СТРАТЕГИЯ ЗА КИБЕРСИГУРНОСТ НА ЕВРОПЕЙСКИЯ СЪЮЗ

Шабан Фейзи Бошнак – студент
Югозападен университет – „Неофит Рилски” – гр. Благоевград
научен ръководител проф. д-р Любомир Тимчев

STRATEGY FOR CYBERSECURITY ON EUROPEAN UNION

Shaban Feizi Boshnak – student
South-West University – „Neofit Rilski” – Blagoevgrad

Abstract: *The policy of the European Union on cybersecurity issues represents a specific and extremely topical problem, the solution of which requires the active engagement of both countries and international organizations, as well as stakeholders from a variety of fields.*

Key words: *strategy, security, cybersecurity, Bulgaria, European Union, threats*

Ключови думи: *стратегия, сигурност, киберсигурнос, България, Европейски съюз, заплахи.*

Въведение

Проблемите, свързани с киберсигурността, възникват в началото на 90-те години на XX век, но през първите години негативният ефект от тях все още не се усеща толкова силно. След 2010 г. обаче киберсигурността става все по-актуална тема. Търсенето на решение на проблема отдавна надхвърля границите на една отделна наука и изисква сложен интердисциплинарен подход, с участието на всички заинтересовани страни.

Новите предизвикателства пред международната общност и информационните и комуникационните технологии пресичат националните граници и държавите, които не успяват да се справят самостоятелно и ефективно с въпросите на киберсигурността и новите заплахи. Само чрез политиките на национално ниво не могат да осигурят висока степен на защита на своите граждани и мрежите на държавната власт и все по-силно се усеща необходимостта от колективни усилия за защита на киберпространството.

Във връзка с гореизложеното и имайки предвид динамичното развитие на заплахите за киберсигурността, следва да се подчертае обстоятелството, че към настоящия момент Европейският съюз е един от най-влиятелните участници в международната политика за киберсигурност.

Към настоящия момент, ЕС е един от световните лидери в сферата на международното сътрудничество в областта на киберсигурността. Неговите действия са неразривно свързани с глобалните действия в тази сфера, включително и провежданите под егидата на ООН. Нещо повече, инициативите на държавите членки на ЕС изпреварват съществено останалите континенти и региони в света.

Актуалността на темата се определя още от факта, че е изтъкнато обстоятелството, че Европейският съюз би могъл да се превърне в основен двигател на международните процеси, като използва своя полезен опит в областта на интеграцията, но пречупен през призмата на обединяване на усилията на международната общност за постигане на високо ниво на киберсигурност.

Само по този начин би могло да се постигне реално взаимодействие между различните страни и региони, и да се постави началото на широко подкрепен от международната общност процес на по-тясно сътрудничество в областта на киберсигурността.

ЕС разполага с широка, макар и споделена с държавите членки законодателна компетентност в областта киберсигурността. Неоспорим факт е обаче, че въпреки съществуващата правна уредба, която е в процес на развитие на основните въпроси, свързани с киберсигурността, невинаги са налице необходимите социални условия или финансови ресурси за прилагането на тези разпоредби в по-слабо развитите държави членки и особено сред страните от Централна и Източна Европа. Основна причина за това е неустановеният баланс на технологично и икономическо развитие между държавите членки. В този контекст изработването на единна политика по опазване на киберсигурността се явява сложна и отговорна задача, която изисква обединение на усилията на междудържавно равнище.

1. Условия за създаване и развитие на политика на Европейския съюз по проблемите на киберсигурността

Едно от необходимите условия за създаването и развитието на политика на Европейския съюз за киберсигурността е разбирането за това какъв смисъл се влага в понятието „киберсигурност”. Постигането на това може да бъде трудно поради няколко причини. Сред основните предизвикателства и трудности е неговата широта и многоаспектност, влияеща върху различни сфери на обществените отношения между гражданите ЕС и между отделните държавите членки на Европейския съюз. Разбира се, налице са много компоненти на киберпространството и различни потенциални участници в провеждането и осъществяването на политиката по линия на киберсигурността. Различните заинтересовани страни могат да бъдат ангажирани като обекти или субекти в различни области и етапи на разглежданата политика и следователно, опитите за създаване на координирана политика в рамките на Европейския съюз може да се окажат предизвикателство, но и една абсолютно необходима реалност, съдържаща концентриране и обединение на традиционното политическо сътрудничество с други нови и непрекъснато променящите се съставни части на новите информационни технологии.

Друг проблем е, че не съществува общоприето определение за киберсигурност и се употребяват няколко различни термина, които са с близки значения, но същевременно имат известни отличителни характеристики.

Първият акт на институциите на ЕС, който е част от вторичното право на Европейския съюз, който дава съществен тласък в развитието на дефиницията за информационната сигурност е Директива 95/46/ЕО[1]. Тя обаче е насочена по-скоро към защита на лицата по отношение на обработката на лични данни и за свободното движение на тези данни вътре в пространството на ЕС и спрямо трети държави, с които ЕС има сключени споразумения за обмяна на данни като например със САЩ.

За сравнение според законодателството на Съединените американски щати и по-конкретно във Федералния закон за управление на информационната сигурност дефиницията на това понятие се свързва със „защита на информацията и информационните системи от неоторизиран достъп, използване, разкриване, смущения, про-

[1] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data https://ccdcoe.org/sites/default/files/documents/EU-951024-Data ProtectionDirective.pdf

мяна или унищожаване.”[2] Става дума за един по-широк и изчерпателен подход при регламентиране на различните аспекти на информационната сигурност и сигурността на защита на информацията, обменяща се по електронен път.

