IT4Sec Reports 116
http://dx.doi.org/10.11610/it4sec.0116

Политики за защита на критичната инфраструктура от кибер атаки

Йоана Иванова

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, декември 2014 г.

Йоана Иванова, Политики за защита на критичната инфраструктура от кибер атаки**,** *IT4Sec Reports* 116 (София, Институт по информационни и комуникационни технологии, декември 2014 г.), http://dx.doi.org/10.11610/it4sec.0116.

IT4SecReports 116 „Политики за защита на критичната инфраструктура от кибер атаки“
В разработката са детайлно разгледани политиките на САЩ по отношение на проблемите на киберсигурността, които се съдържат в Президентска директива PPD-21 (Presidential Policy Directive). Дефинирани са ясно задачите, които трябва да се решат за оценяване и планиране на защитата на критична инфраструктура. Дадени са конкретни примери за подходи и средства за защита на критичната инфраструктура от кибер атаки.

IT4Sec Reports 116 In this paper is addressed in details the policy of the US regarding the issues of cyber security that are contained in Presidential Policy Directive (PPD-21). The tasks that should be solved for evaluation and planning of critical infrastructure protection are clearly defined. The following are specific examples of approaches and means to protect critical infrastructure from cyber attacks.

ISSN 1314-5614

СЪДЪРЖАНИЕ

1. УВОД

Терминът „инфраструктура“ (от лат. „*инфра*“ – фундамент, „*структура*“ – строеж, разположение, взаимодействие) започва да се използва през XIX век от швейцарския офицер и генерал Антуан-Хенри Жомини (Antoine-Henri Jomini), който е забележителен военен стратег. По време на Втората световна война този специфичен военен термин добива гражданственост, като основно се употребява в логистиката за обозначаване на всички фиксирани и недвижими инсталации и средства за осигуряване и контрол на въоръжените сили (открити комуникационни връзки - пътища, железопътни линии, мостове, съоръжения за поддръжка; съоръжения по осигуряването).[1] Постепенно понятието инфраструктура започва да се използва широко и в други сфери – икономиката, компютърните науки, сигурността.

По своята същност критичната инфраструктура на всяка държава представлява „*система от съоръжения, услуги и информационни системи, чието спиране, неизправно функциониране или разрушаване би имало сериозно негативно въздействие върху здравето и безопасността на населението, околната среда, националното стопанство или върху ефективното функциониране на държавното управление*“.[2] Критичната инфраструктура се състои от много елементи, чието сигурно и безопасно функциониране трябва да бъде следено стриктно от съответните органи и институции, за да бъдат предвидени и избегнати крайно нежелани последици за населението. Следователно мерките за укрепване и поддържане на сигурна, функционираща и устойчива критична инфраструктура са от първостепенна важност за националната сигурност като цяло.

За постигането на удовлетворителни крайни резултати е необходимо е да бъдат ясно формулирани задачите, които трябва да се решат за оценяване и планиране на защитата на критичната инфраструктура. Освен това трябва да бъдат обмислени средствата за защита на критичната инфраструктура от кибер атаки, за да може практическата реализация на политиките да отговори на очакванията, заложени в хода на процесите по прогнозиране и планиране. За тази цел в разработката предстои да бъдат представени политиките на САЩ и други страни за сигурност и устойчивост на критичната инфраструктура, включително защита от кибер атаки. Политиките конкретно на САЩ се съдържат в Президентска директива PPD-21 (Presidential Policy Directive).[3] Усилията са насочени към противодействие на физически заплахи и кибер атаки, като специално внимание се обръща на превантивните мерки, които могат да бъдат взети на база на предварителна оценка на риска от дадена заплаха.

---

[1] ЛОГИСТИКА – РЕЧНИК НА ИЗПОЛЗВАНИТЕ ТЕРМИНИ. 09 04, 2014. http://rnda.armf.bg/rechnik-logistika/ (accessed 11 07, 2014).

[2] Закон за управление при кризи, § 1, т. 8 на Допълнителната разпоредба. Отменен.

[3] Хаджитодоров, Стефан. ЗАЩИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА В НАЦИОНАЛНОТО ЗАКОНОДАТЕЛСТВО НА РЕПУБЛИКА БЪЛГАРИЯ И... 12 01, 2007. http://www.expert-bdd.com/index.php?option=com_content&task=view&id=745 (accessed 11 07, 2014).

