IT 4 Sec Reports

Кибернетична сигурност – аспекти на проявление и отражение върху отбраната

Петко Петков

Cybersecurity: Emerging Characteristics and Impact on Defence

Petko Petkov

98

IT4Sec Reports 98
http://dx.doi.org/10.11610/it4sec.0098

Кибернетична сигурност – аспекти на проявление и отражение върху отбраната

Петко Петков

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

София, юни 2012 г.

Петко Петков, Кибернетична сигурност – аспекти на проявление и отражение върху отбраната**,** *IT4Sec Reports* 98 (София, Институт по информационни и комуникационни технологии, юни 2012 г.), http://dx.doi.org/10.11610/it4sec.0098

IT4SecReports 98 „Кибернетична сигурност – аспекти на проявление и отражение върху отбраната“ Изследват се кибернетичните заплахи и се анализира влиянието им върху отбранителния потенциал. Изложението е структурирано в три части. В първата част са представени характеристиките и е предложена класификация на заплахите в кибернетичното пространство и са описани съответни стандарти за сигурност. Във втората част се анализират примери за организация на противодействието срещу кибер заплахи на основата на опита на САЩ, Великоритания, Франция и други. В третата част се анализират възможности за прилагане на този опит в България, и в частност в Министерството на отбраната.

IT4Sec Reports 98 “Cybersecurity: Emerging Characteristics and Impact on Defence“ This report provides an overview of threats in cyber space and their potential impact on the defence potential. First, it outlines the features of cyber threats, suggests a respective classification and presents related standards. The second part provides analysis of selected examples for organizing cyber security in the experience of the US, UK, France, etc. The final part discusses the potential implementation of identified good practice in Bulgaria, and specifically in the defence ministry.

ISSN 1314-5614

СЪДЪРЖАНИЕ

УВОД 4

1. ВИДОВЕ КИБЕРНЕТИЧНИ ЗАПЛАХИ 5

1.1. Характеристики на информацията 5

1.2. Класификация на кибер-заплахите 6

1.3. Стандарти за кибернетична сигурност 8

1.4. Изводи 10

2. ПРИМЕРИ ЗА ОТГОВОР СРЕЩУ КИБЕР-ЗАПЛАХИ 11

2.1. Подход на Европейския съюз 11

2.2. Нацинална стратегия за кибернетична сигурност на Германия 12

2.3. Национална стратегия за защита на информационните системи на Франция 13

2.4. САЩ 14

2.5. НАТО 16

2.6. Изводи 16

3. БЪЛГАРИЯ И КИБЕРНЕТИЧНАТА СИГУРНОСТ 18

3.1. Организациии в областта на кибер-защитата 18

3.2. Кибернетична сигурност и отбрана 19

3.3. Изводи 20

ЗАКЛЮЧЕНИЕ 21

УВОД

Съвременният свят, и особено този, който познаваме, през последните 10-15 години, е неразривно свързан с информационните технологии и комуникациите. Почти няма човек в България и в значителна част от света, който да не се докосва под една или друга форма до тази всеобща свързаност – било чрез социалните мрежи, гледането на телевизия on-line или просто теглене на пари от банкомат. Лавинообразно нараства и използването на безжичния пренос на данни, което още повече допринася за всеобщата и постоянна свързаност - вече навсякъде има покритие с някоя от технологиите: Wi-Fi, WiMAX, GPRS, HDSPA и др. Макар и за малцина да са понятни всички тези съкращения, ние всички ги ползваме чрез нашите по-модерни мобилни телефони (smart-phones), таблети, лаптопи и т.н. По данни на *Internet world stats*[1] към 31.12.2011 г. 71,5% от жителите на ЕС са потребители на Интернет. Потопени в този информационен океан, ползваме неговите предимства за незабавен достъп до информация и услуги, но много рядко се замисляме за опасностите, които крие.

Нашата ежедневна активност е свързана с използване на компютри както на работното място, така и вкъщи, за парични преводи, за заплащане на сметки или просто за забавление. При всички тези дейности се генерира значителен информационен поток, който минава през различни преносни среди – безжично, по оптичен кабел, през телефонния оператор и дори през сателити. Малцина се замислят колко възможности има информацията да бъде подменена, изкривена или просто съхранена за бъдеща употреба/злоупотреба.

Освен заплаха за нашата лична неприкосновеност и финансова сигурност, разкриването на конфиденциална информация е с особено опасни и непредвидими последици в областта на сигурността. Настоящата работа няма за цел да изследва конкретни проблеми, нито да дава препоръки за защита на информацията, а по-скоро да погледне на проблема от държавно и организационно ниво и да определи какво е мястото на отбраната в този процес.

В изследването са използвани предимно интернет източници и някои закони, (които също могат да бъдат намерени в интернет), което е обусловено от естеството на проблема – ако имаме такъв в кибер-пространството, то отговорът следва да се търси на същото „бойно поле".

Разгледани са подходите към проблема на водещи в областта нации като САЩ, а също така и на организациите, на които България е член – НАТО и ЕС, и какво от техния опит можем да ползваме.

Представените в работата аргументи и изводи са лично мнение на автора и не ангажират институциите, с които служебно е свързан.

---

[1] *Usage and Population Statistics*, Internet World Stats, June 30, 201, вж. http://www.internetworldstats.com/ stats9.htm

1. ВИДОВЕ КИБЕРНЕТИЧНИ ЗАПЛАХИ

За да бъде разбрана кибернетичната сигурност (в много от публикациите на български език се използва и термина „киберсигурност") следва да се започне от определението: що за състояние е това и каква част от сигурността е. Терминът произлиза от английското (или по-скоро американското) „cyber security" и според речника Merriam-Webster е употребен за първи път през 1996 г.[2] Едно от кратките и достатъчно ясни определения е, че това е състоянието да бъдем защитени от злоумишлено или непозволено използване на информация в електронен вид или от действия, целящи това.[3]

Друго определение (на Харвардския университет) показва обхвата на проблема в цялостния контекст на сигурността, започвайки от престъпленията в електронния свят и достигайки до кибер-война.[4] Така дефинирана, кибернетичната сигурност обхваща елементи от националната и международната сигурност, както и редица нейни аспекти като спазване на закона, вътрешен ред, икономическа сигурност (така напр. банковите измами в Интернет вече са ежедневие) и достигайки дори до националната сигурност. Още на ниво определение се вижда, че този проблем надхвърля ведомствените отговорности и националните граници и под една или друга форма е грижа на всеки един, който има досег с информационните технологии.