В правото на ЕС под киберсигурност обикновено се разбират предпазните мерки и действия, които могат да бъдат приложени за защита на киберпространството както в гражданската, така и във военната област, от заплахи, които са свързани с неговите независими мрежи и информационна инфраструктура или могат да нарушат работата им. Видовете атаки и смущения могат да бъдат разделени на две групи:

1) такива, които са извършени от лица с користни цели *като престъпници,* терористи, срещу национални държави;

2) кризи или извънредни ситуации, предизвикани от човешка дейност или природни бедствия. Целта на киберсигурността е да се съхрани наличността и целостта на мрежите и инфраструктурата, както и защитата на сигурността на информацията, която се съдържа в тях.[3]

Под **киберпрестъпност** обикновено се разбира широк кръг от различни противозаконни деяния (действия и бездействия), в които компютри и информационни системи са или основен инструмент, или основна цел. Киберпрестъпността обхваща традиционни престъпления, престъпления, свързани със съдържанието, и престъпления, които са възможни само при компютри и информационни и комуникационните системи.[4]

„Информационна система е устройство или група от взаимосвързани или сходни устройства, едно или повече от които, съобразно дадена програма, автоматично обработва компютърни данни, както и компютърните данни, съхранявани, обработвани, извличани или пренасяни от това устройство или група от устройства за целите на неговата или тяхното функциониране, използване, опазване/защита и поддържане”[5]

Според предложението за Рамково решение на Съвета на ЕС, COM (2022) 173 информационните системи включват „самостоятелни” персонални компютри, персонални цифрови организатори, мобилни телефони, интранет, екстранет мрежи и, разбира се, мрежите, сървърите и друга инфраструктура на Интернет.[6]

Употребата на киберпространството е недостатъчно регламентирано в света както по отношение на националното така и на международното публично право. Досега не съществува правно обвързващ международен договор, касаещ киберсигурността, който да изразява общата воля на държавите и да служи като основа за формирането на обща международноправна уредба, задължаваща участващите държави да я спазват и изпълняват съгласно принципа pacta sund servanda. В рамките на ЕС, с оглед спецификите на принципите и на действието на актовете на европейските институции, да оказва влияние, ставайки част от националното право на държавите членки. Тъй като това е една бързо развиваща се област на правото, всички възможни киберзаплахи все още не са дефинирани. Новите заплахи се появяват постоянно, което налага и своевременното намиране на мерките за борба с тях.

---

[2] FISMA, PL 107-296, дял X, 44 USC 3532

[3] Стратегия на Европейския съюз за киберсигурност. Отворено безопасно и сигурно киберпространсвто, JOIN (2013) 1 final, Брюксел, 7.2.2013 г., с. 3

[4] Стратегия на Европейския съюз за киберсигурност. Отворено безопасно и сигурно киберпространсвто, JOIN (2013) 1 final, Брюксел, 7.2.2013 г., с. 3

[5] Article 2 DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[6] Рамково Решение на Съвета относно атаките срещу информационните системи, Брюксел, 19.04.2002

За липсата на единна дефиниция на понятието киберсигурност е показателен и фактът, че няма единно определение дори в стратегиите на отделните държави членки на ЕС.

В **Стратегията за киберсигурност на Естония** е посочено, че не съществуват общи правила за предотвратяване и борба с киберзаплахите нито дори набор от общи определения на тези заплахи. Липсата на ясна дефиниция на няколко често използвани термина като киберсигурност, кибервойна, кибератаки, кибертероризъм или на критичната информационна инфраструктура, е предпоставка тяхното точно значение да се променя в зависимост от контекста[7].

Според Стратегията за киберсигурност на Финландия под понятието „киберсигурност” се разбира желаното крайно състояние, при което **кибердомейнът** е надежден и се осигурява неговото безпроблемно функциониране.[8] В Стратегията са направени следните три уточнения:

- В крайното желано състояние на кибердомейна няма да са застрашени, повредени или нарушени действието и функциите, зависими от електронната информация (данните) за обработка.
- Кибердомейнът зависи от участниците, като се разчита на изпълнение на необходимите и достатъчни процедури по сигурността на информацията („сигурност на комунални данни”). Тези процедури могат да попречат на осъществяването на киберзаплахите и за предотвратяване и смекчаване на последствията от тях.
- Обхваща мерките относно функциите на жизненоважни за обществото операторите на критичната инфраструктура, които имат за цел да се постигне способността на предсказуемо управление на киберзаплахите и техните последици, и могат да причинят значителни вреди или опасност за дадена държава или нейното население.

Стратегията за киберсигурност на Финландия е една от малкото (ако не и единствената), която прави разграничение между двете понятия – „киберсигурност” и „информационна сигурност”, и дава дефиниции и на двете. Според приетата дефиниция под **информационна сигурност се разбира административните и технически мерки, предприети за гарантиране на наличността, целостта и поверителността на данните**.

В Националната стратегия за киберсигурност на Германия е направено разделение между три термина **киберсигурност**, **гражданска** и **военна сигурност** в кибернетичното пространство.:

(Глобална) киберсигурност е желаната цел за състоянието на сигурността на информационните технологии (ИТ), в която рисковете за глобалната сигурност в киберпространството са намалени до приемлив минимум. Киберсигурност (в Германия) е сборът от подходящи и целесъобразни мерки.

Гражданската кибернетична сигурност се фокусира върху всички информационни системи, употребявани за граждански цели. **Военната кибернетична сигурност** се фокусира върху всички информационни системи за военна употреба на националното киберпространството.

Заслужава да се отбележи нестандартният и конструктивен за унифициране на определенията подход, приет в **Стратегия за киберсигурност на Латвия**. Дефиницията

[7] http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf
[8] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ FinlandsCyberSecurityStrategy.pdf Finland's Cyber Security Strategy (2013)

на понятието „киберсигурност” е същата като в препоръката на Международния съюз по далекосъобщения (МСД), който е една от специализираните организации на ООН.

Една от най-добрите и пълни дефиниции на разглежданото понятие е призната на Международния съюз по далекосъобщения. В нея се посочва, че „киберсигурност е набор от инструменти, политики, концепции за сигурност, защитни мерки за сигурност, насоки, подходи за управление на риска, действия, обучение, добри практики, осигуряване и технологии, които могат да бъдат използвани за защита на киберсредата и организацията и активите на потребителя. Организация и активи на потребителите включват свързани компютърни устройства, персонал, инфраструктура, приложения, услуги, телекомуникационни системи, както и съвкупност от предавана и/или съхранявана информация в киберсредата. Киберсигурността се стреми да гарантира постигането и поддържането на свойствата за сигурност на организацията и активите на потребителя срещу съответните рискове за сигурността в киберсредата. Общите цели за сигурност включват следното:

1) Наличието;

2) цялост, която може да включва автентичност и недопускане на отхвърляне;

3) поверителност”.[9]

В същия документ се посочва, че е възможно дефиницията за киберсигурност да се променя през определен период от време, за да може да се адаптира към промените в политиката. По този начин се подчертава динамична позиция, приета от специализираната организация на ООН. Този подход показа, че в началната фаза са направени само ограничени усилия за предоставяне на общо разбиране за това какво означава киберсигурност и кой има право да участва в управлението.