2. ЗАДАЧИ, КОИТО СЕ РЕШАВАТ ЗА ОЦЕНЯВАНЕ И ПЛАНИРАНЕ НА ЗАЩИТАТА НА КРИТИЧНА ИНФРАСТРУКТУРА

Изграждането на съгласувана и цялостна политика за сигурност в киберпространството е практически трудно изпълнимо, защото е свързано с цензурата в интернет пространството, националния суверенитет и обстоятелството, че съществуват правителства, които не признават общоприети международни споразумения. Въпреки че Съветът на Европа е единствената международна институция, приела официално документ за борба с киберпрестъпността през 2004 г., подписан от 22 държави, включително САЩ, достоверни сведения сочат, че системите на ЕС са най-ненадеждно защитени. Това е така поради факта, че решенията на проблемите, свързани със сигурността на критичната инфраструктура, могат да бъдат еднозначни само, ако проблемите са структурирани. Но под въздействие на множество фактори с различна сила това е трудно постижимо. Каквото и решение да бъде взето, съществува риск да не бъде постигнат желания резултат. Затова от голямо значение е да бъдат поставени конкретни задачи за оценяване и планиране на критична инфраструктура и да са работи последователно и организирано за тяхното изпълнение.

Задачите за вземане на решение могат да бъдат обединени в групи, както това е направено в следната таксономия:

A. Оценка и представяне на заплахи

- Определяне, характеризиране и оценка на заплахите и опасностите;
- Описване на тяхната реализация чрез достоверни сценарии и избиране на набор от сценарии, на база на които да бъде създадена политика и да бъдат планирани целите.
- Представяне на по-дълбока несигурност.

B. Оценка на уязвимостите

- Определяне на сектори, подсектори и активи на критичната инфраструктура;
- Оценка на уязвимостта на отделни активи.
- Анализ на чувствителността.

C. Изследване и разбиране на взаимозависимостите

- Оценка на съществуващите взаимозависимости между активи, подсистеми и инфраструктури;
- Опрделяне на взаимозависимостите, които биха могли да доведат до каскадни ефекти.

D. Оценка на негативните въздействия

- Проектиране на критерии и мерки;
- Анализ на всеки сценарий;
- Избиране на начин на действие;
- Определяне на въздействието на сценарий;
- Агрегиране на оценка на въздействието или казано с други думи отчитане на вероятността за едновременно реализиране на два или повече сцанария;

E. Формулиране на политиката за защита на критичната инфраструктура (CIP Policy) [4]

- Вземане на решение относно обхвата на понятието „критична инфраструктура“, отичтайки възприятия, готовност за ангажираност и др.;
- Формулиране на цели и задачи и вземане на решение относно;
- Разработване на стратегия;
- Възлагане на отговорности;
- Разпределяне на ресурси.

F. Вземане на решения за инвестиции в защита на критичната инфраструктура

- Определяне на изискванията относно способностите;
- Изследване на инвестиционните алтернативи;
- Оценка на възможностите;
- Анализиране на начините за предоставяне на мерки и способности за защита, като например например приложими форми на публично-частни партньорства;
- Оценка на инвестиционния риск;
- Вземане на решение относно инвестициите.

G. Стратегическо управление

- Анализ и подобряване на управленските процеси;
- Анализ на иновативни подходи, концепции и стратегии;
- Създаване и въвеждане на стандарти за безопасност и сигурност на критичната инфраструктура;
- Гарантиране на почтеност, прозрачност и отчетност.[5]

3. ЗАЩИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ОТ КИБЕР АТАКИ

Един национален подход за справяне със заплахи има за цел да бъде изготвена стратегия за реагиране на база на вече направените предварителни анализи и оценки. Както вече стана дума, това изисква разработване и въвеждане в експлоатация на нови високи технологии. Това от своя страна е свързано с големи финансови инвестиции, които следва да бъдат напълно оправдани при правилно извършена предварителна селекция. Резултатите биха били удовлетворителни, ако са изпълнени редица изисквания. Напрактика, колкото и мощна финансово да е дадена държава, не би могла да осигури тясно специализирана технология за противодействие само на един определен вид заплаха. Това налага да бъде избрана най-оптималната като цена и възможности технология, която да се характеризира с гъвкавост и многофункционалност. По този начин се очаква тя да

[4] Critical Infrastructure Protection

[5] Todor Tagarev, Venelin Georgiev, and Petya Ivanova. "Analytical Support to Critical Infrastructure Protection Policy and Investment Decision - Making." http://procon.bg n.d. file:///C:/Users/User/AppData/Local/Temp/28.01_Tagarev_Georgiev_Ivanova-2.pdf.

бъде високо ефективна срещу различни по своята същност заплахи. В широкия смисъл една такава технология трябва да притежава следните основни характеристики:

- да бъде изработена от висококачествени и по възможност нови материали;
- да не представлява смъртоносно оръжие;
- да извършва анализ на данни;
- да бъде съвместима с други съоръжения.

