БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ИНСТИТУТ ЗА ДЪРЖАВАТА И ПРАВОТО

СЕКЦИЯ „МЕЖДУНАРОДНОПРАВНИ НАУКИ“

МАРГАРИТА ЕВГЕНИЕВА ОЙСОЛОВА

АВТОРЕФЕРАТ

за присъждане на образователна и научна степен
„доктор“
на тема:

РЕГЛАМЕНТАЦИЯ НА КИБЕРСИГУРНОСТТА В ЕВРОПЕЙСКИЯ СЪЮЗ – ПРОБЛЕМИ И ПЕРСПЕКТИВИ

Научна област: 3. Социални, стопански и правни науки

Професионално направление: 3.6. Право

Научна специалност: Международно право и международни отношения

Научен ръководител: проф. д-р Ирена Илиева

София,

2025 г.

Докторантът е зачислен в задочна докторантура по докторска програма „*Международно право и международни отношения*" от научна област 3. Социални, стопански и правни науки, проф. направление, шифър 3.6. Право, съгласно заповед № РД-09-23/29.01.2021г. на директора на ИДП при БАН.

Темата на дисертационния труд е „Регламентация на киберсигурността в европейския съюз - проблеми и перспективи“, с научен ръководител проф. д-р Ирена Илиева.

Представеният дисертационен труд е обсъден и насочен за публична защита на заседание на секция „Международноправни науки" в ИДП при БАН на 02.09.2025 г.

На основание заповед № РД-09-68/25.09.2025 г. на директора на ИДП при БАН е утвърден състав на научното жури и е определена дата за провеждане на открито заседание за защита на дисертационния труд.

Вътрешни членове на научното жури:

доц. д-р Тони Димов

доц. д-р Паунита Петрова

Резервен член:

доц. д-р Тодор Кобуров

Външни членове на научното жури:

проф. д.н. Стоян Денчев от УНИБИТ

проф. д-р Евгения Ковачева от УНИБИТ

проф. д.н. Георги Димитров от ВТУ „Св. Св. Кирил и Методий“

Резервен член:

доц. д-р Гергана Гозанска от ПУ „Паисий Хилендарски“

На дата **19.11.2025 г.** *ще бъде проведено открито заседание на научното жури за защита на дисертационния труд в заседателната зала на ИДП на адрес: гр. София, ул. Сердика “ № 4.*

Дисертационният труд и материалите по защитата са на разположение в ИДП на адрес: гр. София, ул. „Сердика” № 4 и на интернет страницата на ИДП: www.ipn-bg.org

Съдържание

I. Обща характеристика на дисертационния труд 4

1. Цел на дисертационния труд 4

2. Предмет на труда 4

3. Основни изследователски задачи 4

4. Основна изследователска теза 5

5. Методология 5

6. Очаквани резултати 7

II. Обем и структура 7

1. Увод 8

2. Глава първа. Стратегически документи 11

3. Глава втора. Регламенти в областта на киберсигурността 15

4. Глава трета. Директиви в областта на киберсигурността 20

5. Заключение 26

III. Теоретични и практически приносни моменти на дисертационното изследване 26

IV. Публикации по темата на дисертационния труд 36

I. Обща характеристика на дисертационния труд

1. Цел на дисертационния труд

Основна цел на този труд е да се направи преглед на регламентацията за киберсигурност в Европейския съюз, чрез анализ на съдържанието на всеки от тях и, както и където е възможно, съпоставка между различни версии на документите. Чрез подобен цялостен преглед, ще бъде постигната по-голяма яснота по отношение на регламентацията на Европейският съюз в сферата, което ще бъде от полза и улеснение не само за юристите, занимаващи се с проблематиката на киберсигурността, но и за експерти неюристи, технически лица, които трябва да прилагат на практика изискванията заложени в регламентацията, както и дори на обикновените граждани, които се явяват потребители на Интернет и могат да бъдат или са пряко засегнати от всички аспекти на киберсигурността, дори и невинаги да го съзнават. В Приложение I е направени списък на използвани нормативни актове в разработката, подредени в хронологичен ред.

2. Предмет на труда

Предмет на труда е регламентацията на киберсигурността в правото на Европейския съюз.

3. Основни изследователски задачи

1. Събиране на всички нормативни актове и стратегии на Европейския съюз в сферата на киберсигурността.

2. Предаване в синтезиран вид на съдържанието на събраните нормативни актове и стратегии на Европейския съюз в сферата на киберсигурността.

3. Анализ на събраните нормативни актове и стратегии на Европейския съюз в сферата на киберсигурността.

4. Определяне на основни проблеми и слабости в събраните нормативни актове и стратегии на Европейския съюз в сферата на киберсигурността.

5. Изготвяне на предложения *de lege ferenda*, като възможни перспективи за подобряване и актуализиране на нормативните актове и стратегии на Европейския съюз в сферата на киберсигурността.

4. Основна изследователска теза

Европейският съюз е предприел значителни крачки в изготвянето на законодателството си в сферата на киберсигурността. Приети са стратегии, регламенти и директиви, свързани с киберсигурността, но в тях, след направен анализ, бяха установени някои пропуски и необходимост от допълнения и включване на актуални заплахи, които ежедневно възникват в киберпространството. Дадени са предложения за допълване на тези пропуски и за актуализиране на нормативната рамка на Европейския съюз.

5. Методология

Методологията на изследването се основава на класическия за правните науки телеологичен подход за задълбочен анализ на нормативните източници в правото на Европейския съюз в областта на киберсигурността. Той е допълнен от критичен анализ на съвременните изследвания в предмета на дисертационния труд. Използваните научноизследователски методи за решаване на поставените пред научното изследване задачи, водещи до постигане на поставената цел, включват:

Изводите и заключенията в настоящата работа са направени на базата на наблюдения/анализи и проучвания на формирането и развитието на регулаторната рамка в Европейския съюз в областта на киберсигурността.

Исторически подход при изследването – с проследяване и отчитане развитието на възгледите, идеите, технологиите и законодателството на Европейския съюз в сферата на киберсигурността.