Тази тематика в някаква степен е засегната и в Стратегията за национална сигурност, но от гледна точка на заплахите: "Киберпрестъпността е глобална и анонимна заплаха за информационните системи. Деструктивните въздействия върху информационните системи и мрежи могат да доведат до криза чрез затрудняване и/или блокиране нормалното функциониране на важни за икономиката, финансовата система и държавното управление системи или отделни компоненти."[5]

Всички посочени до тук определения и цитати акцентират върху главната цел на кибернетичната сигурност – информацията. В съвременния свят, а и преди това, тя дава предимство на този, който я притежава и управлява, но същевременно може да се обърне и в негова слабост, ако бъде компрометирана. Това води до въпроса: „Кои са основните характеристики на информацията, които следва да бъдат защитавани"?

1.1. ХАРАКТЕРИСТИКИ НА ИНФОРМАЦИЯТА

На първо място се поставя *конфиденциалността* – това са номера на банкови сметки, лични данни, пароли, лична и служебна кореспонденция и т.н. – цялата тази информация следва да бъде виждана само от онези, за които е предназначена. Това е и един от най-честите обекти на кибер-престъпността. В областта на отбраната и в целия сектор Сигурност информацията е обект на специална защита, като още през 2002 г. в България е приет Закон за защита на класифицираната информация (Обн. ДВ бр. 45, 30.04.2002 г.), който обхваща не само кибернетичната, но и физическата сигурност на информацията. Има

---

[2] Според речника Merriam-Webster е употребен за първи път през 1996 вж. http://www.merriam-webster.com/dictionary/cybersecurity

[3] Oxford dictionaries, Oxford University Press, 2012, вж. http://oxforddictionaries.com/definition/cybersecurity. В оригинал: „the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this". (Всички преводи в материала са от автора).

[4] Harvard University, 2012, вж. http://cyber.law.harvard.edu/cybersecurity/Main_Page. Оригиналното определение гласи: „The term "Cyber security" encompasses a range of issues from Cybercrime to Cyberwar. These in turn embrace a diverse set of activities and interests"

[5] *Стратегията за национална сигурност* /СНС/ *на Република България*, приета с Решение на Народното събрание от 08 март 2011 г., с. 6. http://www.mi.government.bg/bg/themes/strategiya-za-nacionalna-sigurnost-na-republika-balgariya-904-300.html

създаден и специален орган ангажиран с това – Държана комисия по сигурността на информацията, една от многото задачи на която е да „осъществява общ контрол по защитата на класифицираната информация - съхранявана, обработвана и предавана в автоматизирани информационни системи или мрежи."[6] По отношение на личните данни има Закон за защита на личните данни (Обн. ДВ. бр. 1, 04.01.2002 г.) и съответна Комисия за защита на личните данни. За важността на тези данни и тяхната защита от несанкциониран достъп може да се съди по инцидент от 2008 г., когато служител на НЗОК продава информацията за милиони българи на фармацевтични компании и здравни фондове.[7]

Втората много важна характеристика на информацията е нейната *достоверност* – тя може да обхваща както същността и целостта на данните, така и техния произход. Примери в тази посока има достатъчно много – фалшифициране на избори, умишлено манипулирани статистически данни, а във военната област – дезинформация на противника.

Друг важен показател на информацията е нейната *достъпност* – информацията е ценна именно с това, че може да бъде използвана. Какво от това, ако имате най-защитената с пароли и физически средства електронна поща, ако тя може да бъде проверявана само от едно единствено място в света. От друга страна много хора, а и цели организации подценяват важността на защитата на информацията. Именно противоречието между защита и достъпност създава заплахите в кибер-пространството.

1.2. КЛАСИФИКАЦИЯ НА КИБЕР-ЗАПЛАХИТЕ

Видовете заплахи могат да се класифицират по три основни признака – кой ги извършва, какво цели и какви средства използва.

По отношение на *извършителите* спектърът може да обхваща от тийнейджър с ограничени познания и достатъчно свободно време, през организираната престъпност, целяща данните от Master card, до китайски кибер-бойци от Синята армия (Blue army).[8]

Популярност в интернет публикациите е придобила класификацията на *Robert Siciliano* [9] (консултант на компанията за антивирусен софтуер McAfee) за седем вида мотивация на атакуващите, които са популярни с термина „хакер": „Под **хакер** обикновено се разбира някой, който разбива определена компютърна система най-често с цел собствена облага - независимо дали това е придобиването на информация, данни, присвояване на данни, създаване на неоторизирани/непозволени или изискани от поддържащите системата специалисти промени в системата, които често водят до нейния срив, недобра функционалност и т.н."[10]

Той разделя хакерите на следните типове:

Хакери с бели шапки (*в оригинала: White Hat Hackers*): Това са „добрите", ползващи техники за пробив с цел да открият уязвимости на системите, които тестват – това са ИТ

---

6 *Закон за защита на класифицираната информация* /ЗЗКИ/, обн. *Държавен вестник*, бр. 45 от 30 април 2002 г., вж http://www.dksi.bg/NR/rdonlyres/5F7CC69F-7496-4A8A-8E13-4D983F720B15/0/ZZKI_14_10_2011.pdf

7 *Лични данни на милиони българи са изтекли от НЗОК*,BTV news, 07.08.2008 вж. http://btvnews.bg/116465-Lichni_danni_na_milioni_balgari_sa_iztekli_ot_NZOK_(video).html (20.06.2012)

8 *China Confirms Existence of Elite Cyber-Warfare Outfit the 'Blue Army*, Fox news, May 26, 2011, вж. http://www.foxnews.com/scitech/2011/05/26/china-confirms-existence-blue-army-elite-cyber-warfare-outfit (20.06.2012)

9 Seven Types of Hacker Motivationsy, Infosec island, March 25, 2011, вж. http://www.infosecisland.com/blogview/12659-Seven-Types-of-Hacker-Motivations.html (20.06.2012)

10 *Дефиниция за Хакер*, Уикипедия, вж. http://bg.wikipedia.org/wiki/Хакер

професионалисти, работещи за държавни организации или за фирми в областта на сигурността.

Хакери с черни шапки (*Black Hat Hackers*): Това са „лошите", които създават вируси, „троянски коне" и др. и проникват в компютърни мрежи и системи. Те най-пълно съответстват на цитираното по-горе определение за хакер и успяват да изпреварят технологично системите и мерките за защита чрез използване на човешки грешки или чрез откриване на нови методи за проникване.

