СПЕЦИАЛНИ РАЗУЗНАВАТЕЛНИ СРЕДСТВА И КИБЕРСИГУРНОСТ

Огнян Стоичков

SPECIAL INTELLIGENCE AND CYBER SECURITY

Ognyan Stoichkov

***Резюме**: Изследвани са правните аспекти на киберсигурността, като елемент на националната сигурност и нормативните възможности за използване на специални разузнавателни средства в това направление. Анализирани са тенденциите в развитие на законодателството и проблемните области на регулираните обществени отношения. Констатирани са несинхонизирани актове, с понижена ефективност на прилагане, с оглед на динамиката на информационните технологии. Формулирани са основните изводи и препоръки за усъвършенстване на организацията, с оглед пълноценното използване на специалните разузнавателни средства за защита на киберсигурността.*

***Ключови думи:** специални разузнавателни средства, национална сигурност, киберсигурност, наказателно право, информационни технологии.*

***Summary**: The legal aspects of cyber security, as an element of national security, and the normative possibilities for using special intelligence means in this area have been studied. The trends in the development of legislation and the problem areas of regulated public relations are analyzed. Non-synchronized acts, with reduced effectiveness of implementation, have been found, in view of the dynamics of information technologies. The main conclusions and recommendations for improvement of the organization are formulated, with a view to the full use of special intelligence means for the protection of cyber security.*

***Keywords**: special intelligence, national security, cyber security, criminal law, information technology.*

Въведение

Промените в геополитическото пространство, в резултат на глобализацията и информационните технологии, увеличават предизвикателствата за сигурността на отделните страни и за международната стабилност като цяло, принуждават държавите да се съобразяват с тях и да търсят решения за успешното им преодоляване.

Технологичният прогрес изведе на преден план проблемите, свързани с киберсигурността и нейните съставни компоненти –

мрежовата и информационната сигурност, противодействието на киберпрестъпността и киберотбраната.

Киберсигурността и нейните компоненти представляват обособена подсистема в системата за защита на националната сигурност.

Националната сигурност е сравнително ново понятие за българското право, за разлика от законодателството на редица други държави, където тя отдавна заема полагащото ѝ се място на висша конституционна ценност.[1] Удовлетворява фактът, че след 2015 г., българският законодател за кратко време успя да компенсира закъснението, приемайки основополагащи закони в тази област – Закона за управление и функциониране на системата за защита на националната сигурност[2], Закона за Държавна агенция „Разузнаване“, Закона за военното разузнаване, Закона за противодействие на тероризма, Закона за противодействие на корупцията и за отнемане на незаконно придобитото имущество, Закона за киберсигурността. През 2018 г. беше приета и Актуализирана стратегия за национална сигурност на Република България.

Променените обществено-политически и социално-икономически условия извеждат нови предизвикателства при защита на националната сигурност и необходимост от *нова наказателна политика*, която да се базира на обективните данни за актуалната криминогенна среда.

Потвърждение на тази теза е едно от най-тежките извършени до момента „киберпрестъпления“ – престъпното посегателство срещу информационната система на Националната агенция по приходи (НАП) от 2019 г., когато се установи, че е осъществен неоторизиран достъп до данните на 6 074 140 физически лица. Неправомерно е разпространена и данъчно-осигурителна информация за местни и чуждестранни физически и юридически лица[3] и Агенцията е санкционирана.[4]

---

[1] Стойков, С. Предизвикателството на дилемата за сигурност – или какво не искаме да знаем за сигурността? 2017 г, МПЦ (ILAC) , сп. Право, Политика, Администрация - ISSN: 2367-4601, изд. ЮЗУ „Неофит Рилски“.

[2] Закон за управление и функциониране на системата за защита на националната сигурност (Обн. ДВ. бр.61 от 11.08. 2015г., последно, доп. ДВ. бр.15 от 22.02. 2022 г.), Чл. 2. **Национална сигурност** е динамично състояние на обществото и държавата, при което са защитени териториалната цялост, суверенитетът и конституционно установеният ред на страната, когато са гарантирани демократичното функциониране на институциите и основните права и свободи на гражданите, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива, както и когато страната успешно защитава националните си интереси и реализира националните си приоритети.

[3] Национална агенция по приходите – Съобщение за разпространени данни от 15.07.2019 г. https://nra.bg/wps/portal/nra/za-nap/Razprostraneni-danni-ot-NAP

[4] Комисия за защита на лични данни – Информация за извършена проверка в НАП от 29.08.2019 г. https://www.cpdp.bg/index.php?p=news_view&aid=1519 С оглед на осъществен неоторизиран достъп, неразрешено разкриване и разпространение на личните данни, КЗЛД наложи санкция на НАП в размер на 5 100 000 лева. **Б.автора –** Една част от засегнатите граждани завеждат искове за обезщетение срещу НАП, по Закона за отговорността на държавата и общините за вреди (ЗОДОВ), като се позовават и на Регламент (ЕС) 2016/679, и с влезли в сила решения на Върховния административен съд през периода 2019 г. -– 2021 г. Агенцията бе осъдена да изплати парични суми.

Безспорно негативните последици от кибератаката пряко рефлектират върху доверието на гражданите в институциите, отнасят се до сигурността на работа на самите институции, до надеждността им да съхраняват информация, което води до компрометиране на функциите на държавното управление в национален и международен план. Изброените последици пряко засягат и защитата на националната сигурност.

За случая е образувано досъдебно производство и са повдигнати обвинения по чл.108а НК за тероризъм – с цел да се създаде смут и страх в населението са извършени компютърни престъпления. В хода на разследването се установява подготовка за достъп и до информационната система на Агенция „Митници“[5], както и интерес към досиетата на лица, заемащи висши публични длъжности.[6]

Повече от три години след случая, се провежда разследване по досъдебно производство, без да е внесен обвинителен акт в съда. Вероятно част от трудностите пред обвинителната теза е доказване на специалната „терористична“ цел, за разлика от други възможните цели – користна цел при компютърните престъпления.[7]

Изложеният казус, както и други примери[8], представляват опит за „адаптиране“ на престъпни състави по глава първа от особената част на НК към деяния, свързани с киберсигурност и киберзаплахи[9].

1. Правни аспекти на киберсигурността.

1.1. Приложими актове на Европейския съюз.

В областта на киберсигурността са приети редица актове на ЕС и за нуждите на настоящата разработка са посочени част от най-съществените, релевантни за изследваната тема.

