РЕЦЕНЗИЯ

от доц. д-р Паунита Михайлова Петрова

член на научното жури съгласно Заповед № РД-09-68 от 25.09.2025г. на проф. д-Ирена Илиева, Директор на Института за държавата и правото при БАН относно открита процедура за защита на дисертационен труд 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“

на дисертационния труд на Маргарита Евгениева Ойсолова – задочен докторант към секция „Международноправни науки“ на Института за държавата и правото при БАН

на тема: „Регламентацията на киберсигурността в Европейския съюз – проблеми и перспективи“

Уважаеми членове на научното жури,

Докторантът Маргарита Евгениева Ойсолова е завършила Информационна сигурност в Университет по библиотекознание и информационни технологии /бакалавърска и магистърска степен/ през 2018г.. От 01.02.2021г. е зачислена за задочен докторант в докторска програма „Международно право и международни отношения“ към секция „Международноправни науки“ на Института за държавата и правото при БАН с научен ръководител проф. д-р Ирена Илиева, а на 01.02.2025г. след изтичане на срока на докторантурата й е отчислена с право на защита. Маргарита Ойсолова е експерт по мрежова и информационна сигурност в последните години от професионалното си развитие, а преди това е била редактор на сп. „Правна мисъл“ и администратор на компютри и мрежи в Институт за държавата и правото при БАН, както и член на екипа за управление на Програма BG15 Норвежки финансов механизъм (2009-2014) в Министерство на правосъдието и координатор на националния организационен комитет на 75-та конференция на Световната асоциация по международно право (ILA) към Фондация „Конференция на Световната асоциация по международно право – София“.

I. Актуалност и значимост на темата

Актуалността на темата се обуславя от нарастващото значение на киберсигурността като ключов елемент на националната, европейската и глобалната сигурност. В ерата на цифровата трансформация всички сфери на обществения и икономическия живот – от публичната администрация и енергетиката до здравеопазването и финансите – са зависими от стабилна и защитена информационна инфраструктура. Рязкото увеличаване на кибератаките, включително срещу стратегически обекти, институции и бизнеси в

държавите членки на ЕС, показва необходимостта от ефективна правна и институционална рамка за превенция, защита и реагиране при инциденти.

В този контекст Европейският съюз предприема последователни мерки за изграждане на обща киберсигурностна архитектура. Приемането на Директива (ЕС) 2022/2555 (NIS 2), Актът за киберсигурност (Регламент (ЕС) 2019/881) и новите инициативи за Дигитална Европа и Киберщит на ЕС показват, че киберсигурността се превръща в основен приоритет на Съюза. Тези актове целят хармонизиране на правилата, засилване на сътрудничеството между държавите членки и създаване на механизми за контрол и сертифициране на киберустойчивостта на услуги и продукти.

От българска гледна точка темата е особено актуална, тъй като страната е част от общото европейско киберпространство и следва да адаптира националното си законодателство в съответствие с европейските стандарти. България предприе стъпки с приемането на Закона за киберсигурност (2019 г.), но остават предизвикателства, свързани с ефективното прилагане на директивите на ЕС, укрепване на капацитета на институциите и подобряване на координацията между публичния и частния сектор.

Актуалността на изследването се засилва и от перспективния характер на темата – бъдещите предизвикателства на изкуствения интелект, интернет на нещата (IoT), квантовите технологии и киберпрестъпността изискват непрекъснато развитие на правната уредба. В този смисъл, изследването на регламентацията на киберсигурността в ЕС не само отразява настоящите проблеми, но и очертава стратегическите насоки за изграждане на сигурна, устойчива и конкурентна дигитална среда в Европа.

Значимостта на темата „Регламентацията на киберсигурността в Европейския съюз – проблеми и перспективи“ се проявява както в теоретичен, така и в практически аспект. От теоретична гледна точка, тя обединява въпросите на международното право и правото на ЕС, правото на вътрешния пазар, защитата на личните данни, както и правото на националната и обществената сигурност. Киберсигурността представлява динамична и междусекторна правна материя, която изисква изграждането на цялостна концепция за управление на рисковете и сътрудничество между институции на национално, наднационално и глобално равнище.

Практическата значимост на темата произтича от необходимостта държавите членки, включително България, да изградят ефективни механизми за превенция и реагиране на киберзаплахи. Кибератаките вече не засягат само отделни мрежи или институции, а представляват заплаха за икономическата стабилност, обществения ред и демократичните процеси. В този смисъл правната уредба на киберсигурността се превръща в неразделна част от националната сигурност и защитата на основните права на гражданите.

Значимостта на темата се засилва и от нейния стратегически потенциал за развитието на Европейския съюз като глобален лидер в дигиталната трансформация и технологичната независимост. Създаването на единна европейска рамка за киберсигурност допринася за повишаване на доверието в цифровите услуги, за

стабилността на вътрешния пазар и за изграждането на сигурна и устойчива цифрова икономика.

II. Обща характеристика на дисертацията

Представената дисертация на тема: „Регламентацията на киберсигурността в Европейския съюз – проблеми и перспективи“ е в обем от 270 страници, включително съдържание, списък на използваните съкращения, използвана терминология, библиография, списък на използваните документи и закони и списък на използвани нормативни актове.

Уводът представя контекста, актуалността и значимостта на темата, като подчертава централната роля на мрежите и информационните системи за функционирането на съвременното общество и икономика. Изтъква се, че цифровизацията и бързото навлизане на технологиите след пандемията от Covid-19 превръщат киберсигурността в ключов фактор за обществената и икономическата стабилност. Авторът посочва, че въпреки напредъка, нивото на сигурност остава недостатъчно, поради липсата на принципа „secure by design“ и ограниченото сертифициране на ИКТ продукти. Това поражда уязвимости и недоверие сред потребителите, както и необходимост от цялостна правна регламентация на киберпространството.

В увода се акцентира върху етичните измерения на киберсигурността – киберетиката, разглеждана като пресечна точка между право, етика и технологии. Изведено е значението на европейските инициативи в тази област – Стратегията за киберсигурност (2020), Директивите NIS и NIS2, създаването на ENISA и Общия регламент за защита на данните (GDPR), които формират интегрирана система от правни и етични стандарти, целящи да постигнат баланс между сигурност и защита на основните права. Отбелязва се и липсата на цялостно изследване в българската научна литература, обхващащо всички актове на ЕС, регулиращи киберсигурността.

