# НАСОКИ ЗА УПРАВЛЕНИЕ ПРИ КРИЗИ В КИБЕРСИГУРНОСТТА

доц. д-р Юлияна Каракънева,
Нов български университет

**Assoc. Prof. Uliyana KARAKANEVA, PhD**
New Bulgarian University

***Резюме:*** Докладът дава насоки за управление при кризи в киберсигурността, която се намира в една нова среда за сигурност. Конкретните насоки са свързани с: подобряване на киберсигурността в системите на държавната администрация и критичната информационна инфраструктура; развитие на адекватни законодателни инициативи; активно участие на частния сектор в противодействието срещу кибер заплахите; създаване на звена за натрупване и анализ на информация; подобряване на партньорството между държавните ведомства и частния бизнес; партньорство с компаниите, производители на технологии за сигурност; защита на потребителите.

***Ключови думи:*** управление, криза, киберсигурност, кибер атака, кибер заплаха.

***Summary:*** The report provides guidance for crisis management in cybersecurity, which is in a new security environment. Specific guidelines are related to: improve cybersecurity systems of public administration and critical information infrastructure; development of adequate legislative initiatives; active participation of the private sector in fighting against cyber threats; creation of units for information accumulation and analysis; improving the partnership between public authorities and private businesses; partnership with companies manufacturers of security technologies; consumer protection.

***Keywords:*** management, crisis, cyber security, cyberattack, cyber threat.

**Въведение**

През последните двадесет години киберсигурността се превърна от явление в естествена характеристика на виртуалното пространство, създадено посредством Интернет и другите компютърни мрежи. Своевременното информиране за новопоявилите се кибер заплахи стана жизнено важно за държавните и частните организации в стремежа им да противодействат на инцидентите в сигурността.

Кибератаките се разглеждаха като рискови действия с ограничен обхват и неголям потенциал за вреди, изискващ само стандартна техническа намеса. Но злоумишлениците станаха все по-организирани и техните атаки – по-сложни, което направи традиционните методи и средства за отбрана по-малко ефективни при справянето с новите заплахи. От дребно вредителство, въздействието на зловредния софтуер се превърна в сериозен проблем за сигурността на информацията и широко използвано средство за шпионаж. Кибернетичното измерение на политическите конфликти еволюира от саботиране на информационна политическа или индустриална кампания до водене на информационна война.

Събитията в кибепространството през последните десет години промениха старата представа и насочиха вниманието на държавите и техните правителства към

нарастващата заплаха за сигурността на обществото и стабилността на държавното управление.

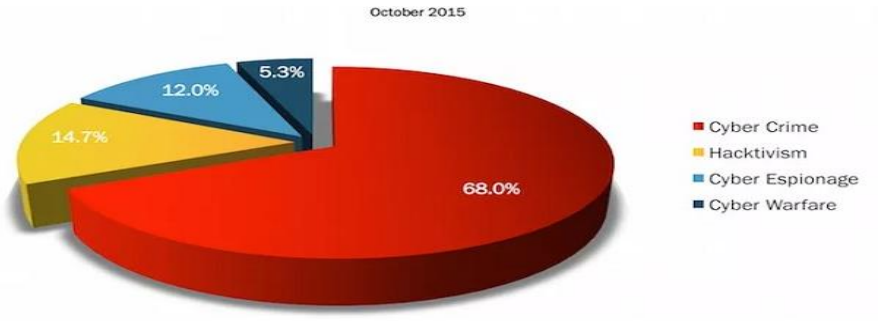
През 2011 г. се отчита, че кибератаки са засегнали сериозно 72 компании, 22 правителствени служби и 13 фирми, сключили договори с отбраната на САЩ [1]. Тези инциденти предизвикаха трансфер на конфиденциална информация в ръцете на анонимни и вероятно злонамерени лица и групи.