Използван е интердисциплинарен подход, който включва проучване и анализ на документи – събрани, систематизирани и проучени са стратегии, регламенти и директиви на Европейския съюз в сферата на киберсигурността.

Използван е методът на интервюта чрез събеседване с експерти – участие в научни конференции и семинари в процеса на писане на настоящата разработка, чрез което е постигнат обмен на мнения и опит с сферата на киберсигурността.

Използвани са формално-логически подходи: синтез и дедуктивен метод. Синтезът е приложен за различни типове нормативни документи на Европейския съюз в сферата на киберсигурността.

Обобщението е използвано за оценка на относимостта на нормативните актове на Европейския съюз към киберсигурността и това дали те изцяло или частично съдържат релевантни текстове.

За целите на разработката е направено проучване на актовете на Европейския съюз в областта на киберсигурността, както и на някои проучвания и изследвания, направени от органите на Съюза. Основният подход при структуриране на разработката е преглед по отделно на всеки нормативен акт на Европейския съюз, свързан с киберсигурността, кратко представяне на съдържанието му, където е възможно съпоставка между няколко версии на акта и негов анализ.

6. Очаквани резултати

Направено е проучване на актовете на Европейския съюз в областта на киберсигурността, както и на някои проучвания и изследвания, изготвени от органите на Съюза. По този начин ще бъде постигнат един цялостен преглед на законодателството на Европейския съюз по отношение на киберсигурността, което ще спомогне за по-ясен анализ и за по-лесни изменения при бъдещите промени на нормативните актове. В допълнение, ще бъде постигната по-голяма яснота в цялостната картина на предприетите мерки и по отношение на това какво трябва да бъде добавено и/или променено, съобразно новите тенденции в сферата.

Въз основа на направения анализ на нормативните актове на Европейския съюз са направени коментари, отнасящи се до приложното и практическото поле на разпоредбите.

Изследването е ограничено в периода след 2000 г. Това се налага поради големият брой нормативни актове и неактуалността на остарелите такива, датирани преди 2000 г.

II. Обем и структура

Изследването се състои от 270 стр., от които 252 стр. същинско изложение, обособени в увод, три глави и заключение, а останалите са заглавна страница, списък на използваните съкращения, използвана терминология, съдържание, библиография и Приложение I - Списък на използвани нормативни актове в разработката, подредени в хронологичен ред.

Глава първа се отнася до стратегическите документи за киберсигурност в Европейския съюз, като съдържа пет раздела. Глава втора се отнася до регламенти в областта на киберсигурността, като съдържа осем раздела. Глава

трета се отнася до директиви в областта на киберсигурността, като съдържа девет раздела.

Разделите са обособени в отделни точки.

III. Структурно съдържание на дисертационния труд

1. Увод

Мрежите и информационните системи играят жизненоважна роля за обществото и са се превърнали в основата на икономическия растеж. Информационните и комуникационните технологии са в основата на сложните системи, които поддържат ежедневната обществена активност, правят възможно функционирането на нашите икономики в основни сектори като здравеопазване, енергетика, финанси и транспорт, и по-специално поддържат функционирането на вътрешния и международен пазар. Използването на мрежите и информационните системи от гражданите, организациите и предприятията в целия Европейски съюз е вече повсеместно. Цифровизацията и свързаността се превръщат в основни характеристики на все по-голям брой продукти и услуги и с навлизането на „интернет на нещата“ се очаква на територията на Съюза през следващото десетилетие да има изключително голям брой свързани цифрови устройства. През последните години, особено в периода на пандемията от Covid-19 киберпространството и употребата на технологиите навлезе изключително бързо във всички сфери на обществото. Ежедневието на хората, основните права, социалните взаимодействия и дори икономиките на държавите зависят от безупречната работа на информационните и комуникационните технологии. В наши дни множество сложни системи в различни сектори, като например финанси, здравеопазване, енергетика, транспорт и други, разчитат на информационните и комуникационните технологии, а след пандемията от Covid-19, вече и голяма

част от бизнеса разчита на непрекъснатостта на достъпа до интернет и безупречното функциониране на информационните системи.

Въпреки нарастващия брой на цифровите устройства вграждането на сигурност и устойчивост в тях „още при проектирането“ (Secure by design) все още не се извършва в задоволителен мащаб, което води до недостатъчно ниво на киберсигурност на фона на нарастващата зависимост на бизнеса и живота от информационните и комуникационните технологии и Интернет. Злонамерените играчи се възползват от тези „пропуски“ и липсата на сигурност в тях и ги използват за незаконна дейност. Инцидентите, свързани с киберсигурността могат не само да подкопаят доверието на потребителите в технологиите, мрежите и услугите, като по този начин засегнат способността им да се възползват от пълния потенциал на вътрешния пазар и широко разпространеното ползване на информационните и комуникационните технологии, но и да допринесат за огромни загуби за организациите.

В този контекст, ограниченото използване на сертифицирането води до недостиг на информация за ползвателите физически лица, организации и предприятия относно характеристиките на ИКТ продукти, ИКТ услуги и ИКТ процеси в областта на киберсигурността, като подкопава доверието в цифровите решения. Мрежите и информационните системи могат да улеснят всички аспекти на нашия живот и да стимулират икономическия растеж на Съюза. Те са основата за постигането на цифровия единен пазар.

Сложният характер на кибератаките за получаване на неоторизиран достъп до компютърни системи и мрежи представлява значително предизвикателство в областта на киберсигурността. Атакуващите разработват и използват много сложни и усъвършенствани техники за получаване на неоторизиран достъп или използват вече известни уязвимости в системите.

През последните години Европейският съюз направи редица важни крачки за повишаване на нивото на мрежова и информационна сигурност, чрез приемане на стратегии за киберсигурност и редица регламенти и директиви, чрез които се цели повишаване на нивото на киберсигурност и защита на информационните и комуникационните технологии. Тези рискове пораждат необходимост не само от технически решения за защита, но и от формирането на етични стандарти за поведение в киберсредата. Тук се очертава и ролята на киберетиката.

