ЕДИН ПОГЛЕД ВЪРХУ СЪЩНОСТТА НА КИБЕРПРЕСТЪПЛЕНИЯТА

Илин САВОВ*

The need for cyber security nowadays is tangible. The article reviews and assesses the notions of cyber space, cyber crime, and cyber security. In order to meet the operational needs of the security sector, it is necessary that information systems that work are adequate to cyber-threats and minimize vulnerabilities in their own system. In view of the adopted national, European and international treaties, the Republic of Bulgaria is obliged to develop and pursue a specific cyber security policy as a measure to counter cybercrime and cyber terrorism and to protect national interests.

Бързото развитие на съвременните информационни технологии, широкото внедряване на цифрови средства за видео- и аудиозапис, за фотоснимки и мобилна комуникация доведе до това, че разследващите служители в последно време постоянно се сблъскват с нова среда на извършване на престъпления – киберпространството, образувано от носителите на компютърна информация, представена в дискретен вид. Тези технологии чрез интернет постоянно формират нова среда за общуване и като цяло на живот на членовете на човешкото общество, броят на които непрекъснато нараства.

Увеличава се нуждата от сътрудничество между държавите в борбата с престъпността, което се обуславя от особения характер на киберпрестъпленията. Този вид престъпления засягат много държави. Необходимостта от координация за предотвратяване на престъпните деяния и оказване на взаимопомощ при разследването на наказателни дела става все по-голяма. Престъпленията, свързани с киберпространството, по своето естество надхвърлят националните граници и борбата срещу тях може да бъде резултатна единствено чрез тясно международно сътрудничество.

Рисковете и заплахите в киберпространството са трудни за дефиниране поради сложността за определяне на източника на въздействие и

* Авторът е професор, доктор, декан на Учебно-научен център „Национална сигурност и обществен ред“ – Висше училище по сигурност и икономика.

мотивите, бързото ескалиране на заплахата, сложността и интензивността на съвременните комуникационни и информационни процеси, динамиката на логическите и физическите връзки и неопределеността на процесите.

Понятието „интернет“ се появява за пръв път през 1968 г. в документ, изготвен от Министерството на отбраната на Съединените щати, с който се създава Агенцията за сложни изследователски проекти (Defence Advanced Research Projects Agency, DARPA). Първата поява на термина „киберпространство“ се появява в романа „Neuromancer“ на американския писател Уилям Гибсън през 1984 г.

Терминът на английски език „cyberspace“ (букв. „киберпространство“) е използван от автора на киберпънк научна фантастика Уилям Гибсън и в неговия разказ „Горящ хром“, макар че концепцията е описвана и преди това, например в късия разказ на Върнър Виндж „Истински имена“ („True Names“), и дори по-рано от Джон М. Форд в романа „Мрежа от ангели“ („Web of Angels“).

„Киберпространство“ е термин, който означава глобалната мрежа като съвкупност от независими информационнотехнологични инфраструктури, телекомуникационни мрежи и компютърни процесорни системи, в които се осъществява онлайн комуникация.

Първата криминална проява в киберпространството датира от 40-те години на миналия век, почти от времето, когато е създаден първият компютър. През следващите години, с развитието на глобалната мрежа в условията на „световна икономическа цялостност“ международните интернет престъпления се разрастват и започват да придобиват различни форми на проявление.

В тази връзка съвсем обосновано е мнението, че повишаването на ролята и значението на киберпространството като интерактивна информационно-комуникационна среда влече след себе си появата на цял комплекс от нови рискове и заплахи, свързани с увеличаване на уязвимостта на информационната инфраструктура, деструктивното информационно въздействие на хора с използване на възможностите на киберпространството за извършване на криминално наказуеми деяния.

