УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНЛОГИИ

РЕЦЕНЗИЯ

от проф. д.н. Стоян Георгиев Денчев, научна специалност Професор - 9.1. Национална сигурност, Професор - 3.5. Обществени комуникации и информационни науки

на дисертационен труд за присъждане на образователната и научна степен „доктор“
по: област на висше образование 3. Социални, стопански и правни науки
професионално направление 3.6. Право
докторска програма Международно право и международни отношения

Автор: **Маргарита Евгениева Ойсолова**

Тема: „Регламентация на киберсигурността в Европейския съюз – проблеми и перспективи”

Научен ръководител: **проф. д-р Ирена Цонева Илиева – Институт за държавата и правото при Българската академия на науките**

30.10. 2025 г.
София

I. Общо представяне на процедурата

Със заповед № РД 09-68 от 25.09.2025 г. на Директора на Института за държавата и правото при Българската академия на науките (ИДП - БАН) съм определен за член на научното жури за осигуряване на процедура за защита на дисертационен труд на тема „Регламентация на киберсигурността в Европейския съюз – проблеми и перспективи" за придобиване на образователната и научна степен „**доктор**" в област на висше образование 3. Социални, стопански и правни науки професионално направление 3.6. Право, докторска програма Международно право и международни отношения.

Автор на дисертационния труд е Маргарита Евгениева Ойсолова – докторант, 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-09-23/29.01.2021 г. на директора на ИДП при БАН.

Представеният от Маргарита Ойсолова комплект материали на хартиен носител е в съответствие с изискванията на Закона за развитие на академичния състав в Република България (ЗРАСРБ), Правилника за прилагане на ЗРАСРБ и допълнителните изисквания според Правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности в Българската академия на науките и Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности в Института за държавата и правото при Българската академия на науките.

Докторантът е приложил общо три броя публикации по темата на дисертационния труд.

II. Кратки биографични данни за докторанта

Маргарита Евгениева Ойсолова е завършила средното си образование през 2005 г. в 31-во Средно училище за чужди езици и мениджмънт „Иван Вазов" в

гр. София. В периода 2013 – 2017 г. е изучавала Информационна сигурност в Университета по библиотекознание и информационни технологии, от където има придобита бакалавърска степен. От 2018 г. има магистърска степен по Информационна сигурност, придобита в Университета по библиотекознание и информационни технологии.

Работила е последователно като редактор на сп. „Правна мисъл“ и администратор на компютри и мрежи в Института за държавата и правото при БАН (2013 – 2018), както и като експерт по мрежова и информационна сигурност I степен в Държавна агенция „Електронно управление“ (2018 – 2021). От 2021 г. до момента работи като експерт по мрежова и информационна сигурност I степен в Национална агенция за приходите.

III. Актуалност на тематиката

Дисертационният труд е посветен на проблемите, свързани с недостатъчното ниво на киберсигурност, съчетано с нарастваща зависимост на бизнеса и живота от информационните и комуникационните технологии и Интернет. Дефицитите или липсата на сигурност са предпоставки за злонамерени атаки, водещи до инциденти, свързани с киберсигурността. Те подкопават доверието на потребителите в технологиите, мрежите и услугите, като по този начин ограничават способностите им да се възползват пълноценно от възможностите, които предлагат съвременните информационни и комуникационни технологии. А мрежите и информационните системи са тези, които днес значително улесняват комуникацията и дейностите във всички сфери на обществения живот, стимулират икономическия растеж и човешкото развитие. В рамките на Европейския съюз (ЕС) те стоят в основата на постигането на цифровия единен пазар.

Като основен аналитичен фокус и предмет на труда са поставени за разглеждане усилията на ЕС през последните години за повишаване на нивото на мрежова и информационна сигурност, чрез приемане на стратегии за киберсигурност и законодателство. Всички те са насочени към защита на

информационните и комуникационните технологии, въвеждането на нови технически решения за защита, както и формулирането на етични изисквания и стандарти за поведение в киберсредата.

Водещите изследователски задачи пред труда: са представяне в синтезиран вид и анализ на основните стратегически и нормативни актове на ЕС в сферата на киберсигурността; набелязване на основни проблемни области в очертаната стратегическа и правна рамка и 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. Във връзка с горните задачи е формулиран и предмета и целите на труда: да се направи цялостен преглед на актуалната регламентация на киберсигурността според действащото право на Европейския съюз.

IV. Познаване на проблема

Докторантът е демонстрирал задълбочено познаване на проблемите, които са поставени в центъра на дисертационния труд. Още в неговото начало са разгледани четирите водещи стратегически документа на ЕС, които включват стратегиите за киберсигурност от 2013 и 2020 г., Стратегията на ЕС за Съюза на сигурност и Стратегията за цифровизиране на финансовите услуги в Европейския съюз. Ролята на съюзните стратегически документи е ключова, защото освен, че те определят посоката и приоритетите за развитие в тази област на обществения живот, задават рамката за дългосрочно планиране и управление.