Киберетиката може да бъде определена като интердисциплинарна област, която съчетава принципите на етиката, правото и информационните технологии. Тя се занимава с въпроси като: как да се гарантира справедливо и отговорно използване на дигиталните ресурси; как да се защитава личната автономия и правото на неприкосновеност на данните; къде е границата между свободата на словото и отговорността за онлайн съдържанието. В контекста на глобализираното киберпространство киберетиката придобива особено значение, тъй като липсата на физически граници изисква универсални, споделени стандарти и ценности.

Европейският съюз е сред водещите играчи в опита да интегрира етичните и правни измерения на киберсигурността в единна стратегическа рамка. Документи като Стратегията на ЕС за киберсигурност (2020), Директивата за мрежова и информационна сигурност NIS и нейното обновление NIS2, както и създаването на Агенцията на ЕС за киберсигурност (ENISA) показват системния подход на съюза към този проблем. Основните цели са укрепване на устойчивостта на критичната инфраструктура, създаване на механизми за бързо реагиране при инциденти, засилване на

трансграничното сътрудничество и стимулиране на иновациите в областта на киберзащитата.

Наред с институционалните и технологичните аспекти, Европейския съюз поставя акцент и върху етичните измерения. Защита на личните данни (чрез Общия регламент за защита на данните – GDPR), гарантиране на дигиталните права на гражданите, борба срещу кибердискриминацията и речта на омразата – това са все елементи, които свидетелстват за интеграцията на киберетиката в стратегиите за сигурност. Така се постига баланс между изискването за защита и опазването на демократичните принципи и права.

В този контекст можем да разглеждаме киберетиката като допълващо измерение на политиките за киберсигурност. Докато стратегиите осигуряват правната и институционалната рамка за защита, етиката задава нормативните ориентири за тяхното приложение – отговорност, прозрачност, справедливост и уважение към човешкото достойнство. Само чрез взаимодействието между тези две сфери може да бъде изградена устойчива и сигурна дигитална екосистема, която едновременно да гарантира сигурност и да насърчава иновациите.

След направено проучване в базите данни на Национален център за информация и документация, беше установено, че към настоящият момент няма цялостен преглед на актовете на Европейския съюз, които имат отношение към темата „киберсигурност“.

2. Глава първа. Стратегически документи

В първа глава на дисертацията, озаглавена „Стратегически документи“ са разгледани четири стратегически документа на Европейския съюз. Два от тях са стратегиите за киберсигурност, съответно от 2013 година и от 2020

година. Другите разгледани стратегии са Стратегията на Европейския съюз за Съюза на сигурност и Стратегията за цифровизиране на финансовите услуги в Европейския съюз. Киберпространството следва да бъде защитено от инциденти, злонамерени действия и злоупотреби. Заплахите са от различно естество, поради това е важно да се гарантира свободата и безопасността в киберпространството. Стратегическите документи играят ключова роля в определянето на посоката и приоритетите за развитие на дадена област, независимо дали става въпрос за регионално развитие, икономически растеж, социално благополучие и/или други аспекти на обществения живот. Тяхната основна роля е да предоставят рамка за дългосрочното планиране и управление на развитието на дадена област. Някои сектори в Европейския съюз, като например здравеопазване, енергетика, водоснабдяване и други, вече разчитат на информационните технологии за своето функциониране. Европейският съюз преценява, че е от изключителна важност да се започне работа по въпроса за високо общо ниво на киберсигурност и приема Стратегия на Европейския съюз за киберсигурност. В нея се очертават вижданията на Европейския съюз в тази област, изясняват се ролите и отговорностите и се определят необходимите действия за защита и насърчаване на правата на гражданите, като основната цел е онлайн пространството в Европейския съюз да се превърне в една по-безопасната среда. В нея са залегнали принципите и стратегическите насоки за подобряване на киберсигурността в Европейския съюз. В стратегията са определени пет стратегически приоритета по отношение на киберсигурността. В стратегията е предвидено и запълването на празноти в Европейския съюз по отношение на националния капацитет на държавите-членки, координацията в случай на инциденти с трансграничен характер, както и по отношение на участието на частния сектор и подготвеността за евентуални киберкризи. Като важни елементи за

подобряването на законодателството в сферата са маркирани необходимостта да се установят общи минимални изисквания за киберсигурност на национално равнище. През 2020 г. Стратегията на Европейския съюз за киберсигурност е преразгледана и съответно актуализирана, като е съобразена с новите тенденции в сферата на киберсигурността и разработена, съобразно изпълнените задачи на предходната Стратегия за киберсигурност. В новата Стратегия се наблюдават значителна политическа промяна от цялостен към интегриран подход. В нея заплахите са ясно конкретизирани в икономическата, политическата и военната сфера, като дори те са в почти равни пропорции. В нея са предложени и набор от конкретни мерки за подобряване на нивото на киберсигурност. Стратегията за 2020 г. поставя акцент върху създаването на общи стандарти за киберсигурност в рамките на Европейския съюз, но различията в националните подходи и техническите изисквания често водят до трудности при тяхното прилагане.

Стратегията за единен цифров пазар на Европейския съюз от 2015 г. е инструмент за ускоряване на цифровата трансформация, укрепване на вътрешния пазар и гарантиране на конкурентоспособността на Европа в глобален мащаб. В нейната основа стои убеждението, че само чрез създаването на общи правила, инфраструктури и механизми за доверие могат да бъдат постигнати пълните ползи на цифровизацията. Киберсигурността е един от централните елементи на стратегията. Сигурността на мрежите, системите и личните данни е условие за изграждането на доверие у гражданите и бизнеса, което от своя страна е необходимо за развитието на електронната търговия, цифровите услуги и иновациите. Сред основните законодателни инициативи в тази област са Директивата за мрежова и информационна сигурност (МИС), Общият регламент относно защитата на данните (GDPR) и Акта за киберсигурността. Значителни усилия се насочват към изграждането на

високоскоростна и надеждна инфраструктура, включително гигабитни мрежи и внедряване на 5G във всички държави членки. Тези действия са предпоставка за функционирането на интелигентни градове, автономни транспортни системи и масово навлизане на IoT технологии. Стратегията обхваща и регулацията на изкуствения интелект чрез разработването на Европейски акт за изкуствения интелект. Неговата цел е да създаде правна рамка, която едновременно насърчава иновациите и гарантира етичната и безопасна употреба на AI технологии в съответствие с европейските ценности и основни права.