Script Kiddies (*няма термин на български*): Това е пренебрежително название за онези, които нямат достатъчно технически компетентности и ползват инструменти и подходи създадени от „истински хакери", като чрез зловредните си действия се опитват да се докажат и да си създадат име.

Хактивисти (*Hacktivists*): Това са хакери, мотивирани от политически, религиозни или други причини и обединени от обща кауза - да навредят на определен субект. Терминът е използван още през 1996 г. и от тогава е натоварен с много различни значения.[11]

Държавни хакери (*State Sponsored Hackers*): Това са хакери с почти неограничени ресурси и целите им са корпорации, държавни и частни институции на потенциалния противник на държавата - спонсор. Държавите ги финансират, перефразирайки старото правило, че „който владее морето, владее света" в областта на кибер-пространството. Пример в това отношение е кибер-атаката срещу средствата за масова информация в Грузия, предшестваща военните действия в Руско-Грузинската война от 2008 г.[12] Подобно развитие на събитията има и през април-май 2012 г. с координирани и добре организирани кибер-атаки срещу петролните компании в Иран[13] и срещу държавните институции на същата страна.[14]

Хакери-шпиони (*Spy Hackers*): Големите корпорации наемат такива с цел да проникнат в системите на конкуренцията и да се доберат до търговски и технологични тайни. Те могат да ползват технологични методи или просто внедрени „къртици". Методите им на действие са като на хактивистите, но целта им е да добият информация за своя клиент.

Кибер-терористи (*Cyber Terrorists*): Това са хакери, водени от религиозни или политически мотиви, като целта им е да създадат страх и хаос чрез атаки над обекти на т.н. критична инфраструктура – водоснабдяване, ядрени централи и др.

В публикация на Nelson и др.[15] от 1999 г. са дефинирани три вида *кибер-атаки* според тяхната организираност, които и сега са актуални:

Обикновена (в оригинала: *Simple – Unstructured*) – Това е атака срещу отделен компютър чрез използване на софтуер, създаден от други хора (и най-често намерен в Интернет). Действието се осъществява без предварителен анализ на целта и при ограничени специални умения – често жертвата не е конкретен компютър, а такъв, при който има пробив в сигурността.

---

[11] Hacktivism, From Wikipedia, the free encyclopedia вж. http://en.wikipedia.org/wiki/Hacktivism

[12] *Хакерски атаки парализираха Естония и Грузия*, e-vestnik**,** 7 Май 2009, вж. http://e-vestnik.bg/6110

[13] *Хакери ударихa петролния сектор на Иран*, news.bg, 23.04.2012, вж. http://news.ibox.bg/news/id_278277909

[14] *Нов могъщ компютърен вирус атакува Иран*, Капитал, 29 май 2012, вж. http://www.capital.bg/politika_i_ikonomika/sviat/2012/05/29/1836221_nov_mogusht_kompjuturen_virus_atakuva_iran/

[15] Nelson, B., Choy, R., Iacobucci, M., Mitchell, M., Gagnon, G., *Cyberterror Prospects and Implications*, White Paper of Centre for the Study of Terrorism and Irregular Warfare Monterey (US Navy, Naval Postgraduate School, 1999).

Структурирана (*Advanced – Structured*) – Това е атака срещу по-сложни и сравнително добре защитени компютърни системи. Атакуващият има умения да създава и модифицира софтуерни хакерски инструменти и е извършен предварителен анализ на целта.

Сложна координирана (*Complex-Coordinated*) – Това е атака, целяща сериозна щета на атакуваната информационна система и се осъществява координирано от много места едновременно. За целта се използват добре обучени хора, както и специализиран софтуер и хардуер. Предварително е проучена целта на атаката.

Погледнато от *техническата страна* на нещата кибер-заплахите могат да бъдат дефинирани по много различни начини, които се допълват с появата на всеки нов феномен в информационното пространство. В една от публикациите[16] се посочват двадесет и един вида различни атаки според технологиите, които използват. Без да се навлиза в някакви технически подробности, могат да бъда споменати няколко от тях, като тези термини са навлезли трайно дори в ежедневния ни речник – вируси, троянски коне, интернет - червеи и т.н. до двадесет и един. В статия на Sharon Weinberger[17] от 2010 г. всички тези видове са допълнени с още пет – атаки срещу социалните мрежи (*Facebook, Twitter* и т.н), прихващания на web-камери и *smart-phones*, пробиви в софтуера в най-новите коли и дори подслушване на сложни медицински устройства, управлявани от компютри и обменящи данни по безжичен път (*wireless pacemakers*).

Всички тези класификации могат да бъдат допълвани и с всяка нова технология ще бъдат разширявани, но основният извод, който следва да се направи е, че кибер-заплахите обхващат целия спектър на кибер-пространството и е илюзия, че съществуват изцяло защитени системи – все някога някой намира начин да преодолее и най-добрата защита. За сериозността на проблема говори и един съвсем обикновен експеримент – при направено търсене на 28.05.2012 г. в най-големия on-line магазин за книги amazon.com с ключова дума „*cyber security*", резултатът е 3033 заглавия или свързани с темата продукти.

От описаните до тук класификации става ясно, че има реален проблем със сигурността на информацията в компютърните системи и мрежи, и че все повече организации и хора се ангажират с неговото решаване, като още от 1995 г. започва и разработването на стандарти за кибернетична сигурност.

1.3. СТАНДАРТИ ЗА КИБЕРНЕТИЧНА СИГУРНОСТ

Тези стандарти позволяват на организациите да прилагат такива процедури и технологии, че да минимизират броя на успешните кибер-атаки.[18]

Необходимостта от развитие на подобни стандарти възниква след като много често информация, която не е за широката публика, започва да се съхранява на компютри, свързани с Интернет. Първите потребители, разбира се, са военните, но също така бизнесът и различни правителствени организации.

Един от най-широко използваните стандарти днес е ISO/IEC 27002, създаден през 1995 г. от Британския институт по стандартизация (BSI). Стандартът е създаден отначало в две части: BS *7799 part1* и *BS 7799 part2*, които понастоящем са обединени в стандарта

---

[16] *21 Types of Computer Security Threats,* What's the latest?, February 21, 2010, вж. http://www.whatsthelatest.net/news/types-computer-security-threats-cybercrime (20.06.2012)

[17] Sharon Weinberger, Five New Frightening Types of Cyberattacks, AOL News, Oct 18, 2010 , вж. http://www.aolnews.com/2010/10/18/five-new-frightening-types-of-cyberattacks (20.06.2012)

[18] *Cyber security standards*, Wikipedia, вж. http://en.wikipedia.org/wiki/Cyber_security_standards

ISO/IEC 27001[19] - Система за управление на информационната сигурност. Отделните компоненти на този стандарт са:

ISO/IEC 27000 – Обзор и терминология;

ISO/IEC 27002 – Добри практики;

ISO/IEC 27003 – Ръководство за внедряване;

ISO/IEC 27004 – Метрики;

ISO/IEC 27005 – Управление на риска;

ISO/IEC 27006 – Изисквания за акредитация;

ISO/IEC 27007 – Ръководство за одит.

