ни. След поредицата природни бедствия и терористични актове през последните години, световната общност вече призна, че не е възможно да се предотвратят всички заплахи за всички активи по всяко време. Така и политиките на ЕС и САЩ по отношение на сигурността на критичната инфраструктура (КИ) се фокусират най-вече върху нейната физическа защита.

Неправилното функциониране на системите или не добрата им защита водят до изключително сериозни негативни последици, дължащи се на факта, че информационните системи са се превърнали в необходимост за човешкото благосъстояние. Постепенното въвеждане на тотално управление на всички мрежи, въвеждането на системи за мониторинг и контрол, както и взаимозависимостта, която винаги в такива случаи възниква, със сигурност оптимизира и подобрява нивото на изпълнение в такава инфраструктура. За съжаление така се разрешава и достъп на киберпрестъпници и терористи, с произтичащите от това негативи. Така сценария става все по-сложен, тъй като въвеждането на съвременни технологии добавя на нови източници на потенциален риск, наред с традиционните заплахи.

В тази логическа последователност, идеята за определяне на устойчивостта на критичната инфраструктура се очертава като възможност за решение на проблема, като част от комплекса от дейности, насочени към превенция. Докато политиките за сигурност на критичната инфраструк-

тура са съсредоточени основно върху предотвратяването на терористични актове, аварии и други разрушителни явления, дейностите по изграждане на устойчивост на критичната информационна инфраструктура целят засилва способността ѝ да продължи да предоставя услуги, дори в случай на разрушена/нарушена функционалност.

Приложени съвместно, стратегиите за сигурност и в частност стратегиите за устойчивост на критичната инфраструктура осигуряват по-пълен набор от дейности за постигане на висока степен на готовност на КИ системите за работа в несигурна среда с множество опасности.

Най-разпространената теза за устойчивостта е, че инфраструктурната система се справя с промени, които могат да повлияят на нейната функционалност. Много определения предлагат механизми, с които инфраструктурата да реагира на промените и най-често споменаваните са:

• способности да устои на въздействието на негативната промяна;

• способности за бързо адаптиране в отговор на промяната;

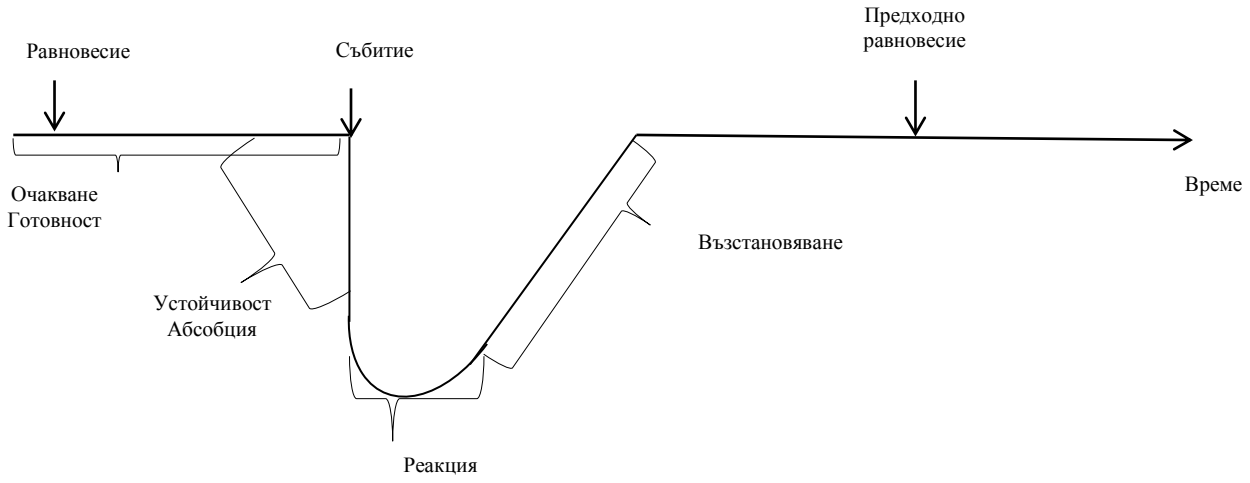
• възможности за възстановяване на системата и системната функционалност.