Във връзка са приложението на цитирания регламент ВАС отправи преюдициално запитване до Съда на Европейския съюз.

[5] Съгласно разпространена информация от Специализираната прокуратура - https://news.lex.bg/wp-content/uploads/2019/08/12.pdf

[6] Опит за нерегламентиран достъп до база данните на министър-председателя Б. Борисов, гл. прокурор С. Цацаров, нар. представител Д. Пеевски и др. https://news.lex.bg/wp-content/uploads/2019/08/4.pdf

[7] Виж Денчев, Ст, Информация и сигурност, 2019г, изд. „За буквите - О писменехъ“ УНИБИТ (ISBN:978-619-185-369-4), за киберпрестъпниците – стр.311-314

[8] Атаката срещу сървърите на **„Български пощи“** в София, свързана т. нар. крипто вирус, който криптира информацията на 16.04.22 г. и изплащанията на пенсии се преустановява. *Виж и Димов, П., Информационната война между Украйна и Русия, сп. Сигурност и отбрана, Издателски комплекс на НВУ „В.Левски“, бр.1/2022 г., стр.130-131.* Перманентно възникват проблеми и в информационната системата „Български документи за самоличност“ на МВР, които водят до временна невъзможност за предоставяне на услуги – регистрация на МПС в пунктовете на КАТ, получаване на документи за самоличност и др.

[9] Стойков, С, Кочев, Й, Маринов, Р., Лазаров, Л. Изграждане на система за ранно реагиране на кибер заплахи, НВУ „Васил Левски“- ISSN 1314-1937, стр. 145-159

През 2020 г. Европейската комисия представи *Стратегията на ЕС за киберсигурност за цифровото десетилетие*[10]. Новата стратегия има за цел да гарантира глобален и отворен интернет, като същевременно съдържа конкретни предложения за регулаторни, инвестиционни и политически инициативи в три области на действие на ЕС:

1. устойчивост, технологичен суверенитет и лидерство;

2. изграждане на оперативен капацитет за предотвратяване, възпиране и реагиране;

3. постигане на напредък в създаването на световно и отворено киберпространство чрез засилено сътрудничество. Предлага се *директива за устойчивост на особено важните субекти*, с която да се разшири обхвата на *Директива за критичната инфраструктура от 2008 г.*

Държавите членки се приканват да завършат, с подкрепата на Комисията и Европейската агенция за киберсигурност, прилагането на инструментариума на ЕС за 5G и бъдещите поколения мрежи[11].

С *Директива 2013/40/ЕС на Европейския парламент и на Съвета относно атаките срещу информационните системи*[12] се установяват минимални правила за определянето на престъпленията и наказанията в областта на атаките срещу информационните системи. Тя има за цел също да способства за предотвратяването на тези престъпления и да подобри сътрудничеството между съдебните и други компетентни органи.

Съгласно Директивата санкциите следва да се увеличат, с оглед причинени сериозни вреди или извършени посегателства срещу информационна система, която е част от *критична инфраструктура*. Нарушаването на нормалното ѝ функциониране може да доведе до сериозни финансови загуби, до заплаха за националната сигурност на страната, което води до прекомерно увеличаване на тежестта на засягане на обществените отношения от компютърни и компютърно свързани престъпления.

Задължават се държавите членки да предприемат необходимите мерки при „незаконен достъп до информационни системи“, „незаконна

[10] Стратегията на ЕС за киберсигурност за цифровото десетилетие, Европейската Комисия, 16.12.2020 г. file:///D:/Downloads/join2020_18_en_act_part1_v9_-_copy_2DD42D12-B246-B9BE-E927D92051AE4753_72164.pdf

[11] Виж https://cybbar.eu/wp-content/uploads/2022/08/2022-08-03_CYBBAR-D2.2-Bulgaria-Country-Profile.pdf

[12] Директива 2013/40/ЕС на Европейския парламент и на Съвета относно атаките срещу информационните системи (Транспонирана е в разпоредбите на Наказателния кодекс)., https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32013L0040

намеса в система“[13], „незаконна намеса в данни“[14], „незаконно прихващане“[15].

Препоръчва се да се предвидят по-строги наказания, когато атаката срещу дадена информационна система е *извършена от престъпна организация, съгласно определението в Рамково решение 2008/841/ПВР* на Съвета, относно борбата с организираната престъпност, когато атаката е широкомащабна и е засегнала значителен брой информационни системи или е причинила сериозни щети.

В *Директива (ЕС) 2016/1148 на ЕП и на Съвета* относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза[16] се определени понятията и стандартите в предметната област, като се задължава всяка държава членка да приеме национална стратегия, относно сигурността на мрежите и информационните системи.

По силата на *Регламент (ЕС) 2019/881 на ЕП и на Съвета от 17 април 2019 г., относно Агенцията на Европейския съюз за киберсигурност (ENISA) и сертифицирането на киберсигурността на информационните и комуникационните технологии,*[17] се уреждат правомощията на ENISA и се създава Европейската рамка за сертифициране на киберсигурността, с цел да се подобрят условията за функционирането на вътрешния пазар и хармонизиране на европейските схеми за сертифициране на киберсигурността, с оглед на създаването на цифров единен пазар за ИКТ продукти, ИКТ услуги и ИКТ процеси.

С Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета от 20 май 2021 година се създава Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове.[18]

---

[13] Пак там, чл. 4 – ... сериозното възпрепятстване или спиране на функционирането на информационна система чрез въвеждане на компютърни данни, пренасяне, увреждане, изтриване, влошаване, променяне или скриване на такива данни или спиране на достъпа до компютърни данни, когато е извършено умишлено и неправомерно, е наказуемо като престъпление, освен в маловажни случаи.

[14] Пак там, чл. 5 – ... изтриването, увреждането, влошаването, променянето, скриването на компютърни данни в дадена информационна система или спирането на достъпа до такива данни ...

[15] Пак там, чл. 6 – ... извършено с технически средства прихващане на непублични компютърни данни, изпращани до дадена информационна система, от нея или в нейните рамки, включително електромагнитните емисии от информационна система, пренасящи такива компютърни данни ...