Изследването, публикувано в „Foreign Affairs“[11] показва, че за десет години (2001-2011) от 20 противопоставяния между държави, САЩ и Китай са провели най-голям брой атаки един срещу друг. Пекин е атакувал инфраструктурата на САЩ 18 пъти, а Вашингтон е отговорил 2 пъти. При двете най-съществени покушения срещу Пентагона са откраднати конфиденциални файлове на Министерството на отбраната и чертежите на изтребителя F-35 на компанията Lockheed Martin. Авторите считат, че тези атаки не са предизвикали вреди в големи размери и не са повлияли съществено на общественото мнение.

За същия период Индия и Пакистан са се атакували взаимно 11 пъти – проведени са 5 атаки от страна на Индия и 6 – от страна на Пакистан. Също така, Северна Корея е атакувала Южна Корея 10 пъти, при само един отговор в обратната посока. Тези атаки са свързани с незначителни инциденти, като опитът на Пакистан да атакува сайта на правителството на Индия, до по-сериозни – като кражбата на документи на южнокорейското правителство.

Практиката показва, че отговорът на проблема „кибер атака“ в междудържавните отношения не е в противопоставянето, а в намаляването на вредните последствия чрез превантивни мерки и прилагане на средства за управление на инцидентите. Организациите и правителствата преследват основните цели на управлението при кризи – осигуряване на непрекъснатост на процесите и изпълнение на процедурите за възстановяване на работата на информационните системи в максимално кратък срок [2].

Компании като Information Security Timelines and Statistics[12] публикуват месечна статистическа информация за идентифицираните атаки в киберпространството (фиг. 1), при което се създава възможност за последващи анализи и разработване на стратегия и политики за сигурност.




**Фиг. 1**

[11] *Valeriano, B., R. Maness, The Fog of Cyberwar. Why the Threat Doesn't Live Up to the Hype, Foreign Affairs, 2012.*

[12] http://www.hackmageddon.com/

Анализите и заключенията на международните експерти по киберсигурност намериха отражение в модела, представен в стандарта по киберсигурност, приет от Международната организация по стандартизация (ISO/IEC 27032) [3]. Този стандарт очерта сериозни предизвикателства пред международната общност в полето на сигурността във виртуалното пространство.

В новата среда за сигурност, усилията на държавите са насочени в две направления – национална и транснационална политика за киберсигурност и подобряване на кибер отбраната чрез действия в три основни аспекта:

- провеждане на превантивна дейност и разузнаване;
- създаване на способности за противодействие и
- разработване на инструменти за управление на инцидентите в сигурността.

**Основни направления на усилията**

Заинтересованите страни в киберпространството са държавните организации, частните компании, особено транснационалните корпорации, доставчиците на интернет и виртуални услуги, разработчиците на софтуер, както и обикновените потребители.

За да се реализират предимствата на киберпространството, е необходимо заинтересованите страни да играят активна роля, отвъд защитата на техните собствени ценни активи.

*Подобряване на киберсигурността в системите на държавната администрация и критичната информационна инфраструктура*

Във връзка с въвеждането на електронно правителство в системите за държавно управление, от изключително значение е сигурността на тези системи и данните, които създават, обработват и пренасят в компютърните мрежи. Системите на държавната администрация са Интернет и/или интранет базирани или, в случаите в които служат за обработка на класифицирана информация – базирани на доверена преносна среда. Тези системи реализират е-правителството и администрирането на публичните услуги, при което осигуряват стабилността и доверието на обществото. В по-широк обхват в тази група може да се включат системите на критичната информационна инфраструктура, които гарантират сигурността на функциониране на най-важните отрасли в държавата.

От решаващо значение е използването на технологични инструменти за разкриване на уязвимостите и заплахите и споделяне на информацията за тях. Основните задачи в това направление са свързани с:

- Идентифициране на чувствителната информация и ценните информационни активи на организацията;
- Ефикасна идентификация на кибер заплахите за системите;
- Вграждане на защитни механизми, реализиращи превенция срещу атаките (Системи за превенция срещу проникване – Intrusion Prevention System);
- Прилагане на инструменти за разкриване на атаки в най-близко до реалното време (Системи за откриване на проникване – Intrusion Detection System);
- Планиране и изпълнение на процедури за бързо възстановяване след инциденти.