Предвид, че настоящият материал е посветен на киберсигурността, следва наред с физическата сигурност, да бъдат взети мерки, които да гарантират защитеността на виртуалното пространство. За тази цел се разработват специализирани софтуерни продукти, които подлежат на многократно тестване преди да бъде заключено, че притежават необходимата надеждност. Всички предварителни експерименти, изпитвания и анализи се извършват от високо квалифицирани експерти при строг контрол, за да бъдат сведени до минимум възможни неточности и грешки. Необходимо е да се обърне сериозно внимание и на комуникационните системи, чието прекъсване би разрушило възможностите за обмен на информация. Това на свой ред би имало инвалидизиращо въздействие върху всички сектори на критичната инфраструктура.

При избора на технологии и изграждането на политики за киберсигурност следва да се предвиди, че една кибер атака може да бъде обусловена от различни мотиви – финансови, политически и дори лични. Наред с безспорните предимства от широката употреба на дигитални технологии и използването на Интернет, трябва да се отбележи, че те благоприятстват зачестяването на кибер атаките. В повечето случаи жертва на кражба на самоличност стават обикновени граждани, които не проявяват необходимото внимание при работа в Интернет пространството. Системите за извършване на on-line финансови транзакции и операции трябва да включват надеждни механизми за защита на своите потребители. С тези примери не се изчерпват всички възможни престъпления в Интернет.

Финансовите инвестиции, които трябва да бъдат направени, за да се противодейства на различни по сила и характер кибер атаки, са сериозно изпитание за икономиката дори на държави от ранга на САЩ и Великобритания. В много случаи атаките са неуспешни, но това не понижава разходите за смекчаване на последиците от тях. Практическото изпълнение на политическите програми за сигурност не е лека задача не само заради финансовата страна, но и поради сложността на йерархичната система, която трябва да бъда изградена. Човешкият ресурс в този случай е от изключителна важност и затова подборът на служителите и ръководителите на съответните служби и агенции също трябва да бъде извършен строго професионално при спазване на всички изисквания за конфиденциалност и запазване неприкосновеността на личното пространство. Все пак остава въпросът как да бъдат оптимизирани финансовите разходи без това да повлияе на резултатите от борбата с кибертероризма. Най-сигурният и сравнително спестяващ средства начин се базира на моделиране и симулации, които осигуряват висок реализъм и дават възможност за прогнозиране с голяма точност на база на предварителен анализ. При едно компютърно подпомагано учение се оперира изцяло във виртуална среда, пресъздаваща реална обстанова или ситуация. Това е най-иновативният и ефективен изследователски метод, който дава възможност за проиграване на широк диапазон от ситуационни сценарии. Много от тях не биха могли да бъдат реално проиграни поради факта, че са животозастрашаващи. Във виртуална среда не само могат да бъдат симулирани различни извънредни ситуации, но е възможен допълнителен анализ, включващ обработка на изходните данни, както и съхранението им в база, от която при необходимост да се ползват и споделят. Такива мащабни учения по киберсигурност вече са провеждани с цел съответните органи да бъдат

обучени как да реагират в случаи на кибер атаки, целящи да засегнат комуникациите или други сектори на критичната инфраструктура.

Необходимо е да се обърне внимание на архитектурата за киберсигурност на стратегическо, оперативно и тактическо ниво. Казано с други думи, една такава архитектура трябва да осигури защита на практически всички уязвими места от локалните работни станции до т. нар. „облак“. Най-широко се използват следните архитектури:

- ***SANS - SysAdmin, Audit, Networking and Security***[6] - тази архитектура е известна като „20 критични контроли на сигурността”, защото се определят 20 контролни точки за изграждане и функциониране на единна система за киберзащита.
- ***Архитектура на Northrop Grumman Corp.*** - това е 5-слойна архитектура, която има за цел осигуряване сигурност на периметъра, мрежова сигурност, сигурност в крайните точки, сигурност на приложенията и сигурност на данните.
- ***Архитектура на канадските въоръжени сили (DNDAF)***[7] - за разлика от другите архитектурни рамки, DNDAF гарантира сигурността на информацията посредством три изгледа: оценка на риска; матрица за сигурността на данните; матрица на агрегираната информация за сигурността.[8]

За по-голяма конкретизация Таблица 1 представя една примерна класификация на средствата за защита от кибер атаки, с което не се изчерпват всички възможности за противодействие при заплахи.