Основната концепция на прилагането на този стандарт е непрекъсната оценка и управление на риска, така че той да бъде сведен до приемливо ниво, като се запазва оптимален баланс между конфиденциалност, пълнота и достъпност на информацията.

Една неправителствена организация – Форум по информационна сигурност (*Information security forum*) – предлага методи и процеси за защита на информацията, базирани на най-добрите практики. Организацията е създадена през 1989 г. и публикува на всеки две години „**Стандарти за добри практики**" [20], като последното издание е от 2011 г. Тези публикации имат повече техническа насоченост към решаване на конкретни проблеми в сигурността на информационните системи, стигайки в детайли до потребителския софтуер (напр. уязвимост в електронните таблици *Excel*[21]).

Американският национален институт по стандарти и технологии **NIST**[22] има поредица от публикации в областта на сигурността, като три от тях имат пряко отношение към кибернетичната сигурност:

800-12 (*Computer security handbook*) – Дава общ поглед върху компютърната сигурност като основно е насочен към хората от правителствените служби отговорни за системи, в които се съхранява чувствителна информация.

800-14 (*Generally Accepted Principles and Practices for Securing Information Technology*) – в тази публикация са описани осем принципа и четиринадесет практики за подобряване на съществуващите системи за сигурност и подходи при създаване на нови такива. Този документ дава детайлно описание на конкретни технически подходи към повишаване на информационната сигурност.

800-26 (*Security Self-Assessment Guide for Information Technology Systems*) – дава съвети по управление на IT сигурността, като се отделя особено внимание на самооценката, оценката и управлението на риска.

В публикациите на *NIST* има и повече от сто документа с номера от 800-27 до 800-155, даващи насоки за прилагане на конкретни технически мерки в различни аспекти на информационната сигурност: например 800-154 е за подобряване на сигурността на безжични мрежи; 800-123 е по отношение на сигурността на сървърите и т.н. Прави впечатление, че над двадесет от тези документи са издадени или актуализирани през 2011-2012 г., което е показател за нарастване на заплахите в последните няколко години.

---

[19] ISO 27001, ISO27001 Information Security Standard, вж. http://www.xmarks.com/site/www.itgovernance.co.uk/iso27001.aspx (20.06.2012)

[20] *Managing your information security challenges*, Information Security Forum, вж. https://www.securityforum.org

[21] Част от пакета Microsoft Office.

[22] National Institute of Standards and Technology, вж. www.nist.gov/index.html.

Има още редица стандарти като ISO 15408, ISA-99 и стандарти на международното общество на електроинженерите *IEEE*, които допълват изброените до тук или са насочени към конкретни области на приложение.

1.4. ИЗВОДИ

В последните години кибернетичната сигурност заема все по-голямо място в общата система на сигурността като реален проблем, а не като сценарий от научнофантастичен филм. Проявленията на кибер-заплахите, както и техните източници, са навсякъде около нас и вече са дефинирани и класифицирани, но все още са непознати за повечето хора.

Като отговор на реално съществуващите опасности в информационното пространство са създадени редица стандарти за кибернетична сигурност, прилагането на които намалява риска в тази област. Те са разработени както от държавни, така и от неправителствени организации; непрекъснато се разработват нови стандарти и е сериозно предизвикателство да бъдат намерени и приложени тези, които най-добре ще отговорят на изискванията на отбраната.

2. ПРИМЕРИ ЗА ОТГОВОР СРЕЩУ КИБЕР-ЗАПЛАХИ

Страните с развита информационна инфраструктура, която активно се използва в икономическия и обществен живот, разбира се, са най-уязвимите срещу кибер-заплахи. Не случайно през 2007 г. бяха атакувани банковата система и правителствените сайтове точно на „отличника" по въвеждане на електронно правителство - Естония. В държави като САЩ, Германия, Франция и др. проблемът отдавна е идентифициран и са създадени редица организации, работещи в областта на кибернетичната защита. ЕС също не изостава от тази тенденция както на ниво европейски институции, така и на ниво отделни държави - членки.

2.1. ПОДХОД НА ЕВРОПЕЙСКИЯ СЪЮЗ

На 10.03.2004 г. Европейският парламент и Съветът приеха Регламент № 460/2004 относно създаване на Европейската агенция за мрежова и информационна сигурност **ENISA**[23] (*European Network and Information Security Agency*). Същата започва реална работа през 2005 г. и е базирана на о. Крит, Гърция. Работата на тази агенция е съсредоточена върху засилване на мрежовата и информационна сигурност в Европа и на способността на държавите-членки както самостоятелно, така и заедно да отговорят на големи проблеми с мрежовата и информационна сигурност. Агенцията има за цел да осигури сътрудничество по тези въпроси и да служи като своеобразен център за разпространяване на знания и култура по използване на информационните системи така, че от това да се възползват ЕС, страните - членки, а и всеки гражданин.

За всяка държава ENISA изготвя отчет (*individual country reports*), който предоставя информация по следните въпроси, свързани с мрежовата и информационната сигурност (посочени са само по-важните):

- национална стратегия в областта, регулаторна рамка и ключови политически мерки;
- модел на управлението на мрежовата сигурност;
- основни „играчи" в областта, техните отговорности и дейности в областта на информационната сигурност;
- взаимодействие и обмен на информация между субектите от предходната точка;
- създаване на общност, която да работи в областта;
- специфични за държавата факти, тенденции, добри практики и характерни случаи;
- механизми за реакция при инциденти;
- защита на критичната инфраструктура;
- статистически данни за страната.

Тези отчети са базирани на публична информация, както и на мнението на служителите за връзка с ENISA от съответната държава (списъкът им е публикуван на сайта на та[24]).

За България отчетът[25] е в обем на тридесет и шест страници и между имената на авторите му няма българско име. Датата на последния отчет е май 2011 г. (към 04.06.2012 г.).