[16] Директива (ЕС) 2016/1148 на ЕП и на Съвета относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016L1148 Виж Регламент за изпълнение (ЕС) 2018/151 на Комисията

[17] Регламент (ЕС) 2019/881 на ЕП и на Съвета, относно Агенцията на Европейския съюз за киберсигурност (ENISA), https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32019R0881

[18] Регламент (ЕС) 2021/887 на ЕП и на Съвета , https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32021R0887

1.2. Киберсигурността в националното право

Основните актове, отнасящи се до киберсигурността са: Актуализирана стратегия за национална сигурност на Република България[19], Актуализирана национална стратегия за киберсигурност „Киберустойчива България 2023”[20], Закона за киберсигурност[21], Наредба за минималните изисквания за мрежова и информационна сигурност[22], Закон за електронното управление[23], Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност,[24] Устройствен правилник на Министерство на електронното управление,[25] Наредба за условията и реда за определяне на мерките за защита на информационните и комуникационните системи на стратегическите обекти от значение за националната сигурност и за осъществяване на контрол,[26] Правилник за организацията и дейността на Съвета по киберсигурността[27] и др.

Съгласно т.166 от Актуализираната стратегия за национална сигурност на Република България единната национална политика за киберсигурност[28] включва и защита на критичната комуникационна и информационна инфраструктура, като се предоставя възможност на гражданите, бизнеса и публичните институции да обработват и обменят свободно и надеждно дигитална информация[29].

Политиката за киберсигурност[30] е очертана в Националната стратегия „Киберустойчива България 2020”, приета през 2016 г.[31] и

[19]Актуализирана стратегия за национална сигурност на Р България (Обн. ДВ. бр.26 от 23.03. 2018 г.)

[20] Актуализирана национална стратегия за киберсигурност „Киберустойчива България 2023”, приета с Решение на № 301 /2021 г. на МС

[21] Закона за киберсигурност (Обн. ДВ. бр.94 от 13.11. 2018 г., последно изм. ДВ. бр.25 от 29 Март 2022 г.)

[22] Наредба за минималните изисквания за мрежова и информационна сигурност (Обн. ДВ. бр.59 от 26 Юли 2019 г., изм. ДВ. бр.36 от 13 Май 2022 г., изм. ДВ. бр.47 от 24 Юни 2022 г.)

[23] Закон за електронното управление (Обн. ДВ. бр.46 от 12.06.2007 г., последно изм. и доп. ДВ. бр.15 от 22 .02.2022 г.)

[24] Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност, издадени от Комисията за регулиране на съобщенията (Обн. ДВ. бр.42 от 7 Юни 2022 г.)

[25] Устройствен правилник на Министерство на електронното управление (Обн. ДВ. бр.38 от 20 Май 2022г., последно, доп. ДВ. бр.85 от 25 Октомври 2022 г.)

[26] Наредба за условията и реда за определяне на мерките за защита на информационните и комуникационните системи на стратегическите обекти от значение за националната сигурност и за осъществяване на контрол (Обн. ДВ. бр.81 от 15 Октомври 2019 г.)

[27] Правилник за организацията и дейността на Съвета по киберсигурността (Обн. ДВ. бр.102 от 31 Декември 2019г., последно., изм. и доп. ДВ. бр.47 от 24 Юни 2022 г.)

[28] Каракънева, Ю., Киберсигурност, Изд. „Авангард Прима“, 2013 г.

[29] Георгиев, В. Управление на риска за киберсигурността, Изд. „Авангард Прима“, 2015 г.

[30] Георгиев, В. , Стратегически аспект на киберсигурността на национално и регионално равнище, НБУ

[31] Национална стратегия за киберсигурност „Кибер устойчива България 2020”, приета с Решение № 583 на Министерския съвет от 18.07.2016 г., валидна до 2020 г. https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1120

нейната актуализация през 2021 г. – Национална стратегия за киберсигурност „Киберустойчива България 2023”.

Приоритетни области на първата стратегия е мрежовата и информационната сигурност, както и защитата и устойчивостта на критичната инфраструктура. Сред целите на Актуализираната стратегия е *ефективното противодействие на киберпрестъпността, с акцент върху превенцията и защитата,* разследването и правоприлагането, както и подобрения оперативен капацитет и способности[32]. И двете стратегии определят термина *киберпрестъпление* – обхващащо традиционни престъпления (като измами, фалшифициране и кражба на самоличност), престъпления, свързани със съдържанието (като онлайн разпространение на детска порнография или насаждане на расова омраза) и престъпления, които са възможни само с компютърна технология и информационни системи (като атаки срещу информационни системи, отнемане на достъп и зловреден софтуер)[33].

Киберсигурността се определя като състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им. Мрежова и информационна сигурност, като част от киберсигурността[34] е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях.[35]

Към Министерския съвет е създаден Съветът по киберсигурността, с председател – министърът на електронното управление.

В *Закона за киберсигурност (ЗК*) са определени основните понятия в предметната област – ДР, §3, „Информационна защита“, „Инцидент със „значително увреждащо въздействие“, „Кибератака“, „Киберзаплаха“, „Киберинцидент“, „Киберинцидент със значителен приоритет“, „Киберинцидент с висок приоритет“, „Киберинцидент със среден приоритет“, „Киберотбрана“, „Мрежа и информационна

[32] Георгиев В. Информационно-аналитична дейност в системата за сигурност. София, Авангард, 2015 г.

[33] Изпълнението на двете стратегии е подкрепено от пътни карти, които очертават конкретни проекти, свързани със стратегическите цели, институциите, отговорни изпълнението на проектите и финансирането, https://cybbar.eu/wp-content/uploads/2022/08/2022-08-03_CYBBAR-D2.2-Bulgaria-Country-Profile.pdf

[34] Стойков, С, Марин, Н, Маринов, Р., Кочев, Й, Проблеми пред информационната сигурност, 2015г., сп. Сигурност - ISSN-2367-6833

[35] Закон за киберсигурност, чл.2

система“ и др. При сравнение с някои от дефинициите по чл. 93, т. 21-27 НК, се очертава необходимостта от синхронизиране на понятиен апарат.

В *Наредбата за минималните изисквания за мрежова и информационна сигурност* са регламентирани най-съществените мерки на защитата.[36]

Наредбата е издадена на основание чл. 3, ал. 2 ЗК, като изискванията определени с нея са с първостепенно значение за надеждността на редица процеси. Например, съгласно ПЗР, § 145 (14) от Изборен кодекс[37] – Дистанционното електронно гласуване се осъществява с помощта на система за дистанционно електронно гласуване… Системата трябва да отговаря на изискванията за мрежова и информационна сигурност, определени в наредбата по чл. 3, ал. 2 ЗК.

Със *Закона за електронните съобщения* е делегирано правомощие на Комисията за регулиране на съобщенията (КРС) да приеме правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги .

Правилата за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност, издадени от КРС, се прилагат спрямо изброени обществени електронни съобщителни услуги.[38]

В Устройствения правилник на Министерство на електронното управление са уредени функциите на Дирекция „Мрежова и информационна сигурност“ като Национален орган за сертифициране на киберсигурността по смисъла на Регламент (ЕС) 2019/881 на ЕП и на Съвета; като Национален Координационен център по смисъла на Регламент (ЕС) 2021/887 и др.

По силата на *Наредба за условията и реда за определяне на мерките за защита на информационните и комуникационните системи на стратегическите обекти от значение за националната сигурност и за осъществяване на контрол*, ръководителите на

[36] Наредбата за минималните изисквания за мрежова и информационна сигурност, чл.13 – чл.29: сегрегация; филтриране на трафика; неоторизирано използване на устройства; криптография; администриране на информационните и комуникационните системи; среда за администриране; управление на достъпите; защита при отдалечен достъп/работа от разстояние; защита на хардуерни устройства; защита на софтуер и фърмуер; защита от зловреден софтуер; защита на уеб сървъри; защита на Domain Name System (DNS); физическа сигурност; наблюдение; системни записи (logs) и др.

[37] Изборен кодекс (Обн. ДВ. бр.19 от 5 Март 2014 г., последно изм. ДВ. бр.15 от 22 Февруари 2022 г.)

[38]Правила за минималните изисквания за сигурност ... чл.3: 1. мобилна гласова услуга; 2. мобилен достъп до интернет; 3. фиксирана гласова услуга; 4. фиксиран достъп до интернет; 5. междуличностна съобщителна услуга без номер; 6. услуги за разпространение на радио- и телевизионни програми; 7. услуги, при които се използва комуникация машина - машина; 8. други услуги за пренос на сигнали.

стратегическите обекти и възлагащите стратегически дейности, които са от значение за националната сигурност, определят информационните и комуникационните системи с критично значение за дейността, след изготвяне на оценка и план за управление на рисковете за сигурността.

За изследваната област от значение са и разпоредбите на *Закона за защита при бедствия*[39], както и на *Наредбата за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях*.[40]

Съгласно *Закон за електронната търговия*[41], доставчикът на електронна услуга е длъжен да предостави всяка информация относно получателя на услугата и дейността му, включително и по електронен път при кибератака, киберинцидент или киберкриза. Тази информация е от вида на изброената в чл. 251и, ал. 3 ЗЕС и е от категорията данни, подчинени на режима на чл. 251и, ал. 3, т. 2 ЗЕС и сл.[42]

2. Наказателно правна уредба на компютърните и компютърно свързаните престъпления.

Понятието „компютърни престъпления“ е въведено в научната литература през 60-те години на XX век, след като са регистрирани случаи на незаконно използване на компютърни системи, компютърен саботаж и шпионаж. Приема се, че първият компютърен вирус „Creeper“ е създаден през 1971 г. и е насочен към телефонна компания, за да се осъществят безплатни международни разговори. В отговор на тази първата проява на киберпрестъпление, се създава първия антивирус „ Reaper“[43].

---

[39] Закон за защита при бедствия (Обн. ДВ. бр.102 от 19.12 2006 г., последно изм. и доп. ДВ. бр.60, 7.07. 2020 г.), ДР, § 1, т.15 **„Критична инфраструктура“** е система или части от нея, които са от основно значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на населението и чието нарушаване или унищожаване би имало значителни негативни последици за Република България, в резултат на невъзможността да се запазят тези функции., 16."Европейска критична инфраструктура".

[40] Наредба за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях (Обн. ДВ. бр.81 от 23.10. 2012 г., посл. изм. ДВ. бр.27 от 5.04. 2016 г.), ПЗР, § 2.Стратегическите обекти и дейности от значение за националната сигурност, определени в списъка – приложение към ПМС № 181 / 2009 г. за определяне на стратегическите обекти и дейности, които са от значение за националната сигурност, **се приемат за установени критични инфраструктури**. (Относими са изброените по р. VIII. Сектор „Телекомуникации и информация“ и др.).

От Приложение № 1 към чл. 2, ал. 1 от Наредбата, относими са следните секторите от р. III. „Информационни и комуникационни технологии“, 1. Електронни съобщителни мрежи; 2. Информационна и комуникационна инфраструктура и др.

[41] Закон за електронната търговия (Обн. ДВ. бр.51 от 23 Юни 2006 г., последно доп. ДВ. бр.53 от 8 Юли 2022 г), чл. 16, ал. 2.

[42] Решение № 932 /2019 г. по адм. д. № 5375/2017 г., V отд. на ВАС - Позоваването на чл. 16, ал. 3 ЗЕТ не удовлетворява законовото изискване за посочване на фактически и правни основания за събиране на информация за потребителя на електронната поща, по реда на ЗЕС.

[43] Иванов, И., Лазаров, Св., Киберзаплахи, НВУ „Васил Левски“– Велико Търново, 2019 г., с.11.

Динамиката, с която се развиват технологиите налага актуализация на законодателството. В годишните си доклади Центърът по киберсигурност към Европол препоръчва държавите членки да усъвършенстват нормативната уредба, която да отговаря на новите предизвикателства.

В доклада от 2019 г. се посочва тенденция за увеличаване на т.н. *компютърен саботаж в частния сектор* – компютърните престъпления, при които неправомерно се осъществява достъп до информационна система и данните в нея се увреждат или унищожават, с цел затрудняване на работата на съответното юридическо лице. През последните години подобни кибератаки, предназначени да причиняват щети, са се удвоили, като 50% от атакуваните фирми са били в производствения сектор.

Понятието „Киберсигурност“ не се използва в българското наказателно право. В чл. 93, т. 21-27 от Наказателния кодекс са дефинирани следните понятия: „Информационна система“ , „Компютърни данни“, „Доставчик на компютърно–информационни услуги“, „Компютърна мрежа“, „Компютърна програма“, „Компютърен вирус“.

В различни глави на НК са уредени тежки умишлени престъпленията, отнасящи се до информационни системи, компютърни данни и съобщения, за които е допустимо използване на СРС: тероризъм (чл. 108а), компютърна измама (чл. 212а), унищожаване и повреждане (чл. 216, ал. 3 и ал. 5), използване на компютърни програми и данни, за изготвяне на неистински парични знаци (чл. 246, ал. 3) или относно археологически обекти (чл. 277а, ал. 7), компютърни престъпления (чл. 319а – чл. 319е) и др.[44]

Към изброените престъпления, следва да се добавят и престъпления, за които не се допуска използване на СРС: нарушаване на неприкосновеността на кореспонденцията (чл. 171, ал.3 - 5 и чл. 171а НК).