В Стратегията на Европейския съюз за киберсигурност са изяснени ролите и отговорностите и са определени необходимите действия за защита и насърчаване на правата на гражданите, като основната цел е онлайн пространството в Съюза да се превърне в една по-безопасна среда. Освен генералните принципи и приоритети в нея са предвидени и способите за запълване на празноти по отношение на националния капацитет на държавите членки, координацията в случай на инциденти с трансграничен характер, както и участието на частния сектор в постигане на подготвеност за евентуални

киберкризи. Като важни елементи за подобряване на законодателството в сферата са посочени необходимостта да се установят общи минимални изисквания за киберсигурност на национално равнище.

През 2020 г. Стратегията на Европейския съюз за киберсигурност е преразгледана и актуализирана, като се наблюдава значителна промяна чрез смяна на подходите от цялостен към интегриран. В нея по нов начин ясно са конкретизирани заплахите в отделните сфери икономическа, политическа и военна и е предложен набор от конкретни мерки за подобряване на нивото на киберсигурност.

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. Киберсигурността е един от централните елементи на стратегията. 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.

Стратегията е актуализирана през 2025 г. като отразява нуждите на бързо развиващата се цифрова икономика и настъпилите социални промени. Целта е да се укрепи конкурентоспособността на Европейския съюз, да се насърчат 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.

В Стратегията на Европейския съюз за Съюза на сигурност се очертават приоритетните действия, инструменти и мерки за постигане на по-високо ниво на киберсигурност, както във физическия, така и в цифровия свят, а така също и сред всички слоеве на обществото. В нея 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 Европейският съюз може да предвижда и да дава отговор на променящите се заплахи.

Стратегията за цифровизиране на финансовите услуги 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.

При прегледа на *основните регламенти* на ЕС в сферата на киберсигурността е разгледана проблематиката, отнасяща се до електронната идентификация и удостоверителните услуги при електронни транзакции на вътрешния пазар. Връзката между киберсигурността и управлението на националната електронна идентификация е от съществено значение, защото всяка електронна транзакция ще използва идентичността и сигурността при обмена на информация. Друг важен проблем, относим към киберсигурността е защитата на физическите лица при обработването на личните данни. В тази връзка е анализирана защитата на физическите лица при обработването на лични данни от институциите, органите, службите и агенциите на Европейския съюз.

Въпросът за сътрудничеството между националните органи, отговорни за законодателството за защита на потребителите, също е част от дисертационното изследване. Целта на сътрудничеството между националните органи, отговорни за прилагането на законодателството за защита на потребителите е да предпазва потребителите от трансгранични нарушения на законодателството на Европейския съюз. Последователно са проучени правнообвързващите съюзни актове, касаещи установяването на обща рамка за управление на киберзаплахите и реагиране в случай на кибератаки и Актът за киберсигурността. Те предвиждат ограничителни мерки, които могат да бъдат приложени срещу лица или организации, замесени в кибератаки, като финансови санкции, забрани за влизане и замразяване на активи. Установени са и процедури за координация и

сътрудничество между държавите членки на ЕС в случай на кибератака или заплаха от такава. Основната цел е да се постигне високо ниво на киберсигурност, киберустойчивост и доверие в Европейския съюз и държавите членки. В тези актове са уредени целите, задачите и функциите на основните институционални структури, отговорни за съюзната киберсигурност, каквито са Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове и Агенцията на Европейския съюз за киберсигурност, които са анализирани в детайли.

Отделна глава от труда е посветена на *основните директиви* в областта на киберсигурността. Аналитично представени са директивите, отнасящи се до обработката на лични данни и защитата на правото на неприкосновеност на личния живот в сектора на електронните комуникации, сътрудничеството между националните органи, отговорни за прилагане на законодателството за защита на потребителите и защитата на правата на потребителите. Изследвана е и правната уредба на атаките срещу информационните системи. Анализът обхваща и директивата относно платежните услуги във вътрешния пазар на Европейския съюз, която цели да хармонизира правилата и стандартите за платежните услуги във вътрешния пазар, правната уредба на процедурата за предоставяне на информация в сферата на техническите регламенти и правила относно услугите на информационното общество, правната рамка на полицейското и съдебно сътрудничество в областта на защитата на личните данни и др. За всяка от проучените в дисертационния труд директиви е предоставена актуална информация относно етапа, на който се намира нейното транспониране в българското законодателство.

V. Методика на изследването

Докторантът е приложил възможно най-подходящия инструментариум за провеждане на изследването, какъвто е интердисциплинарният, който включва проучване и анализ на документи, като са събрани, систематизирани и проучени

основните стратегии, регламенти и директиви на Европейския съюз в сферата на киберсигурността.

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, попадащи в предмета на дисертационния труд. Използваните научноизследователски методи за решаване на поставените пред научното изследване задачи, включват:

1. Наблюдения, анализи и проучвания на формирането и развитието на регулаторната рамка в Европейския съюз в областта на киберсигурността, които са послужили за извеждането на основните заключенията в работата;

2. Ретроспективен анализ, използван за проследяване и отчитане развитието на възгледите, идеите, технологиите и законодателството на Европейския съюз в сферата на киберсигурността;

3. Методът на интервюто, чрез събеседване с експерти по време на участие в научни конференции и семинари в процеса на писане на настоящата разработка, чрез който е постигнат обмен на мнения и опит с сферата на киберсигурността;

4. Формално-логически подходи като синтез и дедуктивен метод. Синтезът е приложен за различните типове нормативни документи на Европейския съюз в сферата на киберсигурността. Дедуктивният метод е използван за оценка на относимостта на нормативните актове на Европейския съюз към киберсигурността и това дали те изцяло или частично съдържат релевантни текстове.