За целите на настоящото изследване е приета следната работна дефиниция:

Киберсигурност е набор от инструменти, политики, концепции за сигурност, защитни мерки за сигурност, насоки, подходи за управление на риска, действия, обучение, добри практики, осигуряване и технологии, на ключовите играчи, свързани с ограничаване, превенция, анализ, сътрудничество и ранно предупреждение по отношение на различните кибер заплахи, както и проблемите, които правят възможно тяхното реализиране.

2. Формиране и структура на политиката по киберсигурността в Европейския съюз

Европейският съюз работи по проблемите на киберсигурността и киберпрестъпността повече от десетилетие, тъй като новите технологии са неизменна част от ежедневието на гражданите на съюза. **Създаването на сигурна и надеждна цифрова среда** е един от основните приоритети на институциите на ЕС. Стратегията е придружена и от предложение на **Европейската комисия за приемане на директива за мрежова и информационна сигурност от Съвета на ЕС и Европейския парламент**. Целта е да се създадат **стандарти за правни мерки и да се стимулира тяхното прилагане в правото на ЕС,** за да може онлайн средата на ЕС, да стане още по-сигурна и надеждна и да се отговори на потенциалните заплахи в киберсигурността. В структурно отношение концепцията по киберсигурността в Европейския съюз се състои от **три основни стълба, както следва:**

- **мрежова и информационна сигурност (МИС),**
- **правоприлагане,**

[9] http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136 ITU-T X.1205, 2007 г., стр. 2.

- **отбрана – като съществуват органи на национално и европейско равнище, отговорни за гарантиране на киберсигурността.**

Институциите и органите, които участват в процесите на вземане на решения в областта на **мрежовата и информационна сигурност в ЕС** са: Европейската комисия, Европейската агенция за мрежова и информационна сигурност (ЕАМИС; ENISA), CERT-EU, мрежа от компетентни органи, както и Европейското публично-частно партньорство за устойчивост (EP3R). Техните функции и задачи ще бъдат по-детайлно разгледани в отделен параграф.

Основните органи на ЕС, които участват **в областта на правоприлагането са**: Европейският център за киберпрестъпления (ЕС3) и Европол, CEPOL и Евроюст.

В **областта на отбраната**, основните органи и агенции на ЕС са Европейската служба за външна дейност (ЕСВД), Военния щаб/секретариат на Европейския съюз (EUMS) и Европейската агенция по отбрана (ЕАО; EDA).

Мрежовата и информационна сигурност

Днешните информационни системи могат да бъдат сериозно засегнати от най-различни **инциденти, свързани със сигурността, като технически повреди и вируси**. Този вид правонарушения и престъпления, често са наричани инциденти, свързани с мрежовата и информационната сигурност (МИС), зачестяват все повече и стават все по-трудни за отстраняване.

Необходимостта от подобряване на сигурността на интернет и частните мрежи и информационни системи стои в основата на функционирането на съвременните общества и икономики. Според **МИС** мрежовата и информационната сигурност **се разбира да се осигури наличието на услуги и данни, като се предотврати прекъсването и неоторизирано прихващане на комуникации. Също така се изисква потвърждение, че данните, които са били изпратени, получени или съхранявани, са пълни и непроменени.** ***Това е необходимо, за да се осигури поверителността на данните и за защита информационните системи от несанкциониран достъп и атаки, както на гражданите на съюза, така и на останалите заинтересовани страни в киберпространството.*** За да се гарантира високо ниво на МИС държавите членки следва да **засилят информационните и образователни кампании за повишаване на осведомеността по въпросите на мрежовата и информационна сигурност на всички заинтересовани страни и да се насърчава използването на най-добрите практики.**

Правителствата и дружествата ще могат да разчитат в по-голяма степен на цифровите мрежи и инфраструктури за предоставянето на основните си услуги на национално и наднационално равнище. Наличието на повече сигурни платформи за електронна търговия ще спомогне за привличането на повече клиенти онлайн и да за създаване на нови възможности. **Доставчиците** на информационни и комуникационни (ИКТ) продукти и услуги в областта на сигурността също биха имали полза от това, тъй като търсенето на техните продукти и услуги ще се повиши, което ще доведе до въвеждане на иновативни продукти и икономии от мащаба.

Много предприятия и правителства в ЕС разчитат на цифрови мрежи и инфраструктури за предоставянето на основните си услуги. Това означава, че когато възникнат свързани с МИС инциденти, те могат да окажат огромно въздействие, **като нарушат предоставянето на услуги и спрат нормалната работа на предприятията**. Освен това с непрекъснатото развитие на вътрешния пазар на ЕС, в който се включват и нови информационни технологии се налага да се осигури работата и функционирането на редица мрежови и информационни системи, работещи транс-

гранично както на територията на ЕС, така и спрямо трети страни. Поради това свързан с МИС инцидент в една държава може да окаже въздействие в други държави и дори в целия ЕС. Свързаните със сигурността инциденти **подкопават и доверието на потребителите** в системите за онлайн плащания и в ИТ мрежите.

Ето защо е необходимо въвеждането на **по-последователни мерки за управление на риска** и систематичното **докладване за инциденти. В тази връзка** приемането на директива за мрежова и информационна сигурност, ще направи по-надеждни и устойчиви зависещите от информационните системи сектори, и ще направи киберпространството по-сигурно за гражданите на Европейския съюз.

Също така се поставя акцент и върху насърчаване на използването **на международно признати стандарти** и улесняване на **международното сътрудничество**.

Правоприлагане

Ежедневното приложение на новите технологии в най-различни области, създава предпоставки за тяхното използване за извършване на различни видове престъпления, включващи се в киберпрестъпността. Големите финансови печалби и възможността за лесно прикриване на следите, прави този вид незаконни дейности все по-разпространени. **Органите и специализираните агенции в областта на правоприлагането** са натоварени с тежката задача да противодействат на едни от най-сложните престъпления, при които съществува възможност за „дистанционно” извършване посредством интернет средата и информационните и комуникационни технологии. **Едни от основните изисквания и задължения, произтичащи от споменатата по-горе проектодиректива за мрежова и информационна сигурност, на националните институции са именно в областта на правоприлагането.** Всяка от държавите членки на ЕС трябва да определят компетентен орган по въпросите на киберсигурността на национално ниво[10], който да бъде и единно звено за контакт (Single Point of Contact) в тази област, както и екип за спешно реагиране на национално ниво (CERT)[11], който обаче не е задължително да е част от компетентния орган. Те трябва да работят в сътрудничество с правоохранителните органите на другите държави членки, както и специализираните агенции и органи на Европейския съюз, в областта на правоприлагането, в отговор на престъпленията в киберпространството. Тук е мястото да се отбележат едни от основните трудности, пред които е изправено това сътрудничество, а именно **разликата в технологичното и икономическото развитие на държавите, както и ресурсите** (финансови, човешки и технологични), с които разполагат компетентните органи. Често разликата в законодателствата на страните членки на ЕС пречи на правоприлагащите органи при противодействие на киберпрестъпленията, които не се ограничават в рамките на националните граници на една държава.