Таблица 1

КИБЕРСИГУРНОСТ	*СРЕДСТВА ЗА ЗАЩИТА*
Уеб сигурност	**Антивирусни програми**
E-mail сигурност	**Софтуер за защита от спам, шпионски софтуер, BotSniffer**
Мрежова сигурност	**UTM, Firewall, VPN, IPS**
Защита на приложения	**Антивирусни програми**
Защита от неоторизиран достъп до информация	**UTM, Firewall**

Поради факта, че една от най-сериозните и зачестили заплахи за киберсигурността в световен мащаб са BotNet – мрежите, интерес представлява антиботнет софтуерът BotSniffer, който е разработен като plug in към IDS[9] и е с отворен код Snort. BotNet - мрежите

[6] SANS - SysAdmin, Audit, Networking and Security

[7] DNDAF - Canadian Department of Defense / Canadian Forces Architecture Framework

[8] http://cio.bg/5603_arhitektura_za_kibersigurnost__tehnologichni_aspekti

[9] IDS - Intrusion Detection System

представляват софтуерни приложения или компютри, които разпространяват злонамерен софтуер с цел кражба на лични данни. BotSniffer трябва да разпознае зловредния софтуер. Това става по комуникацията за управление и контрол чрез статистически методи.[10]

4. ПОЛИТИКА ЗА КИБЕРСИГУРНОСТ НА САЩ

Безспорно САЩ са един от лидерите в сферата на киберсигурността. Техният пример указва пътя, който трябва да се следва, за да бъде изградена сигурна и стабилна система за защита на критичната инфраструктура и гарантиране на националната сигурност като цяло. За засилване на киберсигурността би допринесло внедряването на „по-модерни механизми за мрежово взаимодействие между организациите от системата за сигурност за публично-частно взаимодействие“ (Проф. Тодор Тагарев, министър на отбраната в служебното 88-мо правителство на РБ).[11]

Ако изходим от определението за критична инфраструктура съгласно Закона за управление при кризи, е необходимо да отбележим, че определението на САЩ включва и виртуални системи и приложения.[12] САЩ разполагат с киберкомандване към Стратегическото командване на Пентагона; специализирани кибервойски; специална програма „Айнщайн“ в рамките на Министерството на националната безопасност, която има за цел пресичане на хакерски атаки, насочени към правителствените компютърни мрежи; „кибер-оръжия“ под формата на логически бомби, микровълнови излъчватели с обхват няколко мили за поразяване на микросхеми, ботнети и др.[13]

Федералното правителство взема активно участие във всички процеси, имащи за цел укрепване на сигурността и устойчивостта на критичната инфраструктура, чрез прилагане на специфичен подход, който се базира на следните три стратегически императива:

1) Уточняване и изясняване на функционалните взаимовръзки във Федералното правителство с цел осигуряване на националното единство в стремежа към укрепване сигурността и устойчивостта на критичната инфраструктура;

Една ефективна национална инициатива за укрепване на сигурността и устойчивостта на критичната инфраструктура трябва да се ръководи от национален план, който определя ролите и отговорностите и добива информация от експертни познания, опит, способности и отговорности на секторните агенции, федералните служби и агенции с

[10] Нови методи за борба с ботнетите 19.02.2008. http://chzv.net/security/war-against-botnest (accessed 08 22, 2014)

[11] Проектът за киберсигурност бил отхвърлен, сега се работи по възраждането му . 04 29, 2013. http://pan.bg/view_article-4-16963-Proektyt-za-kibersigurnost-bil-othvyrlen-sega-se-raboti-po-vyzrazhdaneto-mu.html (accessed 11 10, 2014).

[12] Тодор Тагарев, Николай Павлов. "Методика за определяне на критична инфраструктура и разработване на стратегия за защита." в Първа национална научно-практическа конференция по управление в извънредни ситуации и защита на населението (София, БАН, 10 ноември 2005 г.), стр. 352-361; Todor Tagarev and Nickolay Pavlov, “Planning Measures and Capabilities for Protection of Critical Infrastructures,” Information & Security: An International Journal 22 (2007): 38-48, http://dx.doi.org/10.11610/isij.2205.

[13] Димитров, Стефан. "Кръгла маса "Състояние и проблеми на сигурността в киберпространството на България"." *http://www.atlantic-bg.org*. 09 28, 2010. http://www.atlantic-bg.org/images/news/round-table-cyber-sec-28_09-2010/docs/intro-dimitrov-28-09-10.pdf (accessed 10 11, 2014).

критични инфраструктурни роли, SLTT субекти и собствениците и операторите на критична инфраструктура.

През последното десетилетие са създават нови програми и инициативи в отговор на въпроси, отнасящи се до критичната инфраструктура и приоритетите биват променяни и разширявани. В резултат функциите на федералните органи, свързани със сигурността и устойчивостта на критичната инфраструктура, трябва да бъдат изяснени и усъвършенствани с цел да се установят основните възможности, които ще отразяват тази еволюция на знания за определяне съответните функции на федералната програма и улесняване сътрудничеството и информационния обмен между и в рамките на Федералното правителство, собствениците и операторите на критичната инфраструктура и SLTT субектите.

Като част от тази прецизна структура, би трябвало да има два национални критични инфраструктурни центъра, управлявани от Министерство на вътрешната сигурност, – съответно за физическа и за кибер инфраструктура. Те функционират по интегриран начин и служат като фокусни точки за партньорите на критичната инфраструктура да получат информация за ситуацията и интегрирана, действена информация за защита на физическите и кибер аспекти на критичната инфраструктура. Предвид, че физическите и кибер елементи на критичната инфраструктура са неразривно свързани и в еднаква степен уязвими, функция „интегриране и анализ“ (допълнително разработена в Стратегически императив 3) следва да бъде изпълнена между тези два национални центъра.