Определени са целта и предметът на труда – да се направи пълен преглед и анализ на нормативната и стратегическата уредба на Европейския съюз в областта на киберсигурността, включително стратегии, регламенти и директиви, както и да се идентифицират пропуски и възможности за усъвършенстване на законодателната рамка.

Формулирани са тезата, целта и основните изследователски задачи, свързани със събиране, систематизиране и анализ на правните актове, изследване на техните слабости и изготвяне на предложения de lege ferenda. Основната теза гласи, че ЕС е постигнал значителен напредък в изграждането на законодателство по киберсигурност, но съществуват пропуски, които следва да бъдат преодолени чрез актуализация и включване на новите заплахи.

Изложена е методологията на изследването, основана на телеологичен, исторически, интердисциплинарен и формално-логически подход, както и на анализ на нормативни актове, документи и експертни интервюта.

В увода се посочват и очакваните резултати – цялостен преглед на законодателството на ЕС по киберсигурността, систематизация на актовете и оценка на тяхната ефективност. Очертава се структурата на труда, включваща три основни глави: анализ на стратегическите документи, регламентите и директивите в областта на киберсигурността.

Изключително полезна и ценна е включената справка с използваните термини, в която е обяснено тяхното съдържание. Това помага за по-лесно ориентиране на юристите и неспециалистите в спецификите на материята, свързана с киберсигурността.

В първа глава от дисертационния труд, озаглавена „Стратегически документи“, дисертантът разглежда основните стратегически документа на Европейския съюз, които изграждат концептуалната рамка на европейската политика по киберсигурност. Това са двете Стратегии на ЕС за киберсигурност от 2013 и 2020 г., Стратегията на Съюза за сигурност и Стратегията за цифровизиране на финансовите услуги.

В дисертацията е изяснена ролята на стратегическите документи като основа за дългосрочно планиране, координация и определяне на приоритети в областта на киберсигурността. Авторът подчертава, че чрез тях Европейският съюз цели да осигури високо ниво на защита на мрежите и информационните системи, да повиши устойчивостта срещу кибератаки и да гарантира сигурна цифрова среда за гражданите и бизнеса.

Дисертантът проследява еволюцията на стратегическото мислене в рамките на ЕС – от първата Стратегия от 2013 г., поставила основите на общите принципи и приоритети, до актуализираната Стратегия от 2020 г., в която се въвежда интегриран подход, обхващащ икономическите, политическите и военните аспекти на киберзаплахите. Акцентирано е върху стремежа към уеднаквяване на стандартите за сигурност между държавите членки и подобряване на координацията при трансгранични инциденти.

В дисертацията е включен и анализ на Стратегията за единен цифров пазар от 2015 г. и нейната актуализация от 2025 г., насочени към ускоряване на цифровата трансформация, укрепване на вътрешния пазар и създаване на нормативна рамка за етична и безопасна употреба на изкуствения интелект.

Дисертантът разглежда и Стратегията на ЕС за Съюза на сигурността, която акцентира върху кибератаките като ключов риск за обществената и институционална сигурност и поставя ударение върху формирането на култура на киберсигурност и киберхигиена.

Последната анализирана Стратегия за цифровизиране на финансовите услуги е представена като инструмент за изграждане на конкурентен, устойчив и киберсигурен финансов сектор, основан на иновации и доверие.

Следователно, в глава първа авторът демонстрира системен и аналитичен подход, очертавайки стратегическата рамка, чрез която Европейският съюз последователно развива и укрепва политиката си по киберсигурност, интегрирайки технологични, правни и етични измерения.

Във втора глава от дисертационния труд, озаглавена „Регламенти в областта на киберсигурността“, дисертантът разглежда и анализира основните регламенти на Европейския съюз, които изграждат правната рамка на киберсигурността и цифровата защита. В изследването е поставен акцент върху взаимовръзката между киберсигурността, електронната идентификация, защитата на личните данни и оперативната устойчивост на цифровите технологии.

Авторът анализира Регламента за електронна идентификация и удостоверителни услуги (eIDAS), който създава система за сигурни електронни трансакции между гражданите, бизнеса и публичните институции. В дисертацията се подчертава ролята му за изграждане на доверие и ефективност при електронните услуги и търговия в рамките на вътрешния пазар на ЕС.

Дисертантът разглежда подробно и Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните – GDPR), който укрепва правата на гражданите по отношение на обработването на лични данни и осигурява прозрачност и сигурност при тяхното използване. В тази връзка е анализиран и Регламент (ЕС) 2018/1725, който урежда обработването на лични данни от институциите и органите на Европейския съюз и осигурява съгласуваност с нормите на GDPR.

В дисертацията е включен и Регламент (ЕС) 2017/2394 относно сътрудничеството между националните органи, отговорни за защитата на потребителите. Авторът отбелязва неговия принос за засилване на контрола при трансгранични нарушения и за модернизиране на взаимодействието между държавите членки в интерес на потребителите.

Особено внимание е отделено на Регламент (ЕС) 2019/796, който създава рамка за реагиране при кибератаки и въвежда ограничителни мерки срещу лица или организации, замесени в кибератаки. Дисертантът подчертава неговата роля за подобряване на координацията и готовността на държавите членки при киберинциденти.

Важен акцент представлява и Регламент (ЕС) 2019/881 – т.нар. Акт за киберсигурността, с който се засилва ролята на Агенцията на Европейския съюз за киберсигурност (ENISA) и се създава европейска рамка за сертифициране на ИКТ продукти и услуги. Той се разглежда като ключов инструмент за осигуряване на високо ниво на доверие и устойчивост в цифровата среда на Съюза.

В дисертацията е анализиран и Регламент (ЕС) 2021/887, с който се създават Европейският център за промишлени, технологични и изследователски експертни познания по киберсигурност и мрежа от национални координационни центрове. Авторът подчертава, че тези структури укрепват сътрудничеството, обмена на информация и иновациите между държавите членки.