Стратегията е актуализирана през 2025 г. Тя отразява нуждите на бързо развиващата се цифрова икономика и социалните промени, предизвикани от технологичния напредък. Целта е да се укрепи конкурентоспособността на Европейския съюз, да се подкрепят иновациите, да се премахнат оставащите бариери пред движението на стоки и услуги и да се създаде сигурна, устойчива и достъпна цифрова среда за гражданите и бизнеса. За разлика от стратегията, приета през 2015 г., в новата от 2025 г. не са залегнали текстове, отнасящи се до киберсигурността.

В Стратегията на Европейския съюз за Съюза на сигурност се очертават приоритетните действия, инструменти и мерки за постигане на тази цел, както във физическия, така и в цифровия свят, а също и сред всички слоеве на обществото. Това неминуемо включва и кибератаките, които са голям проблем за сигурността. Те стават все по-чести и усъвършенствани. В Стратегията е предвидено да бъде направен преглед на Директивата за мрежите и информационните системи (която е основното европейско законодателство в областта на киберсигурността) и да се очертаят стратегическите приоритети в областта на киберсигурността, за да се гарантира, че Европейския съюз може

да предвижда и да дава отговор на променящите се заплахи. Освен техническите мерки, Стратегията на Европейския съюз за Съюза на сигурността поставя акцент върху изграждането на култура на киберсигурност и киберхигиена сред гражданите, бизнеса и държавните институции.

Стратегията за цифровизиране на финансовите услуги в Европейския съюз е последната включена в разработката. Достъпът на потребителите и предприемачите до финансовите услуги е все по-често електронен. Иновативни пазарни участници внедряват нови технологии, а съществуващите бизнес модели се променят. Осигуряването на сигурно и надеждно функциониране на цифровите инфраструктури става все по-важно, тъй като все повече хора използват предоставяните онлайн финансови услуги, а самите служители в сектора на финансовите услуги работят дистанционно. Именно тези тенденции при финансовите услуги са подтикнали Европейския съюз да приеме Стратегията за цифровизиране на финансовите услуги в Европейския съюз. Тя има за цел да създаде интегриран и иновативен финансов сектор, който напълно използва предимствата на цифровите технологии и осигурява устойчивост и защита за всички участници. Основните цели на Стратегията включват насърчаване на иновациите и конкуренцията в цифровите финанси, укрепване на защитата на потребителите и финансовата стабилност, както и повишаване на киберустойчивостта.

3. Глава втора. Регламенти в областта на киберсигурността

Във Втора глава на дисертацията са разгледани и анализирани регламенти в областта на киберсигурността. Включена е проблематиката за електронната идентификация и удостоверителни услуги при електронни транзакции на вътрешния пазар. Връзката между киберсигурността и управлението на националната електронна идентификация, защото всяка

електронна транзакция ще използва идентичността и сигурността при обмена на информация. Разгледан е Регламента за електронна идентификация и удостоверителни услуги (eIDAS). Той създава нова система за сигурни електронни трансакции в рамките на Европейския съюз между бизнеса, гражданите и публичните органи. Регламентът има за цел да подобри доверието в електронните трансакции в целия Европейски съюз, да повиши ефективността на публичните и частните онлайн услуги и електронната търговия.

Друг важен въпрос, относим към киберсигурността е защитата на физическите лица във връзка с обработването на личните данни. Тук е разгледана и защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Европейския съюз. В дисертационния труд е разгледан не безизвестният сред обществото Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на личните данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните). Той цели да укрепи и хармонизира правата на гражданите на Европейския съюз по отношение на защитата на личните им данни в цифровото пространство. Включващ разпоредби за събиране, обработка, съхранение и обмен на лични данни, регламентът налага строги изисквания за организации и предприятия, които обработват такива данни. Неговата цел е да гарантира прозрачност, справедливост и сигурност в обработката на данни, за да се предотвратят злоупотреби и нарушения на личната неприкосновеност. Защитата на личните данни и киберсигурността са тясно свързани аспекти на защитата на данните в цифровото пространство, като подробно са разгледани аспектите на взаимодействието между Регламента и киберсигурността. Разгледана е и

проблематиката за защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза. Тя е свързана с Регламент (ЕС) 2018/1725 на Европейския парламент относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни. В него се определят правила как институциите, органите, службите и агенциите на Европейския съюз следва да обработват личните данни, които те имат за лицата. Също така Регламентът защитава основните права и свободи на физическото лице, по-специално правото на защита на личните данни и правото на неприкосновеност на личния живот и съгласува правилата за институциите, органите, службите и агенциите на Европейския съюз с тези на Регламент (ЕС) 2016/679.

Въпросът за сътрудничеството между националните органи, отговорни за законодателството за защита на потребителите е разгледан, чрез анализа на Регламент (ЕС) 2017/2394 на Европейския парламент и на Съвета, относно сътрудничеството между националните органи, отговорни за прилагането на законодателството за защита на потребителите и за отмяна на Регламент (ЕО) № 2006/2004. Той има за цел да предпазва потребителите от трансгранични нарушения на законодателството на Европейския съюз в областта на защитата на потребителите чрез модернизиране на сътрудничеството между съответните национални органи в държавите-членки. Регламентът обхваща 26 законодателни акта на Европейския съюз, които защитават интересите на потребителите и които са изброени в приложението му.

Един от основните аспекти на Регламент (ЕС) 2019/796 е установяването на обща рамка за управление на киберзаплахите и реагиране в случай на кибератаки. Той е разгледан подробно в дисертационния труд. Този

регламент създава механизми за бързо и ефективно реагиране в случай на сериозни кибератаки, които могат да застрашат интересите на Европейския съюз или на неговите държави-членки. Сред тези механизми са предвидени ограничителни мерки, които могат да бъдат приложени срещу лица или организации, замесени в кибератаки, като финансови санкции, забрани за влизане и замразяване на активи. Регламентът установява и процедури за координация и сътрудничество между държавите-членки на Европейския съюз в случай на кибератака или заплаха от такава. Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и мрежа от национални координационни центрове.

