ТЕХНОЛОГИЧНИ И ПРАВНИ АСПЕКТИ НА ЗАЩИТА ПРИ КИБЕРКРИЗИ

доц. д.н. Драгомир Кирилов Кръстев
ВСУ „Черноризец Храбър”

TECHNOLOGICAL AND LEGAL ASPECTS OF PROTECTION IN THE CYBER CRISIS

Assoc. Prof. Dragomir Kirilov Krastev, DSc.
Varna Free University „Chernorizets Hrabar”

Анотация: В статията се изследват въпроси свързани с генезиса, развитието и различните форми на престъпления извършвани с помощта на компютърни системи. Отделено е внимание на факторите, които оказват влияние върху киберсигурността. Анализирана е националната и международната правна рамка за противодействие на киберпрестъпленията.

Ключови думи: противодействие на престъпността, киберпрестъпления, киберсигурност, Европейски съюз.

Abstract: The article explores issues related to the genesis, development and various forms of crime perpetrated using computer systems. Attention is paid to the factors that affect cybersecurity. The national and international legal framework for combating cybercrime is analyzed.

Key words: counteracting crime, cybercrimes, cybersecurity, European Union

Понятието *„компютърни престъпления"* се появява в научната литература през 60-те години на XX век, след като стават известни случаи на незаконно използване на компютърни системи, компютърен саботаж, компютърен шпионаж. По-подробни анализи на престъпления от този род започват да се правят през 70-те години на века. През 1971 г. е създаден първият компютърен вирус „Creeper", който е насочен към телефонна компания, за да осъществява безплатни междуградски разговори. Това е първата проява на киберпрестъпление, което довежда до стартирането на първия антивирус, наречен „Reaper"[1].

Приблизително по същото време в редица държави се приема специализирано законодателство в областта на защитата на личните данни, санкциониращи посегателствата върху тези данни, събирани, съхранявани и предавани по електронен път. От историческа гледна точка това са първите законодателни разпоредби в тази област[2].

Специален момент в правната уредба е дефинирането на понятието *„компютърно престъпление"*. Под *"престъпление в кибернетичното пространство" ("компютърно престъпление", "свързано с компютрите престъпление"* или *"престъпление в сферата на високите технологии")* следва да се разбира *"престъпни деяния, извършени посредством използване на електронни съобщителни мрежи и информационни системи или срещу такива мрежи и системи"*[3]. В действителност понятието се отнася до три категории престъпни деяния, осъществявани във виртуално-реалното пространство.

Първата обхваща традиционните видове престъпления като измама или фалшификация, въпреки че в контекста на престъпленията в кибер пространството тази категория се отнася по-конкретно до престъпления,

извършени посредством електронни съобщителни мрежи и информационни системи *("електронни мрежи"*).

Втората се отнася до публикуването в електронна медия на незаконно съдържание (например детска порнография или материали подбуждащи расова омраза).

Третата включва престъпленията, характерни единствено за електронните мрежи, например атаки срещу информационни системи, отказ на услуга и чужд достъп (хакерство).

В литературата като синоним на термина компютърно престъпление, се използва понятието "киберпрестъпление". Но по-скоро между тях има някои различия. При компютърното престъпление, изпълнителното деяние се осъществява чрез компютъра, а при киберпрестъплението се използват компютърните системи за връзка към глобалната мрежа (Интернет). Характерното и общо за повечето становища за понятието *„компютърно престъпление"* е, че това е престъпление, извършвано в специфична среда компютърни, информационни системи, мрежи и т.н.; използва се специфичен метод. Но компютърното престъпление може да осъществи изпълнителното деяние на традиционно престъпление като кражба, измама и т.н. или деяние, което е уникално за този вид престъпност - хакерство и т.н. Но не може в никакъв случай да се приеме, че компютърните престъпления са традиционните престъпления, но осъществявани с компютър, защото тогава бихме изключили престъпления като хакерството, разпространяването на компютърните вируси и други. Няма единно определение за това какво представляват киберпрестъпленията, няма също така развита и единна законодателна рамка.

Широкото разбиране на термина *„киберпространство“* се отнася до виртуалната среда, в която протича информацията и се осъществява взаимодействие между хората.

1. По-точното определение е *„мрежа от взаимосвързани информационно-технологични инфраструктури, която включва интернет, телекомуникационни мрежи, компютърни системи и критична информационна инфраструктура“;*

2. Киберпространството е интерактивен домейн, включващ дигитални мрежи, използвани за съхраняване, модифициране и предаване на информация. Освен интернет включва и други информационни системи, които поддържат държавната администрация, бизнеса, инфраструктурата и различни услуги.