Това се обяснява с факта, че много процеси от производствен и финансов характер, които по-рано традиционно са се правели ръчно, сега са просто немислими без използването на компютърни технологии. Ако някакъв компютърен вирус[1] се намеси например в работата на локалната или глобалната информационна мрежа, то ще се прекратят банкови пла-

[1] **Наказателен** кодекс, чл. 93 (Допълнителна разпоредба), т. 27 (нова – ДВ, бр. 38 от 2007 г.). „Компютърен вирус“ е компютърна програма, която се разпространява автоматично и против волята или без знанието на ползващите компютърните системи лица и е предназначена за привеждане на компютърни системи или компютърни мрежи в нежелани от ползващите ги състояния или в осъществяване на нежелани резултати.

щания, ще започне изключване на електроенергията, пътници ще останат без билети за влакове и самолети. И това е само незначителна част от възможните вредни последици.

Необходимостта от киберсигурност нараства бързо, тъй като все повече информация и технологии се предоставят в киберпространството. В днешно време се наблюдава нарастващо безпокойство сред правителствата по отношение на това, че виртуалното пространство ще се превърне в следваща сцена на военни действия. По този начин през 2011 г. Марк Клейтън от „Christian Science Monitor“[2] описва в статията си, озаглавена „The New Cyber Arms Race“, ново поколение кибератаки (както между впрочем е и заглавието на статията):

„В бъдещето войните няма да бъдат водени от войници с оръжие или чрез самолети бомбардировачи. Войната ще се започва с едно щракване на мишката на другия край на света, отприщвайки внимателно превърнати в оръжие компютърни програми, които нарушават или унищожават критични индустрии, като комунални услуги, транспорт, комуникации и енергетика. Подобни атаки биха могли също така да деактивират военни мрежи, които контролират движението на войски, пътя на реактивни изтребители, командването и контрола на военни кораби“.

Изразените становища и анализи на много експерти и специалисти в областта на националната сигурност по света доведоха до въвеждането на нови термини, като „кибервойна“ и „кибертероризъм“ в националните доктрини за национална сигурност. Наблюдава се, че все повече и критичната инфраструктура се контролира чрез компютърни системи и програми, които същевременно повишават ефективността на отделните процеси, но и откриват нови, уязвими звена.

С отчитане на по-горе изложеното трябва да признаем, че информационните процеси и взаимодействия, свойствени за киберпространството, вече съставят основата на огромното многообразие на явления в материалния свят, интелектуалната сфера на обществото, в живота на всеки цивилизован човек. Признаването на това важно обстоятелство стана голямо постижение на научната мисъл пред последните десетилетия. Едновременно с това трябва да се констатира, че насищането на окръжаващата действителност с компютърни системи и телекомуникационни мрежи не само забележимо повлия на престъпността, но и откри нови подходи за разследване на престъпленията, извършвани в киберпространството, което бързо се превръща в основно поле на търговските взаимоотношения.

Характерна особеност на киберпространството от криминалистична гледна точка е това, че взаимодействащите си в него обекти (файлове с информация и програми), които участват в процеса на образуване на възник-

[2] „Крисчън Сайънс Монитор“ – американски ежедневник.

ващите при това следи, нямат външна структура. Целият арсенал от средства и методи за работа с материалните следи, натрупани от трасологията,[3] тук се оказва практически безполезен. Методите на работа с виртуалните следи не са намерили засега, а и не биха могли да намерят правилното отразяване в НПК на Република България. Те фигурират само във вид на отделни криминалистични препоръки, при това основно в чужди литературни източници. Така например под „виртуални следи" се предлага да се разбира „следи, съхранявани в паметта на технически устройства, в електромагнитно поле, на носители на машинно читаема информация, заемащи междинно положение между материалните и идеалните"[4].

Престъпленията в киберпространството се отнасят към сферата на високите информационни технологии и се извършват от злосторници, използващи тези технологии за постигане на противоправни цели. Твърде разпространени посегателства станаха разбиване на пароли, кражби на номерата на кредитни карти и други банкови реквизити, разпространение чрез интернет на социално вредна информация (порнографски материали, клеветнически сведения, материали, подбуждащи към междунационална или междурелигиозна вражда, и т.н.).

