ЮГОЗАПАДЕН УНИВЕРСИТЕТ „НЕОФИТ РИЛСКИ”
БЛАГОЕВГРАД
ПРАВНО-ИСТОРИЧЕСКИ ФАКУЛТЕТ
КАТЕДРА „МЕЖДУНАРОДНО ПРАВО И
МЕЖДУНАРОДНИ ОТНОШЕНИЯ”

ЙОСИФ ЙОРДАНОВ КОЧЕВ

АВТОРЕФЕРАТ

ПОЛИТИКАТА НА ЕВРОПЕЙСКИЯ СЪЮЗ ПО ПРОБЛЕМИТЕ НА КИБЕРСИГУРНОСТТА

Автореферат на дисертационен труд
за присъждане на образователната и научна степен „доктор”
в област на висше образование **3.** „Социални, стопански и правни науки”, за професионално направление **3.6**. „Право”, по научна специалност „Международно право и международни отношения”.

Научен ръководител:
Проф. д-р полк.(о.з) Стойко Стойков

Рецензенти:
1. Проф. д-р Габриела Белова
2. Проф. д-р Валери Иванов

Благоевград, 2015 г.

Дисертационният труд на тема: **„Политиката на Европейския съюз по проблемите на киберсигурността”** е обсъден на заседание на катедра „Международно право и международни отношения”, Правно-исторически факултет към ЮЗУ „Неофит Рилски” – Благоевград на 30.06.2015 г. с протокол №7 е насочен за защита пред научно жури.

Материалите по защитата са на разположение на интересуващите се на интернет страницата на Югозападния университет „Неофит Рилски“ – Благоевград и в Катедра „Международно право и международни отношения“ на Правно-историческия факултет.

Докторантът работи като асистент в катедра „Международно право и международни отношения” към Правно-историческия факултет на ЮЗУ „Неофит Рилски”.

Защитата на дисертационния труд ще се състои на 24.07.2015 г. от 10.30 часа в зала 302 на VI-ти учебен корпус на Правно-историческия факултет.

Автор: Йосиф Йорданов Кочев

Заглавие: Политиката на Европейския съюз по проблемите на киберсигурността

СЪДЪРЖАНИЕ

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННОТО ИЗСЛЕДВАНЕ

1. Актуалност на темата

Политиката на Европейския съюз по проблемите на киберсигурността представлява специфична и изключително актуална дейност, която с основание привлича интереса на останалите субекти на международното публично право, каквито са държавите и международните организации.

От гледна точка на географския обхват развитието на политиката по проблемите на киберсигурността се осъществява от почти всички страни в света. Освен държавите като активни участници в разглежданата област се открояват Организацията на обединените нации и нейните специализирани организации, организациите с регионален обхват като Европейския съюз и Организацията на Северноатлантическия договор.

Проблемите, свързани киберсигурността, отдавна надхвърлят границите на една отделна наука и изискват сложен интердисциплинарен подход с участието на всички заинтересовани страни.

Съвременната технологична революция радикално променя живота на хората и се създават нови предизвикателства пред международната общност, които надскачат националните граници. Държавите не успяват да се справят самостоятелно и ефективно с проблемите на киберсигурността. Политиките на национално ниво не могат да осигурят висока степен на защита на киберпространството, а се изискват колективни превантивни мерки за постигане на високо ниво на сигурност в 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. Той 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.

В настоящия дисертационен труд е изразена позицията, че съчетаването на усилията на добре развити държави, каквито са страните членки на ЕС, е предпоставка за анализирането на политиката по проблемите на киберсигурността, именно от гледна точка на правото на Европейския съюз. Нещо повече, достиженията на най-развитите интеграционни субекти в международното публично право би следвало да се споделят и да се разпростират върху все по-голям брой държави, за да се постигне висока степен на сигурност в киберпространството. Още повече, че в Устава на Организацията на обединените нации се посочва изричното развитие на регионалните обединения.

Актуалността на дисертационния труд се определя още от наличието на ограничен брой задълбочени самостоятелни изследвания, поставящи акцент върху правните аспекти на политиката на Европейския съюз по проблемите на киберсигурността както в българската, така и в чуждестранната специализирана научна литература. Изтъкнато е 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.