Накрая е разгледан Регламент (ЕС) 2022/2554 – Digital Operational Resilience Act (DORA), който цели да гарантира устойчивостта на финансовия сектор срещу кибератаки

чрез въвеждане на единни правила за сигурността на информационните системи на финансовите институции.

Следователно, дисертантът успешно е систематизирал и обобщил приетите регламенти, които формират комплексна и взаимосвързана нормативна рамка за киберсигурността в Европейския съюз. Чрез тях се осигуряват правни, организационни и технически механизми за защита на личните данни, гарантиране на сигурността на цифровите услуги и укрепване на устойчивостта на критичната инфраструктура.

В трета глава от дисертационния труд, озаглавена „Директиви в областта на киберсигурността“, дисертантът анализира основните директиви на Европейския съюз, които регламентират правните, организационните и техническите аспекти на сигурността в цифровото пространство.

Авторът започва с анализ на Директива 2009/136/ЕО, която урежда обработката на лични данни и защитата на правото на неприкосновеност в сектора на електронните комуникации. Тази директива представлява важна стъпка към осъвременяване на правната рамка в областта на електронните съобщения, като въвежда ясни правила за защита на личните данни, укрепва доверието в цифровите услуги и гарантира правата на потребителите. В контекста на бързо развиващите се технологии тя се явява основен инструмент за постигане на сигурна и прозрачна цифрова среда.

В последователност дисертантът разглежда и Директива 2013/40/ЕС относно атаките срещу информационните системи, с която се хармонизира наказателното право на държавите членки в борбата срещу киберпрестъпленията. С нея се въвеждат минимални стандарти за криминализиране на кибератаките и се поставя акцент върху сътрудничеството между държавите членки и международните организации за противодействие на подобни заплахи.

В дисертацията е анализирана и Директива 2007/64/ЕО относно платежните услуги във вътрешния пазар, чиято цел е да хармонизира правилата за платежните операции, да засили защитата на потребителите и да осигури по-голяма прозрачност и сигурност при електронните плащания. Дисертантът подчертава нейния принос за изграждане на единен пазар за платежни услуги и насърчаване на конкуренцията и иновациите в този сектор.

Авторът разглежда и Директива (ЕС) 2015/1535, свързана с процедурите за уведомяване на Европейската комисия относно техническите регламенти и правилата за услугите на информационното общество. Чрез нея се цели предотвратяване на търговски бариери и осигуряване на прозрачност при въвеждането на национални технически изисквания, с което се укрепва вътрешният пазар на Европейския съюз.

В главата е включен и анализ на Директива (ЕС) 2016/680, известна като Директивата за полицейското и съдебно сътрудничество в областта на защитата на личните данни. Тя установява баланс между необходимостта от ефективно правоприлагане и защитата на основното право на неприкосновеност на личния живот, като въвежда унифицирани стандарти за обработка на лични данни от компетентните органи.

Съществено място заема и разглеждането на Директива (ЕС) 2016/2102 относно достъпността на уебсайтовете и мобилните приложения на организациите от обществения сектор. Тази директива цели постигане на по-голяма достъпност на публичните услуги, особено за хората с увреждания, чрез въвеждане на хармонизирани стандарти за оперативност, надеждност и разпознаваемост на дигиталните платформи.

Дисертантът отделя внимание и на двете ключови директиви в областта на мрежовата и информационната сигурност – Директива (ЕС) 2016/1148 и актуализираната ѝ версия Директива (ЕС) 2022/2555. Те са представени като основополагащи правни инструменти, чрез които се изгражда обща рамка за високо ниво на сигурност на мрежите и информационните системи. В тях се предвижда създаване на национални компетентни органи, изготвяне на национални стратегии за киберсигурност и засилено сътрудничество на стратегическо и техническо равнище между държавите членки.

Разгледана е и Директива (ЕС) 2022/2557 относно устойчивостта на критичните субекти, която се фокусира върху защитата на основните мрежи и инфраструктури срещу нововъзникващи заплахи, произтичащи от цифровизацията на обществото и икономиката.

Дисертантът подчертава, че разгледаните директиви имат системен и взаимно допълващ се характер, изграждайки единна нормативна рамка, която гарантира високо ниво на защита на цифровата среда, укрепва устойчивостта на критичната инфраструктура и осигурява прилагането на единни стандарти в целия Европейски съюз. За всяка от анализираните директиви е предоставена информация относно нейното транспониране в българското законодателство, което придава на изследването практическа насоченост и повишава неговата приложна стойност.

В заключението дисертантът е обобщил направеното проучване на нормативните актове на Европейския съюз в областта на киберсигурността, като е систематизирал и анализирал стратегии, регламенти и директиви, приети след 2000 г. Изведен е цялостен преглед на законодателството, чрез който е изяснена правната рамка на киберсигурността и взаимовръзките между отделните актове. Акцент е поставен върху новите механизми за сътрудничество на равнище Съюз, повишаването на националните капацитети и въвеждането на общоевропейски правила за сертифициране и санкциониране на киберзаплахи.

Дисертантът е разгледал ролята на Европейската агенция за киберсигурност (ENISA), новите правила в телекомуникационния сектор и създаването на Европейската схема за сертифициране, като е подчертал значението на защитата „още при проектирането“. Отбелязано е, че нормативните актове засягат различни целеви групи – граждани, потребители и оператори на основни услуги, като повишават тяхната информираност и нивото на защита.

В заключението на труда се съдържа критична оценка за сложността и нееднаквото прилагане на част от актовете, особено директивите, както и препоръка за по-ясно и координирано законодателство чрез сътрудничество между институциите и научните среди.

Дисертантът е изпълнил последната си изследователска задача, като е изготвил предложения de lege ferenda както в отделните глави, така и обобщени в заключителната част. Разработката е представена като първото в българската научна литература цялостно и систематизирано изследване на вторичното право на Европейския съюз относно киберсигурността.