С оглед на повишената степен на обществена опасност, би могло да се предложи завишаване на наказанието лишаване от свобода до шест години по чл. 171, ал. 5 НК[45], като се допусне използването на СРС за този състав и за състава по чл. 171а, ал. 2 НК, който към момента е тежко умишлено престъпление.

Голяма част от престъпленията в глава девета „а“ на особената част на НК – „Компютърни престъпления“, бяха леко наказуеми, без да

[44] Биха могли към тези престъпления да се допълнят и диверсия и вредителство (чл.106, чл.107 НК), както престъпления по съобщенията (чл. 347, 348 и 348а) – Б.а.

[45] Състава по чл. 171, ал. 5 НК е квалифициран по отношение на състава по чл. 171, ал. 3 НК, който от своя страна се отнася и до компютърното престъпление по чл. 319д, ал. 1 НК, което е тежко наказауемо.

се отчита завишената степен на обществената опасност. Едва след редакцията от месец юли 2022 г. (изм. и доп. – ДВ, бр. 53 от 2022 г.) всички престъпни състави по чл. 319а – чл. 319е НК, са тежки умишлени престъпления, за които е допустимо използване на СРС.

Съгласно препоръки в т. 13 и т. 27 от Директива 2013/40/ЕС на Европейския парламент и на Съвета, относно атаките срещу информационните системи – да се предвидят по-строги наказания, когато атаката срещу дадена информационна система е извършена от *престъпна организация.* В тази връзка би могло да се обсъди предложението, *разпоредбата на чл. 321, ал. 3 НК да се допълни и с престъпленията по чл. 319а – чл. 319е НК*.[46]

На следващо място, заслужава дебат и *предложението за наказуемост на* ***приготовлението*** *за извършване на компютърните престъпления*. В описаният случай, на „киберпрестъпление“, относно системата на НАП от 2019 г., се събраха доказателства, че единият от обвиняемите, половин година по-рано е проявявал интерес към защитата на тази информационната система, търсил е подходящи за намисленото престъпление кодове и програми. Разкриват се подготвителни действия и за достъп до информационната система на Агенция „Митници“. В сегашната редакция на компютърните престъпления това деяние не е съставомерно[47], за разлика от други престъпления, с по-ниска степен на обществена опасност, при които приготовлението е наказуемо.[48]

С цитираната редакция от 2022 г., относно компютърните престъпления се допълниха три състава с квалифициращ признак, относно изпълнителното деяние, насочено „срещу информационна система, която е част от критична инфраструктура“[49].

Би могло да се постави *концептуалния въпрос за наказателно-правна защита на критичната инфраструктура на държавата, не само във връзка с компютърните престъпления, но и с други престъпления* (квалифицирани състави), относими към обекти, дейности и сектори, част от тази инфраструктура, съгласно Закона за защита при бедствия, Наредбата за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях, ПМС № 181/2009 г. и други релевантни нормативни актове.

---

[46] В сегашната редакция на компютърните престъпления, само по чл. 319а, ал. 2 и чл. 319б, ал. 5, т.1 НК е предвиден квалифициращия признак, относно престъпна организация – Б.а.

[47] Освен в хипотезата на чл. 110, ал. 1, вр. с чл. 108а, ал. 1 НК – Б.а.

[48] Наказателен кодекс – чл. 195, ал. 5, вр. с ал. 1, т. 3, чл. 308, ал. 5, вр. с ал. 1 и 2, и др.

[49] Не е изключена опасността след НАП, „Български пощи“, сайтове на висши държавни институции– Президент, ДАР, МС и др., следващите цели на кибератака да са обекти от критичната инфраструктура.

Това е един от възможните подходи за защита на националната сигурност, чрез квалифицирани състави, независимо че тяхното систематично място е извън глава първа на особената част на НК[50].

Нещо повече, проф. Б. Велчев при изследване на възможни нови изменнически престъпления предлага и допълнителен подход, свързан със *създаване на изцяло нови и непознати за законодателството ни престъпни състави, които да отразяват съществуващи или прогнозирани опасности, относими към вътрешната сигурност.*

3. Специални разузнавателни средства

Връзката между защитата на националната сигурност и специалните разузнавателни средства през последните години привлича общественото внимание и е значима, както за противодействието на рисковете и заплахите, така и за гарантиране на защитата на правата на човека.

В международен план, държавни и частни субекти, активно разработват програми за киберзащита и киберразузнаване, използвайки секретни техники за контрол и събиране на данни, комбинирайки традиционните оперативни способи със специализирани програми и софтуер. Един от комплексите за тайно получаване на информация, отразен и в средствата за масово осведомяване, е софтуера *Pegasus, разработен и внедряван от израелската компания* NSO GROUP - Cyber intelligence for global security and stability (Киберразузнаване за глобална сигурност и стабилност).[51]

Видно от публично достъпната информация,[52] продуктите на NSO се използват от правителственото разузнаване и правоприлагащите органи за борба с престъпността (тероризъм, разкриване на групи за педофилия, трафик на секс, наркотици, пране на пари), както и в помощ на екипите за спешно търсене и спасяване (SAR) на лица в беда.[53]

Но на практика се оказва, че цитираният софтуер се използва и за незаконна дейност. През 2021 г. Върховният комисар на ООН за правата на човека прави изявление, относно разкритията за масово използване на софтуера Pegasus за шпиониране на журналисти,

---

[50] Велчев, Б. „Престъпления против Републиката“, 2014 г. Споделяме становището на проф. Велчев, че не само специалната цел, *но и мащабът на престъпните последици на определени състави могат да засягат основите на държавността*. Посочват се примери с престъпленията против политическите права на гражданите, в които макар формално да не поставя специална цел против Републиката, мащабът на престъпната дейност, свързана с „купуване на гласове“, надхвърля опасността да се засегне единствено активното избирателно право на лицето и пряко може да увреди сигурността на държавата.