Киберпрестъпленията много често се явяват международни, когато престъпниците действат в една държава, а техните жертви се намират в друга държава. Поради това за разкриване и разследване на такива престъпления особено значение има международното сътрудничество.

В същото време съвременният криминален свят вече не вижда своето престъпно функциониране без интернет, с помощта на който се осъществяват:

- дистанционна комуникация между престъпни групировки с различна криминална насоченост;
- обмен на престъпен опит;
- привличане на съучастници в подготвяни престъпления, криминално издирване на жертви и средства;
- продажба на имущество, придобито по престъпен начин;
- осъществяване на разплащателни парични операции между лица в условията на подготовка и извършване на престъпления;
- извършване на престъпления посредством мрежовото информационно пространство.

---

[3] Трасоло́гия (от фр. „la trace" – „следа", и гр. „λόγος" – „учение") – криминалистична наука за следите, един от централните раздели на криминалистичната техника, в който се изучават теоретичните основи и закономерности за възникване на следите, отразяващи механизма за извършване на престъпление; разработват се препоръки за използване на методи и средства за тяхното откриване, изземване и изследване на следите с цел изясняване на обстоятелствата, значими за разкриване, разследване и предотвратяване на престъпления.

[4] **Мещеряков,** В. А. Преступления в сфере компьютерной информации. Воронеж, 2002.

Затова е напълно закономерно, че криминалистите започнаха също да разработват такива направления по използване на компютърната информация и средства за нейната обработка в борбата с киберпрестъпността, като приложение на универсални и специализирани компютърни програми и устройства в качеството на средства на криминалистичната техника, формиране на правови основи и определяне на перспективите за използване на информационните системи и компютърни мрежи за разкриване и разследване на престъпления, използване на компютърни технологии за обучение на сътрудници на правоохранителните органи. През последните години традиционните издирвателни технологии в оперативно-издирвателната дейност забележимо отстъпват място на оперативно-технически мероприятия, като използване на различните оперативни способи при прилагане на специални разузнавателни средства, анализ на телефонния трафик и свързаните с него трафични данни, определяне на източниците на конкретни съобщения и тяхното местоположение и т.н.

В България с разкриване и разследване на киберпрестъпления се занимава специализираният сектор „Киберпрестъпност“ към ГД „Борба с организираната престъпност“ – МВР, който приоритетно изпълнява задачи по противодействие на организирани престъпни групи, извършващи:[5]

1. Нерегламентиран достъп до компютърно-информационни ресурси, унищожаване и промяна на компютърни данни, разпространение на пароли и заразяване с компютърни вируси;

2. Финансови измами в интернет и кражба на виртуална самоличност;

3. Нарушаване на авторски и сродни права;

4. Производство, държане и разпространение на порнографски материали с непълнолетни лица, проповядване или подбуждане към дискриминация, насилие или омраза, основани на раса, народност или етническа принадлежност;

5. Устройване на онлайн хазартни игри без надлежно разрешение на Държавната комисия по хазарта.

Служителите от сектора взаимодействат с правителствени организации, частни фирми, фондации и граждани с цел навременно противодействие на престъпления, в които се използват високотехнологични средства.

Разбирането на същността на интернет позволява да се заключи, че е необходимо той да бъде разглеждан като глобален феномен, оказващ все по-нарастващо влияние върху характера и структурата на съвременната престъпност. В качеството си на такъв той притежава ред специфични свойства, анализът на които позволява по-дълбоко да се разберат криминалистичните проблеми при разкриване и разследване на мрежо-

[5] *www.gdbop.bg*

вите и свързаните с използването на IT технологии киберпрестъпления. Най-значими между тях може би са следните:

1. Интернет има недържавен и децентрализиран характер, отсъства единна организация, изцяло координираща и контролираща неговото функциониране. В повечето държави, в т.ч. и в България, системата за регулиране и контролиране на глобалната мрежа се намира във фазата на създаване.