Дисертантът е приложил и библиографска справка, която съдържа: 18 източници на български език и 16 – на английски език. Използваният нормативен материал и други документи са изнесени също в отделен списък. Посочени са и интернет източници. Въпреки относително малкия брой използвани монографии и статии, библиографската справка е напълно адекватна на темата и съдържанието на дисертационния труд. Темата е силно нормативна и специфична, като фокусът е поставен върху анализ на първичното и вторичното право на Европейския съюз. Поради това основният източник на информация са официалните регламенти, директиви, стратегии и решения на европейските институции, а не обемна теоретична литература. В този контекст ограничената библиография не е белег на недостатъчност, а на целенасоченост и методологическа прецизност. Следва да се отчете и фактът, че киберсигурността е динамична и сравнително нова област на правото, в която научните публикации, особено на български език, са все още ограничени. Това прави избраните източници още по-ценни, тъй като отразяват най-актуалното състояние на научната и нормативна база.

Следователно, малкият брой източници не намалява научната стойност на труда, а напротив – подчертава умението на дисертанта да селектира съществената информация и да изгради аргументацията си върху нормативно точни и концептуално значими документи и публикации.

III. Оценка на научната новост, научните и приложни приноси

Дисертационният труд представлява първото цялостно и систематизирано изследване в българската правна литература, посветено на вторичното право на Европейския съюз в областта на киберсигурността. Новостта се изразява в цялостния обхват и аналитичното представяне на стратегиите, регламентите и директивите на ЕС, както и в съпоставителния анализ между различните стратегически документи (2013–2025 г.), който очертава еволюцията на европейската политика по киберсигурност.

Конкретните научни и практически приноси, които могат да се отличат, са следните:

- Първо цялостно изследване в България на вторичното право на Европейския съюз в областта на киберсигурността.
- Систематизация и синтез на съществуващите стратегии, регламенти и директиви на Европейския съюз, разгледани в тяхната взаимовръзка и последователност.
- Анализ на основните проблеми и слабости в действащата нормативна уредба на ЕС относно киберсигурността.

- Формулиране на конкретни предложения de lege ferenda в седем направления – актуализиране на правната рамка, уеднаквяване на прилагането ѝ в държавите членки, преодоляване на правната несигурност, засилване на санкционните механизми, укрепване на административния капацитет, развитие на международното сътрудничество и повишаване на дигиталната грамотност.
- Сравнителен анализ на стратегическите документи на ЕС в областта на киберсигурността, включително стратегиите за 2013 и 2020 г., както и за единния цифров пазар (2015 и 2025 г.).
- Интердисциплинарен принос, изразен в приложимостта на резултатите не само в правната наука, но и в техническите и информационните изследвания, чрез осигуряване на ясна и систематизирана представа за изискванията и перспективите на киберсигурността в ЕС.
- Нов подход в представянето на правните актове – синтезиране на съдържанието на сложни нормативни документи по начин, достъпен и за неюристи, което подпомага разширяване на аудиторията и повишава правната култура в тази сфера.
- Интегриране на анализа на транспонирането в националното законодателство – за всяка директива е проследено нейното прилагане в българското право, което осигурява практическа стойност и национален ракурс на изследването.
- Проследяване на еволюцията на законодателството във времето – чрез съпоставка между различни версии на директиви (напр. 2016/1148 и 2022/2555) и стратегии (2015 и 2025), което разкрива тенденции в развитието на киберрегулацията.
- Акцентиране върху връзката между правото и технологиите – анализ на предизвикателствата, произтичащи от квантовите компютри, блокчейн и цифровите валути, което поставя правните основи на бъдещи регулации в ЕС.
- Обвързване на киберсигурността с правата на човека и защитата на личните данни – разглеждане на GDPR, eIDAS и други актове в контекста на баланса между сигурност и неприкосновеност.
- Предложение за въвеждане на образователни и информационни политики на ниво ЕС – иновативен елемент, който излиза извън класическата правна рамка и засяга социалното измерение на киберсигурността.
- Посочване на конкретни насоки за усъвършенстване на законодателството на Европейския съюз и държавите членки в сферата на киберсигурността и за утвърждаване на интегриран подход към нейното регулиране.

Дисертационният труд се отличава с обхватен, системен и комплексен анализ на вторичното право на Европейския съюз в областта на киберсигурността, като съчетава нормативен, сравнителен и приложен подход. Приносът му се изразява не само в подробното систематизиране и аналитично тълкуване на ключови европейски актове, но и в предлагането на конкретни, практически ориентирани решения за законодателно и институционално усъвършенстване на политиката по киберсигурност в Европейския съюз и България.

IV. Оценка на публикациите по темата

Резултатите от научното изследване са достигнали реално до научната общност чрез две публикации по темата на дисертацията, които са излезли от печат. Една публикация е приета за печат и предстои публикуването ѝ.

Първата – „Транспониране на Директива (ЕС) 2016/1148 в българското законодателство“ (2021), е посветена на въвеждането на изискванията на посочената директива в националното законодателство. Втората – „Акт за киберсигурността“ (2022), разглежда съответния регламент на Европейския съюз, известен като Акт за киберсигурността. Третата публикация – „Съпоставка между директивите 2016/1148 и 2022/2555“ (под печат), представя сравнителен анализ между двете директиви на Европейския парламент и на Съвета, свързани с киберсигурността.

Публикациите показват последователна научна насоченост към изследване на правната уредба на киберсигурността в Европейския съюз и нейното отражение върху националното законодателство, като допринасят за задълбочаване на темата, разглеждана в дисертационния труд.

V. Критични бележки и препоръки

Представената дисертация се отличава с ясно структурирано изложение, логическа последователност и демонстрира задълбочено познаване на нормативната рамка на Европейския съюз в областта на киберсигурността. Трудът се отличава с прецизна систематизация на значителен обем стратегически и правни документи и с умението на автора да обхване комплексен и многопластов материал по изключително добре организиран начин. Наред с тези безспорни научни достойнства, могат да бъдат направени няколко градивни бележки и препоръки, насочени към бъдещо доразвиване и усъвършенстване на изследването.

На първо място, би било полезно в бъдещи разработки да се задълбочи сравнителният анализ чрез по-детайлно съпоставяне между уредбата в правото на ЕС и универсалната международноправна уредба, като например с актовете, приети в рамките на ООН. Това би позволило изследването да се обогати с глобална перспектива и да се оцени доколко европейският модел на киберсигурност се вписва в световните тенденции.

Второ, изследването би могло да бъде допълнено и с кратък обзор на развитието на българската нормативна рамка в областта на киберсигурността в по-тясна връзка с европейската. Такъв подход би подчертал връзката между наднационалното и националното право и би показал конкретния ефект на европейските регулации върху националната практика.

