РЕЦЕНЗИЯ

на дисертационен труд

за придобиване на образователната и научна степен „Доктор“ в

област на висше образование 4. Природни науки, математика и информатика

професионално направление 4.6. Информатика и компютърни науки

докторска програма: „Информационни системи и технологии, информатика и компютърни науки“

Автор: магистър Рахели Менда Шабат Мор

Тема: „Влиянието на регламент (ЕС) 2019/881 (Акт за киберсигурността) върху разширяването на сертификациите по киберсигурност“

Научни ръководители: доц. д-р Златогор Минчев; доц. д-р Галина Милева

Рецензент: проф. д-р инж. Теодора Иванова Бакърджиева,

Варненски свободен университет „Черноризец Храбър“

катедра „Компютърни науки“

Рецензията е изготвена на основание на решения на Ректора на Варненския свободен университет „Черноризец Храбър“ със заповед №256/30.04.2026 г

1. Обща характеристика на дисертационния труд

Представената от Рахели Менда Шабат Мор дисертация е посветена на актуална и значима тема, свързана с влиянието на Регламент (ЕС) 2019/881, известен като Cybersecurity Act, върху разработването и приемането на схеми за сертифициране на киберсигурността и регулации в областта на частната сигурност в европейската дигитална среда.

Като основна цел на дисертацията е поставено разработването на научно обосновани и хармонизирани модели, които да подпомагат прогнозирането на

успешната интеграция на частните схеми за сертифициране в по-широката сертификационна екосистема, както и формализирането на тези модели в устойчива рамка за вземане на решения при избор на сертифицираща организация.

За реализирането на тази цел се изпълняват следните задачи: оценка на качеството и ефективността; анализ на регулаторното въздействие; разработване на стратегии за хармонизиране; проучване на механизмите за доверие; оценка на приемането на пазара и мащабируемостта; формулиране на модел за вземане на решения от CAB.

Актуалността на темата е особено висока предвид нарастващото значение на управлението на киберсигурността, необходимостта от хармонизиране на стандартите за сигурност и засилената потребност от надеждни цифрови услуги и продукти. В дисертацията се разглеждат въпроси, свързани със сертифицирането на киберсигурността, регулаторните рамки и взаимодействието между публичното регулиране и механизмите за внедряване от страна на частния сектор.

Трудът е изграден логично и е добре структуриран. Той включва въведение, три глави, заключения, използвана литература и приложения. Авторът ясно представя целите, изследователските задачи, методологията и научната хипотеза на изследването.

Представеният труд показва интердисциплинарен подход, като обединява аспекти на киберсигурността, регулаторната политика, управлението на информационната сигурност, управлението на риска и рамките за цифрово доверие. Авторът разглежда както правните основания на Закона за киберсигурността, така и практическите му последици за организациите и частните схеми за сертифициране.

Добро впечатление прави стремежът теоретичният анализ да бъде свързан с практическите перспективи за внедряване, отнасящи се до механизмите за сертифициране, процесите на съответствие и осигуряването на киберсигурност.

2. Оценка на научните и практическите резултати и приноси

Дисертацията включва научноприложни и приложни приноси, свързани с анализа и оценката на въздействието на Регламент (ЕС) 2019/881 върху сертифицирането за киберсигурност и схемите за частна сигурност. Основните научни и приложни приноси могат да се обобщят по следния начин:

Научноприложни приноси

1. Разработена е концептуална рамка, озаглавена „Модел за прогнозиране на частни схеми (PSF)“, предназначена за оценка на ефективността и устойчивостта на частните схеми за сертифициране на киберсигурност в контекста на Регламент (ЕС) 2019/881.
2. Предложен и емпирично валидиран е методологичен подход за оценяване на ефективността на сертифицирането за киберсигурност.
3. Разработен е оригинален модел за избор на частна схема (PSS), насочен към подпомагане на избора и оценката на органи за оценка на съответствието (CABs). Моделът интегрира размита логика и оптимизационни техники чрез прилагането на метода на размита приоритизация (FPM) за обработване на експертни оценки в условия на неопределеност.
4. Формулиран и валидиран е структуриран методологичен процес за избор на CAB, който включва определяне на критерии за оценка, процедури за двойни сравнения, размита трансформация, оптимизация чрез изчисляване на геометрична средна, дефузификация и механизми за подпомагане на процеса на вземане на решения.