---

[23] European Network and information Security Agency (ENISA), вж. www.enisa.europa.eu.

[24] List of National Liaison Officers, ENISA, 22-11-2012, вж. http://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/List_NLO_Website_120312.pdf/view (22.11.2012)

[25] Bulgaria Country Report, European Network and Information Security Agency (ENISA), 2011, вж. http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Bulgaria.pdf (04.06.2012)

През юни 2012 г. ENISA организира в Париж, Франция конференция по кибер-учения[26], насочена предимно към сътрудничество и координиране на действията на ЕС при кризи в кибер-пространството и въпроси по планирането, организацията и провеждането на такъв вид учения, като основните цели са:

- обмен на опит между държавите-членки и споделяне поуки от конкретни кризи;
- събиране заедно на потребителите и експертите, така че да се оползотвори съвместната им работа;
- идентифициране на предизвикателствата и проблемите в областта на международното сътрудничество при кибер-кризи.

Няколко държави в ЕС като Франция, Германия и Дания, следвайки политиката на ENISA, вече са приели свои национални стратегии за кибернетична сигурност. Според статия[27] от 03.04.2012 г. ЕС ще има стратегия за киберсигурност до края на годината - цитирано е мнението на европейския комисар за вътрешните работи Сесилия Малмстрьом при участието ѝ в проведената във Вашингтон конференция, наречена "Трансатлантическите измерения на киберсигурността". Една от водещите държави в света по отношение на регулаторната рамка в кибер-пространството е Германия (по оценка на *CyberHub*[28]).

2.2. НАЦИНАЛНА СТРАТЕГИЯ ЗА КИБЕРНЕТИЧНА СИГУРНОСТ НА ГЕРМАНИЯ

Този документ[29] е с обем от десет страници и основно се фокусира върху стратегическите цели в областта на кибернетичната защита, като дефинира десет такива:

- Защита на критичната информационна инфраструктура е основен приоритет.

Тук е мястото да се посочи дефиниция за термина „критична информационна инфраструктура", като тази в стратегията на Германия е достатъчно кратка и ясна: Критичната инфраструктура са организации или институции с важно значение за общественото благо и ако тяхното функциониране е нарушено или провалено, ще се отрази сериозно на публичната сигурност.[30]

- Създаване на сигурни ИТ системи – информационната структура, ползвана от гражданите и малкия бизнес, трябва да предоставя достатъчно надеждна среда за комуникация (напр. идентификация на изпращача при ползване на *De-mail*).
- Повишаване на сигурността в публичната администрация – целта е създаване на единна, защитена платформа за федералната администрация.
- Създаване на Национален център за реакция при кибер-заплахи – с цел да дава бърза и точна информация при открити уязвимости в ИТ продукти, новооткрити форми на атака и др.

---

[26] First International Conference Cyber Crisis Cooperation: Cyber Exercises, ENISA, June 2012, вж. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-exercise-stocktaking/cyber-exercise-conference/first-international-conference-cyber-crisis-cooperation-cyber-exercises

[27] ЕС ще има единна стратегия за киберсигурност до края на годината, PC World, 03 май 2012, вж. http://pcworld.bg/19514_es_shte_ima_edinna_strategiya_za_kibersigurnost_do_kraya_na_godinata

[28] The Cyber Hub, вж. http://www.cyberhub.com/Home/About, (04.06.12)

[29] Cyber Security Strategy for Germany, 2011, вж. http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 (20.06.2012)

[30] Пак там, стр.9. Дефиницията в оригинал: „Critical infrastructures are organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences."

- Създаване на Национален съвет по кибернетична сигурност – със задача да осъществява координацията между федералните служби и частния сектор, за да бъдат премахнати структурните причини за кризи в кибернетичната сигурност. Министерството на отбраната (Bundeswehr) е активен участник в този съвет.
- Ефективен контрол на престъпността и в кибер-пространството.
- Координиране на действията с ЕС и целия свят за осигуряване на достатъчно безопасно кибер-пространство – организации, които се посочват, са вече споменатата ENISA, OCCE, НАТО, ООН и Съветът на Европа.
- Използване на надеждни информационни технологии – това трябва да бъде постоянна задача, която включва диверсификацията на технологии, активните изследвания и сътрудничество с европейските партньори.
- Развитие на човешките ресурси – обучение и обмен на кадри между различните федерални институции.
- Разработване на инструментариум (организационен и технически) за отговор на кибер-атаки.

2.3. НАЦИОНАЛНА СТРАТЕГИЯ ЗА ЗАЩИТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ НА ФРАНЦИЯ

Френската стратегия (*Défense et sécurité des systèmes d'information Stratégie de la France*)[31] дефинира четири стратегически цели, като първата е доста амбициозна:

- Франция да стане световна сила в областта на кибер-отбраната;
- Гарантиране възможността на Франция да взема решения чрез защита на информацията, свързана със суверенитета;
- Повишаване на кибернетичната защита на критичната национална инфраструктура;
- Сигурност в кибер-пространството.

За постигане на тези цели са дефинирани седем конкретни насоки за действие:

- ефективен анализ на обкръжаващата среда с цел взимане на адекватни решения;
- откриване и неутрализиране на кибер-атаки, предупреждение и подкрепа за потенциалните жертви;
- запазване и разширяване на научните, техническите, индустриалните и човешките ресурси с цел запазване на независимостта;
- защита на държавни и частни обекти от критичната инфраструктура;
- адаптиране на законодателството съобразно технологичния напредък;
- участие в международни инициативи по кибер-защита и срещу кибер-престъпността;
- повишаване на информираността и разбирането на проблемите по кибернетичната сигурност сред френското общество.

[31] *Défense et sécurité des systèmes d'information Stratégie de la France,* Agence nationale de la sécurité des systèmes d'information, 2011 вж. http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

2.4. САЩ

Без съмнение САЩ е водеща държава по отношение на политиката по кибернетична защита. Има поредица от правителствени документи, като първите от тях са реакция на терористичните атаки срещу Световния търговски център на 11.09.2001 г. През 2003 г., като елемент от по-голямата Стратегия за национална сигурност, е публикувана Националната стратегия за сигурно кибер-пространство в обем от седемдесет и шест страници (*National Strategy to Secure Cyberspace*[32]). Тя е разработена от Министерството на вътрешната сигурност на САЩ (*Department of Homeland Security – DHS*) и е резултат от едногодишни научни изследвания и няколко месеца публично обсъждане. В документа не са заложени задължения, а по-скоро има препоръки към бизнеса, университетите и обикновените потребители за повишаване на кибернетичната сигурност. Тази стратегия определя три стратегически цели:

- Предотвратяване на кибер-атаки срещу обекти на критичната инфраструктура;
- Намаляване уязвимостта на САЩ от кибер-атаки;
- Минимизиране на последствията и възстановяване след кибер-атаки.