Трето, макар че библиографската база е напълно адекватна на предмета и целите на изследването, при последваща работа може да се предвиди по-широко използване на международни научни източници, включително доклади на изследователски центрове

и академични публикации от други държави членки. Това би засилило интердисциплинарния характер на изследването и би осигурило още по-богат сравнителен контекст.

В заключение, изложените бележки нямат критичен, а единствено конструктивен характер. Те целят да подчертаят потенциала на изследването да бъде доразвито в още по-широка и интердисциплинарна насока. Дисертацията представлява сериозен и навременен принос към българската правна наука и може да послужи като отправна точка за бъдещи академични и практически разработки в областта на киберсигурността и цифровото право.

VI. Заключение

Представеният дисертационен труд на тема „Регламентацията на киберсигурността в Европейския съюз – проблеми и перспективи“ представлява завършено, цялостно, систематизирано и аналитично изследване на вторичното право на Европейския съюз в областта на киберсигурността. Авторът е демонстрирал задълбочено познаване на нормативната материя, логическа последователност в изложението и умение да обобщава голям обем правни и стратегически документи.

Трудът има ясна структура, прецизна аргументация и висока практическа стойност. Отличава се начинът, по който дисертантът проследява развитието на европейската политика по киберсигурност, извежда проблемите на прилагането ѝ и предлага конкретни препоръки de lege ferenda, насочени към усъвършенстване на нормативната рамка и повишаване на нейната ефективност.

Дисертацията съдържа както теоретичен принос – в систематизацията и правния анализ на многобройните актове на ЕС, така и практически принос – чрез ясно формулираните предложения за подобряване на законодателството и политиките в областта на киберсигурността. Изследването може да служи като ценен източник както за правната наука, така и за институциите, работещи в сферата на цифровата сигурност.

Направените бележки имат градивен характер и целят да очертаят потенциала за бъдещо доразвиване на темата чрез по-задълбочен сравнителен и емпиричен анализ.

В заключение, дисертационният труд отговаря на всички изисквания на Закона за развитие на академичния състав и утвърдените академични стандарти. Представеното изследване е значим принос към българската правна наука и може да послужи като основа за други бъдещи научни и практически разработки в областта на европейското и националното киберправо. Поради това давам категорична положителна оценка и предлагам на почитаемото научно жури да вземе решение за присъждането на Маргарита Евгениева Ойсолова на образователната и научна степен „доктор“.

27.10.2025г. Подпис: ……..

/Доц. д-р Паунита Петрова/

REVIEW

by Assoc. Prof. Dr. Paunita Mihaylova Petrova

member of the scientific jury pursuant to Order No. RD-09-68 of 25.09.2025 of Prof. Dr. Irena Ilieva, Director of the Institute for the State and the Law at the Bulgarian Academy of Sciences, regarding the open procedure for the defense of a dissertation for the acquisition of the educational and scientific degree of "Doctor" in the field of higher education 3. Social, Economic, and Legal Sciences, professional direction 3.6. Law, doctoral program "International Law and International Relations"

of the dissertation thesis of Margarita Evgenieva Oysolova – part-time doctoral student at the "International Legal Sciences" section of the Institute for State and Law at the Bulgarian Academy of Sciences

on the topic: "Cybersecurity Regulation in the European Union – Problems and Prospects"

Dear members of the academic jury,

Doctoral student Margarita Evgenieva Oisova graduated in Information Security from the University of Library Studies and Information Technologies (bachelor's and master's degrees) in 2018. On February 1, 2021, she was enrolled as a part-time doctoral student in the doctoral program "International Law and International Relations" at the "International Legal Sciences" section of the Institute for State and Law at the Bulgarian Academy of Sciences, with Prof. Dr. Irena Ilieva as her academic supervisor. and on 01.02.2025, after the expiry of her doctoral studies, she was expelled with the right to defend her thesis. Margarita Oysolova has been an expert in network and information security in recent years of her professional development, and before that she was editor of the magazine Legal Thought and computer and network administrator at the Institute for the State and Law at the Bulgarian Academy of Sciences, as well as a member of the management team of Program BG15 Norwegian Financial Mechanism (2009-2014) at the Ministry of Justice and coordinator of the national organizing committee of the 75th conference of the International Law Association (ILA) at the International Law Association Conference Foundation – Sofia.

I. Relevance and significance of the topic

The relevance of the topic is determined by the growing importance of cybersecurity as a key element of national, European, and global security. In the era of digital transformation, all spheres of public and economic life – from public administration and energy to healthcare and finance – depend on a stable and secure information infrastructure. The sharp increase in cyberattacks, including against strategic sites, institutions, and businesses in EU member states, demonstrates the need for an effective legal and institutional framework for prevention, protection, and response to incidents.

In this context, the European Union is taking consistent steps to build a common cybersecurity architecture. The adoption of Directive (EU) 2022/2555 (NIS 2), the Cybersecurity Act (Regulation (EU) 2019/881) and the new initiatives for Digital Europe and the EU Cyber Shield show that cybersecurity is becoming a key priority for the Union. These acts aim to harmonize rules, strengthen cooperation between Member States, and create mechanisms for controlling and certifying the cyber resilience of services and products.

From a Bulgarian perspective, the topic is particularly relevant, as the country is part of the common European cyberspace and must adapt its national legislation in line with European standards. Bulgaria has taken steps with the adoption of the Cybersecurity Act (2019), but challenges remain in terms of the effective implementation of EU directives, strengthening the capacity of institutions, and improving coordination between the public and private sectors.

The relevance of the study is also reinforced by the forward-looking nature of the topic—the future challenges of artificial intelligence, the Internet of Things (IoT), quantum technologies, and cybercrime require continuous development of the legal framework. In this sense, the study of cybersecurity regulation in the EU not only reflects current problems but also outlines strategic guidelines for building a secure, sustainable, and competitive digital environment in Europe.

The importance of the topic "Cybersecurity Regulation in the European Union – Problems and Prospects" is evident in both theoretical and practical terms. From a theoretical point of view, it combines issues of international law and EU law, internal market law, personal data protection, and national and public security law. Cybersecurity is a dynamic and cross-sectoral legal matter that requires the development of a comprehensive concept for risk management and cooperation between institutions at the national, supranational, and global levels.