Актуалността на темата се обуславя и от включването в предмета на изследване на едно от най-важните предизвикателства, пред което е изправена международната общност и в частност Европейския съюз към настоящия момент – **постоянно развиващите се киберзаплахи**. Безспорно това е глобален проблем, който може да бъде преодолян с предприемането на действия в световен мащаб.

2. Обект и предмет на дисертационния труд

Обект на настоящето изследване са първоначалната фаза на формиране на правна уредба и развитието на политиката на Европейския съюз по проблемите на киберсигурността, която се обуславя и допълва от дейността на многобройните международни организации на универсално и регионално равнище.

В съвременното международно право и международни отношения все повече започва да се говори за своеобразен процес на „дигитализация", което означава, че политиката по киберсигурност заема водещо място. Обективната динамика на съвременните интеграционни процеси не само в Европейския съюз, но и в други създаващи се организации с подобен характер, както и все по-глобализиращите се международни отношения, предпоставят необходимостта от анализ на проблемите, които се поставят на международната сцена в резултат от изключително бързата еволюция в тенденциите за развитието на политиката в разглежданата област.

Предметът на изследване в дисертационния труд включва анализ на особеностите в развитието на политиката на киберсигурността в Европейския съюз, а също така индетифициране на заплахите и предлагане на решения за справяне с тях. В тази връзка предмет на анализ е и

институционалният механизъм на Европейския съюз както на основните институции, така и на специализираните агенции и органи, които имат компетенции и правомощия при осъществяване на политиката по киберсигурност.

Едновременно с това, за да се подчертаят правните аспекти на политиката за киберсигурност на Европейския съюз и нейното високо ниво на развитие, са изследвани и различни международни организации като ООН, нейните специализирани организации и НАТО, имащи отношение към проблематиката на киберсигурността.

Анализирани са някои от основните актове на вторичното право на ЕС, имащи отношение към изследването, както и по-важните компоненти на киберсигурността.

3. Цел и задачи на изследването

Предизвикателствата и проблемите пред киберсигурността съответстват на динамиката в промените на новата среда за сигурност. В тази връзка целта на представения дисертационен труд е **да се изясни същността на полититака на киберсигурност на ЕС, да се разгледа институционалният механизъм за нейното прилагане с ясно разпределени роли между заинтересованите страни**, както и **да се представят по-важните действия на международните междуправителствени организации по отношение на разглежданите проблеми.**

Така формулираните цели представляват сложна функция на желания резултат, който следва да удовлетворява изискванията за комплексност, системност, съгласуваност и реалност в разглежданата политика.

Научно-изследователските задачи на дисертационния труд са формулирани във връзка с горепосочените предмет и цел на изследването, а именно**:**

- Да се изясни същността на понятието „киберсигурност”, като се анализират определенията, използвани в различни документи и стратегии за киберсигурност на държави членки на ЕС;
- да се проследи историческото развитие на политиката за киберсигурност;
- да се посочат основните особености и заплахи за киберсигурността;
- да се разгледа структурата на политиката по киберсигурност в Европейския съюз;
- да се анализират основните актове на институциите на Европейския съюз по проблемите на киберсигурността;
- да се направи преглед на функциите и задачите на специализирани агенции на Европейския съюз в киберсигурността;
- да се направи анализ на националните стратегии за киберсигурност на държави членки на ЕС;
- да се изяснят същността и характерните особености на международното сътрудничество по управление на критични инфраструктури в ООН;
- да се разгледа и анализира Стратегическата концепция на НАТО 2020 в областта на киберсигурността и нейното влияние в Европейския съюз;
- да се предложи добре аргументиран модел на стратегия за киберсигурност на Република България.

4. Теза на изследването

Основната теза, която се поддържа в дисертационния труд е, че въпреки проблемите, които са налице в областта на политиката по киберсигурноста, международната общност е успяла да ориентира в правилна посока развитието на международното сътрудничество. Независимо от това, авторът прави критични изводи относно някои концепции, позиции и по-бавните темпове, с които се осъществява взаимодействието, особено на международно равнище. Критични бележки са направени и по отношение разликата в законодателствата на държавите членки на ЕС по проблемите на киберсигурността.