В процеса на провеждане на дисертационното изследване, освен актовете на Европейския съюз в областта на киберсигурността, са анализирани и 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 и където е възможно съпоставка между няколко версии на акта, заедно с негов анализ.

VI. Характеристика и оценка на дисертационния труд

Дисертационното изследване 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.

Първата глава на дисертацията е озаглавена „Стратегически документи“. В нея са разгледани четирите ключови стратегически документа на Европейския съюз в областта на киберсигурността цифровизирането на финансовите услуги и т.н. Изходните позиции, заложени в тези най-важни актове на Съюза са, че 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. Това е причината ЕС да реши, че е от изключителна важност да се започне работа за постигане на високо общо ниво на киберсигурност, което има за резултат приемането на Стратегия на Европейския съюз за киберсигурност. В нея са залегнали принципите и стратегическите насоки за подобряване на киберсигурността в Европейския съюз. 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 е разработена, според изпълнените задачи на предходната Стратегия за киберсигурност.

Стратегията за единен цифров пазар на Европейския съюз от 2015 г. освен киберсигурността обхваща и регулацията на изкуствения интелект (ИИ) 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 ИИ 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.

Стратегията на ЕС за Съюза на сигурност предвижда мерки срещу кибератаките, които са голям проблем за сигурността. Те стават все по-чести и усъвършенствани. Освен техническите мерки, Стратегията поставя акцент и върху изграждането на култура на киберсигурност и киберхигиена сред гражданите, бизнеса и държавните институции.

Стратегията за цифровизиране на финансовите услуги в Европейския съюз 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.

Втората глава от дисертационното изследване съдържа преглед на основните регламенти на ЕС в сферата на киберсигурността. В нея последователно е разгледана проблематиката, отнасяща се до електронната идентификация и удостоверителните услуги при електронни транзакции на вътрешния пазар и защитата на физическите лица във връзка с обработването на лични данни. Като важен аспект от нея е анализирана и защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Европейския съюз.

На следващо място е представена правната уредба на сътрудничеството между националните органи, отговорни за законодателството за защита на потребителите също е част от дисертационното изследване. Последователно са проучени правнообвързващите съюзни актове, относно установяването на обща рамка за управление на киберзаплахите и реагиране в случай на кибератаки и

Актът за киберсигурността. Те предвиждат ограничителни мерки, които могат да бъдат приложени срещу лица или организации, замесени в кибератаки, като финансови санкции, забрани за влизане и замразяване на активи. Изследвани са и установените процедури за координация и сътрудничество между държавите-членки на Европейския съюз в случай на кибератака или заплаха от такава. В тези актове са уредени целите, задачите и функциите на основните структури, отговорни за съюзната киберсигурност, каквито са Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове и Агенцията на Европейския съюз за киберсигурност, които са анализирани в детайли.

Третата глава от труда прави аналитичен обзор на основните директиви в областта на киберсигурността. Представени са директивите, отнасящи се до обработката на лични данни и защитата на правото на неприкосновеност на личния живот в сектора на електронните комуникации, сътрудничеството между националните органи, отговорни за прилагане на законодателството за защита на потребителите. Задълбочено е проучена и правната материя, отнасяща се до атаките срещу информационните системи, правната уредба на процедурата за предоставяне на информация в сферата на техническите регламенти, правната рамка на полицейското и съдебно сътрудничество в областта на защитата на личните данни и др.

VII. Приноси и значимост на разработката за науката и практиката

Основният приносен момент на дисертационния труд се изразява в това, че той представлява един от първите опити в българската правна литература за цялостно проучване и анализ на вторичното право на Европейския съюз, касаещо киберсигурността. Отделно от това са подробно анализирани и най-важните стратегически документи на ЕС в същата област.

За всеки от изследваните нормативни актове са дадени 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. Такива са предложенията за:

1. Актуализиране на правната рамка спрямо новите технологии. Действащата нормативна база е създадена в контекст, в който мобилните плащания, блокчейн или цифровите валути не са били широко разпространени. В резултат от това, 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.

Конкретното предложение de lege ferenda е в близко бъдеще 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.

2. Ограничаване на нееднаквото прилагане в държавите членки. Непълното и непоследователно прилагане на директивите в различните държави членки е проблем. То затруднява координацията и сътрудничеството в областта на киберсигурността, води до правна несигурност и до различна степен на защита срещу кибератаки.

Препоръката е ЕС да въведе по-строги минимални стандарти и да изисква унифицирани правила по въпросите на киберсигурността. Особено ценно е предложението да се обмисли въвеждането на 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. Европейският съюз следва да

приема правна уредба, която да включва конкретни дефиниции на ключовите понятия, което да намали правната несигурност и да 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. В някои от разгледаните в дисертационния труд нормативни актове на Европейския съюз размерът на санкциите е конкретизиран изрично. Такава конкретика следва да бъде добавена и в актовете, в които тя липсва, както и да се установят минимални нива на санкции на ниво Европейски съюз и да се въведе общ механизъм за тяхното ефективно прилагане.