В организациите се създава практика за непрекъснато наблюдение на системите, мрежите и потребителите, техните права и роли в оперативния процес, с цел разкриване в реално време на опити за нерегламентиран достъп.

В рамките на политиките за сигурност се изгражда система от процедури за издаване на разрешенията за достъп и мониторинг и усъвършенстване на схемата за достъп. Предвижда се специално внимание на режима за достъп и мерките за защита на некласифицираната информация, която може да е чувствителна.

От съществено значение е непрекъснатото обучение на служителите и потребителите на информация в държавната администрация и секторите на критичната инфраструктура, чрез създаване на специални програми и провеждане на семинари и работни срещи. Например, правителството на САЩ създаде специална онлайн програма за обучение [4], която дава възможност на квалифицираните потребители да поддържат равнището на знания и умения в сигурността.

С цел осигуряване на анализ и превенция на инцидентите в киберпространството беше създадена Европейската агенция за мрежова и информационна сигурност (ENISA)[5]. Основните направления на действие на агенцията са: развитие на стратегии и политики за сигурност, управление риска в киберсигурността, управление на кибер кризи, мониторинг и анализ на критичната инфраструктура и услугите, обучение в сферата на киберсигурността и провеждане на международни учения по киберсигурност, разработване на процедури за докладване на инциденти и стандарти за сигурност.

*Развитие на адекватни законодателни инициативи*

Поради трансграничния характер на инцидентите в киберпространството, от съществено значение е хармонизирането на законодателството на държавите в предметната област. В този дух е Директива 2013/40 на ЕП [6], относно атаките срещу информационните системи. Целта на директивата е „сближаване на наказателните законодателства на държавите чрез установяването на минимални правила относно престъпленията и наказанията за тях в разглежданата област“ и подобряването на сътрудничеството на специализираните органи. Идеята е да се намери общ подход по отношение на незаконния достъп до информационните системи и незаконното разкриване, модифициране и унищожаване на данни.

Изисква се законите да включват отговорност на юридическите лица за престъпления, предвидени в директивата, при определените в нея условия.

Значителните пропуски и различия в законите и наказателните производства на държавите членки в областта на атаките срещу информационните системи могат да възпрепятстват борбата срещу организираната престъпност и тероризма, а също така да усложнят полицейското и съдебното сътрудничество в тази област. Характерът на съвременните информационни системи, които функционират отвъд националните граници, предполага, че атаките срещу тези системи имат трансгранично измерение, което изисква спешно осъществяване на допълнителни действия за сближаване на наказателното право в тази област[7].

*Активно участие на частния сектор в противодействието срещу кибер заплахите*

Стандартът по киберсигурност ISO/IEC 27032 дава една от най-важните насоки в тази сфера – сътрудничество между участниците в КП за споделяне на информация за актуалните заплахи за сигурността и представяне на най-добрите практики за нейното подобряване. Спектърът на страните е изключително широк – неправителствени агенции, икономически организации, частния бизнес, студенти, преподаватели, юридически съветници и др. Активността на частните корпорации има съществен дял в този процес, поради факта, че те обхващат съществена част от икономиката на държавите и имат финансовите възможности да въвеждат технологии и технически средства за сигурност.

Препоръките за действие към всички участници във виртуалната реалност са свързани основно със следните направления:

•Придържане към международните стандарти за сигурност - през последните години международната организация по стандартизация последователно изработи серията стандарти ISO/IEC 270xx, свързани с различни аспекти на информационната сигурност. Организациите се стремят да се сертифицират по тези стандарти, за да отговорят на нарастналите изисквания в тази област при разработване на проекти. Стимулирането на този процес, посредством международни инициативи ще допринесе за утвърждаване разбирането за сигурността в киберпространството и активни действия на компаниите в тази сфера чрез прилагане на технологиите.