От друга страна, трудно може да се постигне принудително изпълнение на законодателството на Съюза в разглежданата сфера. Ако държавата членка е решена да подобри нивото на киберсигурност и да използва ефективно програмите за действие и нормативната уредба на ЕС в съответната област, общностното законодателство е еталонът, с който различните национални мерки могат да бъдат сравнявани, координирани и структурирани. В случай, че държавата членка не възприема киберсигурността като национален приоритет, законодателството на ЕС трудно ще доведе до нейното подобряване. ***Успешното прилагане на политиката на Европейския съюз по проблемите на киберсигурността ще позволи на Република България да бъде източник, а не консуматор на сигурност в съвременното европейско семейство.***

Изработването на изключително развити механизми и въвеждането на общи стандарти и изисквания за киберсигурност на Европейския съюз сред толкова голям брой държави, каквито са страните членки, е наистина безспорно постижение. Разбира се, заслуга за това имат както европейските институции, така и всички държави членки, които се стремят

да изпълняват посочените в правната уредба изисквания и мерки за постигане на високо ниво на киберсигурност.

5. Методология на изследването

Комплексният характер и интердисциплинарното естество на темата, която представлява пресечна точка между международното публично право, правото на Европейския съюз, международните отношения и правото на международните организации, предопределя и използваната интердисциплинарна методология на изследване. За постигане на поставените научно-изследователски задачи са използвани както общите логически методи, така и специфичните за международното право и международните отношения методи. Сред тях акцентът пада върху нормативния, формално-логическия, сравнителния и системния подход.

6. Източници на дисертационния труд

Източници на настоящето проучване са български и чуждестранни международноправни изследвания. Сред използваната литература са изследвания на български, английски, френски и руски език както в областта на международното публично право, така и на правото на ЕС, основни документи от международни конференции на ООН и други международни организации, както и информация от публикуваните в Интернет официални страници на цитираните международни организации.

7. Практическо значение на научната разработка

С оглед на интердисциплинарния характер на изследването, дисертационният труд има практическо значение както за Международното публично право, така и за Правото на Европейския съюз, а в по-широк контекст и за правото на международните организации. Представеният в труда правен анализ на по-важните законодателни актове на вторичното право на ЕС по проблемите на политиката на киберсигурността имат своята практическа стойност при тяхното транспониране в законодателството на Република България.

II. ОБЕМ И СТРУКТУРА НА ДИСЕРТАЦИОННИЯ ТРУД

В структурно отношение дисертационният труд се състои от увод, три глави, заключение, библиография, приложения и списък със съкращенията. Дисертацията е в обем от 224 страници, в това число и библиография. Научният апарат обхваща 269 бележки под линия. Към дисертацията е добавена и библиографична справка на използваната и цитирана литература, която съдържа общо 198 заглавия на кирилица и латиница и електронни адреси на официални интернет сайтове и страници. Сред използваната литература са изследвания на български, английски, и руски език, както в областта на международното публично право, така и на правото на ЕС, основни документи от международни конференции на ООН, Срещи на върха между НАТО и ЕС, стратегии за киберсигурност на държави членки на ЕС, както и информация от публикуваните в Интернет официални страници на споменатите по-горе международни организации.

III. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

В **увода** е обоснована актуалността и обществената значимост на разглеждания проблем. Посочени са обектът, предметът, целта и задачите на дисертационното изследване. Изяснена е основната му цел и са конкретизирани основните задачи, произтичащи от поставената цел.

Формулирана е основната теза на дисертацията, съгласно която въпреки проблемите, които са налице в областта на киберсигурността в Европейския съюз, международната общност е успяла да ориентира в правилна посока развитието на международното сътрудничество. В тази връзка най-голямото постижение на провежданата от Европейския съюз политика по проблемите на киберсигурността е, че принуждава държавите членки да приемат еквивалентни разпоредби в националните си правни системи във връзка с постигането на високо ниво на киберсигурност, прилагане на определени стандарти за сигурност и активно сътрудничество със заинтересованите страни.