Акт за киберсигурността е съкратеното наименование на следващия регламент, включен в дисертацията, а именно Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013. Основната му цел е да се постигне високо ниво на киберсигурност, киберустойчивост и доверие в Европейския съюз и държавите-членки. В него са определени целите, задачите и организационните аспекти на ENISA (Агенцията на Европейския съюз за киберсигурност), също така е определена рамка за създаването на европейски схеми за сертифициране на киберсигурността с цел да се гарантира подходящо ниво на киберсигурност за информационните и комуникационните технологии и продукти, услуги и процеси в Съюза, както и с цел да се избегне разпокъсаност на вътрешния пазар по отношение на схемите за сертифициране на киберсигурността в Съюза.

В Европейският съюз са създадени Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове. По този начин се цели укрепване на киберсигурността в Европейския съюз. Чрез създаването на център за експертни познания и мрежа от национални координационни центрове, ще се допринесе за по-ефективното откриване, предотвратяване и справяне с киберзаплахите в Съюза. Цели се и улесняване на обмена на информация и добри практики между държавите-членки и насърчаване на иновациите и развитието на нови технологии в областта на киберсигурността. Всичко това е включено в разпоредбите на Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове.

Друг регламент, който допринася за развитието на киберсигурността в Европейския съюз е Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011, известен като DORA (Digital Operational Resilience Act) е част от по-голям пакет за цифрови финанси, целящ да насърчи технологичното развитие и да осигури финансова стабилност и защита на потребителите. Другите му елементи обхващат Стратегия за цифрови финанси, пазари на криптоактиви и технология на децентрализирания регистър. Той има за цел да осигури по-голяма устойчивост на финансовия сектор срещу нарастващите заплахи от кибератаки и други инциденти, свързани с киберсигурността. С него се определят единни правила за сигурността на мрежовите и

информационните системи на финансовите институции, като например банки, застрахователни дружества и инвестиционни посредници. Той обхваща широк кръг от регулирани от Европейския съюз финансови субекти, като изисква от тях да устояват, да реагират и да се възстановяват от всяко смущение или заплаха, свързани с информационните и комуникационните технологии (ИКТ).

4. Глава трета. Директиви в областта на киберсигурността

В Трета глава на дисертацията са включени директиви в областта на киберсигурността. Разгледана е Директивата, свързана с обработка на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации. Тя е ключов законодателен акт на Европейския съюз, който има за цел да осигури защита на личните данни и неприкосновеността на личния живот в контекста на електронните комуникации. Информацията се обменя чрез обществените електронни комуникационни услуги, като Интернет и мобилните и стационарните телефонни услуги, както и съпътстващите ги мрежи. Тези услуги и мрежи изискват специални правила и гаранции за осигуряване правото на потребителите на неприкосновеност на личния им живот и на конфиденциалност.

Универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги. Обработка на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации. Сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите. Всичко това е залегнало в Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО

относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите. С нея се цели да бъдат подобрени и актуализирани съществуващите Директиви в областта на електронните съобщения. Основната цел на Директива 2009/136/ЕО е да осигури по-добра защита на правата на потребителите, да укрепи доверието в цифровите услуги и да въведе ясни правила за обработката на лични данни в сектора на електронните съобщения. Това се осъществява в контекста на бързо развиващите се технологии и нарастващите нужди от ясни и ефективни регулации. Директива 2009/136/ЕО представлява важна стъпка към осъвременяване на правната рамка в сектора на електронните съобщения. С акцент върху правата на потребителите, защитата на личните данни и ефективното сътрудничество между надзорните органи, тя създава условия за по-сигурна и прозрачна среда за предоставяне на цифрови услуги. Това допринася за по-добра защита на потребителите и укрепване на доверието в дигиталните технологии.

Правната уредба на атаките срещу информационните системи е уредена в Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета. С нея се въвеждат нови правила, хармонизиращи криминализирането и санкциите за редица престъпления, насочени срещу информационните системи. Директива 2013/40/ЕС е един от ключовите правни инструменти на Европейския съюз, които се отнасят до борбата срещу престъпленията и тероризма чрез установяване на минимални

правила за определени аспекти на прилагането на наказателното право сред държавите-членки на Европейския съюз. Директивата предвижда, че държавите-членки трябва да създадат законодателни рамки за наказание на извършителите на кибератаки и да осигурят по-добро сътрудничество при обмена на информация. Директивата поставя акцент върху наказанията за извършителите на кибератаки, включително присъди за лица, които незаконно проникват в информационни системи. Директивата предвижда засилено сътрудничество между държавите-членки на Европейския съюз, както и с трети държави и международни организации.

Директива 2007/64/ЕО на Европейския парламент и на Съвета от 13 ноември 2007 г. относно платежните услуги във вътрешния пазар е ключов правен акт на Европейския съюз, който цели да хармонизира правилата и стандартите за платежните услуги във вътрешния пазар. Една от основните цели на Директивата е да гарантира правата и интересите на потребителите при извършването на платежни операции. Това включва задължението за предоставяне на ясна и разбираема информация за платежните услуги, таксите и разходите, свързани с тях, както и защита срещу неправомерни плащания и измами. Директивата установява и минимални стандарти за сигурността на платежните инструменти и трансакциите, което допринася за повишаване на доверието в платежната система. Освен защитата на потребителите, Директивата насърчава и развитието на единен пазар за платежните услуги в Европа. Тя улеснява свободното движение на плащанията в рамките на Европейския съюз, като премахва пречките и ограниченията, свързани с граничните и валутните плащания. Това създава по-голяма конкуренция между различните доставчици на платежни услуги и води до повишаване на ефективността и иновациите в сектора.

Правната уредба на процедурата за предоставяне на информация в сферата на техническите регламенти и правила относно услугите на информационното общество е залегнала в Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета. Тя има за цел да подобри функционирането на вътрешния пазар на Европейския съюз, като предвиди ясни процедури за уведомяване на Европейската комисия относно новите изисквания, които се прилагат за стоките и услугите на информационното общество в Европейския съюз. Тя също има за цел да предотврати създаването на бариери за търговията и да осигури по-добра прозрачност по отношение на националните и европейските технически изисквания.