3. Поради свързаност и зависимост в киберпространството няма ясно разграничаване на различните сфери на сигурност, като надеждност на информацията, информационна сигурност, мрежова сигурност, сигурност на критичната информационна инфраструктура, сигурност в интернет. Затова е необходимо да се изгражда концепция за сигурност, която да включва всички аспекти и да гарантира непрекъснатостта на работните процеси в тази нова среда[4].

Практиката показва, че отговорът на проблема *„кибератака“* 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[5].

Няма съмнение, че киберсигурността е един от най-важните аспекти на националната сигурност и тази сигурност изисква много координирани действия и усилия. Осъществяването и поддържането на подобно динамично състояние могат да бъдат постигнати само чрез провеждане на внимателна политика.

Тъй като всичко в киберпространството е на базата на информационния обмен в мрежите, те трябва да бъдат предпазени от кибератаки, небрежност и природни бедствия, а информацията да запази своите основни характеристики – поверителност, цялостност и достъпност. За да се постигне ефективност на дейностите по киберсигурността, е необходимо те основно са бъдат насочени към определяне на технически и процедурни мерки, фокусирани върху информацията, потребителите, мрежовата и информационната инфраструктура (МИИ). По отношение на информацията мерките гарантират нейната достъпност, цялостност и поверителност, за потребителите – управление на идентичността и неопровержимостта на транзакциите, а за МИИ – цялост, достъпност, гъвкавост и всеобхватност. В процеса на взаимодействие обаче се проявяват няколко основни фактора, които могат да окажат съществено влияние върху изпълнението на посочените дейности.

Влияние на човешкия фактор

До голяма степен киберсигурността зависи от влиянието на човешкия фактор и на него следва да се обърне специално внимание. Информацията е основният елемент за киберпространството и запазването на

конфиденциалността, цялостността и достъпността ù е особено важно за нейната сигурност и полезност. Макар че фокусът е поставен главно върху информацията, всъщност потребителите на този ресурс, с техните цели, намерения, култура и поведение, са основният фактор за сигурността. Новите условия налагат и нова култура на общуване, поведение и работа. Ключът към справянето с това предизвикателство може би се крие в управляването на налагащите се промени, в информираността и в образованието.

Промяната на изградени навици за работа в информационна среда по една или друга причина се превръща в предизвикателство. В редица случаи, дори да са ясни бъдещите ползи от промяната за организацията и за хората в нея, тя няма да бъде приета доброволно. Някои възприемат мерките за сигурност като препятствие пред дейността, а не като полза за правилното функциониране или оцеляване на организацията. Част от проблемите, свързани с внедряването на мерки по сигурността, са прекалено ограничаване на потребителските права, влошаване условията на труд, ограничаване на законните права и свиване на оперативната ефикасност. Това може да доведе до загуба на надеждност в цялата система за информационна сигурност. Част от решението е постоянно и мандатно обучение и внушаване на отговорност.

Затова необходимите мерки по киберсигурността трябва да се представят по прост и ясен начин, който да улесни адаптирането към промяната на различните типове потребители. Тук информираността, обучението и практиката по киберсигурност играят съществена роля и трябва да бъдат гъвкави, динамични, разбираеми, балансирани, всеобхватни, постоянни по време на пълния жизнен цикъл на информацията.

Информацията

Информацията е основният елемент в киберпространството и затова и сигурността ù е с най-голямо значение за киберсигурността. Тя трябва да отговаря на редица изисквания и стандарти, за да бъде ефективна и ефикасна в процеса на вземане на решения, за да може да улесни осъществяването на целите на организацията. Тези цели са постигане на оптимални резултати чрез подходящи решения, споделеното им разбиране и по-добра информираност. За да бъде ефикасна информацията в тези цели, тя трябва да е видима, достъпна, управляема, надеждна и полезна.

С други думи, информацията трябва да бъде достъпна в правилния момент и за правилния потребител. Каква е зависимостта между киберсигурността и информационната ефикасност? Отговорът се крие в мерките за сигурност, насочени към самата информация, потребителите на мрежите и интернет

Проблемът с достъпната информация е в това как необходимото ни конкретно късче информация да бъде намерено сред необятния хаос от достъпна информация. Друга трудност е как да се направи видима конкретна информация само за правилния потребител, или с други думи, на принципа „необходимост да се знае“. Тези проблеми са свързани с местонахождението на информацията, с начина, по който може да се стигне до нея, както и с нейното разкриване пред потенциална аудитория. Разкриването се отнася не за това да се прави достъпно съдържанието на дадена информация, а да се обяви нейното съществуване.

Видимостта на информацията може да бъде регулирана чрез спазване на три различни политики:

• индивидуална информационна

видимост на базата на критерия *„необходимост да се знае“;*

• частична информационна видимост за групи по интереси;

• свободна информационна видимост за всички потребители.

Споделянето на информация е един от основните проблеми за сигурността ù в киберпространството, тъй като все още няма общо разбиране за политиките за информационна сигурност и правилата за защита на чувствителната информация и нейната класификация[6].