2. Технологична незащитеност на интернет, който от самото начало се е създавал като открита среда за комуникация на изследователски и военни компютърни центрове (сега в него влизат над 10 500 телекомуникационни мрежи от различен тип).

3. Възможността за анонимна дейност в интернет, опростените процедури за регистрация на потребителите, практически пълното отсъствие на идентификатори на личността на посетителите в глобалната мрежа съществено затрудняват откриването на лица, извършващи киберпрестъпления, особено трансгранични.

Посочените фактори, чийто списък може да бъде съществено разширен, усложняват слаборазвитите научни и правови основи за противодействие на престъпните посегателства в интернет и механизмите за тяхната реализация. Тук за криминалистите има огромно поле за работа, макар че редица стъпки в научен план вече са направени (за съжаление, в нашата страна те все още са твърде малко). Сред условията, подпомагащи криминализирането на киберпространството, трябва да се посочат:

- Нарастване на броя на потребителите на интернет, рязко увеличение на обема на съхраняваната, обработваната и предаваната компютърна информация;

- Изоставане на нормативната уредба от възможностите за противоправно използване на информационно-комуникационните технологии, от темповете за информатизация във всички сфери на обществения живот;

- Формиране на „електронна“ икономика: все по-широко разпространение получават системите за електронни плащания и покупки чрез интернет, финансовите и банковите операции се извършват в електронна форма;

- Ниско ниво на правната и компютърната култура, слаба подготовка или пълно отсъствие на такава в областта на информационната сигурност;

- Наличие на слаби места в програмното осигуряване на компютрите, в т.ч. и на действащите в държавните органи и организации;

- Активно използване в престъпната дейност на най-модерните технически средства и технологии и т.н.

Във връзка с развитието и усвояването на киберпространството спешна задача пред криминалистиката в Република България се явява разработката на оптимални тактически правила за извършване на такива

следствени действия, като оглед на мястото на произшествието, оглед на компютъра, оглед на машинния носител на информация, оглед на електронния документ на машинния носител на информация, изземване на персоналния компютър и компютърната информация, претърсване и изземване на електронната поща, назначаване на съдебни експертизи.

При производството на тези следствени действия разследващият служител трябва добре да се ориентира в особеностите на киберпространството, да познава съответната терминология, за да общува с престъпниците при равни условия, да се справя без помощта на съответния специалист. Няма нужда да се доказва, че такива разследващи служители сега са все още много малко.

Всичко гореказано позволява да се направи извод, че на нашите криминалисти ще се наложи през следващите години детайлно да изучат особеностите на киберпространството и извършваните в него престъпления, да разработят адекватни криминалистични, тактически и методически подходи за тяхното разследване и предотвратяване. Някакъв положителен опит в тази област вече има.

Ако трябва да обобщим, поддържането на сигурността е един от фундаменталните проблеми на международните отношения и на съвременното международно право. Развитието на информационните технологии, освен че допринася за положителното обществено развитие, има и силноизразена негативна страна – това е киберпрестъпността.

Към киберпрестъпленията се отнасят такива криминално наказуеми деяния, които се извършват в киберпространството против компютърните данни с помощта или посредством компютърни системи или мрежи, а също и с други средства за достъп до киберпространството. Следователно към киберпрестъпленията може да бъде отнесено всяко престъпление, извършено в електронна среда (съгласно определение на X конгрес на ООН по превенция на престъпността и отношение към правонарушителите). В по-конкретен контекст киберпрестъпност – това се престъпления в сферата на високите информационни технологии, извършвани от злосторници, използващи тези технологии за постигане на противоправни цели.

Киберпрестъпленията могат да бъдат дефинирани още като: „Правонарушения, които са извършени срещу индивиди или групи индивиди с криминален мотив с цел умишлена вреда върху репутацията на жертвата или причиняване на физическа или морална щета на жертвата директно или индиректно, използвайки модерни телекомуникационни мрежи, като интернет (чат, имейли, форуми и групи) и мобилни телефони (SMS/MMS)“[6].