The practical significance of the topic stems from the need for Member States, including Bulgaria, to develop effective mechanisms for preventing and responding to cyber threats. Cyber attacks no longer affect only individual networks or institutions, but pose a threat to economic stability, public order, and democratic processes. In this sense, the legal framework for cybersecurity is becoming an integral part of national security and the protection of citizens' fundamental rights.

The importance of the topic is further enhanced by its strategic potential for the development of the European Union as a global leader in digital transformation and technological independence. The creation of a single European cybersecurity framework contributes to increasing trust in digital services, the stability of the internal market, and the development of a secure and sustainable digital economy.

II. General characteristics of the dissertation

The presented dissertation on the topic: "Cybersecurity Regulation in the European Union – Problems and Prospects" is 270 pages long, including the table of contents, a list of abbreviations used, terminology used, bibliography, a list of documents and laws used, and a list of regulatory acts used.

The introduction presents the context, relevance, and significance of the topic, emphasizing the central role of networks and information systems for the functioning of modern society and the economy. It points out that digitalization and the rapid introduction of technologies after the Covid-19 pandemic make cybersecurity a key factor for social and economic stability. The author points out that despite the progress made, the level of security remains insufficient due to the lack of the "secure by design" principle and the limited certification of ICT products. This creates vulnerabilities and mistrust among consumers, as well as the need for comprehensive legal regulation of cyberspace.

The introduction focuses on the ethical dimensions of cybersecurity – cyber ethics, viewed as an intersection between law, ethics, and technology. It highlights the importance of European initiatives in this area – the Cybersecurity Strategy (2020), the NIS and NIS2 Directives, the creation of ENISA, and the General Data Protection Regulation (GDPR), which form an integrated system of legal and ethical standards aimed at achieving a balance between security and the protection of fundamental rights. The lack of a comprehensive study in Bulgarian scientific literature covering all EU acts regulating cybersecurity is also noted.

The aim and subject of the study are defined as follows: to conduct a comprehensive review and analysis of the European Union's regulatory and strategic framework in the field of cybersecurity, including strategies, regulations, and directives, and to identify gaps and opportunities for improving the legislative framework.

The thesis, objective, and main research tasks related to the collection, systematization, and analysis of legal acts, the examination of their weaknesses, and the preparation of proposals de lege ferenda have been formulated. The main thesis is that the EU has made significant progress in developing cybersecurity legislation, but there are gaps that need to be addressed by updating and incorporating new threats.

The methodology of the study is presented, based on a teleological, historical, interdisciplinary, and formal-logical approach, as well as on an analysis of normative acts, documents, and expert interviews.

The introduction also outlines the expected results – a comprehensive review of EU cybersecurity legislation, systematisation of acts and assessment of their effectiveness. The structure of the work is outlined, comprising three main chapters: analysis of strategic documents, regulations and directives in the field of cybersecurity.

The included glossary of terms is extremely useful and valuable, explaining their meaning. This helps lawyers and non-specialists to more easily navigate the specifics of cybersecurity.

In the first chapter of the dissertation, entitled "Strategic Documents," the author examines the main strategic documents of the European Union that form the conceptual framework of European cybersecurity policy. These are the two EU Cybersecurity Strategies from 2013 and 2020, the Union's Security Strategy, and the Strategy for the Digitalization of Financial Services.

The dissertation clarifies the role of strategic documents as a basis for long-term planning, coordination, and priority setting in the field of cybersecurity. The author emphasizes that through these documents, the European Union aims to ensure a high level of protection for networks and information systems, increase resilience against cyberattacks, and guarantee a secure digital environment for citizens and businesses.

The dissertation traces the evolution of strategic thinking within the EU – from the first Strategy in 2013, which laid the foundations for common principles and priorities, to the updated Strategy of 2020, which introduces an integrated approach covering the economic, political, and military aspects of cyber threats. Emphasis is placed on the desire to harmonize security standards among member states and improve coordination in cross-border incidents.

The dissertation also includes an analysis of the 2015 Digital Single Market Strategy and its 2025 update, aimed at accelerating digital transformation, strengthening the internal market, and creating a regulatory framework for the ethical and safe use of artificial intelligence.

The author also examines the EU Strategy for the Security Union, which highlights cyberattacks as a key risk to public and institutional security and emphasizes the formation of a culture of cybersecurity and cyber hygiene.

The last analyzed Strategy for the Digitalization of Financial Services is presented as a tool for building a competitive, sustainable, and cyber-secure financial sector based on innovation and trust.

Therefore, in Chapter One, the author demonstrates a systematic and analytical approach, outlining the strategic framework through which the European Union consistently develops and strengthens its cybersecurity policy, integrating technological, legal, and ethical dimensions.

In the second chapter of the dissertation, entitled "Regulations in the Field of Cybersecurity," the author examines and analyzes the main European Union regulations that form the legal framework for cybersecurity and digital protection. The study focuses on the interrelationship between cybersecurity, electronic identification, personal data protection, and the operational resilience of digital technologies.

The author analyzes the Regulation on electronic identification and trust services (eIDAS), which creates a system for secure electronic transactions between citizens, businesses, and public institutions. The dissertation highlights its role in building trust and efficiency in electronic services and commerce within the EU internal market.

The author also examines in detail Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), which strengthens citizens' rights regarding the processing of personal data and ensures transparency and security in their use. In this regard, Regulation (EU) 2018/1725, which regulates the processing of personal data by the institutions and bodies of the European Union and ensures consistency with the provisions of the GDPR, is also analyzed.

The dissertation also includes Regulation (EU) 2017/2394 on cooperation between national authorities responsible for consumer protection. The author notes its contribution to

strengthening control over cross-border infringements and modernizing interaction between Member States in the interest of consumers.

Particular attention is paid to Regulation (EU) 2019/796, which establishes a framework for responding to cyberattacks and introduces restrictive measures against persons or organizations involved in cyberattacks. The author emphasizes its role in improving the coordination and preparedness of Member States in the event of cyber incidents.