Приложни приноси

1. Разработена и валидирана е интегрирана рамка, която съчетава възможностите за стратегическо прогнозиране на модела PSF с оперативните механизми на модела PSS. Рамката формира подход със затворен цикъл, обвързващ планирането на сертифицирането за киберсигурност, процедурите за оценка на съответствието и дейностите по управление на организационната киберсигурност.
2. Валидирането на разработените модели PSF и PSS е осъществено чрез сравнителен анализ, експертни оценъчни процедури и приложение в

сценарии за сертифициране на киберсигурност, свързани с IoT среди и частни схеми за сертифициране съгласно рамката на Закона за киберсигурността.

Разработката показва добро познаване на съвременното състояние на изследванията в областта. Кандидатът използва подходяща научна методология и прилага сравнителни и аналитични подходи, които са релевантни на поставените изследователски цели.

Получените резултати имат както теоретична, така и практическа значимост. Те биха могли да бъдат полезни за изследователи, специалисти по киберсигурност, организации, прилагащи схеми за сертифициране, както и за институции, ангажирани с управление и съответствие в областта на киберсигурността.

3. Публикации, свързани с дисертацията

Докторантът е представил една научна публикация от 2026 г., свързана с темата на дисертацията и включена в научно издание, индексирано в Scopus, както и три презентации на международни научни конференции и форуми, посветени на киберсигурността, информационните системи и цифровите технологии.

Публикационната активност съответства на минималните национални изисквания за присъждане на образователната и научна степен „доктор“.

Не са предоставени данни за цитиране от страна на докторанта.

4. Критични забележки и препоръки

Дисертацията се отличава с висока актуалност и с добре структуриран аналитичен подход. Наред с това могат да бъдат направени няколко препоръки:

В отделни раздели изложението има по-описателен характер и би могло да бъде подобрено чрез по-синтезирано представяне на разглежданите регулаторни рамки.

Практическата приложимост на формулираните изводи може допълнително да се засили чрез по-широка емпирична проверка или чрез

казуси, включващи организации, които внедряват схеми за сертифициране на киберсигурност.

В бъдещи изследвания би могло допълнително да се проучи връзката между европейските разпоредби за киберсигурност, секторно-специфичните рамки за сертифициране и нововъзникващите технологии, сред които облачните услуги, системите с изкуствен интелект и екосистемите от интернет на нещата.

5. Лични впечатления

Представените материали показват добра теоретична подготовка, аналитично мислене и способност за провеждане на самостоятелни научни изследвания. Докторантът демонстрира разбиране на сложни проблеми, свързани с управлението на киберсигурността, както и умение за работа с интердисциплинарен научен материал.

6. Заключение

Формулираните препоръки и забележки не намаляват стойността на разработката.

Докторантът разполага със задълбочени теоретични знания по разглежданата тематика, както и със способности за осъществяване на самостоятелни научни изследвания и за практическо внедряване на постигнатите резултати.

Считам, че дисертацията е актуална, предложените методики могат да намерят широко приложение в различни сфери. Представеният дисертационен труд като значимост на изследванията представлява една задълбочена и завършена изследователска разработка, съдържа достатъчно научноприложни и приложни приноси. Удовлетворени са изискванията на *Закона за развитие на академичния състав в Република България* и на *Правилника* за неговото прилагане, както и на *Правила и процедури за приемане и обучение на докторанти и придобиване на ОНС „Доктор“* във ВСУ „Черноризец Храбър”.

Постигнатите резултати ми дават достатъчно основание да дам положителна оценка на представената дисертация и да предложа на уважаемото **Научно жури да присъди на Рахели Менда Шабат Мор**

образователната и научна степен „доктор“ в докторската програма „Информационни системи и технологии, информатика и компютърни науки“, професионално направление 4.6. „Информатика и компютърни науки“.