•Използване на инструменти за управление на риска - основните технологични инструменти, които се прилагат за противодействие на атаките в киберпространството са:

-Контрол на достъпа: ограничаване на възможността непознат или неопълномощен потребител да използва информацията, работните станции и мрежите. Технологията подпомага защитата на чувствителните данни и системи. Включва средства за защита на периметъра, автентикация и авторизация;

-Контрол на целостта на системата: прилага се, за да се гарантира, че системата и данните не са модифицирани или компрометирани от зловреден код. Използва се антивирусен софтуер и инструменти за проверка на целостта;

-Криптографски контрол: включва криптиране на данните преди трансфер и при съхранение в системата. Криптографски методи се използват при виртуалните частни мрежи, цифровите подписи и сертификати.;

-Наблюдение и одит: подпомагат администраторите да извършват разследване по време на и след реализирането на атаки. Прилагат се четири типа технологии: системи за откриване на проникване, системи за превенция на проникване, корелационен анализ на събитията и компютърно разследване;

-Управление на конфигурацията и въвеждане на контролни механизми за сигурност: подпомага администраторите да установяват и променят настройките за сигурност на хостовете и мрежите, да правят проверка и да поддържат сигурността на операциите при специфични трудни условия. Разглеждат се пет типа управленски технологии: въвеждане на политики за сигурност, активно управление на мрежата,

въвеждане на средства за гарантиране непрекъснатост на операциите в приемлив обем и управление на софтуерните модули за сигурност.

•Споделяне на информация за заплахите - споделянето на резултатите от наблюденията върху функционирането на мрежите и осъществените успешни и неуспешни опити за атаки е от изключително значение за организираното противодействие на киберпрестъпността. Стандартът по киберсигурност[13] препоръчва създаването на информационна среда за обмен на данни, сертифицирана по специфичните изисквания за сигурност, посредством която да се реализира достигане на тази информация до съответните държавни агенции. Разработени са предложения и решения за обмен на информация за киберзаплахите [8], [9].

Препоръчваните практики в това отношение [10] на Националния институт за стандарти и технологии на САЩ са следните:

1. Каталогизиране на информацията, която всяка организация притежава и произвежда. Документиране на обстоятелствата, при които информацията може да бъде споделена.

2. Споделяне на данните за заплахи (придобити чрез разузнаване), инструментите и техниките с цел съвместна защита и противодействие с партньорите. Предприемане на самостоятелни или колективни действия за справяне с известни заплахи.

3. Насърчаване на оперативната съвместимост, за да се създаде интегрирана информационна среда за обмен на различни продукти, бази от данни и инструменти. Използване на стандартни формати за данни и транспортни протоколи за осигуряване на ефективен и ефикасен обмен на информация за кибер заплахи.

4. Събиране на данни, анализ и управление на информационните процеси с помощта на информация от външни източници. Придобиване на знания за функционирането на мрежите на организацията, с цел идентифициране на кибер атаки и по-ефективно разкриване на смесени заплахи, които използват множество методи за атака.

5. Създаване на подход към киберсигурността, адаптиран към жизнения цикъл на атаките и разработване на отбранителни мерки за откриване и ограничаване на възможността за провеждането на злонамерено разузнаване и добиване на важна информация от противника.

6. Осигуряване на потенциал от организацията, за да участва в процеса на споделяне: персонал, обучение и предоставяне на хардуер, софтуер, услуги и друга инфраструктура, необходима за осъществяване на събиране на данни, съхранение, анализ и разпространение.

7. Гарантиране защита на чувствителната информация, касаеща информационната сигурност (уязвимости и заплахи). Организациите да извършват проверки на сигурността, необходими за защита на чувствителната информация, да прилагат правилата за обмен на информация и да гарантират, че информацията, получена от външни източници е защитена, в съответствие с приложимите споразумения за обмен на данни.