През 2011 г. са публикувани три нови ключови документа в областта:

Международна стратегия за кибер-пространството (*President's International Strategy for Cyberspace* [33]), Май 2011 г.

Стратегия на министерството на отбраната за операции в кибер-пространството (*Department of Defense Strategy for Operating in Cyberspace* [34]), Юли 2011 г.

План за сигурно кибер-бъдеще (*Blueprint for a Secure Cyber Future* [35]), 12 декември 2011 г.

Заедно, всички тези документи представят цялостния подход на правителството на САЩ към предизвикателствата в кибер-пространството. Те обхващат намеренията на държавата в международен план по отношение на отбраната и в областта на вътрешната сигурност.

Международната стратегия за кибер-пространство е документ от тридесет страници, в който се подчертава, че сигурността на компютърните мрежи е жизнено важна за икономическия просперитет и изразява готовността на САЩ да работи с други нации по защита на тези технически средства. Особено внимание е отделено и на военния компонент, като се посочват три основни насоки за справяне с предизвикателствата на 21-ви век:

- Да се отговори на нарасналите нужди на въоръжените сили от надеждни и защитени мрежи, отчитайки че те работят в условия, при които противникът се опитва да саботира тяхната дейност.
- Изграждане и разширяване на съществуващи военни съюзи с цел да се противодейства на потенциални заплахи в кибер-пространството. Подчертава се фактът, че никоя нация не може да постигне сама за себе си необходимата сигурност.
- Разширяване на сътрудничеството в кибер-пространството със съюзниците и партньорите на САЩ, така че да се повиши колективната сигурност. Това може да се постигне с общо разбиране на стандартните процедури , обмяна на информация и случаи на добри практики.

---

[32] *The national strategy to secure cyberspace*, The White House, Washington, February 2003 , вж. www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

[33] *International Strategy for Cyberspace,* The White House, Washington, May 2011 вж. www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[34] *Department of Defense Strategy for Operating in Cyberspace*, Department of Defense USA, July 2011, вж. http://www.defense.gov/news/d20110714cyber.pdf (20.06.2012)

[35] *Blueprint for a Secure Cyber Future*, Homeland Security, November 2011, вж. http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (20.06.2012)

Стратегията на министерството на отбраната (*DoD - USA*) **за операции в кибер-пространството –** с обем от деветнадесет страници.

В тази стратегия се подчертават силните страни на отбраната на САЩ като свръхбързите комуникации, възможностите за споделяне на информация и експертизата в областта на кибернетичната сигурност, които са определени като „стратегически предимства" в кибер-пространството. Определени са пет стратегически инициативи, които да служат като „пътна карта" за ефективно водене на операции в кибер-пространството и защита на националните интереси:

- Кибер-пространството да се третира като оперативно пространство, в което могат да се провеждат учения и операции, както това се прави по въздух и по вода. В изпълнение на тази стратегическа инициатива е основано Кибер-командване на САЩ (*US Cyber Command – USCYBERCOM*), подчинено на Стратегическото командване на САЩ (*USSTRATCOM*).

- Прилагане на нови концепции за операции, така че да се защитят мрежите и системите на Министерството на отбраната. Това включва най-добри практики по отношение на „кибер-хигиената", обновяване на софтуера и подобряване настройките на всички системи по отношение на сигурността. Наред с тези пасивни мерки се предвижда и въвеждане на нови концепции като използване на мобилни устройства и облачни технологии (*cloud computing*) така, че да се следват всички технологични нововъведения.

- Партньорство с всички правителствени агенции и частния бизнес за реализиране на цялостната правителствена стратегия за кибернетична сигурност. Много от дейностите на *DoD* зависят от частни производители, интернет доставчици и т.н., и в много области това се припокрива с другите агенции така, че подходът е да се използва обща стратегия в тези партньорства.

- Изграждане на стабилни връзки със съюзниците и партньорите на САЩ за укрепване на колективната кибернетична сигурност. Предвиждат се съвместни учения, споделяне на добри практики и изграждане на механизми за ранно предупреждение при кризи.

- Мобилизиране на научния и икономически потенциал на САЩ и изграждане на широка база от талантливи цивилни и военни специалисти за да се създадат нови способности в областта на кибер-пространството . *DoD* ще създаде възможности за малкия и среден бизнес чрез инвестиции в съвместни предприятия (*joint ventures*).

План за сигурно кибер-бъдеще – петдесет страници.

Кибернетичната сигурност се разглежда като споделена отговорност между всички и Министерството на вътрешната сигурност на САЩ (*DHS*) декларира готовността си за съвместна работа с всички щатски и федерални власти, а така също и с частния сектор. В документа са посочени четири цели по защита на критичната инфраструктура:

- да се намали опасността от излагане на кибер-рискове;
- да се осигури приоритетно отговор на кибер-атаки и инструменти за възстановяване;
- споделяне на информация между всички заинтересовани и поддържане на готовност;
- усилване на издръжливостта (*resilience).*

Дефинира се също така и понятието „кибер-екосистема" (*cyber ecosystem)* и четири начина тя да бъде направена по-сигурна, а именно:

- упълномощаване на организациите и отделния човек с отговорността по осигуряване на кибернетична защита;
- създаване и използване на надеждни протоколи, продукти, услуги и архитектури;

- създаване на общности за сътрудничество в областта на сигурността;
- всичко от изброеното до тук да бъде прозрачен процес.

Всички разгледани до тук документи на САЩ бяха стратегии и за да бъдат приложени в реалния живот се нуждаят от конкретна законодателна рамка. На 27.04.2012 г. Камарата на представителите на САЩ прие проект на „Закон за кибернетична защита и размяна на разузнавателна информация" (CISPA)[36], който предвижда да се даде достъп на правителствени служби до личните данни на потребителите на мрежата при съмнения за кибер-заплаха. Законът ще улесни и размяната на информация между службите за сигурност и частни фирми от Интернет – бизнеса. Facebook, AT&T, Intel, Verizon и Microsoft са сред 800-те компании, които са заявили, че са съгласни с новия законопроект. Преди приемането му в долната камара, в него са внесени поправки, така че да включва информация, събрана в хода на разследвания на кибер-престъпления, да обезпечава защита на живота на отделни лица, а също така да защитава непълнолетни от експлоатация. На фона на типично американските призиви за „свобода на личността" този закон лишава гражданите от част от тези свободи за сметка на сигурност в кибер-пространството.