16.06.2026 г. **Рецензент**

/проф. д-р инж. Теодора Бакърджиева/**РЕЦЕНЗИЯ**

на дисертационен труд

за придобиване на образователната и научна степен „Доктор“ в

област на висше образование 4. Природни науки, математика и информатика

професионално направление 4.6. Информатика и компютърни науки

докторска програма: „Информационни системи и технологии, информатика и компютърни науки“

Автор: магистър Рахели Менда Шабат Мор

Тема: „Влиянието на регламент (ЕС) 2019/881 (Акт за киберсигурността) върху разширяването на сертификациите по киберсигурност“

Научни ръководители: доц. д-р Златогор Минчев; доц. д-р Галина Милева

Рецензент: проф. д-р инж. Теодора Иванова Бакърджиева,

Варненски свободен университет „Черноризец Храбър“

катедра „Компютърни науки“

Рецензията е изготвена на основание на решения на Ректора на Варненския свободен университет „Черноризец Храбър“ със заповед №256/30.04.2026 г

1. Обща характеристика на дисертационния труд

Представената от Рахели Менда Шабат Мор дисертация е посветена на актуална и значима тема, свързана с влиянието на Регламент (ЕС) 2019/881, известен като Cybersecurity Act, върху разработването и приемането на схеми за сертифициране на киберсигурността и регулации в областта на частната сигурност в европейската дигитална среда.

Като основна цел на дисертацията е поставено разработването на научно обосновани и хармонизирани модели, които да подпомагат прогнозирането на успешната интеграция на частните схеми за сертифициране в по-широката сертификационна екосистема, както и формализирането на тези модели в устойчива рамка за вземане на решения при избор на сертифицираща организация.

За реализирането на тази цел се изпълняват следните задачи:

- оценка на качеството и ефективността;
- анализ на регулаторното въздействие;
- разработване на стратегии за хармонизиране;
- проучване на механизмите за доверие;
- оценка на приемането на пазара и мащабируемостта;
- формулиране на модел за вземане на решения от CAB.

Актуалността на темата е особено висока предвид нарастващото значение на управлението на киберсигурността, необходимостта от хармонизиране на стандартите за сигурност и засилената потребност от надеждни цифрови услуги и продукти. В дисертацията се разглеждат въпроси, свързани със сертифицирането на киберсигурността, регулаторните рамки и взаимодействието между публичното регулиране и механизмите за внедряване от страна на частния сектор.

Трудът е изграден логично и е добре структуриран. Той включва въведение, три глави, заключения, използвана литература и приложения. Авторът ясно представя целите, изследователските задачи, методологията и научната хипотеза на изследването.

Представеният труд показва интердисциплинарен подход, като обединява аспекти на киберсигурността, регулаторната политика, управлението на информационната сигурност, управлението на риска и

рамките за цифрово доверие. Авторът разглежда както правните основания на Закона за киберсигурността, така и практическите му последици за организациите и частните схеми за сертифициране.

Добро впечатление прави стремежът теоретичният анализ да бъде свързан с практическите перспективи за внедряване, отнасящи се до механизмите за сертифициране, процесите на съответствие и осигуряването на киберсигурност.

2. Оценка на научните и практическите резултати и приноси

Дисертацията включва научноприложни и приложни приноси, свързани с анализа и оценката на въздействието на Регламент (ЕС) 2019/881 върху сертифицирането за киберсигурност и схемите за частна сигурност. Основните научни и приложни приноси могат да се обобщят по следния начин:

Научноприложни приноси

5. Разработена е концептуална рамка, озаглавена „Модел за прогнозиране на частни схеми (PSF)“, предназначена за оценка на ефективността и устойчивостта на частните схеми за сертифициране на киберсигурност в контекста на Регламент (ЕС) 2019/881.
6. Предложен и емпирично валидиран е методологичен подход за оценяване на ефективността на сертифицирането за киберсигурност.
7. Разработен е оригинален модел за избор на частна схема (PSS), насочен към подпомагане на избора и оценката на органи за оценка на съответствието (CABs). Моделът интегрира размита логика и оптимизационни техники чрез прилагането на метода на размита приоритизация (FPM) за обработване на експертни оценки в условия на неопределеност.
8. Формулиран и валидиран е структуриран методологичен процес за избор на CAB, който включва определяне на критерии за оценка, процедури за двойни сравнения, размита трансформация, оптимизация чрез изчисляване на геометрична средна, дефузификация и механизми за подпомагане на процеса на вземане на решения.