[13] *ISO/IEC 27032*

8. Създаване на инфраструктура за реализиране на киберсигурност и ясно определяне на ролята и отговорностите за инсталиране, функциониране и осъществяване на необходимите дейности. Осигуряване на основни активи и способности за управление на конфигурацията, които да гарантират мониторинга и управлението на хардуера и софтуера на мрежите в реално време, с цел да бъдат разкрити своевременно уязвимостите.

*Създаване на звена за натрупване и анализ на информация*

Тези звена се идентифицират като информационни хранилища в държавния и частния сектор и имат за цел да:

- Изградят система за автоматично споделяне на индикаторите на заплахи;
- Създадат мрежова доверена среда за обмен на информация;
- Изготвят и приемат споразумения за съглашение между участниците;
- Създадат система за управление на докладите за киберзаплахи и уведомяване на компаниите, които може да бъдат цели на зловредна кибер активност.

Пример за такава дейност са мерките на САЩ в предметната област[14]: за периода до м. юли 2015 г. са сключени 125 съглашения между организации и още 156 са в списъка на чакащите за преговори.

*Подобряване на партньорството между държавните ведомства и частния бизнес*

Клетките за натрупване и споделяне на данни в сферата на информационната сигурност свързват държавните и частните ведомства. Сътрудничеството между тях се развива също така в сферата обучението и подготовката. Обучението се извършва на две равнища [11] – управленско (за създаване и прилагане на оперативните процедури) и изпълнителско (за провеждане на противодействие срещу кибер атаки в реално време). Особено полезни са ученията по киберсигурност, които може да се провеждат в различни формати – от учения на маса и ситуационни игри до симулации във виртуална среда. Идеята е чрез симулации на кибер инциденти от различен мащаб и характер да се идентифицират съществените проблеми при противодействието и формиране умения за ефективен отговор.

Друга възможност за обучение са работните групи, в които се изучават заплахите, уязвимостите и инцидентите, и се усвояват оперативни процедури за справяне с подобни ситуации.

Приложението на последните технологични иновации за киберсигурност е от съществено значение за сектора на националната сигурност и критичната инфраструктура. Във връзка с този процес се обръща специално внимание на дисциплината, по отношение приложението на софтуера и хардуера и управлението на риска при доставките.

[14] *FACTSHEET: Administration Cybersecurity Efforts 2015.*

*Партньорство с компаниите, производители на технологии за сигурност*

Ангажирането на заинтересованите страни в сферата на телекомуникациите и информационните системи е необходимо за изграждане на цифровата екосистема [12]. Фирмите, производители на софтуер и хардуер в сферата на сигурността имат сериозни отговорности за провеждане на проучвания и изследвания на заплахите и уязвимостите. Производството на сигурни и защитени технологични средства е решаващо в процеса на гарантиране на сигурността в кибер пространството.

Изграждат се национални центрове по компетентност в сферата на киберсигурността с участие на частния сектор, академии, изследователски организации и правни ведомства. Основната задача на тези центрове е: да се търсят решения за сигурност на базата на последните технологични новости; да се изработят референтни решения, шаблони за масово прилагане, за да се намалят разходите и сложността за въвеждане на средства за сигурност от компаниите. Естествено този процес има и негативни последствия, тъй като предоставя възможности на злоумишлениците да атакуват стандартизираните технологии. Но, трябва да се отчитат и положителните страни на подобни решения за компаниите, които не разполагат с достатъчни финансови средства за инвестиция в сигурността.

*Защита на потребителите*

•Въвеждане на системите за здравно осигуряване в цифровата екосистема - информационната система в здравеопазването съдържа висок риск по отношение на основните характеристики на информацията – тайна, цялостност и наличност. Усилията за изграждане на интегрирана мрежа за здравна информация като част от цифровата екосистема са свързани с решаване на няколко проблема [13]:

-Разработване на регламентиращ акт, относно защитата на чувствителната информация и данни за пациентите (електронните медицински досиета);

-Изграждане на сигурна мрежова и информационна среда, въз основа на дефинираните изисквания;

-Прилагане на единна политика при разработването на здравен софтуер и неговото сертифициране.