Глава първа
Същността на политиката на киберсигурност в ЕС

В Глава първа се изясняват **основни понятия и термини в политиката на Европейския съюз по проблемите на киберсигурността**, направен е обстоен анализ на съществуващи определения за понятието. Потенциалното размиване на разглежданото понятие **може да бъде проблем и препятствие** в развитието на политиката на Европейския съюз по проблемите на киберсигурността и да окаже негативно влияе върху способността на различни **заинтересовани страни (държави, частния сектор – юридическите лица, предоставящи комуникационни услуги и интернет, а също и за участниците в неправителствения сектор и др.)**

да постигнат съгласие относно **елементите, принципите и целите** на политиката, осъществяваща се в нов тип измерение каквото са информационните и комуникационните технологии. Въпреки това, тъй като информационните технологии и самото киберпространство продължават да еволюират бързо, строгото дефиниране на понятието и задаването на определени рамки най-вероятно бързо ще загубят своята актуалност. Затова поддържането на възможно най-гъвкава концепция може да бъде от полза. (с.19)

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 тази връзка е направен анализ на определенията, посочени в националните стратегии на държави членки на ЕС.

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 киберзаплахи, както и проблемите, които правят възможно тяхното реализиране.

Проследени са **историческите предпоставки, възникването и развитието на киберсигурността като последица от информационното общество и интернет технологиите, от създаването на ARPANET през 60-те години на XX век до** комерсиализацията **на Интернет в съвременния етап.**

Акцент е поставен и върху особеностите и заплахите за киберсигурността като пета област на сигурността. Въпреки многото положителни страни на глобалната мрежа, киберпространството е сфера, в която компютъризираното взаимодействие и обмен предлагат широка гама от нови възможности за престъпни действия. Проблемите, свързани с **бързото развитие на интернет технологиите**, се превръщат в основно средство за множество престъпни дейности и реализиране на различни заплахи. **Те представляват набор от нови предизвикателства пред индивидуалната и колективна киберсигурност, обществения ред и стабилност, икономическия просперитет и политическата свобода.**

Все по-голямата зависимост от интернет технологиите прави нашето общество по-уязвимо от мащабни хакерски атаки, които могат да засегнат администрацията, системите за промишлен контрол, банките и това да се отрази пряко на гражданите. Особеностите на киберсигурността като пета област на сигурност се свеждат до:

1. Регистриране и анализ на заплахите, атаките и рисковете.
2. Увеличаване на броя и сложността на заплахите - бъдещи заплахи и тенденции по отношение на киберпрестъпността.
3. Разлика в правната регламентация.
4. Ролята на финансовите ресурси и човешкия фактор в гарантирането на киберсигурността.
5. Включване на повече заинтересовани страни/ключови играчи и по-ефективно сътрудничество.

Изследването на проблемите на киберсигурността не е обект само на една област или едно научно направление, а включва сложен комплекс от правни, политически, икономически, социални и други аспекти. Ето защо за намирането на адекватни решения, е необходимо детайлно анализиране на проблемите, пред които са изправени, както ЕС така и другите играчи, актьори или участници в международните отношения. Ангажирането на

повече експерти от различни области ще спомогне за намирането на по-всеобхватен подход при изготвянето и прилагането на различни програми в сферата на киберсигурността. Активното участие на международните организации и съюзите е от изключителна важност, защото по този начин изпълнението на решенията и сътрудничеството ще включва по-голям брой заинтересовани страни/ключови играчи и техните усилия и действия ще бъдат по-координирани, с по-висока степен на отчетност.

Европейският съюз е едно от най-уязвимите места, в които се развива киберпрестъпността поради наличието на авангардна интернет инфраструктура. Освен това *в ЕС е широко разпространено използването на електронните икономическите и платежни системи, които все повече се опират на интернет.* Поради темповете и сложността на технологичното развитие киберзаплахите постоянно се променят.