5. Укрепване на административния и експертен капацитет. Много национални органи страдат от недостиг на ресурси и експертиза, което води до забавени разследвания, пропуснати нарушения и недостатъчен контрол върху сектора. За решаването на този проблем дисертантът препоръчва Европейският съюз 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. Липсата на ефективно сътрудничество с трети държави и международни организации затруднява разследванията, а киберпрестъпленията и финансовите измами често имат трансграничен характер. Европейският съюз следва да се насочи към постигане на по-тясна мрежа за обмен на информация между националните органи и международните институции.

Особено значима е препоръката ЕС да започне 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. Недостатъчната информираност води до подценяване на рисковете, несъобразено онлайн поведение 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 доста от нормативните актове е засегнат въпроса за обучението. Предложението, отправено от докторанта, е да се приеме нормативен акт на Европейския съюз, в който да залегнат изисквания за регулярно провеждане на образователни кампании, насочени към различни целеви групи – ученици, студенти, работещи в частния и публичния сектор, възрастни хора. На следващо място, могат да се въведат изисквания за държавите членки да интегрират дигиталната грамотност в образователните програми на всички нива – от началното училище до университетите, със специален акцент върху онлайн сигурността, защитата на личните данни и отговорното използване на технологии.

VIII. Преценка на публикациите по дисертационния труд

Публикациите, с които докторантът участва в процедурата, по подобие на самия дисертационен труд, се отличават с оригиналност, включват нестандартен прочит на някои от основните концепции и теории и прилагане на типичния за автора разнороден инструментариум за изследване на материята.

IX. Лично участие на докторанта

Демонстрираният оригинален подход и почерк на докторанта в проведеното дисертационно изследване са безспорно доказателство за неговото лично

участие при разработването му и постигането на резултатите, както и за личната му заслуга при формулирането на научните приноси.

X. Автореферат

Представеният автореферат като съдържание и качество е разработен изцяло според изискванията на съответните правилници и отразява основните резултати, постигнати в дисертацията.

XI. Критични бележки и препоръки за бъдещо използване на дисертационните приноси и резултати

Според мен, някои от предложенията de lege ferenda, направени от автора на дисертационния труд, са твърде колебливи. Това са всички онези препоръки, дадени като потенциални възможности, алтернативи или като евентуални подходи за подобрение. Считам, че предвид направения задълбочен анализ и постигнатата солидна аргументация на основните тези на труда, тези предложения биха могли да бъдат поставени по-твърдо и амбициозно.

В тази връзка основната препоръка, която може да бъде отправена е при прилагането на същите подходи и методи на работа авторът да продължи своите научни търсения и да се опита да предложи свои собствени формулировки на конкретни механизми или норми, които да залегнат при бъдещи преразглеждания и актуализации на основните стратегии и нормативни актове на ЕС в областта на киберсигурността. Тези негови нови публикации по темата следва да бъдат насочени за публикуване в издания, реферирани и индексирани в световноизвестни бази данни като Scopus, Web of Science и др.

ЗАКЛЮЧЕНИЕ

Дисертационният труд съдържа научни, научно-приложни и приложни резултати, които представляват оригинален принос в науката и отговарят на всички изисквания на ЗРАСРБ, Правилника за прилагане на ЗРАСРБ и допълнителните изисквания според Правилника за условията и реда за

придобиване на научни степени и за заемане на академични длъжности в Българската академия на науките и Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности в Института за държавата и правото при Българската академия на науките.

Дисертационният труд показва, че докторантът Маргарита Евгениева Ойсолова притежава задълбочени теоретични знания и професионални умения по научната специалност право на ЕС, международно право и международни отношения като демонстрира качества и умения за самостоятелно провеждане на научно изследване.

Поради гореизложеното, убедено давам своята **ПОЛОЖИТЕЛНА ОЦЕНКА** за проведеното изследване, представено от рецензираните по-горе дисертационен труд, автореферат, постигнати резултати и приноси, и предлагам на почитаемото научно жури да присъди образователната и научна степен „доктор“ на **Маргарита Евгениева Ойсолова** в област на висше образование: 3. Социални, стопански и правни науки, професионално направление 3.6. Право, докторска програма Международно право и международни отношения.

30.10.2025 г. Рецензент: .....