Успехът на тези национални центрове, включително интегрирането и функция „интегриране и анализ“, зависи от качеството и актуалността на информацията и сведенията, които те получават от секторните агенции и други федерални служби и агенции, както и собствениците и операторите на критична инфраструктура и SLTT субекти.

Тези центрове нямат за цел да изземват функциите на ръководителите на федералните служби и агенции и да ги възпрепятстват при изпълнение на техните основни отговорности, свързани с националната отбрана, борбата с престъпността и тероризма, разузнаване и контраразузнаване.

2) Осъществяване на ефективен информационен обмен чрез идентифициране на изходните данни и системни изисквания за Федералното правителство;

Една сигурна, устойчива и функционираща критична инфраструктура изисква ефективен информационен обмен, включващ разузнаване между всички правителствени нива и собственици и оператори на критичната инфраструктура. По този начин би трябвало да се улесни своевременния обмен на информация за заплахите и уязвимите места, както и информация, която дава възможност за осигуряване на ситуационна осведоменост по време на инцидента. Целта е да се гарантира ефективен обмен на информация чрез определяне на изискванията относно данни и информационни формати и достъпността, оперативната съвместимост на системата и резервни системи.

Споделянето на информация с правителството и частния сектор може и трябва да се направи по начин, който не накърнява гражданските права и свободи. Федералните служби и агенции се задължават да гарантират, че всички съществуващи принципи за поверителност, политики и процедури се изпълняват в съответствие с приложимото законодателство и висши служители на съответните служби ще следят стриктно за запазване неприкосновеността на личния живот в усилията си да управляват и контролират правилно споделянето на информация.

3) Прилагане на функцията „интегриране и анализ“ в поддръжка на органите по планиране и взимането на оперативни решения относно критичната инфраструктура.

Третият стратегически императив е изграден на база на първите два и призовава към функция „интегриране и анализ“ за критичната инфраструктура, включваща оперативен и стратегически анализ на инциденти, заплахи и нововъзникващи рискове. Той трябва да намери своето място в пресечната точка на двата национални центъра, определени в Стратегически императив 1 и да включва способност за съпоставяне, оценка и интегриране на уязвимостта и впоследствие на информацията за:

a) Помощ при приоритизирането и управлението на рисковете за критичната инфраструктура;

b) Предвиждане на взаимозависимости и каскадни въздействия;

c) Препоръчване на мерки за сигурност и устойчивост на критичната инфраструктура преди, по време и след събитие или инцидент;

d) Подкрепа на усилията за управление на инциденти и възстановяване, свързани с критичната инфраструктура.

Тази функция не трябва да дублира аналитичната функция на Разузнавателната общност или Националния център за борба с тероризма, нито да включва дейности по събиране на информация. Разузнавателната общност, Министерство на отбраната, Министерство на вътрешната сигурност и други федерални служби и агенции трябва да предоставят актуална и подходяща информация на двата национални центъра относно националната критична инфраструктура. Освен това тази функция трябва да използва информация и сведения, предоставени от други критични инфраструктурни партньори, включително SLTT и неправителствени аналитични субекти.

В заключение, тази функция „интегриране и анализ“ трябва да подпомага способността на Министерството на вътрешната сигурност за поддържане и споделяне както на общата Федерална служба, така и на способността за ситуационна осведоменост в реално време относно критичната инфраструктура, което включва информация за непосредствени заплахи, важни тенденции и информираност за инциденти, които могат да окажат въздействие върху нея.

За ефективно прилагане на PPD - 21 се изисква Министърът на вътрешната сигурност[14] да осигури стратегически насоки, да насърчава националното единство на усилията и да координира усилията на Федералното правителство за подобряване на сигурността и устойчивостта на националната критична инфраструктура. В изпълнение на отговорностите, произтичащи от Закона за национална сигурност от 2002 г., Министърът на вътрешната сигурност изпълнява следните функции:

- оценява националните способности, възможности и предизвикателства при защита на критичната инфраструктура;
- анализира заплахите, уязвимите места и потенциалните последици от всички опасности, на които е изложена критичната инфраструктура;

[14] Secretary of Homeland Security

- определя функции, свързани със сигурността и устойчивостта, които са необходими за ефективно публично-частно партньорство с всички критични инфраструктурни сектори;
- разработва национален план и показатели в координация със секторните агенции и други партньори на критичната инфраструктура;
- интегрира и координира федерланите междусекторни дейности, свързани със сигурността и устойчивостта;
- установява и анализира основните взаимозависимости между секторите на критичната инфраструктура;
- изготвя отчети относно ефективността на националните усилия за укрепване на националната сигурност и устойчивостта.