Мрежова и информационна структура

Следващият фактор, който е от съществено значение за киберсигурността, е мрежовата и информационна инфраструктура (МИИ). Тя е „поддържаща структура, изградена от компютърни мрежи, информационни системи, процеси, процедури, инструменти, помощни средства и технологии, свързваща индивидите с информация, на базата на една или повече специфични взаимовръзки, като позволява сътрудничество, информационно споделяне и намаляване продължителността на цикъла за вземане на решение“[7].

МИИ е от особена важност, защото надеждното ù функциониране гарантира достъп до компютри, компютърни мрежи, информационни системи, процеси, процедури, инструменти и помощни средства в съответствие с определени критерии. Освен това МИИ осигурява както гъвкавост на компютрите, компютърните мрежи и информационните системи, които могат да пострадат от кибератаки, така и способности за изпълняване на базови и критични функции. МИИ спомага за мрежовата конвергенция, като осигурява

оперативна съвместимост по сигурността между всички видове системи и връзки.

Идеята на мрежовата свързаност е предоставяне на много информационни услуги, които не зависят от времето, мястото и дистанцията. За да няма прекъсваемост и отказ от услуги, тяхната сигурност в киберпространството трябва да бъде гарантирана с допълнителни системи, приложения или дейности. Примери за такива дейности са управление на идентичността, кодиране, динамично управление на риска, спазване на принципа „необходимост да се знае“, сертификация на продукти и услуги, стандартизация, политики по сигурност, обучение и др.

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.

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[8].

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[9], 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)[10]. 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.

Законодателни инициативи

Няколко законодателни действия на ЕС допринасят за борбата с престъпленията в кибернетичното пространство. През 2013 г. е изготвена Директива 2013/40 на ЕП[11] относно атаките срещу информационните системи, тя инкриминира използването на инструменти, служещи за кибератаки, като например зловреден софтуер, укрепва уредбата за обмен на информация при атаки и осигурява обща европейска наказателноправна уредба за тази област.

Настоящата директива изисква сближаване на системите на наказателното право на държавите от ЕС и засилване на сътрудничеството между съдебните органи по отношение на:

• незаконния достъп до информационни системи;

• незаконната намеса в система;

• незаконната намеса в данни;

• незаконното прихващане.

За по-ефективна борба с киберпрестъпността Директивата призовава за развитие на международното сътрудничество между съдебните и правоприлагащите органи. За тази цел държавите от ЕС трябва:

- да имат национално оперативно звено за контакт - към ГДБОП е сформиран специализиран сектор „ Киберпрестъпност“ ;
- да използват съществуващата мрежа от звена за контакт 24 часа в денонощието и седем дни в седмицата;
- даотговарят на спешно искане за помощ в рамките на 8 часа и да посочат дали на искането за помощ ще бъде отговорено и кога;
- да събират статистически данни за престъпленията в кибернетичното пространство.

От месец февруари 2007 г. в рамките на сектор "Киберпрестъпност" функционира Националния контактен пункт 24/7 за запазване на компютърноинформационни данни. Той е създаден съгласно Конвенцията като основната му цел е осъществяване на навременен и директен контакт със служители на полицейски или правоприлагащи органи, пряко ангажирани в борбата с киберпрестъпността по света. За да бъде успешна борбата на ЕС с нарастващите заплахи от кибератаки през 2016 г. е приета Директива 1148

относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза, с която се цели въвеждане на построги правила за киберсигурност[12]. Реформата на киберсигурността е един от настоящите основни аспекти по пътя към доизграждането на цифровия единен пазар на ЕС. Изправен пред все по-сериозни предизвикателства в областта на киберсигурността, ЕС трябва да подобри осведомеността на хората и възможностите за реагиране на кибератаки, насочени срещу държавите членки или институциите на ЕС. Същевременно съвременните информационни и компютърни системи могат да бъдат сериозно засегнати от свързани със сигурността инциденти като технически повреди и вируси. Този вид инциденти, свързани с мрежовата и информационната сигурност, зачестяват все повече и стават все по-трудни за отстраняване. В едно свое изказване бившият директор на Европол Роб Уейнрайт съобщава, че се очаква кибератаките да струват на световната икономика 400 милиарда евро годишно.

На 17 май 2019 г. Съветът на Европейския съюз определи рамка, която дава възможност на ЕС да налага целенасочени ограничителни мерки за възпиране и реагиране при кибератаки, които представляват външна заплахаза ЕС или неговите държави членки, включително кибератаки, насочени срещу трети държави или международни организации, когато се смята, че ограничителните мерки са необходими за постигане на целите на Общата външна политика и политика на сигурност (ОВППС).