[51] NSO Group е една от 100 най-влиятелни компании в света и една от двете израелски компании в списъка на TIME за 2022 г. , https://time.com/collection/time100-companies-2022/

[52] NSO Group – Cyber intelligence for global security and stability , https://www.nsogroup.com/

[53] Петров, Хр., Forbes, 2021 г.: В България развива дейност „Съркълс България“ ЕООД, част от кипърската Circles, която през 2014 г. е купена от фонд, притежаващ и NSO. https://forbesbulgaria.com/2021/07/22/circles

защитници на правата на човека, политици и други в различни страни, което представлява злоупотреба с технологията за наблюдение за незаконни цели[54].

Чрез софтуера Pegasus се прониква в електронните устройства и се сканира цялата информация в тях, чрез „технология с кликване“[55] или с „технология с нулево кликване“.[56]

За нерегламентирано използване на софтуера Pegasus, Софийска градска прокуратура образува на 23.02.2022 г. досъдебно производство за престъпление по чл. 319б, ал. 4 във вр. с ал. 1 НК.[57]

В българското законодателство специалните разузнавателни средства (СРС) са уредени в Закон за специалните разузнавателни средства (ЗСРС) и Наказателно-процесуалния кодекс (НПК): *технически средства* – електронни и механични съоръжения и вещества, които служат за документиране на дейността на контролираните лица и обекти, и *оперативни способи* – наблюдение, подслушване, проследяване, проникване, белязване и проверка на кореспонденция и компютърна информация, контролирана доставка, доверителна сделка и разследване чрез служител под прикритие.[58]

Основната цел на използване на СРС е изготвянето на веществени доказателствени средства (ВДС), за нуждите на наказателния процес за разлика от други тайни средства, способи, прийоми и техники, прилагани от службите, резултатите от които нямат процесуална стойност. Единственото изключение от тази цел при използване на СРС

---

[54] Върховния комисар на ООН за правата на човека: „Използването на софтуер за наблюдение е свързано с арести, сплашване и дори убийства на журналисти и защитници на човешките права … Предвид факта, че шпионският софтуер Pegasus, както и този, създаден от Candiru и други, контролира всички аспекти на живота на лицето, използването им може да бъде оправдано само за разследвания на сериозни престъпления и сериозни заплахи за сигурността… Компаниите, които разработват и разпространяват технологии за наблюдение, са отговорни за избягването на увреждане на човешките права... Държавите да въведат по-ефективни механизми за отчетност, по-добро регулиране на продажбата, трансфера и използването на технологии за наблюдение и осигуряване на строг надзор и разрешение“ https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner

[55] Mehul Srivastava in Tel Aviv , Financial Times, 2019 г.: Правителството на Мексико е платило 32 милиона долара през 2014 г. за Pegasus 2, съгласно договор с мексиканската прокуратура. Софтуерът и услугата – Enhanced Social Engineering Message, включва и създаването на примамлив SMS, върху който целта е да се кликне. https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab .

[56] Пак там: Експертите на WhatsApp, който се използва от 1,5 милиарда души по света, констатират , че е инсталиран софтуер за наблюдение – на iPhone и на Android, като се позвънява на цели, чрез приложението. Кодът се предава, дори ако потребителите не отговарят на обажданията. В рамките на минути след пропуснатото повикване, телефонът започва да разкрива своето криптирано съдържание, огледално на екран на приемащ компютър. След това предава целия си архив, включително и *местоположение, и включва камерата и микрофона, за да предава на живо*. Версията Pegasus 3 работи и с други приложения.

[57] Виж и цитираната Директива 2013/40/ЕС, чл. 7 – „Инструменти, използвани за извършване на престъпления“, относно производство, продажба, внос, разпространяване или друга форма на предоставяне на някой от изброените инструменти.

[58] Закон за специалните разузнавателни средства (Обн. ДВ. бр.95 от 21 Октомври 1997 г., последно доп. ДВ. бр.62 от 5 Август 2022 г.) - чл. 2 и Наказателно-процесуален кодекс (Обн. ДВ. бр.86 от 28 Октомври 2005 г., последно доп. ДВ. бр.62 от 5 Август 2022 г.) - чл. 172, ал. 1.

е запазване на информацията, по отношение на дейности за защита на националната сигурност.[59]

3.1. Общ ред за използване на СРС.

По общия ред за предотвратяване и разкриване на лимитивно изброени тежки умишлени престъпления, със срок на прилагане до 6 месеца, компетентни заявители са оперативните служби, включително Главна дирекция „Борба с организираната престъпност“ (ГДБОП) по отношение на организираната престъпна дейност.[60] В ГДБОП през 1998 г. е обособен специализиран отдел „Киберпрестъпност“.[61]

В досъдебното производство, заявител на СРС е наблюдаващият прокурор, а разследващите органи получават текущата информация от прилагането.[62]

3.2. Специален ред за използване на СРС.

В ЗСРС е регламентирана възможност за прилагане на СРС по отношение на дейности, свързани със защита на националната сигурност, в случай на предотвратяване на тежки умишлени престъпления, по глава първа от особената част на НК в удължени срокове – до 3 години.

Съществената особеност в тази хипотеза, освен по-дългите срокове на прилагане е и целта – превенция, предотвратяване на посегателство срещу националната сигурност.[63]

Посоченият специален ред за използване на СРС би могъл да се приложи и за част от компютърните престъпления, с оглед на високата степен на обществена опасност.

---

[59] Закон за специалните разузнавателни средства, чл. 3, ал. 2 , чл. 4 и чл. 31, ал. 6

[60] Закон за МВР (ДВ, бр. 53 от 2706.2014 г.), чл. 39, ал. 2. – Главна дирекция „Борба с организираната престъпност“ е национална специализирана структура за осъществяване на дейностите по чл. 6, ал. 1, т. 1-3, 6-9 по отношение на организирана престъпна дейност, свързана с: т. 1-2, *т. 3. компютърни престъпления или престъпления, извършени във или чрез компютърни мрежи и системи*; т. 4-12

[61] ГДБОП, отдел „Киберпрестъпност“: 1. нерегламентиран достъп до компютърно-информационни ресурси, унищожаване и промяна на компютърни данни, разпространение на пароли и заразяване с компютърни вируси, извършване на атаки за отказ от услуга/DDoS, обезобразяване на интернет сайтове и ресурси/deface; 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. https://www.gdbop.bg/bg/cyber

[62] Считано от 01.09.2022 г. в Националната следствена служба (НСлС) започна да функционира отдел „Киберпрестъпления“.Съгласно чл. 196, ал. 2 НПК следователи от НСлС *не са компетентни* да разследват дела за подобни престъпления, освен ако главният прокурор или зам.-главния прокурор не им възложи изрично конкретно дело – Б.а.