Оптимистична дефиниция се явява следната:

„Устойчивостта на инфраструктурата е способността и да намали силата и/или продължителността на действието на разрушителни събития. Ефективността на дадена устойчива инфраструктура или предприятие зависи от способностите ѝ/му да прогнозира, абсорбира, се адаптира към и/или бързо да се възстановява от потенциално разрушително събитие.“ [4]

Друго разширяващо понятията определение може да бъде: „Способността на дадена система и нейните компоненти да предвиждат и поглъщат, да се адаптират и възстановяват от ефектите на опасно събитие своевременно и ефикасно, гарантирайки запазване, възстановяване или подобряване на нейните основни структури и функции.“ . Фиг 1.

Като следствие от формулираните твърдения трябва да е ясно, че една система трябва да изгражда различни нива на устойчивост към различните по характер зловредни събития. Този извод е продиктуван от факта, че различните разрушителни събития оказват различно влияние на системата и ще се изискват различни процеси и стъпки за нейното възстановяване За жалост идеалната система функционираща в идеалния свят трудно може да се открие.Ефективността за успешно реагиране на системен срив, е по-рядко обсъждан, но също толкова важен въпрос. Във време на криза работната ръка, оборудването и други критични ресурси за реагиране и възстановяване са с голям дефицит.



Фиг. 1. Схема на различните разрушителни събития влияещи на системата
и процеса на нейното възстановяване

Устойчивостта на цялата система се изгражда чрез поддържане на сигурността на отделните подсистеми. Проблемите с възприемане на модела на изграждане е свързана с начина на предста-

вяне на инфраструктурните взаимозависимости. Аспектите на тази характеристика могат да се обобщят в четири основни групи: техническо, персонално, организационно и кооперативно.

Устойчивостта е функционална в резултат на поддържането на четири способности (капацитети): превантивна, абсорбираща, адаптивна, възстановителна.

Следователно, способността на системата да работи по време на разрушителни събития с по-малко потребление на ресурси, отколкото другите системи, би била желана характеристика и ще я направи по-устойчива от системите, изискващи повече ресурси.

Като се има предвид разнообразието от задачи, свързани със защитата на критичната информационна инфраструктура, важно е да се систематизират задачите и определят основните приоритети и отговорности. Тези основни задачи са подредени в модел, определен от четири основни стълба:

- превенция;
- откриване;
- противодействие;
- минимизиране на последствията. [4]

Анализът показва, че функционирането на различните КИ е тясно обвързано с изграждане и поддържане на превантивни способности, като те са основа на различните подходи за защитата на КИ.

Превантивните мерки помагат за намаляване на рисковете в критичните процеси. Те помагат за постигане на целите за тяхната оперативна защита и като по този начин се повишава прагът на критичност за потенциални кризи, възможни в организациите. Това може да намали броя и / или интензивността на кризисните инциденти.

Превантивните стратегии използват инструменти като предотвратяване на риска (за избягване на риска), пристрастие към риска и приемане на риска (ако не е възможно да се помогне за намаляване на действителния риск).

Мерки за намаляване на рисковете, вероятността от които е достатъчна ниска, но ще има драматични последици, ако се появят, често е невъзможно да се обоснове само въз основа на анализа на разходите и техните резултати. В такива случаи трябва да се вземат предвид социалните и етични съображения, както и правната рамка, когато се вземат решения относно предпазните мерки.

За анализ, проектиране и управление на безопасността на КИ се използват превантивно статични многостепенни модели на основните видове КИ. Тези модели се използват за структурирано описание на пространството, където се извършват функционални и информационни процеси и се извършват процедури за управление на тези процеси.

Статичните модели на КИ са важни за безопасността именно защото са източник на правила, условия и ограничения за появата и разпространението в рамките на нивото и между нивата на „неизправности“ на КИ, водещи до авариен инцидент. Основното функционално натоварване на статичния КИ модел е да се идентифицира влиянието на критериите за информационна сигурност върху функционалните критерии за сигурност.[7]

Референтните модели определят пет функционални нива, но това, което обикновено се разбира под КИ, заема нива от второ до нула. Поради високото ниво на своята концептуалност, този модел практически не се използва в независима и не подробна форма и намира приложение като основа за по-развити и специализирани модели.

Понякога се използва, предлага и разработва моделът на физическата архитектура на КИ, който описва физическите компоненти, обединени от мрежата за контрол на информацията.