Отбранителният компонент в киберсигурността

Развитието на информационните и комуникационните технологии в глобален мащаб, доведе до промяна в разбиранията за начина на водене на военни действия. Информационните войни и кибервойните все по-често се използват от различни държави и терористични организации за осъществяване на техните цели, някой от

[10] В Република България този национален орган е в рамките на Министерството на вътрешните работи и се нарича СЕКТОР 05 „ПРОТИВОДЕЙСТВИЕ НА ПРЕСТЪПЛЕНИЯ, СВЪРЗАНИ С ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ, ХАЗАРТА И **КОМПЮТЪРНИ ПРЕСТЪПЛЕНИЯ**”

[11] CERT Bulgaria е Националният Център за Действие при Инциденти в Информационната Сигурност - https://govcert.bg/

тях имат като основно предназначение причиняване на сериозни икономически загуби. Различните видове киберзаплахи, често се използват за нападение на частни и национални обекти на критичната инфраструктура. В тази връзка, освен отделните държави, и Европейският съюз като субект, следва да създадат **необходимия отбранителен капацитет на националното и съответно европейското киберпространство.**

Стратегията на ЕС за киберсигурност идентифицира разработването на политика за киберотбраната и възможности, свързани с рамката на общата политика за сигурност и отбрана, за включването като една от целите за сигурност. Посочен е и списък на дейности, предвидени за сътрудничество между ЕАО и държавите членки.

Важно е да се отбележи, че Стратегията на ЕС за киберсигурност съдържа разпоредба, съгласно която: „особено тежък кибер инцидент или (кибер) атака може да представлява достатъчно основание за дадена държава-членка да се позове на клаузата за солидарност на ЕС (предвидена в член 222 от Договора за функционирането на Европейския съюз)”.

3. Стандарти за сигурност в киберсигурността

Подчертаната **значимост на стандартите за сигурност** е следствие от факта, че те играят **важна роля за подобряване на киберотбраната и киберсигурността, в това число и мрежовата и информационната сигурност. Процесите и процедурите по стандартизиране са от съществено значение за постигане на ефективно сътрудничество в трансгранични и междуобщностни среди**. Броят на организациите по развитие на стандарти и броят на публикуваните стандарти за информационна сигурност е увеличават през последните години, създавайки значителни предизвикателства.

Международните стандарти представляват препоръчителни хармонизирани технически норми, правила, еталони, образци[12] или изисквания в областта на мрежовата и информационна сигурност, електронните комуникации и новите технологии, утвърждавани от международни органи като ISO, ITU на международно ниво или CEN, CENELEC, ETSI – на европейско ниво. Те се явяват препоръчителни регулатори, като повечето от тях се основават на законови изисквания, или са доказани образци на добри практики в областта на информационната сигурност. Посредством стандартите се осигурява съвместимост на подсистемите за информационна сигурност. Ако организацията реши да приеме определен стандарт, той става задължителен при изграждането, управлението и използването на подсистемата ѝ за информационна сигурност. Необходимо е стандартите да се усвояват последователно, например ISO 177799, BS7799, ISO 15408, CC и др.

Стремежът е да се обхванат всички области на информационната сигурност от стандарти, директиви и процедури, като това е основната причина те непрекъснато да се развиват. Някои от областите са: ***Отчетност на контрола; Физически контрол и контрол на околната среда; Административен контрол; Контрол на достъпа до АИС; Контрол на оперирането с АИС; Криптиране; Планиране на развитието на АИС; Действие при инциденти.***

4. Значение на стандартите в информационната сигурност и киберзащитата

Има много причини, поради които стандартите играят важна роля за подобряване на подхода към информационната сигурност, като най-важните сред тях включват:

[12] Стандарт – „комплекс от норми, правила, изисквания към стоки и услуги, еталон мерило, мостра образец или нещо обикновено, общоприето, нормално‖ това е определението от енциклопедията на Уикипедия на интернет адрес: www.wikipedia.org

- Подобряване на ефикасността и ефективността на ключовите процеси;
- улесняване на системната интеграция и оперативната съвместимост;
- активиране на различни продукти или методи;
- осигуряване на начини за потребителите да оценяват нови продукти или услуги;
- структуриране на подход за разгръщане на нови технологии или бизнес модели;
- насърчаване на икономическия растеж.

Процесите и процедури за стандартизация са съществена част от постигането на успешно сътрудничество в трансгранична среда. Стандартизацията помага да се гарантира, че различните страни могат да си взаимодействат помежду си в съответствие с един набор от процедури. Постепенното изграждане на киберсигурността довежда до обособяване на нейното съдържание в тристълбова структура.

Тристълбовата структура на киберсигурността в Европейския съюз спомага за създаването на механизми за реагиране и противодействие на едни от най-сложните и бързо развиващи се заплахи и престъпни актове, каквито са тези, реализиращи се в киберпространството. Ефективното сътрудничество между националните органите на държавите членки и специализираните агенции на Европейския съюз ще се отрази в положителна насока по отношение на постигането на високо ниво на мрежова и информационна сигурност. Увеличаването на икономическите ползи за ЕС, вследствие от МИС и цифровия пазар (доверие на гражданите в ИКТ и електронната търговия), ще спомогнат за отделяне на повече средства за преодоляване на дисбаланса в различното технологичното развитие между държавите членки. Това до голяма степен ще улесни работата на правоохранителните органи в борбата срещу киберпрестъпленията, и ще спомогне за създаването на отбранителен капацитет на отделните държави и на съюза като цяло.

5. Анализ на национални стратегии за киберсигурност на държави членки на Европейския съюз

Възползвайки се ежедневно от позите на новите технологии, гражданите на ЕС и различните обекти на критичната инфраструктура са изложени на редица рискове. Поддържането на високо ниво на киберсигурност изисква координирани действия, както на международно и европейско равнище, така и на национално.