Проф. д. ик. н. Стоян Денчев

UNIVERSITY OF LIBRARY STUDIES AND INFORMATION TECHNOLOGIES

REVIEW

by Prof. DSc. Stoyan Denchev,
Scientific specialization: Professor – 9.1. National Security; Professor – 3.5. Public Communications and Information Sciences

of the dissertation submitted for the award of the educational and scientific degree "Doctor"

in: field of higher education 3. Social, Economic and Legal Sciences
professional field 3.6. Law
doctoral program International Law and International Relations

Author: Margarita Evgenieva Oysolova

Title: "Regulation of Cybersecurity in the European Union – Problems and Perspectives"

Scientific supervisor: Prof. Dr. Irena Tsoneva Ilieva – Institute for State and Law, Bulgarian Academy of Sciences

October 30, 2025

Sofia

I. General Overview of the Procedure

By Order No. 09-68 dated September 25, 2025, issued by the Director of the Institute for the State and the Law of the Bulgarian Academy of Sciences (ISL – BAS), I was appointed as a member of the scientific jury responsible for the defense procedure of the dissertation entitled "Regulation of Cybersecurity in the European Union – Problems and Perspectives", submitted for the acquisition of the educational and scientific degree "Doctor" in the field of higher education 3. Social, Economic and Legal Sciences, professional field 3.6. Law, doctoral program International Law and International Relations.

The author of the dissertation is Margarita Evgenieva Oysolova, a doctoral student enrolled in a part-time PhD program in "International Law and International Relations", within the field of higher education 3. Social, Economic and Legal Sciences, professional field code 3.6. Law, in accordance with Order No. РД-09-23/29.01.2021 issued by the Director of the ISL at BAS.

The set of materials submitted by Margarita Oysolova in hard copy form complies with the requirements of the Law on the Development of the Academic Staff in the Republic of Bulgaria (LDASRB), the Implementing Regulations of the LDASRB, as well as the additional requirements set forth in the Regulations on the Conditions and Procedures for the Acquisition of Scientific Degrees and for Holding Academic Positions at the Bulgarian Academy of Sciences, and the Regulations on the Conditions and Procedures for the Acquisition of Scientific Degrees and for Holding Academic Positions at the Institute for State and Law at BAS.

The doctoral candidate has submitted a total of three publications related to the topic of her dissertation.

II. Brief Biographical Data of the Doctoral Candidate

Margarita Evgenieva Oysolova completed her secondary education in 2005 at the 31st Secondary School of Foreign Languages and Management "Ivan Vazov" in Sofia. Between 2013 and 2017, she studied Information Security at the University

of Library Studies and Information Technologies (ULSIT), where she obtained her Bachelor's degree. In 2018, she received her Master's degree in Information Security from the same university.

Her professional experience includes consecutive positions as Editor of the journal *Legal Thought* and Computer and Network Administrator at the Institute for State and Law at the Bulgarian Academy of Sciences (2013–2018), followed by employment as a Network and Information Security Expert, Grade I, at the State e-Government Agency (2018–2021). Since 2021, she has been working as a Network and Information Security Expert, Grade I, at the National Revenue Agency.

III. Relevance of the Topic

The dissertation is dedicated to the problems related to the insufficient level of cybersecurity, combined with the growing dependence of business and life on information and communication technologies and the Internet. Deficits or lack of security are prerequisites for malicious attacks leading to incidents related to cybersecurity. They undermine users' trust in technologies, networks and services, thus limiting their ability to fully benefit from the opportunities offered by modern information and communication technologies. And networks and information systems are those that today significantly facilitate communication and activities in all spheres of public life, stimulate economic growth and human development. Within the European Union (EU), they are the basis for achieving the digital single market.

As the main analytical focus and subject of the work, the EU's efforts in recent years to increase the level of network and information security, through the adoption of cybersecurity strategies and legislation, are considered. All of them are aimed at protecting information and communication technologies, introducing new technical solutions for protection, as well as formulating ethical requirements and standards of behavior in the cyber environment.

The leading research tasks of the work are: a synthesised presentation and analysis of the main strategic and regulatory acts of the EU in the field of

cybersecurity; identifying key problem areas in the outlined strategic and legal framework and preparing de lege ferenda proposals as possible perspectives for improving and updating the regulatory acts and strategies of the European Union in the field of cybersecurity. In connection with the above tasks, the subject and objectives of the work are also formulated: to conduct a comprehensive review of the current regulation of cybersecurity according to the current law of the European Union.

IV. Knowledge of the Subject Matter

The doctoral candidate has demonstrated a thorough understanding of the issues at the heart of the dissertation. At the very beginning, the four leading EU strategic documents are examined, which include the 2013 and 2020 cybersecurity strategies, the EU Security Union Strategy and the Strategy for the Digitalisation of Financial Services in the European Union. The role of EU strategic documents is key, because in addition to setting the direction and priorities for development in this area of public life, they provide the framework for long-term planning and management. The European Union Cybersecurity Strategy clarifies the roles and responsibilities and defines the necessary actions to protect and promote citizens' rights, with the main goal to make the online space in the Union a safer place. In addition to the general principles and priorities, it also provides for ways to fill the gaps in the national capacity of Member States, coordination in the event of cross-border incidents, and the participation of the private sector in achieving preparedness for possible cyber crises. The need to establish common minimum requirements for cybersecurity at national level is indicated as important element for improving the legislation in the field.

In 2020, the European Union's Cybersecurity Strategy was reviewed and updated, with a significant change observed by changing the approaches from comprehensive to an integrated one. It clearly specifies the threats in the separate economic, political and military spheres in a new way and proposes a set of concrete measures to improve the level of cybersecurity.