Наред с гореизброените основни функции не се изчерпват всички отговорности на Министъра на вътрешната сигурност, които са детайлно описани в Президентската директива относно политиката за сигурност и устойчивост на критичната инфраструктура. Тя предоставя детайлна информация относно йерархичните структури във Федералното правителство, както и ролите и отговорностите на федералните служби и агенции, техните ръководители и служители. В директивата се обръща специално внимание на научните изследвания и иновациите, с които е тясно свързано провеждането на политиките за укрепване сигурността и устойчивостта на критичната инфраструктура. Финансирането на научно-изследователски и развойни дейности е от първостепенна важност за укрепване на сигурността и устойчивостта на критичната инфраструктура. Акцентира се върху съвременните кибер технологии, както и върху моделиране и симулиране на потенциални въздействия върху критичната инфраструктура.

Друг важен документ е подписаната от президента на САЩ Изпълнителната заповед за укрепване сигурността и устойчивостта на критичната инфраструктура и в частност на киберсигурността.[15] Основните изводи, които могат да се направят на база на тази заповед са, че усилията са насочени към осигуряване защита на компютърните мрежи и ситеми на жизненоважни сектори от критичната инфраструктура; споделянето на информация в реално време между управляващите органи и собствениците и опраторите на критична инфраструктура; създаване на методологии и въвеждане на стандарти за подобряване на киберсигурността в частния сектор.

На база на горепосочените материали могат да се направят редица заключения, свързани с факторите, от които зависи сигурността на националнта критична инфраструктура. Необходимо е да се положат усилия за изграждане на вътрешна среда за сигурност, която да е способна да устои на непрекъснато настъпващи промени от различен характер, които на свой ред водят до възникване на рискове за критичната инфраструктура. При отчитане и оценка на тези рискове трябва да се вземат предвид степента на неопределеност и нееднозначност на дадени въздействия. Това усложнява процесите на прогнозиране и вземането на подходящи превантивни мерки срещу дадена заплаха. Опитът на САЩ е много ценен в това отношение и би могъл да служи като пътеводител на България, за да бъде способна страната ни да изгради сигурна и максимално устойчива на външни въздействия вътрешна среда. „Вътрешна среда“ е обобщаващ термин за физическа и киберсреда поради съществуващата взаимозависимост между тях. Проблемът с киберсигурността е глобален и представлява сериозна заплаха за компютърните мрежи и инфор-

[15] Executive Order - Improving Critical Infrastructure Cybersecurity. 02 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed 11 18, 2014).

мационните системи в световен мащаб. За да бъда една страна способна да се справи с рисковете и заплахите за своята сигурност, тя трябва да се стреми към международно сътрудничество с други страни и да бъде възприемчива към прилагане на доказано ефективни методи и подходи от техния опит.

5. Примери за политиката за киберсигурност на други страни

След подробното разглеждане на политиката, възприета от САЩ за укрепване на сигурността и устойчивостта на критичната инфраструктура, предстои да бъдат описани някои специфики на политиките на други страни относно средствата и подходите за противодействие на кибер атаки.

Една от страните с най-голям опит в областта на сигурността е Холандия, чието правителство стартира проект за защита на критичната инфраструктура, известен като „Bescherming Vital Infrastructur" (2002 г.). Акцентира се върху анализ на холандската инфраструктура; насърчаване на публично-частното партньорство; анализ на заплахите и уязвимостите и анализ на необходимите мерки за проитиводействие, както на заплахи за физическата среда, така и на сериозни кибер атаки.

През 2007 г. Центърът за защита на Националната инфраструктура на Великобритания[16] се слива с Националния център за координация на сигурността на инфраструктурата[17] и Националния консултативен център по въпроси на сигурността[18], като основните му функции са актуализирането на системата за идентифициране на критичната национална инфраструктура и защита на Националната критична инфраструктура от физически и кибер атаки.[19] Великобритания разполага с Оперативен център за киберсигурност, който се управлява от Щаба за правителствена свръзка.[20] Обединеното кралство инвестира изключително в киберсигурност, като тенденцията е тези инвестиции да се увеличат през следващите няколко години поради нарастващите кибер атаки, насочени главно към бизнес сектора. Министерство на бизнеса, иновациите и уменията (BIS)[21] осъзнава и признава огромното значение на киберсигурността за икономиката на Обединеното кралство. Във връзка с това то подема инициатива за стартиране на изследователски проект, който има за цел приемането и достъпността на стандарти за киберсигурност в целия частен сектор. Тези стандарти се характеризират с взаимосвързаност, която се основа на взаимно допълване, но не на взаимозависимост или последователност. Например, Европейският институт за телекомуникационни стандарти[22] публикува своите материали под дадена ключова дума, но всъщност всеки от тях се отнася за различна технология. Приемствеността по отношение на стандартите в сферата на бизнеса е подложена на подробен анализ, който се базира на сериозни проучвания. Например, за

[16] CPNI - Centre for the Protection of National Infrastructure

[17] NISCC - National Infrastructure Security Co-ordination Centre

[18] NSAC - National Security Advice Centre

[19] Стойчев, Кирил. "Основи на проблема "Критична инфраструктура"." In Монография "Сигурност и защита на обекти от критичната инфраструктура". София: Национален военен университет "Васил Левски", 2013.