Полицейско и съдебно сътрудничество в областта на защитата на личните данни е регламентирано чрез Директива (ЕС) 2016/680 на Европейския парламент. Тя е известна още като Директивата за полицейското и съдебно сътрудничество в областта на защитата на личните данни и е приета с цел осигуряване на високи стандарти за защита на личните данни на физическите лица при тяхната обработка от компетентните органи. Основната задача на този нормативен акт е да установи баланса между нуждата от ефективно правоприлагане и правото на неприкосновеност на личния живот. Директивата се прилага за обработката на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, както и изпълнението на наказания. Целта се състои в установяване на унифицирани правила за защита на данните в целия Европейски съюз, което да осигури съвместимост и ефективно сътрудничество между държавите-членки.

Изисквания за достъпност на уебсайтовете и мобилните приложения на организациите от обществения сектор са поставени с Директива (ЕС)

2016/2102 на Европейския парламент и на Съвета. Тя има за цел уебсайтовете и мобилните приложения на организациите от обществения сектор да станат по-достъпни, а различните стандарти да се хармонизират в рамките на Европейския съюз, като се намалят пречките пред разработчиците на продукти и услуги, свързани с достъпността. Това дава възможност на гражданите в Европейския съюз и по-специално на хората с увреждания, да получат по-лесен достъп до обществени услуги. Държавите-членки трябва да гарантират, че уебсайтовете и мобилните приложения на организациите от обществения сектор са „по-достъпни“, по-специално за хора с увреждания, като ги правят „с лесно разпознаваеми елементи, оперативни и надеждни“.

Правна уредба на мерките за високо общо ниво на сигурност на мрежите и информационните системи в Съюза е регламентирана с две Директиви на Европейския съюз - Директива (ЕС) 2016/1148 и актуализираната й версия - Директива (ЕС) 2022/2555. Двете Директиви са ключов правен инструмент на Европейския съюз и имат за цел да повишат нивото на киберсигурността в Съюза. Приети са като отговор на необходимостта от укрепване на защитата на информационните мрежи и системи в Европейския съюз, предвид нарастващия брой кибератаки и заплахи. Те предлагат широкообхватни мерки за засилване на нивото на сигурност на мрежите и информационните системи и осигуряват, услуги жизнено важни за икономиката на Европейския съюз на гражданите на държавите-членки. С тях се цели да бъде гарантирано, че държавите от Европейския съюз са добре подготвени и са готови да се справят с потенциални кибератаки. Основните изисквания в Директивите са във всяка държава-членка да бъдат определени национални компетентни органи, които ще имат задължения в областта на киберсигурността – екипи за реагиране при инциденти с компютърната сигурност. Също така важно изискване, въведено с директивите е изготвяне и приемане на национални стратегии за

киберсигурност. Установява се и сътрудничество на равнище Европейски съюз, както на стратегическо, така и на техническо равнище. Директивите установяват минимални изисквания за сигурността на мрежите и информационните системи в ключови сектори на икономиката, като например енергетиката, транспорта, финансите и здравеопазването.

Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета се фокусира върху засилването на киберсигурността в Европейския съюз, като се прилага към нововъзникващите заплахи и уязвимости, свързани с цифровизацията на обществото и икономиката. Тя е част от по-широката стратегия за засилване на киберсигурността и интегрира усилията за осигуряване на защитата на основни мрежи и цифрови инфраструктури в Европейския съюз. Директивата, бидейки част от по-широката Стратегия за цифрова сигурност и защита на критичната инфраструктура, отразява нарастващата необходимост от усилена защита срещу все по-сложните и интензивни киберзаплахи.

Разработката може да бъде използвана и в други научни сфери, като например техническата и сферата на информационните технологии за постигане на по-голяма яснота по отношение на изискванията за киберсигурност, което ще подпомогне и за подобряването на техническите средства за повишаване на нейното ниво.

За всяка то анализираните в дисертационния труд директиви е предоставена информация по отношение на транспонирането й в Българското законодателство.

5. Заключение

В последния раздел е направено заключение. В него е отбелязано, че е направено проучване на актовете на Европейския съюз в областта на киберсигурността, като основният подход при структуриране на дисертационния труд е преглед поотделно на всеки нормативен акт на Европейския съюз, свързан с киберсигурността, кратко представяне на съдържанието му и където е възможно съпоставка между няколко версии на същия акт и анализ на същия. По този начин е направен един цялостен преглед на законодателството на Европейския съюз по отношение на киберсигурността. Изяснена е цялостната картина в различните сфери, свързани с нея, което ще спомогне за по-лесно подобряване на качеството на нормативните актове при бъдещи изменения. Това улеснява бъдещите изменения и промени на нормативните актове както на Европейския съюз, така и на държавите-членки поотделно. Изследването е ограничено в периода след 2000 г. Това се налага поради големият брой нормативни актове и неактуалността на остарелите или отменени, датирани преди 2000 г.

Въз основа на направения анализ са изведени общи предложения *de lege ferenda* за изменение и усъвършенстване на нормативната уредба на Европейския съюз в областта на киберсигурността.

III. Теоретични и практически приносни моменти на дисертационното изследване

С настоящата разработка за първи път в специализираната литература в България е направени цялостно проучване, предаване на съдържанието в синтезиран вид и анализ на релевантното вторично право на Европейския съюз по отношение на киберсигурността. Подробно са анализирани всички източници - регламенти, директиви, стратегии на Европейския съюз.

В дисертационния труд са включени и анализирани шест стратегии на Европейския съюз, осем регламента и единадесет директиви. Тяхното съдържание е предадено в синтезиран вид, което спомага за по-доброто му разбиране дори и от неюристи и специалисти в областта. Определени са основните проблеми и слабости във включените нормативни актове – направен е анализ въз основа на прилагането им в отделните държави-членки и направени изменения в тях от страна на Съюза. За всеки нормативен акт са дадени са предложения *de lege ferenda*, които могат да бъдат използвани като възможни перспективи за подобряване и актуализиране на нормативните актове и стратегии на Европейския съюз в сферата на киберсигурността.