[6] **Halder,** D., K. Jaishankar. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global, ISBN: 978-1-60960-830-9.

Появата на нови видове престъпления изисква нови подходи за борба с тях. Области на криминологията, които се занимават с компютърните престъпления и компютърната престъпност, са компютърната криминология и киберкриминологията.[7]

В зависимост от това с каква цел киберпрестъпникът нахлува в компютърните системи може да се предложи обособяването на три основни типа киберпрестъпления:

1. Криминални посегателства, когато компютърът се използва като предмет на престъпление, т.е. неразрешен достъп до информация, нейното повреждане или унищожение, кражба на важни сведения и т.н.;

2. Деяния, в които компютърът се явява в ролята на оръдие на престъплението, например при електронни кражби;

3. Престъпления, при извършването на които компютърът изпълнява ролята на интелектуално средство, например при създаването на порнографски сайтове или на такива, подтикващи към психични отклонения и самоубийства, разполагане в сайтовете на информация, можеща да доведе до междурелигиозна или междунационална вражда, и т.н.

Обществената опасност от противоправни действия в сферата на компютърната техника и високите информационни технологии (киберпрестъпленията) се състои в това, че те могат да доведат до грубо нарушаване на работата на автоматизираните системи за управление и контрол на различни важни обекти. Освен това в персоналните компютри и създадените чрез тях системи могат да започнат несанкционирани действия по унищожаване, модифициране, копиране на информацията и информационните ресурси, които са способни да предизвикат тежки необратими последствия, свързани не само с имуществени щети, но и с физически увреждания за големи групи хора.

През последните години станаха напълно възможни т.нар. „разклонени атаки“ на затворени сайтове, при провеждането на които се използват голямо количество компютри. Притежателите на компютри, поразени от различни типове вируси, програмирани за унищожаване на „вирусния“ код след завършване на атаката, могат да бъдат без свое знание както участници в кибератаките, така и неволни „съюзници“. Никак не е лесно такива атаки да се проследят, а още повече да се установят конкретните виновници за извършеното особено когато територията на страната е малка (какъвто е случаят с България).

Затова никак не е случайно, че 150 държави от световната общност разработват мерки за борба с кибератаките, а киберпространството все по-често се разглежда като четвърта площадка за водене на военни действия („хибридни войни“) наред със сушата, атмосферата и моретата.

---

[7] **Jaishankar,** K. Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press, 2011.

В международноправен аспект транснационалната киберпрестъпност изисква адекватно противодействие чрез съгласуваните действия на международната общност.

Към настоящия момент в повечето държави все още прилагат основно териториалния принцип и съответно националните си закони по отношение на киберпрестъпленията. Това от своя страна създава редица трудности при определянето на locus delicti[8]. Например при неоторизиран достъп в система има поне три възможни места, които могат да бъдат определени като locus delicti:

- мястото, където физически се намира хакерът в момента на извършване на престъплението;

- мястото, където той действа и където прилага инструментите си за извършване на деянието;

- мястото, където настъпва резултатът и където е локализирана целта и жертвата на деянието и където де факто възниква резултатът от престъплението.

Решението на този проблем не би могло да се намери само на национално равнище. Нараства необходимостта от създаването на общи правила, които да бъдат приложими във всички държави в тази област. На този етап не съществува решение по този проблем на международно равнище. Основният международен акт – „Конвенцията за киберпрестъпленията“, не дава ясен критерий за определяне на местопрестъплението.

Това съответно би означавало създаване на специален режим, валиден само за киберпрестъпленията, който обаче не би бил приложим и за други деяния. На този етап липсва адекватно решение и на международно равнище.