Насоките за действие са свързани с изясняване на специфичните изисквания към сигурността на информацията в здравната сфера, с цел гарантиране безопасността на гражданите като пациенти и отразяването им в националното законодателство.

•Прилагане на по-сигурна технология за разплащане [14].

За гарантиране на приемливо ниво на риска за сигурността е необходимо финансовите институции да извършват анализ на веригата за сигурност: <*уязвимости – заплахи – атаки – противодействие*> и да изграждат и прилагат стратегия и политики за защита на ценните информационни активи на потребителите. Управлението на процеса за сигурност се основава на рамков документ съдържащ ръководство за действие, в съответствие със стандартите [15] във финансовата сфера. Основните направления за действие са:

•Разработване и прилагане на решения за сигурност на онлайн транзакциите;

•Информиране на клиентите за заплахите в мрежата и създаване на уеб сайтове с информация за жертвите на компютърни измами.

**Заключение**

Поради глобалния характер на киберпространството, преодоляването на кризите в киберсигурността е глобален проблем, който не може да бъде решен едностранно. Сътрудничеството на различни равнища – национално и трансгранично – е от първостепенно значение в свят с разнородни интереси и конкуренция.

Създаването на организации и общности за анализ и споделяне на информация за инциденти в сигурността е направлението за действие, от което се очаква реален резултат в процеса за сигурност.

От съществено значение е изграждането на политики и способности за превенция на инцидентите, чрез въвеждане на технологични инструменти. Идентифицирането на събитията в киберсигурността в реално време, както в държавната администрация, така и в частния сектор и повишаването на масовата култура в сферата на киберсигурността ще понижи нивото на остатъчния риск.

На преден план в това отношение са многостранните инициативи за сътрудничество в областта на кибер разузнаването и националната кибер отбрана в рамките на международни съглашения.

***Използвана литература:***


1. *Valeriano, B., R. Maness, The Fog of Cyberwar. Why the Threat Doesn't Live Up to the Hype, Foreign Affairs, 2012.*
2. *Каракънева, Ю., Регулаторни проблеми на киберсигурността, Годишник на департамент НМС, НБУ, 2014.*
3. *ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity.*
4. *National Initiative for Cybersecurity Education, http://csrc.nist.gov/nice/ .*
5. *European Union Agency for Network and Information Security, https://www.enisa.europa.eu/*
6. *http://www.consilium.europa.eu/bg/policies/cyber-security/.*
7. *http://cyber.law.harvard.edu/cybersecurity/An_Assessment_of_International_Legal_Issues_in_Information_Operations.*
8. *Goodwin J Cristin, Paul Nicholas, A framework for cybersecurity information sharing and risk reduction, Microsoft.*
9. *Cyber Threat Information Sharing - Amazon Web Services,*
10. *Chabrow, Eric, NIST Drafts Guidance on Managing the Data, 2014.*
11. *Каракънева, Ю., Концептуален модел на учение по киберсигурност, Научна конференция „Технологии и сигурност", Варненски свободен университет, 2014.*
12. *Digital Ecosystem Technology, European Commission, Information Society and Media, http://www.digital-ecosystems.org/book/Section3.pdf .*
13. *Каракънева, Ю., Аспекти на сигурността на информацията в специализирани системи, Годишник на департамент НМС, НБУ, 2015.*
14. *Каракънева, Ю., Защита на информацията в специализирани финансови системи, Научна конференция „Обучението и изследванията по икономика на отбраната и сигурността – настояще и бъдеще", УНСС, 2015.*
15. *PCI DSS Requirements and Security Assessment Procedures, Version 2.0 October 2010 Copyright 2010 PCI Security Standards Council LLC.*