В разработката е направена съпоставка между стратегиите за киберсигурност на Европейския съюз от 2013 година и от 2020 година. Другите разгледани стратегии са Стратегията на Европейския съюз за Съюза на сигурност и Стратегията за цифровизиране на финансовите услуги в Европейския съюз, в които специално внимание е обърнато на текстовете, свързани с киберсигурността. Направен е сравнителен анализ между стратегията за единен цифров пазар на Европейския съюз от 2015 г. и актуализираната й през 2025 г. версия.

Включена е проблематиката за електронната идентификация и удостоверителни услуги при електронни транзакции на вътрешния пазар. Разгледан е Регламента за електронна идентификация и удостоверителни услуги (eIDAS). Разгледана е и защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Европейския съюз. В дисертационния труд е включен анализ на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на

личните данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните). Разгледана е и проблематиката за защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза, която намира своята нормативна рамка в Регламент (ЕС) 2018/1725 на Европейския парламент относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни.

Въпросът за сътрудничеството между националните органи, отговорни за законодателството за защита на потребителите е разгледан, чрез анализа на Регламент (ЕС) 2017/2394 на Европейския парламент и на Съвета, относно сътрудничеството между националните органи, отговорни за прилагането на законодателството за защита на потребителите и за отмяна на Регламент (ЕО) № 2006/2004.

Подробно е разгледан Регламент (ЕС) 2019/796 за установяването на обща рамка за управление на киберзаплахите и реагиране в случай на кибератаки.

Акт за киберсигурността е съкратеното наименование на следващия регламент, включен в дисертацията, а именно Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 и Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта

на киберсигурността и на мрежа от национални координационни центрове. Анализиран е и Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011, известен като DORA (Digital Operational Resilience Act).

Разгледана е Директивата, свързана с обработка на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации.

Съдържанието на Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите е предадено в синтезиран вид и са определени основни проблеми и слабости в нея. Анализирана е и Директива 2009/136/ЕО, основната цел на която е да осигури по-добра защита на правата на потребителите, да укрепи доверието в цифровите услуги и да въведе ясни правила за обработката на лични данни в сектора на електронните съобщения.

В дисертационния труд е анализирана и правната уредба на атаките срещу информационните системи е уредена в Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на

Съвета, както и Директива 2007/64/ЕО на Европейския парламент и на Съвета от 13 ноември 2007 г. относно платежните услуги. Разгледана е и правната уредба на процедурата за предоставяне на информация в сферата на техническите регламенти и правила относно услугите на информационното общество, която е залегнала в Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета.

Разгледана в контекста на киберсигурността е проблематиката за полицейско и съдебно сътрудничество в областта на защитата на личните данни е регламентирано чрез Директива (ЕС) 2016/680 на Европейския парламент, която цели да установи баланса между нуждата от ефективно правоприлагане и правото на неприкосновеност на личния живот.

Анализирани са и изисквания за достъпност на уебсайтовете и мобилните приложения на организациите от обществения сектор са поставени с Директива (ЕС) 2016/2102 на Европейския парламент и на Съвета.

Направено е сравнение между Директива (ЕС) 2016/1148 и актуализираната ѝ версия - Директива (ЕС) 2022/2555, в които е регламентирана правната уредба на мерките за високо общо ниво на сигурност на мрежите и информационните системи в Съюза и е разгледана е Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета, която се фокусира върху засилването на киберсигурността в Европейския съюз, като се прилага към нововъзникващите заплахи и уязвимости, свързани с цифровизацията на обществото и икономиката.

Разработката може да бъде използвана и в други научни сфери, като например техническата и сферата на информационните технологии за постигане на по-голяма яснота по отношение на изискванията за

киберсигурност, което ще подпомогне и за подобряването на техническите средства за повишаване на нейното ниво.

За всяка от анализираните в дисертационния труд директиви е предоставена информация по отношение на транспонирането ѝ в Българското законодателство.

Въз основа на направения анализ на включените в дисертационния труд нормативни актове са изведени и общи предложения *de lege ferenda* за изменение и усъвършенстване на нормативната уредба на Европейския съюз в областта на киберсигурността:

1. Актуализиране на правната рамка спрямо новите технологии

Сегашната нормативна база е създадена в контекст, в който мобилните плащания, блокчейн или цифровите валути не са били широко разпространени. В резултат, законодателството не предвижда специфични механизми за защита на потребителите и бизнеса в тези нови области. Това създава несигурност, възможности за злоупотреби и неравнопоставеност между традиционните и иновативните доставчици. Европейския съюз следва да актуализира правната си рамка в по-малки времеви интервали и едновременно с това да отчита възникналите нови технологии и практики. Това може да стане чрез периодични прегледи на законодателството на Европейския съюз, публични консултации с бизнеса и потребителските организации, както и чрез създаване на експертни панели по дигитализация. Като конкретно предложение *de lege ferenda* в близко бъдеще, може да се предложи в политиките за киберзащита да бъдат обхванати и квантовите компютри и заплахите за сигурността, които произлизат от тях. Квантовите компютри ще могат да извършват множество изчисления за кратък период от време. Алгоритмите за криптиране, които се използват в момента ще бъдат

счупени, благодарение на използването на квантови компютри . Това е само един малък пример за какво биха могли да бъдат използвани квантовите компютри, но употребата им вероятно няма да се ограничи само дотук, затова Европейският съюз следва да се фокусира върху начините за смекчаване и ограничаване на последиците, особено краткосрочните такива, произтичащи от квантовите предизвикателства пред киберсигурността. С развитието на квантовите компютри, от страна на Европейския съюз ще са необходими действия за запълване на пропуски в киберсигурността, които могат да бъдат използвани като вектор на атака и да се гарантира, че всички държави-членки са еднакво устойчиви на квантови кибератаки.