Европейската агенция за информационна сигурност публикува „Национална стратегия за киберсигурност. Практическо ръководство за развитие и изпълнение” (National Cyber Security Strategies. Practical Guide on Development and Execution), в което се представят добри практики и препоръки за това как да се развива, прилага и поддържа стратегия за киберсигурност.

В ръководството, националната киберстратегия за сигурност се определя като инструмент за подобряване на сигурността и устойчивостта на националните информационни инфраструктури и услуги. Тя създава редица национални цели и приоритети, които трябва да бъдат постигнати в определен период от време. Като такава, тя осигурява стратегическа рамка за подхода на една нация към кибернетичната сигурност.

Жизненият цикъл на националната стратегия за кибернетична сигурност има две ключови фази:

1. Разработване и изпълнение на стратегията.
2. Оценка и адаптиране на стратегията.

На фазата на разработване и изпълнение на стратегията трябва да се реализират следните основни задачи:[13]

[13] Милина, В., Киберсигурността – стратегически национален проблем, IT4Sec Reports 108, Институт по информационни и комуникационни технологии – БАН, секция „Информационни технологии в сигурността”, София, юни 2013 г. с. 10-11.

- установяване на визията, обхвата, целите и приоритетите;
- национална оценка за риска, с конкретен акцент върху критичните информационни инфраструктури;
- преглед на състоянието на основните елементи на стратегията на национално равнище;
- разработване на ясна рамка за управление на място, която да определя ролите и отговорностите на всички заинтересовани страни. Тя осигурява рамка за диалог и координация на различните дейности, предприемани в жизнения цикъл на стратегията;
- ефективно сътрудничество между публичния и частния сектор;
- установяване на надеждни механизми за обмен на информация между частните и публичните заинтересовани страни;
- разработване на национални киберпланове за реагиране;
- упражнения за проверка на съществуващите планове за извънредни ситуации;
- установяване на минимални изисквания за сигурност за даден сектор;
- създаване на механизми за докладване на инциденти;
- осведомяване на потребителите относно киберзаплахи за сигурността и слабите места;
- насърчаване на научноизследователската и развойната дейност;
- засилване на обучението и образователните програми в областта на киберсигурността;
- създаване на възможност за реагиране при инциденти;
- да се подготви съгласувана и координирана реакция срещу престъпленията в кибернетичното пространство;
- международно сътрудничество и обмен на информация;
- създаване на публично-частно партньорство;
- баланс между сигурността и неприкосновеността на личния живот.

След като стратегията е разработена и се изпълнява в съответствие с изброените основни задачи, периодично трябва да бъде оценявана степента до която се постигат целите. Така ще е възможно да се предприемат всички необходими коригиращи и превантивни действия, които да доведат до съответствие или с настъпили промени, или с целите на стратегията. На тази втора фаза от жизнения цикъл на киберстратегията – оценка и адаптиране, основна задача, освен получаване на данни за състоянието на съществуващите политики, е да се определят бъдещите цели и стратегията да се коригира в съответствие с тях.

За да се проследи отделния национален подход на държавите членки на ЕС при изготвяне и реализиране на своите стратегии, е направен **контент анализ** на техните национални документи, касаещи киберсигурността. В тази връзка се открояват някои общи елементи, съдържащи се в разгледаните **петнадесет на брой стратегии**[14], а именно на:

Австрия, Белгия, Чешка република, Литва, Латвия, Естония, Финландия, Германия, Унгария**, Италия, Полша, Испания, Обединеното Кралство, Нидерландия, Словакия**

Останалите пет стратегии не са анализирани, тъй като са публикувани само на официалния език на съответните държави и това би могло да доведе до възможност за определени неточности в техния превод.

[14] https://ccdcoe.org/strategies-policies.html

Сравнителният анализ на националните стратегии за киберсигурност показва, че горепосочените държави, имат еднакви виждания по отношение на редица въпроси. Общи черти са посочването на възможностите и ползите от използването на киберпространството и новите технологии, както и рисковете за киберсигурността в следствие на тяхната употреба. Също така са набелязани стратегически цели, които да бъдат следвани и области на действие, както във всички стратегии се акцентира на важността на *международното сътрудничество в областта на киберсигурността.*

Следва да се отбележи, че Австрия, Естония, Чешката република, Финландия, Германия, Унгария, Латвия, Испания, Холандия, Полша и Обединеното кралство определят и съответни принципи при изпълнение на техните стратегии. Най-общо те могат да бъда систематизирани по следния начин:

1. Киберсигурността е неразделна част от националната сигурност, поддържа функционирането на държавата и обществото и спомага за конкурентоспособността на икономиката и иновациите.

2. Киберсигурността следва да се гарантира при зачитане на основните права и свободи, защита на личните свободи в мрежата, сътрудничество между публичния и частния сектори, както и сътрудничество със съюзници и партньори и международни организации.

3. Киберсигурността предполага и индивидуална отговорност за безопасно използване на ИКТ инструменти.

Въпреки че съществуват редица разминавания по отношение на основни понятия и термини, детайлният анализ на стратегиите показва, че само в 9 от 15-те[15] се съдържат определения на ключови понятия, свързани с киберсигурността.

Прави впечатление, че само **в стратегиите за киберсигурност на три държави**, изрично е спомената съвместимостта на стратегиите с други национални планове и нормативни актове. Тази съвместимост показва връзката и последователността при разработването на общи правила за поведение в рамките на отделните държави членки.

От особен интерес е фактът, че са малко държавите[16], в чиито стратегии са посочени **заинтересованите страни** от високото ниво на киберсигурност и **отговорните национални органи за нейното постигане**. В тази връзка е уместно да се последва примера на Холандия и Латвия и Полша, които са разработили изключително подробни планове за действие, включващи дори конкретните ролите и отговорностите на участниците в киберсигурността.

Въпреки съществуващите разлики в националните стратегии за киберсигурност на държавите членки на Европейския съюз, са налице и много общи моменти. Именно те показват общата воля и подход в постигането на високо ниво на киберсигурност в рамките на ЕС. Необходимо е държавите, които не са приели подобни стратегически документи, да предприемат действия по тяхното изготвяне. В тази връзка, като приложение към настоящия дисертационен труд е прикрепено „Предложение за модел на стратегия за киберсигурност на Република България”.