[20] Димитров, Стефан. "Кръгла маса "Състояние и проблеми на сигурността в киберпространството на България"." http://www.atlantic-bg.org. 09 28, 2010. http://www.atlantic-bg.org/images/news/round-table-cyber-sec-28_09-2010/docs/intro-dimitrov-28-09-10.pdf (accessed 10 11, 2014).

[21] BIS - Department for Business, Innovation and Skills

[22] ETSI - European Telecommunications Standards Institute

стандарт ISO27001:2005 ("Системи за управление на информационната сигурност. Изисквания") резултатите показват, че е приложен изцяло само от 7 от общо 19-те организации (37%). Изводът от изследването показва, че „частичното прилагане“ на стандартите за киберсигурност преобладава с най-висок процент. Следователно, усилията трябва да бъдат насочени към това организациите да осъзнаят необходимостта и ползите от въвеждането на стандартите за повишаване на киберсигурността.[23]

Подходът на правителството на Белгия за укрепване на сигурността и устойчивостта на критичната инфраструктура срещу кибер атаки е разгледан в Ръководството на Белгия за кибер сигурност. Концептуално той има много допирни точки с този на Великобритания, тъй като стремежът е заинтересованите органи, институции и организации да се отнасят сериозно към въпросите на киберсигурността и да прилагат отговорно принципите за защита на комуникационните и информационните системи в хода на рутинния работен процес. В Ръководството на Белгия за кибер сигурност са формулирани 10 ключови принципа в 3 насоки за управление на информационната сигурност, както следва:

(A) виждане;

(B) организация и процеси;

(C) нагласа (начин на мислене).

Нестандартния начин, по който са формулирани самите принципи провокира по-задълбочен анализ:

1) ***Поглед отвъд технологията*** – целта е понятието „информационна сигурност“ да бъде разгледано в широк смисъл, а не само по отношение на информационните технологии. По този начин картината на потенциалните заплахи и въздействия ще бъде много по-детайлна и ясна, защото ще представлява съвкупност от хора, процеси и технологии. Това способства предприемането на мерки с по-висока ефективност.

2) ***Спазването на закони, разпоредби и стандарти не е достатъчно*** – разбира се, спазването на законите е необходимо, но не достатъчно условие за подобряване на киберсигурността. То не бива да се превръща в самоцел или в ограничение, когато се налага да се прояви гъвкавост при вземане на решение.

3) ***Превръщане на амбициите за сигурност в политики*** – въпросите на киберсигурността не могат да бъдат разглеждани едностранчиво, т.е. технологично, защото се касаят до други сфери. За да с премине от идеи към практически действия е необходимо да бъде изготвена политика, включваща насоки и стандарти.

4) ***Гарантирана ангажираност на висшето ръководство*** – това се налага поради необходимостта от осигуряване на ресурси – човешки, финансови, технически.

5) ***Създаване на прозрачност и влагане на лична отговорност*** – отговорните лица трябва да се отчитат за информацията и нейната защита и трябва да

[23] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf

притежават определени правомощия, инструменти и обучение, за да постигнат това.

6) ***Запазване на сигурност при „аутсоурсване“*** - при изпълнение на проекти, в които участват трети страни биха могли да възникнат проблеми, касаещи се до конфиденциалността на споделяната информация. В такива случаи може да се прилага криптиране.

7) ***Гарантирането на сигурността е фактор за иновации*** – внедряването на нови технологии носи редица предимства и крие някои рискове за сигурността. За да се избегнат нежелани последици при въвеждане на нова технология, е необходимо експертен екип по сигурността да се ангажира с тестването ѝ и да се вземат съответни мерки.

8) ***Поддържане на повишено внимание*** – дори добре изградената защита може да се окаже недостатъчна поради непрекъснато развиващите се заплахи. Напрактика установените политики и процедури могат да се окажат недостатъчно ефективни в даден момент. За да бъдат избегнати непредвидени атаки е препоръчително да се прави периодична оценка на устойчивостта, уязвимите места и адекватността на дейностите за защита чрез оценки и одити, тестване на системите чрез симулиране на проникване и своевременното му откриване.

9) ***Фокусиране*** – усилията трябва да бъдат насочени към защита на най-ценната информация, за да не се стига до загуба на конфиденциалност, цялостност или достъпност.