2.5. НАТО

НАТО има опит с кибер-заплахите 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 на това е основан НАТО Център за реакция при компютърни инциденти *(NATO Computer Incident Response Capability - Technical Centre)* [37]. 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 кибер-защита[38] в Талин (*NATO Cooperative Cyber Defence Centre of Excellence*). Между другото Естония предлага създаването на подобна структура още през 2003 г. – преди присъединяването на държавата към НАТО.

В един от коментарите[39] по повод срещата на лидерите на НАТО в Чикаго през май 2012 г. се споменава за договор от 50 млн. евро между НАТО и две фирми: *Northrop Grumman* (САЩ) и *Finmeccanica* (Италия), за изграждане на петдесет центъра в двадесет и осем държави за откриване и реакция при кибер-атаки.

2.6. ИЗВОДИ

ЕС и страни като САЩ, Германия и Франция отдавна са прозрели потенциала на проблема по кибернетичната защитата и са предприели редица стъпки, започвайки от законодателните, в посока към координиране на усилията в тази област. Същевременно стремежът е в областта на информационната сигурност да се включват повече и различни правителствени и неправителствени организации за постигане на една широка база и информираност на обществото.

Като основен проблем в разглежданите държави и организации се извежда защитата на критичната (информационна) инфраструктура.

---

[36] *Cyber Intelligence Sharing and Protection Act* (CISPA), 2011, вж. http://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act.

[37] NATO Computer Incident Response Capability - Technical Centre , вж. www.ncirc.nato.int. (20.06.2012)

[38] NATO Cooperative Cyber Defence Centre of Excellence , вж https://www.ccdcoe.org/ (20.06.2012)

[39] Marc A. Sorel, *"NATO's Cyber Security Strategy: A Good Start, But Much to Do"*. The Chicago Council on Global Affairs, 2012, вж. http://2012summits.org/commentaries/detail/sorel_2. (20.06.2012)

Отбраната винаги е един от ключовите елементи на кибернетичната защита – в НАТО все още има какво да се направи, но организацията уверено следва примера на САЩ.

Всички разглеждани документи акцентират върху широкото междуведомствено и международно сътрудничество като решаващ елемент в борбата за едно по-сигурно киберпространство.

Особено добре структурирана и последователна е политиката на САЩ, което е разбираемо имайки предвид мащаба на страната и нейната зависимост от критичната информационна инфраструктура.

3. БЪЛГАРИЯ И КИБЕРНЕТИЧНАТА СИГУРНОСТ

В глава първа бяха споменати две от държавните структури, имащи пряко отношение към защитата на информацията в България - Държавната комисия по сигурността на информацията и Комисията за защита на личните данни. Освен тях отговорности в тази област имат МВР, изпълнителна агенция „Електронни съобщителни мрежи и информационни системи - ЕСМИС"[40], ДАНС, Министерството на транспорта, информационните технологии и съобщенията и др. Със заповед № Р-216/14.09.2011 г. на министър-председателя на Република България е направен опит за координиране и насочване на усилията на част от тези организации чрез създаване на междуведомствена работна група по проблемите на кибернетичната защита. Председател на групата е секретарят на Съвета за сигурност при Министерския съвет. Включени са представители на МО, МВР, ДАНС, ДКСИ, МТИТС, ЕСМИС, министерство на правосъдието и МВнР. Целта на групата е да „изготви предложение за състава, мисиите, функциите и задачите на Национален работен орган по кибернетична сигурност в Република България…". Към дата 06.06.2012 г. не е създаден такъв орган.

3.1. ОРГАНИЗАЦИИИ В ОБЛАСТТА НА КИБЕР-ЗАЩИТАТА

Следвайки указанията на ENISA (организацията е подробно описана в т. 2.1) в България е създаден Национален Център за Действие при Кризисни Ситуации в Компютърната Сигурност[41]. Мисията на центъра е да подпомага потребителите в дейностите по намаляване на рисковете от инциденти в компютърната сигурност и да съдейства при разрешаването на такива инциденти в случай, че вече са възникнали.

Целите, които се поставят включват:

- защита на информацията и технологичните активи;
- ограничаване директното влияние на инцидентите в сигурността върху информационното общество;
- помощ при възстановяване от инциденти;
- оценяване на въздействието от инциденти в сигурността;
- събиране и разпространение на техническа информация, свързана с инциденти в компютърната сигурност, както и с уязвимости в сигурността на системите и начините за предотвратяването им;
- провеждане на изследвания, свързани с нови технологии в мрежовата и информационна сигурност;
- провеждане на обучения, свързани с информационната сигурност и управлението на инциденти

Доколко тези амбициозни цели се изпълняват, може да се види от факта, че датата на последното обновяване на "техническите съобщения за уязвимости и проблеми в сигурността на системите и начини за предотвратяването им" е от 29.12.2011 г. (този факт е констатиран на 01.06.2012[42]). Това едва ли е последната уязвимост, още повече, че всички съвети са на английски език и са директно копирани от други сайтове, най-вече от *Microsoft*, като все пак не може да не се отбележи, че има кратка анотация на български език. На

[40] Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи - ЕСМИС", вж. www.esmis.government.bg.

[41] Bulgarian Computer Security Incidents Response Team, вж. https://govcert.bg/EN/Pages/default.aspx.

[42] Национален Център за Действие при Инциденти в Информационната Сигурност, вж. https://govcert.bg/BG/Pages/Alerts.aspx

16.05.2012 г. от ЕСМИС е сключен договор за поддръжка на портала, така че е възможно той пак да поднови дейността си.

Българската академия на науките също идентифицира проблема по кибернетичната сигурност и е създала „Национален портал за киберсигурност" (правописът е на създателите на портала – Национална лаборатория по компютърна вирусология към БАН[43]). В частта му „препоръки-софтуер" цялата налична информация е следната: относно злонамерения софтуер - „Необходими са значителни подобрения в съществуващите национални законодателства (включително и в българското), по отношение на наказателните мерки спрямо създателите и разпространителите на злонамерен софтуер".

В Университета по библиотекознание и информационни технологии има създадена Научно-изследователска лаборатория за кибернетична сигурност с ръководител проф. д-р Драгомир Паргов и това е цялата налична информация в сайта[44].