Приложни приноси

3. Разработена и валидирана е интегрирана рамка, която съчетава възможностите за стратегическо прогнозиране на модела PSF с оперативните механизми на модела PSS. Рамката формира подход със затворен цикъл, обвързващ планирането на сертифицирането за киберсигурност, процедурите за оценка на съответствието и дейностите по управление на организационната киберсигурност.
4. Валидирането на разработените модели PSF и PSS е осъществено чрез сравнителен анализ, експертни оценъчни процедури и приложение в сценарии за сертифициране на киберсигурност, свързани с IoT среди и частни схеми за сертифициране съгласно рамката на Закона за киберсигурността.

Разработката показва добро познаване на съвременното състояние на изследванията в областта. Кандидатът използва подходяща научна методология и прилага сравнителни и аналитични подходи, които са релевантни на поставените изследователски цели.

Получените резултати имат както теоретична, така и практическа значимост. Те биха могли да бъдат полезни за изследователи, специалисти по киберсигурност, организации, прилагащи схеми за сертифициране, както и за институции, ангажирани с управление и съответствие в областта на киберсигурността.

3. Публикации, свързани с дисертацията

Докторантът е представил една научна публикация от 2026 г., свързана с темата на дисертацията и включена в научно издание, индексирано в Scopus, както и три презентации на международни научни конференции и форуми, посветени на киберсигурността, информационните системи и цифровите технологии.

Публикационната активност съответства на минималните национални изисквания за присъждане на образователната и научна степен „доктор“.

Не са предоставени данни за цитиране от страна на докторанта.

4. Критични забележки и препоръки

Дисертацията се отличава с висока актуалност и с добре структуриран аналитичен подход. Наред с това могат да бъдат направени няколко препоръки:

В отделни раздели изложението има по-описателен характер и би могло да бъде подобрено чрез по-синтезирано представяне на разглежданите регулаторни рамки.

Практическата приложимост на формулираните изводи може допълнително да се засили чрез по-широка емпирична проверка или чрез казуси, включващи организации, които внедряват схеми за сертифициране на киберсигурност.

В бъдещи изследвания би могло допълнително да се проучи връзката между европейските разпоредби за киберсигурност, секторно-специфичните рамки за сертифициране и нововъзникващите технологии, сред които облачните услуги, системите с изкуствен интелект и екосистемите от интернет на нещата.

5. Лични впечатления

Представените материали показват добра теоретична подготовка, аналитично мислене и способност за провеждане на самостоятелни научни изследвания. Докторантът демонстрира разбиране на сложни проблеми, свързани с управлението на киберсигурността, както и умение за работа с интердисциплинарен научен материал.

6. Заключение

Формулираните препоръки и забележки не намаляват стойността на разработката.

Докторантът разполага със задълбочени теоретични знания по разглежданата тематика, както и със способности за осъществяване на самостоятелни научни изследвания и за практическо внедряване на постигнатите резултати.

Считам, че дисертацията е актуална, предложените методики могат да намерят широко приложение в различни сфери. Представеният дисертационен труд като значимост на изследванията представлява една задълбочена и завършена изследователска разработка, съдържа достатъчно научноприложни

и приложни приноси. Удовлетворени са изискванията на *Закона за развитие на академичния състав в Република България* и на *Правилника* за неговото прилагане, както и на *Правила и процедури за приемане и обучение на докторанти и придобиване на ОНС „Доктор“* във ВСУ „Черноризец Храбър”.

Постигнатите резултати ми дават достатъчно основание да дам положителна оценка на представената дисертация и да предложа на уважаемото **Научно жури да присъди на Рахели Менда Шабат Мор образователната и научна степен „доктор“** в докторската програма „Информационни системи и технологии, информатика и компютърни науки“, професионално направление 4.6. „Информатика и компютърни науки“.