Заплахите за киберсигурността могат да се класифицират по различни начини. Една от най-честите класификации се основава на мотивационните фактори – киберпрестъпност, кибертероризъм, кибервойна, кибершпионаж.

Възможните критерии за класификация на заплахите могат да бъдат въз основа на използваните методи и от степента на нанесените щети, засегнатите активи и вида на засегнатите организации. Настоящото изследване се фокусира върху 15 от най-често срещаните заплахи.

1. Атаки, задействани от изтегляне/сваляне (Drive-by Exploits/ Drive-By Downloads)
2. Червеи/ Троянски коне
3. Комплекти за употреба (Exploit Kits)
4. Ботнет
5. Атаките, свързани с отказ на услуга (Denial of service – DoS)
6. Фишинг
7. Компрометиране на конфиденциална информация

8. Rogueware/Scareware
9. Спам (Spam)
10. Целеви атаки
11. Физическа Кражба / Загуба / Повреда
12. Кражба на самоличност
13. Злоупотреба с изтичане на информация
14. Търсене, предоставящо компрометирани резултати (Search Engine Poisoning SEP
15. Измамни/Фалшиви сертификати за сигурност

Направена е и класификация на заплахите за киберсигурността, като те са групирани от гледна точка на вида заплаха и са отразени източникът и причината за заплаха – физически атаки, бедствия, неправилно функциониране, прекъсванията, неумишлени действия, повреда, престъпните дейности и злоупотреби, подслушване, прихващане или отклоняване на съобщения и кореспонденция, правни заплахи

В тази връзка предизвикателствата, пред които сме изправени, засягат не само Европейския съюз и не могат да бъдат преодолени самостоятелно от него. Киберпространството позволява по-ефикасни комуникации, координиране и сътрудничество, в резултат на което възниква система от иновации във всички области на живота. Заплахите в тази среда обаче също могат да идват отвсякъде и вследствие на глобалните връзки да засегнат всяка част от света.

Информационните и комуникационните технологии, осъществяващи се посредством интернет, стават причина, от една страна, за изключително бързо технологично развитие, а от друга, водят до появата на нови, малко очаквани явления в съвременните международни отношения. Навлизането на интернет се превърна в един многоаспектен процес, променящ основните способи за работа, общуване, търсене и обработка на информация, управление на сложни съоръжения и системи в публичния и

частния сектор. Паралелно с ползите и положителното значение на интернет обаче се очертават и нови негативни процеси и проявления, имащи неблагоприятно въздействие както върху правата на човека, така и върху осигуряването на системите за сигурност, защитаващи суверенитета и териториалната цялост на държавите.

Глава втора
Институционален механизъм за приложение на политиката по киберсигурността в Европейския съюз

В глава втора от изложението се прави анализ на формирането и структурата на политиката по киберсигурността в Европейския съюз, като се акцентира на четири основни компонента на разглежданата политика – мрежова и информационна сигурност (МИС), правоприлагане, отбрана и стандарти за сигурност.

Тристълбовата структура, чрез която се реализира 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. Ефетивното 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 информацинна 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.

Направена е обща характеристика на **основни актове на институциите на Европейския съюз за формиране на политиката за киберсигурност**. Анализират се основни актове на институциите на ЕС, в това число - Програмата в областта на цифровите технологии (DAE), която е част от стратегията Европа 2020, двете стратегии за сигурност на ЕС – „Сигурна Европа в един по-добър свят" и Стратегията за вътрешна сигурност (СВС) на Европейския съюз – „Към европейски модел за сигурност". Безспорно най-големият напредък в областта на киберсигурността е постигнат със Стратегията на Европейския съюз за киберсигурност и предложението на Европейската комисия за Директива, „касаеща мерките за осигуряване на високо общо ниво на мрежовата и информационната сигурност (МИС) в Съюза".

Внимание е отделено и на функциите и задачите на специализираните агенции на Европейския съюз в областта на киберсигурността, като е поставен акцент върху Европейска агенция за мрежова и информационна сигурност (ENISA), Екипи за незабавно реагиране при компютърни инциденти - CERT-EU, Европейски публично-частните партньорства за устойчивост - EP3R, ролята на Европейкия център за борба с киберпрестъпността (European Cybercrime Centre – EC3), Европол, Евроюст и CEPOL.