10) ***Готовност за справяне с инциденти*** – въпреки мерките, които се вземат, кибер атаките срещу дадена институция могат да се окажат успешни и да причинят поражения. Възможността за бърза и адекватна реакция определя до каква степен нанесените щети ще бъдат пагубни. При добра комуникация между съответните звена и структури атаката може да бъде незабавно овладяна.[24]

Проблемите на киберсигурността са комплексни и не могат да бъдат разглеждани еднозначно от гледна точка единствено на кибер атаки, чийто проводник е Интернет. Например, в гражданското въздухоплаване не се набляга на мерки за киберсигурност, но това би могло да се окаже голям проблем впоследствие поради внедряването на нови информационни технологии, което на свой ред повишава рисковете от кибер атаки. Навигационните системи използват протокол от следващо поколение ADS-B, внедрен в Австралия и в райони с натоварено въздушно движение в САЩ. Той дава възможност за прецизно проследяване на полетите и по този начин повече самолети могат да летят близо един до друг, превозвайки повече пътници, което от своя страна увеличава финансовите постъпления за съответните авиокомпании. Но при злонамерено външно вмешателство в данните на протокола, е възможно да бъде симулирано движението на самолети, които в дадения момент не летят. Практическа симулация на подобна атака доказва, че ADS-B има свои недостатъци, които могат да бъдат компенсирани само чрез вземане на съответни мерки срещу атаки от такъв характер.[25]

[24] http://vbo-feb.be/Global/Nieuws%20-%20media/Nieuws/cyber%20securit%20guide/icc_belsec_guide_LR_v2.pdf

[25] http://computerworld.bg/41982_vazduhoplavatelnata_agenciya_na_oon_preporacha_rabotna_grupa_po_kibersigurnost

ЗАКЛЮЧЕНИЕ

Прогнозите на експертите, че в ерата на Интернет проблемът със сигурността ще се разраства, вече се сбъдват. Но при осъзнаване на риска, предприемане на необходимите предпазни мерки и поемане на отговорност ситуацията може да бъде овладяна. На база на проучените политики за защита на критичната инфраструктура от кибер атаки може да се направи извод, че между вътрешната и външната сигурност няма ясна граница поради тяхната взаимозависимост. Политиката на САЩ в тази насока има за основна задача да поддържа международното сътрудничество. От друга страна мениджмънтът в информационното пространство изисква прилагане на нови стратегии за справяне с кибер заплахите, базирани на подобрени методи и подходи за работа. Мениджмънтът на киберсигурността се основава изцяло на знания за информационните системи и технологии и на натрупан предходен опит.

При търсене на решение на проблемите на киберсигурността трябва да се изходи от необходимостта да бъде осигурена защита на кибер мрежите чрез иновативни софтуерни решения и съвременни архитектури за осигуряване на цялостна защита. За постигането на сигурност и устойчивост на критичната инфраструктура са необходими значителни ресурси, които могат да бъдат редуцирани с развиване на по-голяма възприемчивост към новите тенденции в сферата на високите технологии. Те дават възможност за провеждане на реалистични симулации във виртуални среди, които за разлика от реалните учения, спомагат за избягване на редица рискове при минимална загуба на време и финансови средства.

Моделирането на въздействието на киберзаплахи върху сектори на критичната инфраструктура е иновативен подход за тестване и анализ на въздействия и атаки, както и за изграждане на ефективни защити срещу тях. Компютърните симулации правят възможно провеждането на експерименти във виртуална среда с използване на математически модели на реални системи. По този начин може да се направи реалистична оценка на риска и да се решат редица изследователски проблеми, свързани с изработването на стратегии за превенция, избора на мерки за защита и подобряване сигурността и устойчивостта на критичната инфраструктура.

ЛИТЕРАТУРА

Логистика – речник на използваните термини., 2014.

Hadjitodorov, Stefan. Защита на критичната инфраструктура в националното законодателство на република българия., 2007.

Tagarev, Todor, Venelin Georgiev, and Petya Ivanova. "Analytical Support to Critical Infrastructure Protection Policy and Investment Decision-Making." Information & Security: An International Journal 28, no. 1 (2012): 13-20.

Tagarev, Todor, and Nickolay Pavlov. "Planning Measures and Capabilities for Protection of Critical Infrastructures." Information & Security : An International Journal 22 (2007): 38-48.

Dimitrov, Stefan. Състояние и проблеми на сигурността в киберпространството на България In Кръгла маса., 2010.

Executive Order - Improving Critical Infrastructure Cybersecurity., 2013.

Stojchev, Kiril. "Основи на проблема "Критична инфраструктура"." In Монография “Сигурност и защита на обекти от критичната инфраструктура. София: Национален военен университет "Васил Левски", 2013.