Едно от основните предизвикателства на международното наказателно право е определянето на приложимата юрисдикция при извършването на киберпрестъпленията. С оглед на бързоразвиващите се информационнотехнологични системи и комуникации е труднопостижимо постигането на универсално решение на проблема. Увеличава се нуждата на различен подход към всеки казус, както и гъвкави правни инструменти, готовност на всяка юрисдикция да тълкува правилно наказателноправното законодателство на съответната държава.

Освен основната уредба, която се съдържа в „Конвенцията за престъпления в кибернетичното пространство“, има и множество приети международни актове. Изнесената информация от германския вестник „Билд“,[9] според която става ясно, че терористите от кървавите атентати в

[8] Мястото, където е било извършено престъплението; местопрестъплението.

[9] Германските следствени органи, които се занимават с изясняване на обстоятелствата около парижките нападения (с цел предотвратяване на подобни атаки на територията на Германия), установили, че автоматите „Калашников“ са били закупени онлайн от търговец на оръжие и доставени от Германия.

Париж на 13 ноември 2015 г. са си поръчали автоматите по интернет от Германия, засилва необходимостта от усъвършенстване на международноправната уредба на киберпрестъпленията.

Пътят на противодействието на киберпрестъпността минава през провеждането на комплексни мероприятия и мерки с цел отстраняване на причините и условията, способстващи за извършването на тези деяния. Все по-голяма е необходимостта от създаването на качествена международноправна наказателна уредба, свързана с този вид престъпления.

В заключение можем да определим, че противодействието срещу киберпрестъпността се усложнява от разнообразието на атаки, очаквани поражения и мотивация на хората, извършващи атаките. В областта на криминалистиката има необходимост през следващите години детайлно да се изучат особеностите на киберпространството и извършваните в него киберпрестъпления, да се разработят адекватни криминалистични, тактически и методически подходи за тяхното разследване, разкриване и предотвратяване. Киберсигурността се основава на ефективно изграждане и поддържане на активни и превантивни мерки. Една от основните цели на киберсигурността е да се съхранят наличността и целостта на мрежите и инфраструктурата, както и поверителността на информацията, която се съдържа в тях. Има необходимост от хармонизиране на националното законодателство и нормативна база с това на евроатлантическите партньори с оглед на тенденциите в развитието на заплахите, злоумишлените и престъпни действия и регламентиране на съвместни действия за превенция, противодействие на киберпрестъпленията и защита на киберпространството.

Литература

1. **Актуализирана** Национална програма „Цифрова България (2016 – 2020)“.
2. **Директива** 2013/40 на Европейския парламент и на Съвета относно атаките срещу информационните системи. Да се предприемат подходящи мерки за по-ефективната им защита от кибератаки, да се подобри сътрудничеството между компетентните правоприлагащи и съдебни органи в Съюза, да се зачитат правата на човека и основните свободи на гражданите.
3. **Директива** на Европейския парламент и на Съвета на Европа относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза. Приета на 6.07.2016 г.
4. **Закон** за управление и функциониране на системата за защита на националната сигурност (ЗУФСЗНС), 2015 г.
5. **Иновационна** стратегия за интелигентна специализация на Република България 2014 – 2020 г. и процес на интелигентна специализация. Приета с Решение на МС № 857 от 3.11.2015 г; актуализиран вариант 15.10.2015 г.
6. **Конвенция** за престъпления в кибернетичното пространство. Приета на 109. заседание на Комитета на министрите на Съвета на Европа и открита за подписване в Будапеща на 23 ноември 2001 г.

7. **Мещеряков,** В. А. Преступления в сфере компьютерной информации. Воронеж, 2002.

8. **Наказателен** кодекс на Република България.

9. **Наказателнопроцесуален** кодекс на Република България.

10. **Национална** стратегия за киберсигурност. Приета от Министерския съвет на Република България на 13 юли 2016 г.

11. **Стратегия** за развитие на електронното управление в Република България 2014 – 2020 г.

12. **Halder,** D., K. Jaishankar. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global, ISBN: 978-1-60960-830-9.

13. **Jaishankar,** K. Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press, 2011.