Направен е и анализ на национални стратегии за киберсигурност на държави членки на Европейския съюз. За да се проследи отделният 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.**

Съвсем логично се достига до извода, че държавите членки на ЕС трябва да обединят усилията си, за да успеят да се справят с едно от предизвикателствата, пред които е изправена международната общност през 21 век и в частност отделните държави и техните граждани – киберпрестъпността.

Глава Трета

Международно сътрудничество по проблемите на киберсигурността в дейността на водещи международни междуправителствени организации

Глава трета поставя на преден план сравнителноправения подход, отразяващ дейността на ООН и НАТО в областта на киберсигурността. Водещо място в изложението се поставя на **същността и особеностите на международното сътрудничество по управление на критичната инфраструктура в ООН.** Важността на критичните инфраструктури (КИ) се състои в мащаба на евентуалните щети в случай на престъпни действия срещу тях. Ето защо, от гледна точка на международноправното регулиране на Интернет и възможностите за компрометиране на критичната инфраструктура, най-важно значение има Организацията на Обединените нации и нейните специализирани агенции.

Новите киберзаплахи изискват непрекъснато внимание на всички фронтове: национални, регионални и международни. Въпреки че, процесът на „глобализация" продължава да се ускорява, все още няма глобален отговор на проблемите на сигурността в цифровия век и усилията за осигуряване на киберпространството са **реактивни, а не проактивни**. Развитието на транснационален контрол по отношение на „киберпространството" е от съществено значение в борбата с

киберпрестъпленията и защитата на критичните инфраструктури. Именно затова във фокуса на научните изследвания се поставя **международната общност** и постигнатото досега в тази област. (с.124)

Обсъждането на проблемите, касаещи международното сътрудничество по управление на критичната инфраструктура в ООН се инициира и осъществява в рамките на международните междуправителствени организации. Една от особеностите в дейността на международните междуправителствени организации както универсални, така и регионални, включени в този процес, се изразява в това, че в нея **взимат участие представители на всички заинтересовани страни**: гражданско общество, частен сектор, международни неправителствени организации, техническо и академичната общност. Другата особеност се състои в това, че форматът на дейността на международните междуправителствени организации е свързан с реализацията на задачите и решенията, заложени в документите, приети на двата етапа на Световната среща на високо равнище по въпросите, касаещи информационното общество.

Традиционната идея за киберсигурност с акцент върху защитата на личните данни и самата система в рамките на една държава или международна организация, вече не е в състояние да улови обхвата на рисковете и заплахите, реализиращи се в пълен мащаб благодарение на цифровата и безжична свързаност. С навлизането и нарастването на взаимосвързаността на цифровите технологии, все по-често терористични организации и трансгранични организирани престъпни групи, привлечени от мащабността и нанесените щети, насочват своите усилия и действия към компрометиране на недостатъчно добре защитени обекти на критичната инфраструктура. Решаващо значение има фактът, че повечето киберпрестъпления се извършват отвъд рамките на националната

юрисдикция. Именно затова единственият начин да се противодейства на правонарушителите и те да бъдат заловени е чрез ефективно международно сътрудничество, както между отделните държави, така и между самите международни организации.

Акцент е поставен и на някои по-важни аспекти на киберпрестъпленията, отразени в Конвенцията на ООН срещу транснационалната организирана престъпност, както и борбата на ООН и ЕС с кибертероризма.

Вторият параграф на глава трета се разглежда стратегическата концепция на НАТО 2020 в областта на киберсигурността и нейното влияние в Европейския съюз. Проследени са резултатите от Срещите на върха в Лисабон (ноември 2010 г.), Чикаго (май 2012 г.) и Уелс (септември 2014 г.).

В параграф трети на глава трета от дисертационния труд е направено предложение за модел на стратегия за киберсигурност на Република България.