[63] ЗСРС – чл. 21, ал. 1, т. 2 и ал. 2, т. 2. За тероризма по чл. 108а НК и свързаните с него престъпления е предвиден и превилигирован ред за искане и разрешаване по чл. 13, ал. 4, чл. 14, ал. 3 и чл. 15, ал. 2.

Това са квалифицираните състави на компютърните престъпления, при които деянията са извършени по отношение на лични данни, на информация, представляваща държавна или друга, защитена от закон тайна или срещу информационна система, която е част от критична инфраструктура – **чл. 319а, ал. 4 и ал. 5** [64], **чл. 319б, ал. 5, т. 2**[65], **чл. 319г, ал. 4** [66] и **чл. 319д, ал. 2** НК[67].

Предложението, което би могло да се постави на обсъждане е за изброените състави, да се приложи редът за използване на СРС за дейности, свързани със защита на националната сигурност, в случаите на предотвратяване на посочените престъпни състави, наред с престъпленията по глава първа от особената част на НК, *за срок до 6 месеца, с възможност за продължаване на срока до 3 месеца, общо за не повече от 12 месеца*[68].

Целта на предложената законодателна промяна е да се постави акцента на превенцията срещу заплахата, предотвратяването на риска[69] от посегателства срещу информационната сигурност на държавата, чрез ефективно използване на „инструментариума“ на специалните разузнавателни средства.

Предложението за превенция срещу бъдещи посегателства, при установени данни за престъпни намерения или други форми на опасност, не е в колизия с приетия принцип за ретроактивно действие на наказателната санкция, т.е. наказуемост за осъществени, включително и на стадия на опита и приготовлението, деяния.

Удължеият срок на прилагане на СРС се мотивира с продължителната подготовка на подобна дейност, която протича в условията на конспиративност, при предварителни детайлни проучвания на условията, обстановката, отговорните лица, структурата и функциите на мрежовата и информационната сигурност и др.

---

[64] Наказателен кодекс, **чл. 319а (4)** Ако деянията по ал. 1-3 са извършени по отношение на информация, представляваща държавна или друга защитена от закон тайна или срещу информационна система, която е част от критична инфраструктура, наказанието е от четири до осем години лишаване от свобода, ако не подлежи на по-тежко наказание. **(5)** Ако от деянието по ал. 4 са настъпили тежки последици, наказанието е от пет до дванадесет години.

[65] Наказателен кодекс, **чл. 319б (5**) Наказанието е лишаване от свобода от девет до дванадесет години и глоба до тридесет хиляди лева, когато деянието по ал. 1: 1. е извършено от лице, което действа по поръчение или в изпълнение на решение на организирана престъпна група; **2**. *е извършено срещу информационна система, която е част от критична инфраструктура.*

[66]Наказателен кодекс, **чл. 319г (4)** Ако деянието по ал. 1 и 2 е *извършено срещу информационна система или компютърна мрежа, която е част от критична инфраструктура,* наказанието е лишаване от свобода от пет до дванадесет години и глоба до двадесет хиляди лева.

[67]Наказателен кодекс, **чл. 319д (2)** Когато с деянието по ал. 1 са разкрити лични данни, класифицирана информация или друга защитена от закона тайна, доколкото извършеното не съставлява по-тежко престъпление, наказанието е лишаване от свобода от четири до седем години.

[68] Закон за специалните разузнавателни средства – чл. 21, ал. 1, т. 2 и ал. 2, т. 2 (Б.а. – с предлож. редакции)

[69] Stoykov, S., Risk management as a strategic management element in the security system, International conference on Creative Business for Smart and Sustainable Growth-CreBus 2019, INSPEC Accession Number: 18994790, DOI: 10.1109/CREBUS.2019.8840098, Publisher: IEEE

елементи на системата, за която е налице престъпно намерение за посегателство.

Използване на СРС по този превилигирован ред е допустим само по оперативни дела, за това е уреден в ЗСРС, не и в НПК, тъй като по досъдебни производства е неприложим.

Посегателствата срещу киберсигурността обичайно се реализират с технически средства и способи, затова и противодействието им с техническите средства и оперативни способи, съставляващи специалните разузнавателни средства би бил адекватен и симетричен „отговор".

а) ограничен кръг заявители

Компетентни заявители на СРС за тези престъпления са: Държавна агенция „Национална сигурност", с правомощията си по Закон за държавна агенция „Национална сигурност"[70], Държавна агенция "Разузнаване", съгласно Закона за държавна агенция „Разузнаване"[71] и Служба „Военно разузнаване", по силата на Закона за Военно разузнаване[72].

б) специална цел на искането

Това е предотвратяването на определен кръг тежки умишлени престъпвания, като превенция за защита на националната сигурност. При започване извършването на тези престъпления се използват СРС по общия ред. За целта е необходимо в искането за използване на СРС **изрично да се съдържа позоваване на специалните текстове на чл. 21, ал. 1, т. 2 ЗСРС**, относими към предотвратяване на престъпления. Само в тези хипотези, съдът би разрешил по-дълги законово допустими

[70] *Закон за държавна агенция „Национална сигурност"* (Обн. ДВ. бр.109 от 20.12. 2007 г., последно доп. ДВ. бр.51 от 5.06.2020 г.), Чл. 4. (1) Държавна агенция „Национална сигурност" извършва дейности за защита на националната сигурност от посегателства,…, свързани със: **8**. нарушаване функционирането на Националната система за защита на класифицираната информация; **9**. застрашаване сигурността на стратегически за страната обекти и дейности; **10**. деструктивно въздействие върху комуникационни и информационни системи;

[71] *Закон за държавна агенция „Разузнаване"* (Обн. ДВ. бр.79 от 13.10. 2015 г., последно, изм. ДВ. бр.69 от 4.08.2020 г.), чл. 8. Дейности на ДАР: **13**. изграждане и поддържане на собствена автоматизирана информационна система за събиране, обработване, съхраняване, ползване и обмен на информация; **14**.разработване и използване на криптографски ключове, средства и системи за защита на информацията, съгласно закона и в рамките на своята компетентност; **15**. създаване и организиране на самостоятелно звено за осъществяване на електронните комуникации и криптографската сигурност между Агенцията и задграничните представителства на Р България и други ведомства; **16**. организиране и осъществяване на собствени комуникации за разузнавателни цели и за обмен на информация със свои структури;