Another important focus is Regulation (EU) 2019/881 – the so-called Cybersecurity Act, which strengthens the role of the European Union Agency for Cybersecurity (ENISA) and establishes a European framework for the certification of ICT products and services. It is seen as a key instrument for ensuring a high level of trust and resilience in the Union's digital environment. It is seen as a key instrument for ensuring a high level of trust and resilience in the Union's digital environment.

The dissertation also analyzes Regulation (EU) 2021/887, which establishes the European Center for Industrial, Technological, and Research Expertise in Cybersecurity and a network of national coordination centers. The author emphasizes that these structures strengthen cooperation, information exchange, and innovation between Member States.

Finally, Regulation (EU) 2022/2554 – the Digital Operational Resilience Act (DORA) – is examined, which aims to ensure the resilience of the financial sector against cyberattacks by introducing uniform rules for the security of financial institutions' information systems.

Therefore, the author has successfully systematized and summarized the adopted regulations, which form a comprehensive and interconnected regulatory framework for cybersecurity in the European Union. These regulations provide legal, organizational, and technical mechanisms for protecting personal data, ensuring the security of digital services, and strengthening the resilience of critical infrastructure.

In the third chapter of the dissertation, entitled "Directives in the field of cybersecurity," the author analyzes the main European Union directives that regulate the legal, organizational, and technical aspects of security in the digital space.

The author begins with an analysis of Directive 2009/136/EC, which regulates the processing of personal data and the protection of privacy in the electronic communications sector. This directive represents an important step towards modernising the legal framework in the field of electronic communications, introducing clear rules for the protection of personal data, strengthening trust in digital services and guaranteeing consumer rights. In the context of rapidly evolving technologies, it is a key tool for achieving a secure and transparent digital environment.

The dissertation also examines Directive 2013/40/EU on attacks against information systems, which harmonises the criminal law of Member States in the fight against cybercrime. It introduces minimum standards for the criminalization of cyber attacks and emphasizes cooperation between Member States and international organizations to counter such threats.

The dissertation also analyzes Directive 2007/64/EC on payment services in the internal market, which aims to harmonize the rules for payment transactions, strengthen consumer protection, and ensure greater transparency and security in electronic payments. The author highlights its contribution to the creation of a single market for payment services and the promotion of competition and innovation in this sector.

The author also examines Directive (EU) 2015/1535 on the procedures for notifying the European Commission of technical regulations and rules on information society services. It aims to prevent trade barriers and ensure transparency in the introduction of national technical requirements, thereby strengthening the internal market of the European Union.

The chapter also includes an analysis of Directive (EU) 2016/680, known as the Directive on police and judicial cooperation in the field of personal data protection. It strikes a balance between the need for effective law enforcement and the protection of the fundamental right to privacy by introducing uniform standards for the processing of personal data by competent authorities.

The consideration of Directive (EU) 2016/2102 on the accessibility of websites and mobile applications of public sector bodies also occupies an important place. This directive aims to achieve greater accessibility to public services, especially for people with disabilities, by introducing harmonized standards for the operability, reliability, and recognizability of digital platforms.

The author also focuses on the two key directives in the field of network and information security – Directive (EU) 2016/1148 and its updated version Directive (EU) 2022/2555. They are presented as fundamental legal instruments through which a common framework for a high level of security of networks and information systems is established. They provide for the establishment of national competent authorities, the development of national cybersecurity strategies, and enhanced strategic and technical cooperation between Member States.

Directive (EU) 2022/2557 on the resilience of critical entities is also examined, which focuses on the protection of essential networks and infrastructures against emerging threats arising from the digitalisation of society and the economy.

The author emphasizes that the directives examined are systematic and complementary in nature, forming a unified regulatory framework that guarantees a high level of protection for the digital environment, strengthens the resilience of critical infrastructure, and ensures the application of uniform standards throughout the European Union. For each of the directives analyzed, information is provided on its transposition into Bulgarian legislation, which gives the study a practical focus and increases its applied value.

In the conclusion,the author summarizes the study of European Union legislation in the field of cybersecurity, systematizing and analyzing strategies, regulations, and directives adopted since 2000. A comprehensive overview of the legislation is provided, clarifying the legal framework for cybersecurity and the interrelationships between the individual acts. Emphasis is placed on new mechanisms for cooperation at Union level, the enhancement of

national capacities, and the introduction of common European rules for the certification and sanctioning of cyber threats.

The author examines the role of the European Network and Information Security Agency (ENISA), the new rules in the telecommunications sector, and the creation of the European certification scheme, emphasizing the importance of "security by design." It is noted that the legislative acts affect different target groups – citizens, consumers, and operators of essential services – by raising their awareness and level of protection.

The conclusion of the thesis contains a critical assessment of the complexity and uneven application of some of the acts, especially the directives, as well as a recommendation for clearer and more coordinated legislation through cooperation between institutions and scientific circles.

The doctoral student has completed his final research task by preparing proposals de lege ferenda both in the individual chapters and summarized in the concluding part. The study is presented as the first comprehensive and systematic study of European Union secondary law on cybersecurity in Bulgarian scientific literature.

The doctoral student has also included a bibliography containing 18 sources in Bulgarian and 16 in English. The normative material and other documents used are also listed separately. Internet sources are also cited. Despite the relatively small number of monographs and articles used, the bibliography is entirely adequate for the topic and content of the dissertation. The topic is highly normative and specific, with a focus on the analysis of primary and secondary European Union law. Therefore, the main source of information is the official regulations, directives, strategies, and decisions of the European institutions, rather than voluminous theoretical literature. In this context, the limited bibliography is not a sign of insufficiency, but of purposefulness and methodological precision. It should also be noted that cybersecurity is a dynamic and relatively new area of law in which scientific publications, especially in Bulgarian, are still limited. This makes the selected sources even more valuable, as they reflect the most current state of the scientific and regulatory framework.

Therefore, the small number of sources does not diminish the scientific value of the work; on the contrary, it highlights the author's ability to select essential information and build their argumentation on normatively accurate and conceptually significant documents and publications.

III. Assessment of scientific novelty, scientific and applied contributions

The dissertation is the first comprehensive and systematic study in Bulgarian legal literature devoted to secondary EuropeanUnion law in the field of cybersecurity. Its novelty lies in its comprehensive scope and analytical presentation of EU strategies, regulations, and directives, as well as in its comparative analysis of various strategic documents (2013–2025), which outlines the evolution of European cybersecurity policy.