Рационалната симбиоза на тези два модела (референтна и физическа архитектура) може да е моделът на зониране. Този модел може да бъде платформа за предвидимост на заплахи, уязвимости, рискове и контрамерки (контрол и дейности). Моделът за зониране е многостепенна диаграма на критическия обект и се състои от следните нива (зони):

- ENTERPRISE SYSTEMS, цялостно (стратегическо) управление на сигурността в обекта;

- MES, буферно ниво за изпълнение на цялостни политики за управление;
- SCADA, диспечерско ниво;
- CONTROL SYSTEM, локално ниво включващо процес на сигурност;
- I/O, терминално ниво.

Анализът на известните практически методи за моделиране на тези процеси през целия им жизнен цикъл и в цялото пространство от фактори и обстоятелства, влияещи върху тях, показа, че с помощта на такива модели е възможно ефективно да се контролират превантивно причинно-следствените вериги на инцидента.

Една от най-разработените стратегии за решаване на този проблем е концепцията „Защита в дълбочина“ , която включва използването и прилагането на голям брой контрамерки по стъпаловиден начин (разделяне на нива). Смисълът на концепцията се крие във факта, че след проникване, нападателят през едно от защитните нива, той се среща с нова, може би принципно различна защита на атакувания обект. Тази хибридна многопластова отбранителна стратегия използва цялостен подход към сигурността в цялата КИИ. Според редица експерти в бъдеще тази концепция ще се превърне в стандарт за осигуряване на безопасност в КИ.

- основни модели на заплаха - идентифицирани и квалифицирани видове външни (агресивност на околната среда) и вътрешни (несъвършенство на обекта) събития и ситуации, които са причина за инцидента;
- статични модели на структурирано описание на пространството, в което се извършват функционални и информационни процеси, и се извършват процедури за управление на тези процеси, за да се идентифицира влиянието на критериите информационна сигурност, базирана на функционални критерии за сигурност;
- динамични модели на възникване и разпространение на инциденти със сигурност в средата на ИСИ, които осигуряват способността за изследване и управление на тези процеси;

Защита на критичната информационна инфраструктура е цикличен процес и не се ограничава само до осигуряване на незабавна и ефективна реакция. Участващите в този процес трябва да прилагат ефективни мерки за превенция, за откриване на основни заплахи, ранжиране на рисковете и разкриване на слаби места в системите.

Основните цели на защита на критичната инфраструктура могат да се конкретизират до:

- установяване на критичната информационна инфраструктура;
- дефиниране и описание на междусекторните зависимости;
- определяне на зависимостите на критичната информационна инфраструктура от информационните системи, включени в управлението на държавата;
- създаване на национална програма за защита на критичната информационна инфраструктура;
- разработване на оперативни процедури за подпомагане на собственици и оператори на критична информационна инфраструктура, (както на правителствено ниво, така и на частния сектор) с цел минимизиране на риска при пропадане на части или цели сегменти от нея;
- съгласуване на правилата и оперативните процедури съвместно с международните Critical Information Infrastructure Protection (CIIP) организации за определяне на транснационални решения и минимизиране на последствията; [7]
- измерване на нивото на ефективност достигнато с течение на времето и корекции в законодателството, стратегиите, правилата и процедурите, на основата на такова измерване.

Национални усилия за укрепване на критичната сигурност и устойчивостта на инфраструктурата зависи от способността на общността на критичната инфраструктура да приеме солидни, информирани за риска, решения за разпределяне на ограничени ресурси както за ежедневни, така и за кризисни операции. Следователно управлението на риска, което трябва да се превърне в крайъгълния камък на Националната програма за защита на инфраструктурите, е от значение както на държавно, така и на местно ниво.

Безопасността и устойчивостта на две нива зависи от създаването и поддържането на надеждни партньорства между бизнес общността и държавата, местните власти и обществените организации.

References:

1. Директива (ЕС) 2016/1148 на Еевропейския парламент и на съвета, 2016г.
2. Национална стратегия за киберсигурност „Киберустойчива България 2020".
3. Закон за киберсигурност.
4. Траянов И., Haldane Systems Ltd (UK), 2017г.
5. Centre for European policy studies – Brussels, „Protecting critical infrastructure in the EU", CEPS task force report;
6. Bernhards Blumbergs, „Technical analysis of advanced threat tactics, targeting critical information infrastructure" GXPN, NATO CCD CoE, CYBER SECURITY REVIEW, Winter 2014;
7. Петухов, Гусин Эталонная модель безопасности критических информационных инфраструктур.
8. NSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration — Part 1: Models and Terminology
9. NIST Special Publication 800-82 Revision 2 «Guide to Industrial Control Systems (ICS) Security», May 2015.