The European Union's Digital Single Market Strategy of 2015 is an instrument for accelerating the digital transformation, strengthening the internal market and ensuring Europe's competitiveness on a global scale. Cybersecurity is one of the central elements of the strategy. It is based on the belief that only by creating common rules, infrastructures and trust mechanisms the full benefits of digitalisation can be achieved.

The strategy was updated in 2025 to reflect the needs of the rapidly developing digital economy and the social changes that have occurred. The aim is to strengthen the competitiveness of the European Union, to encourage innovation, to remove the remaining barriers to the movement of goods and services and to create a secure, sustainable and accessible digital environment for citizens and businesses.

The European Union Strategy for a Union of Security outlines priority actions, tools and measures to achieve a higher level of cybersecurity, both in the physical and digital worlds, and among all segments of society. It aims to review the Network and Information Systems Directive (which is the main European legislation on cybersecurity) and outlines strategic priorities in the field of cybersecurity to ensure that the European Union can anticipate and respond to evolving threats.

The Strategy for the Digitalisation of Financial Services aims to create an integrated and innovative financial sector that fully exploits the benefits of digital technologies and ensures resilience and protection for all actors. The main objectives of the Strategy include promoting innovation and competition in digital finance, strengthening consumer protection and financial stability, and increasing cyber resilience.

The review of the *main EU regulations* in the field of cybersecurity addresses the issues related to electronic identification and trust services for electronic transactions in the internal market. The link between cybersecurity and national electronic identification management is essential because every electronic transaction will use identity and security in the exchange of information. Another important issue related to cybersecurity is the protection of individuals with regard to the processing of personal data. In this regard, the protection of individuals with

regard to the processing of personal data by the institutions, bodies, offices and agencies of the European Union is analyzed.

The issue of cooperation between national authorities responsible for consumer protection legislation is also part of the dissertation research. The aim of cooperation between national authorities responsible for the implementation of consumer protection legislation is to protect consumers from cross-border infringements of European Union law. The legally binding Union acts concerning the establishment of a common framework for managing cyber threats and responding to cyber attacks and the Cybersecurity Act have been consistently studied. They provide for restrictive measures that can be applied against individuals or organizations involved in cyber attacks, such as financial sanctions, entry bans and asset freezes. Procedures for coordination and cooperation between EU Member States in the event of a cyber-attack or threat thereof have also been established. The main objective is to achieve a high level of cybersecurity, cyber resilience and trust in the European Union and its Member States. These acts regulate the objectives, tasks and functions of the main institutional structures responsible for Union cybersecurity, such as the European Cybersecurity Industrial, Technology and Research Competence Centre and a network of national coordination centres and the European Union Agency for Cybersecurity, which are analysed in detail.

A separate chapter of the work is devoted to the *main directives* in the field of cybersecurity. The directives relating to the processing of personal data and the protection of the right to privacy in the electronic communications sector, cooperation between national authorities responsible for the implementation of consumer protection legislation and the protection of consumer rights are analytically presented. The legal framework for attacks against information systems is also examined. The analysis also covers the Directive on Payment Services in the Internal Market of the European Union, which aims to harmonize the rules and standards for payment services in the internal market, the legal framework of the procedure for providing information in the field of technical regulations and rules on information society services, the legal framework of police and judicial

cooperation in the field of personal data protection, etc. For each of the directives studied in the dissertation, up-to-date information is provided on the stage at which its transposition into Bulgarian legislation is at.

V. Research Methodology

The doctoral student has applied the most appropriate toolkit for conducting the research, which is interdisciplinary, which includes the study and analysis of documents, collecting, systematizing and studying the main strategies, regulations and directives of the European Union in the field of cybersecurity.

The methodology of the research is based on the classical teleological approach for legal sciences for an in-depth analysis of the normative sources in the law of the European Union in the field of cybersecurity. It is supplemented by a critical analysis of modern research falling within the subject of the dissertation work. The scientific research methods used to solve the tasks set for the scientific research include:

1. Observations, analyses and studies of the formation and development of the regulatory framework in the European Union in the field of cybersecurity, which serve to draw the main conclusions in the work;

2. Retrospective analysis is used to track and report the development of views, ideas, technologies and legislation of the European Union in the field of cybersecurity;

3. The interview method, through conversations with experts during participation in scientific conferences and seminars in the process of writing this paper, through which an exchange of opinions and experience with the field of cybersecurity was achieved;

4. Formal-logical approaches such as synthesis and deductive method. The synthesis is applied to the different types of regulatory documents of the European Union in the field of cybersecurity. The deductive method is used to assess the relevance of the regulatory acts of the European Union to cybersecurity and whether they fully or partially contain relevant texts.

In the process of conducting the dissertation research, in addition to the acts of the European Union in the field of cybersecurity, studies and research conducted by the Union bodies were also analyzed. The main approach in structuring the paper is a separate review of each regulatory act of the European Union related to cybersecurity, a brief presentation of its content and, where possible, a comparison between several versions of the act, along with its analysis.

VI. Characteristics and Assessment of the Dissertation

The dissertation research consists of 270 pages, of which 252 pages are the actual presentation, divided into an introduction, three chapters and a conclusion, and the rest are a title page, a list of abbreviations used, terminology used, table of contents, bibliography and Appendix I - List of regulatory acts used in the development, arranged in chronological order.