[72] *Закон за Военното разузнаване* (Обн. ДВ. бр.88 от 13.11. 2015г., последно попр. ДВ. бр.25 от 26.03. 2021г.) , Чл. 12. Основни задачи на Службата на стратегическо ниво са: **2**. информационно осигуряване на дейностите на държавните институции в областта на сигурността и отбраната на страната; **6**. осъществяване на обмен на разузнавателна информация и провеждане на съвместни операции с ……, разузнавателните органи на държавите членки на НАТО и ЕС, и с партньорските служби; **7.** осигуряване на разузнавателна информация в интерес на сигурността на операциите и мисиите извън територията на страната, в които участват български военни контингенти и отделни военнослужещи;

срокове, с мотиви, относно *„установена опасност от извършване на престъпления, относими към защитата на националната сигурност.*“

в) удължен срок за прилагане – до 12 месеца

г) завишаване на съдебния контрол, с оглед гарантиране на необходимостта от използване на СРС, като извънреден способ, само когато е „ необходимо в едно демократично общество“

д) при искане за продължаване на първоначалния срок, следва да се посочат на съда резултати, свързани с предотвратеното престъпление, в следствие на прилагането на СРС, както и фактите и обстоятелствата за потенциалната опасност за извършване на това престъпление и за бъдещия период на използване на СРС.

Като една от „дисциплиниращите“ процеса мерки, би могло да се обсъди възстановяване в ЗСРС на отменени норми, относно *финансовата обвързаност на заявителя*, която да се приложи при продължаване на срока за прилагане на СРС.

Предлагаме като втора възможна мярка, искането за продължаване на срока *да е утвърдено предварително от вишестоящия ръководител* на специалната служба – председателят на ДАНС или оправомощен от него заместник-председател[73].

е) подобряване на режима за уведомяване на засегнатите лица в тези процедури и улесняване на реда за обезщетяването им, при неправомерно прилагане на СРС.

В хода на действащо оперативно дело, при съобразяване с целите на закона, отлагане на уведомяването може да се прилага, за не повече от 12 или 18 месеца. След този срок, *спорът между надзорния орган и заявителя за уведомяване на засегнатото лице, да се реши от съда.*

Предложеният модел за използване на СРС, включва комплекс от мерки – нормативни, организационни, финансови и би могъл да се приложи и за други престъпления/квалифицирани състави, относими към защитата на националната сигурност.

Намирането на баланса между увеличаване на правомощията на службите за сигурност и повишаване на гаранциите за защита на правата на засегнатите лица, е едно от необходимите условия при всяка нормативна промяна на законодателството и процедурите по прилагането му. В противен случай, би се стигнало до българския вариант на „Pegasus“ – добро намерение и средство, без защитен правен механизъм, води до злоупотреба с право, когато се използва от държавни структури или до зловредни действия, осъществени от частни субекти.

[73] Към момента, директорите на специализирани, териториални дирекции, и самостоятелни отдели на ДАНС заявяват използване на СРС, както и искане за продължаване на срока. За ДАР и СВР – само председателят/директорът има подобни правомощия.

Заключение

Може да се обобщи, че изследваната тема показва необходимост от актуализиране на държавната политика в областта на използването на СРС за защита на националната сигурност, включително и при киберзаплахи и обезпечаване на киберсигурността.

Актуализиране на наказуемостта на компютърните престъпления през 2022 г. би следвало да е първи етап в процесите за адаптиране на престъпните състави към съвременната криминогенна среда и синхронизиране на нормативните актове в предметната област. Поради сложността, комплексността, интердисциплинарността и динамичността на тези процеси, би било претенциозно да се ангажираме с готови решения по всички дискусионни теми. Трудно е да се дадат точни и еднозначни отговори на всички възникнали въпроси, но би било успех, ако те бъдат поставени на вниманието на обществото.

ЛИТЕРАТУРА:

1. **Велчев,** Б., Престъпления против Републиката, 2014г., Сиела

2. **Георгиев,** В., Стратегически аспект на кибирсигурността на национално и регионално равнище, НБУ

3. **Георгиев** В. Информационно-аналитична дейност в системата за сигурност. София, Авангард, 2015 г.

4. **Георгиев,** В. Управление на риска за киберсигурността, Изд. „Авангард Прима“, 2015 г.

5. **Денчев,** Ст. Информация и сигурност, 2019 г., изд. „ За буквите - О писменехъ“ УНИБИТ (ISBN:978-619-185-369-4)

6. **Димов,** П., Информационната война между Украйна и Русия, сп.Сигурност и отбрана, Издателски комплекс на НВУ „В. Левски“, ISSN 2815-388X- бр. 1/2022 г.

7. **Иванов,** И., **Лазаров,** Св., Киберзаплахи, В, НВУ „В.Левски“-В.Търново, 2019

8. **Каракънева,** Ю., Киберсигурност, Изд. „Авангард Прима“, 2013 г.

9. **Стойков**, С. Предизвикателството на дилемата за сигурност - или какво не искаме да знаем за сигурността? 2017 г., МПЦ (ILAC), сп. Право, Политика, Администрация - ISSN: 2367-4601

10. **Стойков,** С, **Кочев,** Й., **Маринов,** Р., **Лазаров**, Л. Изграждане на система за ранно реагиране на кибер заплахи, НВУ „В.Левски“-ISSN 1314-1937, с. 145-159

11. **Стойков,** С, **Марин,** Н, **Маринов**, Р., **Кочев,** Й, Проблеми пред информационната сигурност, 2015 г., сп. Сигурност - ISSN-2367-6833

12. **Stoykov,** S., Risk management as a strategic management element in the security system, International conference on Creative Business for Smart and Sustainable Growth-CreBus 2019, INSPEC Accession Number: 18994790, DOI:10.1109/CREBUS.2019.8840098, Publisher: IEEE

Интернет ресурси (посетени на 12.11.2022г):

1. https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner
2.https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab
3. https://nra.bg/wps/portal/nra/za-nap/Razprostraneni-danni-ot-NAP
4.https://www.cpdp.bg/index.php?p=news_view&aid=1519
5.https://news.lex.bg/wp-content/uploads/2019/08/12.pdf
6. file:///D:/Downloads/join2020_18_en_act_part1_v9_-_copy_2DD42D12-B246-B9BE-E927D92051AE4753_72164.pdf
7.https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32013L0040
8. https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32019R0881
9. https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016L1148
10. https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32021R0887
11. https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1120
12. https://www.gdbop.bg/bg/cyber