2. Ограничаване на нееднаквото прилагане в държавите-членки

Нееднаквото прилагане най-вече на директивите в различните държави-членки се оказва проблем. В момента държавите-членки разполагат със значителна свобода при транспонирането на директивите, което води до различни национални практики. Тези различия затрудняват координацията и сътрудничеството в областта на киберсигурността, водят до правна несигурност и до различна степен за защита срещу кибератаки. Европейския съюз следва да въведе по-строги минимални стандарти и да изисква унифицирани правила по въпросите на киберсигурността. Освен това, може да се обмисли общ механизъм за мониторинг и коригиране на несъответствията в прилагането, за да се гарантира еднакво високо общо ниво на киберсигурност за всички държави-членки.

3. Преодоляване на правната несигурност

Сложността на новите технологии изисква ясно дефиниране на ролите и отговорностите на различните участници – банки, финтех компании, технологични платформи. При липса на такава яснота се създават конфликти

между доставчиците и потребителите, а съдебните процедури стават по-трудни и бавни. Европейския съюз следва да се ориентира към изменения в нормативната си уредба, които да включват конкретни дефиниции за ключови понятия (например „услуга по мобилни плащания“, „доставчик на платформа“) и да се определят ясни отговорности. Това ще намали правната несигурност и ще повиши предвидимостта на пазара.

4. Повишаване на ефективността на санкциите

Когато санкциите за нарушения са твърде ниски, те не изпълняват превантивна функция и не мотивират доставчиците да спазват правилата. Това води до различни нива на защита за потребителите в различните държави. В някои от разгледаните в дисертационния труд нормативните актове на Европейския съюз размерът на санкциите е конкретизиран изрично и такава конкретика следва да бъде добавена и в актовете, в които тя липсва. Също така може да се установят минимални нива на санкции на равнище Европейски съюз и да се въведе общ механизъм за тяхното ефективно прилагане. Това ще гарантира по-справедливи условия и ще възпре нелоялните практики.

5. Укрепване на административния и експертен капацитет

Много национални органи страдат от недостиг на ресурси и експертиза, което ограничава ефективността на техните действия. Това води до забавени разследвания, пропуснати нарушения и недостатъчен контрол върху сектора. За решаване на този проблем, Европейския съюз следва да осигури общоевропейско финансиране за засилване на капацитета, включително програми за обучение на кадри в сферата на киберсигурността, обмен на експерти и създаване на специализирани звена за дигитални престъпления и финансови иновации, като всичко това може да бъде регламентирано с подходящ акт на Съюза.

6. Засилване на международното сътрудничество

Международното сътрудничество е важен аспект и се появява все повече и повече в нормативната уредба на Европейския съюз. Киберпрестъпленията и финансовите измами често имат трансграничен характер и изискват координация отвъд границите на Съюза. Липсата на ефективно сътрудничество с трети държави и международни организации затруднява разследванията. Европейския съюз следва да повиши работата си за постигане на по-тясна мрежа за обмен на информация между националните органи и международните институции. Европейския съюз може да играе водеща роля в световен мащаб в създаването на глобални стандарти и механизми за сътрудничество в областта на информационните технологии и киберсигурността, като за целта може да се започне с разработване и утвърждаване на специална правна рамка.

7. Повишаване на дигиталната грамотност и обществената осведоменост

Въпреки напредъка в технологичното развитие и въвеждането на различни стандарти за сигурност, човешкият фактор остава най-уязвимото звено в системата за киберсигурност. Голям процент от успешните кибератаки – включително фишинг кампании, измами чрез социално инженерство, зловредни прикачени файлове или подвеждащи линкове – разчитат на липсата на достатъчна дигитална култура у потребителите. Недостатъчната информираност води до подценяване на рисковете, несъобразено поведение онлайн и ниска чувствителност към съмнителни действия, което улеснява престъпниците. Това засяга не само отделните граждани, но и бизнеса, особено малките и средни предприятия, където често липсват вътрешни екипи по киберсигурност. В същото време, липсата на целенасочени образователни

програми за служители в публичната администрация създава риск от пробиви и изтичане на данни на институционално ниво. В доста от нормативните актове е засегнат въпроса за обучението, но би следвало да се наблегне на този аспект и да се регламентира по подходящ начин с нормативен акт на Европейския съюз. В него може да залегнат изисквания за регулярно провеждане на образователни кампании, насочени към различни целеви групи – ученици, студенти, работещи в частния и публичния сектор, възрастни хора. Също така може да се въведе изискване за държавите-членки да интегрират дигиталната грамотност в образователните програми на всички нива – от началното училище до университетите, със специален акцент върху онлайн сигурността, защита на личните данни и отговорното използване на технологии. Обучението може да бъде подпомогнато и със създаване на национални и европейски платформи за обучение, предлагащи достъпни и практични курсове за граждани и бизнес (онлайн модули, интерактивни симулации, тестове за повишаване на осведомеността).

Не на последно място, важна роля играят и информационните кампании. Въвеждането на изискване за провеждане на регулярни информационни кампании, съпроводени с конкретни съвети за защита – например как да се разпознават фишинг атаки, как да се управляват пароли или как да се реагира при съмнение за измама, ще спомогне за повишаване на киберграмотността сред гражданите на държавите-членки. Повишаването на дигиталната грамотност ще доведе до по-устойчиво общество, в което гражданите и организациите са по-малко уязвими на кибератаки. Това ще намали броя на инцидентите, ще облекчи натиска върху институциите и ще повиши доверието в дигиталните услуги и иновациите. В дългосрочен план, изграждането на култура на киберсигурност ще бъде един от най-важните фактори за успешното развитие на единния цифров пазар в Европейския съюз.

IV. Публикации по темата на дисертационния труд

Ойсолова, М., Транспониране на Директива (ЕС) 2016/1148 в българското законодателство, в: Сборник с доклади от XI национална конференция на докторантите в областта на правните науки (2021г.), с. 360.

Ойсолова, М., Акт за киберсигурността, в: Сборник с доклади от XII национална конференция на докторантите в областта на правните науки (2022г.) с. 240.

Ойсолова, М., Съпоставка между директивите 2016/1148 и 2022/2555 на Европейския парламент и на Съвета (под печат)