The first chapter of the dissertation is entitled "Strategic documents". It examines the four key strategic documents of the European Union in the field of cybersecurity, the digitalization of financial services, etc. The starting positions set out in these most important acts of the Union are that cyberspace should be protected from incidents, malicious actions and abuse. The threats are of different nature, therefore it is important to guarantee freedom and safety in cyberspace. This is why the EU decided that it was of utmost importance to start working towards a high common level of cybersecurity, which resulted in the adoption of the European Union Cybersecurity Strategy. It sets out the principles and strategic guidelines for improving cybersecurity in the European Union. Important elements for improving legislation in the field include the need to establish common minimum requirements for cybersecurity at national level. In 2020, the European Union Cybersecurity Strategy was reviewed and updated accordingly, taking into account new trends in cybersecurity and developing the tasks of the previous Cybersecurity Strategy.

The European Union's Digital Single Market Strategy of 2015, in addition to cybersecurity, also covers the regulation of artificial intelligence (AI) through the development of a European Act on Artificial Intelligence. Its aim is to create a legal

framework that both encourages innovation and guarantees the ethical and safe use of AI technologies in accordance with European values and fundamental rights. The Strategy was updated in 2025. It reflects the needs of the rapidly developing digital economy and the social changes brought about by technological progress.

The EU Security Union Strategy provides for measures against cyberattacks, which are a major security challenge. They are becoming increasingly frequent and sophisticated. In addition to technical measures, the Strategy also focuses on building a culture of cybersecurity and cyber hygiene among citizens, businesses and public institutions.

The Strategy for the Digitalisation of Financial Services in the European Union aims to create an integrated and innovative financial sector that fully exploits the advantages of digital technologies and ensures resilience and protection for all participants. The main objectives of the Strategy include promoting innovation and competition in digital finance, strengthening consumer protection and financial stability, and increasing cyber resilience.

The second chapter of the dissertation research contains an overview of the main EU regulations in the field of cybersecurity. It consistently examines the issues related to electronic identification and authentication services in electronic transactions in the internal market and the protection of individuals with regard to the processing of personal data. As an important aspect of it, the protection of individuals with regard to the processing of personal data by the institutions, bodies, offices and agencies of the European Union is also analyzed.

Next, the legal framework for cooperation between national authorities responsible for consumer protection legislation is presented. The legally binding Union acts on the establishment of a common framework for managing cyber threats and responding to cyber attacks and the Cybersecurity Act are consistently studied. They provide for restrictive measures that can be applied against individuals or organizations involved in cyber attacks, such as financial sanctions, entry bans and asset freezes. The established procedures for coordination and cooperation between the Member States of the European Union in the event of a cyber attack or threat

thereof are also studied. These acts regulate the objectives, tasks and functions of the main structures responsible for Union cybersecurity, such as the European Cybersecurity Industrial, Technology and Research Competence Centre and a network of national coordination centres and the European Union Agency for Cybersecurity, which are analysed in detail. The third chapter of the work provides an analytical overview of the main directives in the field of cybersecurity. The directives relating to the processing of personal data and the protection of privacy in the electronic communications sector, cooperation between national authorities responsible for the enforcement of consumer protection legislation, and the consumer protection. The legal matter relating to attacks against information systems, the legal framework of the procedure for providing information in the field of technical regulations, the legal framework of police and judicial cooperation in the field of personal data protection, etc. has also been studied in depth.

VII. Contributions and Significance of the Study for the Science and in the Practice

The main contribution of the dissertation is that it represents one of the first attempts in Bulgarian legal literature to comprehensively study and analyze the secondary law of the European Union concerning cybersecurity. Apart from this, the most important strategic documents of the EU in the same area are also analyzed in detail.

For each of the studied regulatory acts, de lege ferenda proposals are given, which can be used as possible perspectives for improving and updating the regulatory acts and strategies of the European Union in the field of cybersecurity. Such are the proposals for:

1. Updating the legal framework in relation to new technologies. The current regulatory framework was created in a context in which mobile payments, blockchain or digital currencies were not widespread. As a result, the legislation does not provide for specific mechanisms for the protection of consumers and

businesses in these new areas. This creates uncertainty, opportunities for abuse and inequality between traditional and innovative providers.

The specific proposal de lege ferenda is to propose in the near future that cyber security policies also cover quantum computers and the security threats they pose. Quantum computers will be able to perform multiple calculations in a short period of time. The encryption algorithms currently in use will be broken thanks to the use of quantum computers.

2. Limiting uneven implementation in Member States. The incomplete and inconsistent implementation of directives in the different Member States is a problem. It hinders coordination and cooperation in the field of cybersecurity, leads to legal uncertainty and to different levels of protection against cyber attacks.

The recommendation is that the EU should introduce stricter minimum standards and require uniform rules on cybersecurity issues. The proposal to consider introducing a common mechanism for monitoring and correcting inconsistencies in implementation in order to ensure a high common level of cybersecurity for all Member States is particularly valuable.