6. Стратегическата концепция на НАТО 2020 в областта на киберсигурността и нейното влияние в Европейския съюз

[15] Австрия, Финландия, Германия, Италия, Латвия, Испания, Полша, Холандия и Великобритания.
[16] Естония, Латвия, Полша Италия, Литва, Холандия, Испания и Великобритания

Активното международно сътрудничество между водещите международни междуправителствени организации изисква непрекъсната ангажираност, за да може да се адаптира към изискванията на политическите и технологичните промени.[17]

В отговор на технологичните промени и **новите рискове пред киберсигурността,** Алиансът приема Стратегическа концепция на НАТО 2020. Тя има за цел да изясни както това, което НАТО трябва да се прави за всеки съюзник така и това, което съюзниците трябва да правят за НАТО. В тази връзка усилията на Алианса са насочени към **защита от неконвенционални заплахи.** Заплахите в началото на XXI век са по-нетрадиционни и включват атаки и терористични удари, осъществявани чрез кибернападения или неправомерно нарушаване на критичната инфраструктура. За да се предпази от този вид нападения, които не са изрично посочени в разпоредбите на член 5 от Северноатлантическия договор, НАТО трябва да актуализира своя подход към защитата на територията на Алианса, в това число и киберпространството.

За осъществяването на концепцията 2020, НАТО не работи самостоятелно, а се стреми **да задълбочи съществуващите отношения с ключови партньори** в областта на киберсигурността, както и **да установи нови отношения**, за да се разшири обхватът на дейностите в тази област. Европейсият съюз е уникален и основен партньор на НАТО по разглежданите въпроси, като по-доброто сътрудничество може да бъде от полза в борбата с неконвенционалните заплахи като кибертероризма и кибератаките. Една от възможностите за подобряване на сътрудничеството между двете организации е да се избегне капана на категоризиране на всички заплахи и отговорности като „военни” или „невоенни” и да насочат възможностите си за намиране на решения по проблемите на киберсигурността.

За да отговори на опасността от кибератаки, Ализнсът трябва да ускори усилията си за защита на своите собствени комуникационни и командни системи. Най-вероятните заплахи за съюзниците през следващото десетилетие са нетрадиционните, а именно: 1) нападение от балистични ракети (със или без ядрено оръжие); 2) удари от международни терористични групи; и 3) кибернападения с различна степен на нанесени щети.

От гледна точка на сигурността през XXI век, следва да се подчертае, че събитията в една част на света е твърде вероятно да имат отражение или последици и на друго, отдалечено място. Кибератака срещу обекти на критичната инфраструктура, която води до хаос в един град или държава, може да накарат държави или терористични организации да я повторят на друго място. В тази връзка опасността от неконвенционални заплахи има очевидни последици за НАТО. Ето защо, споделям мнението, че е необходимо осъвременяване на концепцията/схващането за това какво се разбира в член 5 под **атака**, за да може, Алиансът:

- да подпомага съюзниците си за предотвратяване и възстановяване от атаки;
- да изгради набор от отбранителни способности в кибернетичното пространство, насочени към по-ефективно откриване и възпиране на заплахите.

Кибератаките срещу системи на НАТО се срещат често, като това може лесно да се обоснове консултации по член 4 и да доведе до мерки за колективна отбрана по член 5. Тя от своя страна, изисква средства и способности за предотвратяване, разкриване, отговор и възстановяване от атаки. Конкретни действия на НАТО в тази насока са създаването на Орган за управление на киберотбраната и **Кооперативен център за високи постижения по киберотбраната (**CCD CE) **на НАТО/Център за върхови постижения и сътрудничество в кибер отбраната на НАТО, базиран в**

[17] Белова, Г., Европейска интеграция, Сиела, София, 2008 г.

Талин, Естония. Въпреки това, все още има сериозни пропуски в способностите за киберотбрана на НАТО. Стратегическата концепция поставя висок приоритет на решаването на тези уязвимости, които са едновременно неприемливи и все по-опасни.

Трансграничният характер на съвременните заплахите и огромните щети, които нанасят в световен мащаб, налагат необходимостта от многостранно международно сътрудничество, при което усилията и действията на водещите международни междуправителствени организации са насочени в една посока. Несъмнено, Организацията на Северноатлантическия договор и Европейския съюз, имат голямо влияние във формирането на глобалните тенденции на политиката в областта на киберсигурността и киберотбраната. През последни години, тяхното стратегическо партньорство и решенията, които взимат, могат да бъдат проследени в няколко Срещи на върха.

Кибератаките стават все по-чести, по-организирани и по-скъпоструващи в щетите, които нанасят върху държавните администрации, бизнеса, икономиките, мрежите и другите критични инфраструктури. Те биха могли да достигнат праг, който застрашава националния и евроатлантическия просперитет, сигурност и стабилност. Всяка от външните за двете организации военни и разузнавателни служби, организирани престъпни групи, терористични и / или екстремистки групи може да бъде източник на подобни атаки.

НАТО и ЕС може и трябва да играят взаимно допълващи се и подкрепящи се роли в защита на международния мир и сигурност, както във физическия свят, така и в киберпространството. В тази насока, действията и приносът на двете организации се изразява в:

- укрепване на стратегическото партньорство, в духа на взаимна откритост, прозрачност, допълване и зачитане на автономията и институционалната цялост на двете организации;
- засилване на практическото сътрудничество в операции – от координирано планиране до взаимна подкрепа;
- разширяване на политическите консултации, за да се включат всички въпроси от общ интерес, с цел споделяне на оценки и перспективи;
- по-пълноценно сътрудничество в развитието на способностите, за да сведе до минимум дублирането и да се увеличи максимално ефективността на разходите.

Тясното сътрудничество между НАТО и ЕС е важен елемент в развитието на международен цялостен подход към киберсигурността, която изисква **ефективното прилагане на военни и граждански средства**. Срещата на върха в Чикаго през май 2012 г. повтаря същите принципи, като отново се подчертава, че НАТО и ЕС споделят общи ценности и стратегически интереси, като пълното укрепване на стратегическото партньорство е от съществено значение в настоящата среда на строги икономии и продължаваща икономическа (и не само) криза.

На Срещата на върха в Чикаго се приемат няколко важни декларации, свързани с киберсигурността и сътрудничеството между НАТО и ЕС. Декларация за отбранителните способности: към силите на НАТО 2020 призовава за насърчаване на сигурността в света. Тя стъпва върху направения стабилен напредък в разработването на редица възможности.[18]

Конвенционалните сили на съюзниците допринасят за посрещане на бъдещите предизвикателства за сигурността, като например **кибератаки**, тероризъм, нарушаване на критични каналите за доставки, както и разпространението на оръжия за ма-

[18] Иванов, В., Интелигентна система за национална сигурност. Възможности, подходи, решения. София, 2014 г., стр. 120-121.