Тези примери, макар и неизчерпателни показват, че в България проблемът с кибернетичната сигурност вече е на дневен ред, но все още не се възприема с необходимата сериозност, което може би е обусловено и от неголямата зависимост на икономиката и обществения сектор от безотказното функциониране на компютърните мрежи. Въпреки многото декларации и опити електронното правителство все още не е факт, нито пък електронните здравни карти.

3.2. КИБЕРНЕТИЧНА СИГУРНОСТ И ОТБРАНА

Министерството на отбраната традиционно е считано за добър пазител на тайните си, което произтича от естеството на работа му. Не случайно в спомената по-горе заповед № Р-216/14.09.2011 г., МО е определено да отговаря за административното и деловодното обслужване, а дирекцията на МО „Сигурност на информацията" да изпълнява функциите на секретариат.

По отношение на кибернетичната сигурност МО има няколко неоспорими предимства пред останалите органи в държавата. Първо - това е организационната култура при работа с конфиденциална информация, която е придобила и институционалност чрез дирекция „Сигурност на информацията". В министерството има и изградена система за контрол за спазване на Закона за защита на класифицираната информация, както и за назначаване на конкретни длъжностни лица, отговорни за това. На второ място това е начинът, по който е изградена Автоматизираната информационна система на БА. Тя не е свързана с Интернет или други мрежи и е с ограничен кръг от лица с достъп до информацията в нея. От друга страна, естеството на работа в повечето военни формирования не предполага използване на Интернет в ежедневната дейност, нито пък има такива съоръжения, които да са критично зависими от мрежовата си свързаност. Не трябва обаче да се забравя нарастващата тенденция за всеобхватна и непрекъсната мрежова свързаност – голям процент от военнослужещите ползват различни видове мобилни устройства с една или друга безжична технология и това е потенциален проблем, който следва да се отчита.

Като член на НАТО и ЕС, България има възможност да черпи от опита на партньорите си и да прилага техните достижения – още повече, че тези партньори са сред нациите, напреднали значително в кибернетичната сигурност в сравнение с останалия свят.

---

[43] Национален портал за киберсигурност, , вж. http://ncs.nlcv.bas.bg/

[44] Научно-изследователска лаборатория за кибернетична сигурност, Университет по библиотекознание и информационни технологии (УНИБИТ), вж. http://www.unibit.bg/about-unibit/administrative-units/centers-laboratories#research-laboratory-of-cybersecurity

Също така, по традиция, МО подготвя собствени кадри в областта на компютърните системи и технологии, много от които са се доказали и извън системата на отбраната и може би това е причината в едно свое изказване президентът Росен Плевнелиев (02.04.2012 г., на Конференция за Интелигентната отбрана) да заяви: „България има достатъчно интелигентни млади хора, които биха могли да работят за киберотбраната. … ще бъде прекрасно да има такъв център на НАТО у нас, защото България ще се позиционира на картата на войните на 21-ви век като една от най-високотехнологичните държави”.[45]

Дали обаче кибернетичната сигурност е толкова безпроблемна за отбраната в действителност. Наистина имаме партньори с експертиза в областта, но няма данни да сме се възползвали като нация от възможностите на Центъра за кибер-защита на НАТО в Естония чрез включване на офицери за обучение или чрез участие в учения там. Свиването на нашата собствена военно-образователна система не позволява тясно специализираното обучение в областта на компютърните технологии и като пример може да се посочи приема в НВУ „В.Левски” за 2012 г. В подобна област се приемат само седем курсанти и то с гражданска професионална квалификация „Инженер по комуникации”[46].

Във Факултет „А, ПВО и КИС” на НВУ има катедра „Информационна сигурност”, като там се провежда обучение за магистри и бакалаври, но само за студенти[47].

3.3. ИЗВОДИ

В Република България е започнало изграждането на структури, които да осигуряват кибернетичната сигурност, но все още няма национална стратегия в тази област и няма единна координация.

Министерството на отбраната има организационен и човешки потенциал за работа в това направление, но за в бъдеще може би ще се наложи да разчитаме на експерти, подготвени в граждански висши училища.

---

[45] *Президентът вижда реализацията на младите в киберотбраната*, Сега, Брой 4358 (78) 02 Април 2012, вж. http://www.segabg.com/article.php?sid=2012040200019985007 (20.06.2012)

[46] Национален Военен Университет „В.Левски”, Велико Търново, вж. http://www.nvu.bg/node/484

[47] Факултет "Артилерия, ПВО И КИС" на Национален Военен Университет „В.Левски”, Велико Търново , вж. http://aadcf.nvu.bg/struktura/katedri/IS/index/index.html

ЗАКЛЮЧЕНИЕ

Без съмнение, България отдавна е навлязла в информационната ера, макар и не с мащабите на водещите държави. От това следват не само ползите от мигновенната свързаност и богатството на информационния океан, но и опасностите, които кибер-пространството крие.

В началото на 21-ви век страната ни има не само шанса, но и отговорностите да бъде член на два съюза – ЕС и НАТО, които са направили значителни стъпки в областта на кибернетичната защита. Ние също следваме общите политики на европейските си партньори и НАТО, но може би не с необходимата настойчивост и последователност. Кибер-сигурността вече е на дневен ред и е по-добре навреме да се изгради пълният комплект мерки – от стратегии до конкретни технически изисквания, така че да посрещнем предизвикателствата на информационната ера подготвени.

Отбраната е основен елемент от националната сигурност и като такава има своето място и в кибер-пространството. Поради своята численост и стратегически цели ние не може да разгърнем кибер командвания като САЩ или да създадем батальони от кибер-бойци като Китай, но можем да се възползваме от генерираните знания и способности, които колективната отбрана предлага. За това обаче е необходим и съответен капацитет и принос от наша страна – както да можем да пазим общите инфомационни ресурси, така и да боравим с предоставените ни възможности.

Ключът към постигане на достатъчно високо ниво на кибернетична защита е в два подхода, които не изискват много ресурси:

1. Кооперирание – да се създаде широка база за сътрудничество между институциите в България, както и с международни организации и съюзниците ни.
2. Образование и квалификация – в областта на отбраната има изградена една от най-добрите системи за учене през целия живот и ние притежаваме достатъчно ресурси и механизми да постигнем едно добро ниво на информираност и адекватно поведение на военнослужещите.

МО има организационната култура и образователния потенциал да бъде водеща институция в областта на кибернетичната защита, но дали може да прояви достатъчно иновативност, гъвкавост и адаптивност е въпрос, който само бъдещето ще покаже.