Стратегическото планиране се състои в изготвянето на стратегическия план, който съдържа анализ на средата, (крие редица заплахи и рискове), изготвяне на SWOT анализ, очертаване на приоритетите, изготвяне на визия за развитие, реализация на плана. Планирането започва с анализ на тенденциите и движещите сили на организацията, като се оценява тяхното влияние за в бъдеще. По принцип тенденциите се определят по възможност за по-дълго време, а движещите сили описват резките промени, които настъпват бързо. Изясняването на външните и вътрешните фактори ни предоставя възможност да се изясни нашата визия за бъдещето. От анализа на външните фактори се определят възможностите и заплахите, а от анализа на вътрешните – силните и слабите страни. (с. 162)

В предложения модел за стратегия са посочени заплахите и рисковете за сигурността и принципите, при които следва да бъде изграден националният подход за управление на сигурността в кибернетичното пространство. Посочени са заинтересованите страни и ролята на всеки участник за гарантиране на високо ниво на киберсигурност.

Заключение

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.

Като резултат от проведеното изследване могат да се формулират следните изводи:

1. Изведени са основните проблеми, касаещи киберсигурността

- ✓ Включване на повече заинтересовани страни/ключови играчи и по-ефективно сътрудничество;
- ✓ Ролята на финансовите ресурси и човешкия фактор в гарантирането на киберсигурността;
- ✓ Разлика в правната регламентация ;
- ✓ Увеличаване на броя и сложността на заплахите;

- ✓ Регистриране и анализ на заплахите, атаките и рисковете.

2. Необходимо е намирането на по-адекватни мерки и действия по ограничаване на заплахите и преодоляване на проблемите в областта на киберсигурността.
3. От направения анализ на стратегиите за киберсигурност на държавите членки на ЕС, както и на водещи държави в областта на мрежовата и информационната сигурност става ясно, че за разлика от водещите в технологично отношение страни, в България няма приета стратегия за киберсигурност. Този факт показва, че нормативната база в България все още не отговаря на съвременните изисквания за гарантиране на киберсигурност
4. Държавите членки на ЕС трябва да обединят усилията си, за да успеят да се справят с едно от предизвикателствата, пред които е изправена международната общност през 21 век и в частност отделните държави и техните граждани – киберпрестъпността.
5. Всички държави членки на ЕС трябва да предприемат в националните си правни системи еквивалентни мерки за превенция, предотвратяване и наказание на киберпрестъпността. Последните трябва да бъдат съобразени с правните предписания/инструменти и принципи на правната система на ЕС .
6. Необходимо е създаването на нова мрежа за обмен на информация по съдебни въпроси и добри практики при разследване и наказателно преследване на престъпления в кибернетичното пространство;
7. Предлагане на повече обучения и възможности за работещите в сферата на киберсигурността.

IV. СПРАВКА ЗА ПО-СЪЩЕСТВЕНИТЕ ПРИНОСИ НА ДИСЕРТАЦИОННОТО ИЗСЛЕДВАНЕ

1. Запълва известна празнота в научно-изследователското пространство, като се анализира политиката на ЕС по проблемите на киберсигурността.
2. Изведена е дефиниция на понятието “киберсигурност”.
3. Направена е класификация на заплахите за киберсигурността
4. Доказана е необходимостта от по-широки и целенасочени действия за по-нататъшното устойчиво регулиране на този водещ международен проблем.
5. Направен е сравнителен анализ на национални стратегии за киберсигурност на държави членки на ЕС
6. Направено е предложение за модел на стратегия за киберсигурност на Република България

V. СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ТЕМАТА НА ДИСЕРТАЦИЯТА

1. Кочев, Й., Човешкият фактор в киберсигурността**.** НВУ „Васил Левски”, Университетска годишна научна конференция 27-28 юни 2013 г.
2. Кочев, Й., Политиката на киберсигурност в ЕС: предизвикателства и перспективи. Международно лятно училище за докторанти “Европейският съюз и Черноморския регион: предизвикателства и перспективи, 17-19 Септември 2013 г.
3. Kochev, Y., Cyber Security Policy in the EU: Problems and Suggestions for Possible Solutions - V Международной научно-практической конференции «Кутафинские чтения», 26-28 Ноември, 2013 г., Москва.