3. Overcoming legal uncertainty. The complexity of new technologies requires a clear definition of the roles and responsibilities of the various actors – banks, fintech companies, technology platforms. In the absence of such clarity, conflicts arise between providers and consumers, and legal procedures become more difficult and slow. The European Union should adopt a legal framework that includes specific definitions of the key concepts, which would reduce legal uncertainty and increase market predictability.

4. Increasing the effectiveness of sanctions. When sanctions for violations are too low, they do not fulfill a preventive function and do not motivate providers to comply with the rules. In some of the regulatory acts of the European Union examined in the dissertation, the amount of sanctions is explicitly specified. Such specifics should also be added to the acts in which it is missing, as well as to establish minimum levels of sanctions at the European Union level and to introduce a common mechanism for their effective implementation.

5. Strengthening administrative and expert capacity. Many national authorities suffer from a lack of resources and expertise, which leads to delayed investigations, missed violations and insufficient control over the sector. To address this problem, the dissertation author recommends that the European Union provide pan-European funding for capacity building, including cybersecurity training programmes, exchange of experts and the establishment of specialised units for digital crime and financial innovation, all of which could be regulated by an appropriate Union act.

6. Strengthening international cooperation. The lack of effective cooperation with third countries and international organisations makes investigations difficult, and cybercrime and financial fraud often have a cross-border nature. The European Union should aim to achieve a closer network for information exchange between national authorities and international institutions.

Of particular importance is the recommendation that the EU should start playing a leading role globally in creating international standards and cooperation mechanisms in the field of information technology and cybersecurity, and this could start by developing and approving a special legal framework.

7. Increasing digital literacy and public awareness. Despite advances in technological development and the introduction of various security standards, the human factor remains the most vulnerable unit in the cybersecurity system. Insufficient awareness leads to underestimation of risks, inappropriate online behavior and low sensitivity to suspicious actions which makes it easier for criminals. This affects not only individual citizens, but also businesses, especially small and medium-sized enterprises, which often lack internal cybersecurity teams.

Many of the regulations address the issue of training. The proposal, made by the doctoral student, is to adopt a regulatory act of the European Union, which would establish requirements for regular educational campaigns aimed at different target groups - schoolchildren, students working in the private and public sectors, elderly people. Next, requirements could be introduced for Member States to integrate digital literacy into educational programs at all levels - from primary schools to

universities, with a special emphasis on online security, personal data protection and the responsible use of technology.

VIII. Assessment of the Publications Related to the Dissertation

The publications with which the doctoral student participates in the procedure, similar to the dissertation work itself, are distinguished by originality, include a non-standard reading of some of the basic concepts and theories and the application of the author's typical diverse toolkit for researching the subject.

IX. Personal Contribution of the Doctoral Candidate

The original approach and distinctive scholarly style demonstrated by the candidate in the dissertation research provide indisputable evidence of her personal involvement in developing the work and achieving its results, as well as of her personal merit in the formulation of the scientific contributions.

X. Abstract (Autoreferat) of the Author

The submitted abstract, in terms of both content and quality, has been developed entirely in accordance with the requirements of the relevant regulations and reflects the main results achieved in the dissertation.

XI. Critical Remarks and Recommendations for the Future Use of the Dissertation's Contributions and Results

In my opinion, some of the de lege ferenda proposals made by the author of the dissertation are too hesitant. These are all those recommendations given as potential options, alternatives or as possible approaches for improvement. I believe that given the in-depth analysis and the solid argumentation of the main theses of the work, these proposals could be put forward more firmly and ambitiously.

In this regard, the main recommendation that can be made is that, while applying the same approaches and methods of work, the author should continue his scientific research and try to propose his own formulations of specific mechanisms

or norms that would be the basis for future revisions and updates of the main strategies and regulatory acts of the EU in the field of cybersecurity. These new publications on the topic should be directed for publication in refereed and indexed editions in world-renowned databases such as Scopus, Web of Science, etc.

Conclusion

The dissertation contains scientific, scientifically applied and applied results that represent an original contribution to science and meets all the requirements of the the Law on the Development of the Academic Staff in the Republic of Bulgaria (LDASRB), the Implementing Regulations of the LDASRB, as well as the additional requirements set forth in the Regulations on the Conditions and Procedures for the Acquisition of Scientific Degrees and for Holding Academic Positions at the Bulgarian Academy of Sciences, and the Regulations on the Conditions and Procedures for the Acquisition of Scientific Degrees and for Holding Academic Positions at the Institute for State and Law of the Bulgarian Academy of Sciences.

The dissertation shows that the doctoral student Margarita Evgenieva Oysolova possesses in-depth theoretical knowledge and professional skills in the scientific specialty of EU law, international law and international relations, demonstrating qualities and skills for independently conducting scientific research.

Due to the above, I confidently give my **POSITIVE OPINION** for the conducted research, presented by the above-reviewed dissertation, abstract, achieved results and contributions, and I propose to the esteemed scientific jury to award the educational and scientific degree "doctor" to Margarita Evgenieva Oysolova in the field of higher education: 3. Social, economic and legal sciences, professional field 3.6. Law, doctoral program International Law and International Relations.

October 30, 2025 Reviewer: .....

Prof. DSc Stoyan Denchev