The specific scientific and practical contributions that can be distinguished are as follows:

- First comprehensive study in Bulgaria on secondary European Union law in the field of cybersecurity.
- Systematization and synthesis of existing European Union strategies, regulations, and directives, examined in terms of their interrelationship and consistency.
- Analysis of the main problems and weaknesses in the current EU regulatory framework on cybersecurity.
- Formulation of specific proposals de lege ferenda in seven areas – updating the legal framework, harmonising its application in Member States, overcoming legal uncertainty, strengthening sanctioning mechanisms, strengthening administrative capacity, developing international cooperation and increasing digital literacy.
- Comparative analysis of EU strategic documents in the field of cybersecurity, including the 2013 and 2020 strategies, as well as those for the digital single market (2015 and 2025).
- Interdisciplinary contribution, expressed in the applicability of the results not only in legal science, but also in technical and information studies, by providing a clear and systematic overview of the requirements and prospects of cybersecurity in the EU.
- A new approach to the presentation of legal acts – summarizing the content of complex regulatory documents in a way that is accessible to non-lawyers, which helps to expand the audience and raise legal awareness in this area.
- Integration of the analysis of transposition into national legislation – for each directive, its implementation in Bulgarian law has been tracked, which ensures the practical value and national perspective of the study.
- Tracking the evolution of legislation over time – by comparing different versions of directives (e.g., 2016/1148 and 2022/2555) and strategies (2015 and 2025), which reveals trends in the development of cyber regulation.
- Focus on the relationship between law and technology – analysis of the challenges posed by quantum computers, blockchain, and digital currencies, which lays the legal foundations for future regulations in the EU.
- Linking cybersecurity with human rights and personal data protection – examining the GDPR, eIDAS, and other acts in the context of the balance between security and privacy.
- Proposal for the introduction of educational and information policies at EU level – an innovative element that goes beyond the traditional legal framework and addresses the social dimension of cybersecurity.
- Specific guidelines for improving EU and Member State legislation in the field of cybersecurity and for establishing an integrated approach to its regulation.

The dissertation is distinguished by its comprehensive, systematic, and complex analysis of secondary EuropeanUnion law in the field of cybersecurity, combining a normative, comparative, and applied approach. Its contribution lies not only in the detailed systematization and analytical interpretation of key European acts, but also in offering

specific, practical solutions for the legislative and institutional improvement of cybersecurity policy in the European Union and Bulgaria.

IV. Assessment of publications on the topic

The results of the scientific research have reached the scientific community through two publications on the topic of the dissertation, which have been published. One publication has been accepted for publication and is awaiting publication.

The first, "Transposition of Directive (EU) 2016/1148 into Bulgarian legislation" (2021), is devoted to the introduction of the requirements of the aforementioned directive into national legislation. The second, "Cybersecurity Act" (2022), examines the relevant European Union regulation, known as the Cybersecurity Act. The third publication, "Comparison between Directives 2016/1148 and 2022/2555" (in press), presents a comparative analysis of the two European Parliament and Council directives related to cybersecurity.

The publications demonstrate a consistent scientific focus on researching the legal framework for cybersecurity in the European Union and its impact on national legislation, contributing to a deeper understanding of the topic addressed in the dissertation.

V. Critical remarks and recommendations

The dissertation is distinguished by its clearly structured presentation, logical consistency, and demonstrates in-depth knowledge of the European Union's regulatory framework in the field of cybersecurity. The work is distinguished by its precise systematization of a significant volume of strategic and legal documents and the author's ability to cover complex and multifaceted material in an extremely well-organized manner. Alongside these indisputable scientific merits, several constructive comments and recommendations can be made with a view to the further development and improvement of the study.

First, it would be useful in future studies to deepen the comparative analysis by making a more detailed comparison between EU law and universal international law, such as the acts adopted within the framework of the UN. This would enrich the study with a global perspective and assess the extent to which the European cybersecurity model fits into global trends.

Second, the study could be supplemented with a brief overview of the development of the Bulgarian regulatory framework in the field of cybersecurity in closer connection with the European one. Such an approach would emphasize the link between supranational and national law and show the specific effect of European regulations on national practice.

Third, although the bibliographic base is entirely adequate for the subject and objectives of the study, subsequent work could envisage wider use of international scientific sources, including reports from research centers and academic publications from other Member States. This would strengthen the interdisciplinary nature of the study and provide an even richer comparative context.

In conclusion, the comments made are not critical, but merely constructive in nature. They aim to highlight the potential for the research to be further developed in an even broader and more interdisciplinary direction. The dissertation represents a serious and timely contribution to Bulgarian legal science and can serve as a starting point for future academic and practical developments in the field of cybersecurity and digital law.

VI. Conclusion

The presented dissertation on "Cybersecurity Regulation in the European Union – Problems and Perspectives" is a complete, comprehensive, systematic, and analytical study of secondary European Union law in the field of cybersecurity. The author has demonstrated in-depth knowledge of the subject matter, logical consistency in the presentation, and the ability to summarize a large volume of legal and strategic documents.

The work has a clear structure, precise argumentation, and high practical value. The author distinguishes himself by the way he traces the development of European cybersecurity policy, identifies the problems of its implementation, and offers specific recommendations de lege ferenda aimed at improving the regulatory framework and increasing its effectiveness.

The dissertation contains both a theoretical contribution—in the systematization and legal analysis of numerous EU acts—and a practical contribution—through clearly formulated proposals for improving legislation and policies in the field of cybersecurity. The study can serve as a valuable source for both legal science and institutions working in the field of digital security.

The comments made are constructive in nature and aim to outline the potential for further development of the topic through more in-depth comparative and empirical analysis.

In conclusion, the dissertation meets all the requirements of the Law on the Development of Academic Staff and established academic standards. The presented study is a significant contribution to Bulgarian legal science and can serve as a basis for other future scientific and practical developments in the field of European and national cyber law. Therefore, I give a categorical positive assessment and propose that the honourable scientific jury decide to award Margarita Evgenieva Oisova the educational and scientific degree of "Doctor".

27.10.2025 Signature: ……..

/Assoc. Prof. Dr. Paunita Petrova/