сово унищожение. За тази цел е необходимо да се подобрят възможностите на Силите за бързо реагиране на НАТО за съвместна работа на територията на Алианса, Европейския съюз и отвъд техните граници. Нуждата от практикуване на съвместната работа на силите чрез **комбинирани обучения и упражнения** между ЕС и НАТО се обуславя от необходимостта от стандартизиране на техните умения и по-доброто използване на технологиите. Обхватът на С4 (Командване, Контрол, Комуникации и Компютри) и разузнаване, наблюдение и целеуказване (С4ISR), предоставляващ спойката, която свързва силите на НАТО заедно, **трябва да се разшири и да включва и ЕС.** Инициативата е свързана с по-голямо използване на образование, обучение и упражнения за укрепване на връзките между държавите в поддържане на киберсигурността.

Кибер заплахите постоянно увеличават своите мащаби с бързи темпове и се усъвършенстват. За да остане жизнеспособен и ефективен като политико-военна организация през XXI век, *Алиансът непрекъсното следва да се променя и адаптира*, адекватно на промените в средата за сигурност и новите рискове и предизвикателства.[19] За да се осигури постоянен и неограничен достъп на НАТО до киберпространството и неприкосновеността на своите критични системи, трябва да се вземат предвид кибер измеренията на съвременните конфликти и да бъдат отразени в доктрините на НАТО, с оглед подобряване на възможностите за откриване, оценяване, предотвратяване, защита и възстановяване в случай на кибер атака срещу системи от решаващо значение за Алианса.

Новата политика рационализира управлението на киберотбраната и предвижда процедури за подпомагане на страните от Алианса, както и интеграция на киберотбраната в оперативното планиране. Освен това, политиката определя начини за осъществяване на напредък по отношение на информираността, образованието, обучението и ученията. Насърчава по-нататъшния напредък в различни инициативи за сътрудничество, включително и тези с партньорските държави и международни организации и индустрията/производителите.

На Срещата на върха в Уелс държавите поемат ангажимент за подобряване на обмена на информация и взаимна помощ при предотвратяване, намаляване на и възстановяване от кибератаки, като новата политика се допълва от план за действие с конкретни цели и срокове за изпълнение. НАТО работи с националните органи, за да се разработят принципи, критерии и механизми за осигуряване на подходящо ниво на кибер защитата за националните комуникационни и информационни системи (КИС). Подпомагането на страните членки в усилията им да защитят своите собствени критични инфраструктури (КИ) чрез обмен на информация и добри практики, както и чрез провеждане на упражнения за кибер защитата, спомага за развитието на националната експертиза и способности за отбраната. Кибер отбраната също е интегрирана в инициативата Интелигентна отбрана на НАТО (NATO Smart Defence).

За увеличаването на капацитета на отбраната на НАТО в кибернетичното пространство, на срещата в Уелс, е призната подещата роля на Кооперативния център за високи постижения по киберотбраната (CCD CE) на НАТО в Талин, Естония. Той представлява първото, акредитирано съоръжение за изследвания и обучение, занимаващи се с образование по киберзащитата, консултации, извлечени поуки, научноизследователска и развойна дейност. Въпреки че не е част от командната структура на НАТО, CCD CE, предлага признати експертни познания и опит. Подобни възможности

[19] Иванов, В., Интелигентна система за национална сигурност. Възможности, подходи, решения. С, 2014 г., с. 123.

за увеличаване на капацитета в областта на кибер отбраната се предлагат от школата на НАТО за Комуникационни и информационни системи в Латина, Италия, школата на НАТО в Оберамергау – Германия[20], Колежа на НАТО по отбраната в Рим.

Предизвикателства в областта на сигурността представляват сложен пъзел от променливи опасности, които включват международния тероризъм, организираната престъпност, заплахите за **киберпространството**, доставките на енергия, климатичните проблеми, причинените от човека аварии и много други. За да се противодейства ефективно на тези заплахи, е необходимо **широкообхватно партньорство и тясно взаимодействие между НАТО и Европейския съюз**. Двете организации трябва да възприемат холистичен/цялостен подход по проблемите на сигурността и да си сътрудничат в областта на сигурността и отбраната.

Двете организации НАТО и ЕС трябва да поставят ударението върху укрепването на основните си бойни способности, засилването на оперативната съвместимост и координацията на докрините, планирането,технологията, оборудването и подготовката.

Съществуващите форми и механизми на **сътрудничеството** между двете организации представляват солидна основа за обезпечаването на киберсигурността, но въпреки това, трансграничният характер на кибер заплахите изискват то да се издигне на ново – глобално равнище.

Осъзнавайки все по-глобалното измерение на международната сигурност след атентатите от 11 септември, вероятно в бъдеще ще станем свидетели на една нова култура на сътрудничество между НАТО, ЕС и останалите актьори, която ще помогне да се преодолеят недоразуменията и различията, за да се намери най-подходящата и ефективна реакция на съвременните заплахи. В контекста на разширеното оперативно сътрудничество с географски отдалечени партньори взаимодействието НАТО-ЕС трябва да се превърне в основа на една силна трансатлантическа общност, бореща се за сигурност в киберпространството.

Постоянният диалог и хармонизирането на военните трансформации, са необходими, за да се гарантират гладкото сътрудничество в предварителното планиране и способностите и гъвкави структури за комуникация, тъй като НАТО и Европейският съюз за изправени пред сходни проблеми в редица области, включително и киберсигурността.

Друга област на сътрудничество НАТО-ЕС може да стане факт ако министрите на отбраната на страните от Югоизточна Европа включат в срещите си планирането на гражданската защита при извънредни ситуации и министрите на вътрешните работи в рамките на министерски форум за отбрана и национална сигурност на Югоизточна Европа.

Ако този нов форум се обвърже с Регионалния център за борба с трансграничната престъпност към Инициативата за сътрудничество в Югоизточна Европа, разположен в Букурещ, това ще бъде най-подходящата организационна форма за прилагане на координираната стратегия на НАТО и ЕС за Западните Балкани. Тя може да се използва и в борбата с киберпрестъпността.

Понастоящем терористичните групи и организираната престъпност имат международен характер и се възползват от новите технологии, бързите комуникации, обмена на информация и относително голямата свобода на движение. Затова е изключително важно държавите и организациите като НАТО и Европейския съюз да обменят информация и тясно да си сътрудничат в борбата с тях, за да може да се противодейства успешно на опасността от терористични атентати.