В обхвата на този нов режим на санкции попадат кибертаки със значително въздействие и които:

- водят началото си или се извършват от място извън Съюза, или
- за които се използва инфраструктура извън Съюза, или

- се извършват от лица или образувания, които са установени или действат извън Съюза, или
- се извършват с подкрепата на лица или образувания, които действат извън Съюза.

Настоящият режим на санкции обхваща също опити за кибератаки с потенциално значително въздействие.

По-специално рамката позволява на ЕС за първи път да налага санкции на лица и образувания, които носят отговорност за извършването на кибератаки или опити за кибератаки, които предоставят финансова, техническа или материална помощ за извършването на такива атаки или които участват в тях по друг начин. Могат да се налагат санкции и на лица или образувания, които са свързани с тях.

Ограничителните мерки включват забрана за лицата да пътуват до ЕС и замразяване на активи на лица и образувания. Наред с това, на лица и образувания от ЕС е забранено да предоставят средства на лицата и образуванията, посочени в списъка със санкции.

В заключение на казаното до момента, можем да извлечем факта, че компютърните престъпления са изключително актуални и с пренасянето на реалния свят във виртуалността, значително се повишава нуждата от адекватни мерки за защита както в националното, така и в международното законодателство.

Най-важно в борбата с този тип престъпления е превенцията им и може би като най-ефективен метод за предотвратяването на киберпрестъпността се явява осведомеността на гражданите и организациите, осъществена чрез

провеждане на различни информационни кампании в средствата за масова комуникация и интернет.

Необходимо е полезната информация, изнесена в сайтовете на специализираните органи за борба с киберпрестъпността, да бъде разпространена и в медиите, както и чрез организиране на специални мероприятия, посветени на темата.

В същото време е необходимо по-отговорно и разумно отношение на всеки един от нас, с оглед необозримите възможности, които предоставя интернет, да не се превърнем в жертва на собственото ни творение - Интернет.

Престъпленията във виртуалното пространство са с не по-малка степен на обществена опасност от тези, които се извършват в традиционната среда, затова те не трябва да бъдат подценявани, което изисква по-голяма ангажираност на гражданите по отношение информацията, която са готови да предоставят в глобалната мрежа и въобще използването на компютърни и информационни системи.

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[13].

Европейският съюз има стратегически интерес да гарантира, че технологичните инструменти за гарантиране на киберсигурността се разработват по начин, който позволява на цифровата икономика да се развива, като същевременно се защитават сигурността, обществото и демокрацията ни. Това включва защитата на критичен хардуер и софтуер.

В бъдеще би могла да се разгледа възможността за създаване на нов фонд за реакция при спешни случаи в областта на киберсигурността в полза на тези държави членки, които отговорно са изпълнили всички мерки за киберсигурност, изисквани съгласно правото на Европейския съюз. Фондът би могъл да предоставя спешна подкрепа в помощ на държавите членки — по същия начин, по който механизмът на ЕС за гражданска защита се използва за предоставяне на помощ при случаи на горски пожари или природни бедствия.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

[1] Иванов, И., Св. Лазаров Кибер заплахи, В: НВУ „Васил Левски“, Велико Търново 2019, с.11.

[2] Димитров, Г. Правосъдието в дигиталната ера; Аналитичен доклад, С. 2008. Law and Foundation, Justice in the Digital Era Project, Analytical Report BG.http://library.netlaw.bg/l_bg/?s=1.

[3] Манов, Б, И. Иванов, П. Петров. Аспекти на киберсигурността в комуникационното общество, В: сп. Notabene, ЮЗУ „Н. Рилски", Благоевград, бр.26, 2014.

[4] Козарова-Арменчева, Ил. Фактори на сигурността в киберпространството В: Военен журнал. - ISSN 0861-7392. - Год. 121, бр. 1 (2014), с. 94-99.

[5] Каракънева, Ю., Регулаторни проблеми на киберсигурността, Годишник на департамент НМС, НБУ, 2014.

[6] Козарова-Арменчева, Илина Стефанова Фактори на сигурността в киберпространството / Илина Козарова-Арменчева. - В: Военен журнал. - ISSN 0861-7392. - Год. 121, бр. 1 (2014), с. 94-99.

[7] Пак там, с. 96.

[8] Каракънева, Ю., Регулаторни проблеми на киберсигурността, Годишник на департамент НМС, НБУ, 2014.

[9] National Initiative for Cybersecurity Education, *http://csrc.nist.gov/nice/* .

[10]European Union Agency for Network and Information Security, *https://www.enisa.europa.eu/*

[11] *http://www.consilium.europa.eu/bg/policies/cyber-security/.*

[12] Иванов, Хр. Европейска нормативна база – гарантираща киберсигурността, В: НВУ „Васил Левски“, Велико Търново 2019, с.100.

[13]*http://cyber.law.harvard.edu/cybersecurity/An_Assessment_of_International_Legal_Issues_in_Information_Operations.*