[20] The NATO School in Oberammergau, Germany, http://www.natoschool.nato.int/, https://natoschool.org/organization/nato-school-oberammergau

Може да се каже, че Европейският съюз и НАТО са изправени пред **общи проблеми в областта на киберсигурността**, като само продължаването на засиленото сътрудничество между двете организации може да подобри резултатите в гарантирането на глобалната, съюзната, националната и гражданската сигурност. Еднаквият подход, използван в публикуваните стратегии на държавите членки на НАТО и ЕС е доказателство за тяхното взаимодействие и усилия в борбата срещу кибер заплахите.

Настоящото сътрудничество между НАТО и ЕС по проблемите на киберсиурността до голяма степен се регулира от действащите към настоящия момент споразумения. Считам, че след Срещата на върха в Уелс се поставя началото на нова форма на сътрудничество между техническия център NCIRC на НАТО, националните екипи за действие при инциденти (CERT) и представителите на частния сектор на страните членки на НАТО. Разширяването на това сътрудничество и в други области – по-специално в борбата с киберпрестъпността и защитата на критичната инфраструктура среща определена съпротива заради опасения, свързани с правомощията на НАТО в тези области, както и статута на страни членки на ЕС извън НАТО.

Организацията на Северноатлантическият договор и Европейският съюз играят основна роля за подобряване на международната сигурност, гарантиране на човешките свободи и насърчаване на принципите на правовата държава. Тези цели не зависят от технологичния напредък. Те не зависят от конкретния противник. Те са трайни и необходими и ще бъдат отстоявани толкова дълго, колкото НАТО, ЕС и ООН, ги защитават чрез единството на своите членове, смелостта на своите граждани, и свободното изразяване на своята колективна воля.

ЗАКЛЮЧЕНИЕ

В началото на XXI век въпросите за глобализацията и новите технологии и тяхното въздействие върху обществото са сред основните приоритети в политиката за киберсигурност на универсалните и регионални международни организации и на отделните държави. Широко разпространеното приложение на Интернет, както е известно, наред с положителните носи и много отрицателни последици.

Проблемите, свързани с киберсигурността са изключително актуални за нашата съвременност и ще продължават да представляват неизменен интерес както за правната теория, така и за практиката по прилагане на политиката за киберсигурност в международен план. Това предопределя и нареждането им сред приоритетните направления в дейността на ЕС. Целта на политиката на Съюза в разглежданата област е да постави основата за нейното формиране, да осъвремени инструментите по нейното прилагане и да изготви дългосрочен план на перспективите за развитие на дейности в различните сфери на политическия и обществения живот, осигуряващи балансираното й развитие.

В тази сфера са издадени значителни по количество, като брой и обем, нормативни актове на европейските институции, наднационални структури за мониторинг и навременен обмен на информация за състоянието на киберсигурността. Неоспорим факт е, че въпреки съществуващата детайлна правна уредба на основните въпроси, свързани с киберсигурността, не винаги са налице необходимите социални условия или финансови ресурси за прилагането на тези разпоредби. Съвсем основателно е страните от по-слабо развитите държави и особено от Централна и Източна Европа да изпитват известни трудности и при спазване на установените високи стандарти за киберсигурност.

Факт е, че понякога в законодателството липсва необходимата прецизност и подробна уредба. Като най-ярък пример в това отношение се откроява липсата на легална дефиниция на правното понятие „киберсигурност” в първичното право на Съюза.

Като следваща празнота в законодателството може да бъде посочено прилагането на не достатъчно координирана политиката по киберсигурност в отделните държави членки на ЕС. По-конкретно, някои страни нямат разработени стратегии за киберсигурност, което е показателно за липса на последователни действия в тази област. Изтъква се обстоятелството, че никоя държава не може самостоятелно да противодейства на киберзаплахите. Необходимо е да се приеме многостепенен подход, при който има баланс в разпределянето на отговорностите между ЕС и държавите членки, и всяко управленско ниво (европейско, национално, регионално и местно) поема своята отговорност и определя мерки, които могат и трябва да се предприемат на съответното равнище.

Държавите членки разчитат основно на ЕС да предприема необходимите мерки за киберсигурност, т.е., ако Съюзът не предприеме законодателни мерки, такива няма да бъдат приети и в повечето държави членки или в тези с изоставащо икономическо развитие от средното за ЕС, тъй като тези мерки допълнително биха натоварили бизнеса независимо от положителния ефект.

Използвана литература

1. Белова, Г., Европейска интеграция, Сиела, София, 2008 г**.**
2. Велкова, Л., Милина, В., Дочева, И., Панчев, И., Слатински, Н., За еволюцията на понятието „Сигурност”, Аспекти на Сигурността, С., 2012 г.
3. Директива 2013/40/ЕС относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета
4. Договор от Лисабон за изменение на Договора за Европейския съюз и на Договора за създаване на Европейската общност, подписан в Лисабон на 13 декември 2007 г.
5. Закона за СРС на Република България, Глава четвърта „а” Контрол и наблюдение на специалните разузнавателни средства в чл. 34а и чл. 34б
6. Иванов, В., Интелигентна система за национална сигурност. Възможности, подходи, решения. София, 2014 г.
7. Касенова, М. КИБЕРБЕЗОПАСНОСТЬ И УПРАВЛЕНИЕ ИНТЕРНЕТОМ, Основы трансграничного управления интернетом, Статут, 2013
8. Марин, Н., Юрисдикцията на Съда на Европейския Съюз в пространството на свобода, сигурност и правосъдие, Университетско издателство „Неофит Рилски”, Благоевград, 2011 г.
9. Маркова, Цв., Правен режим на информационната сигурност, София 2015, ISBN: 978-619-7143-03-4
10. Милина, В.,”Предизвикателства пред международната киберсигурност”, списание „Военен журнал”, Издание на министерството на отбраната, 2012 г., бр. 3-4
11. Официален вестник на Европейския съюз
12. Попова, Ж., Засиленото сътрудничество като форма на упражняване на компетентност от няколко държави членки на ЕС, „Право, управление и медии през XXI век, Юбилеен сборник на ЮЗУ, ПИФ, Том II, Университетско издателство „Неофит Рилски”, Благоевград, 2012 г. с. 18.
13. Стратегия на Европейския съюз за киберсигурност. Отворено безопасно и сигурно киберпространсвто, JOIN (2013) 1 final, Брюксел, 7.2.2013 г.