

РЕЦЕНЗИЯ

от проф. д-р инж. Найден Вълков Ненков
Шуменски университет “Епископ Константин Преславски“
относно: Дисертационен труд за присъждане на образователната и научна
степен „ДОКТОР“ на **Рахели Менда-Шабат**
на тема: „**Влияние на Регламент (ЕС) 2019/881 (Акт за
киберсигурността) върху разширяването на сертификациите по
киберсигурност**“

Професионално направление: **4.6 „Информатика и компютърни науки“**
Докторска програма: „**Информационни системи и технологии,
информатика и компютърни науки**“

1. Уводни данни за докторанта и процедурата

Представеният дисертационен труд е разработен от **Рахели Менда-Шабат**, докторант на самостоятелна подготовка към катедра „Компютърни науки“ на ВСУ „Черноризец Храбър“. Научни ръководители са доц. д-р Галина Милева и доц. д-р Златогор Минчев. Дисертацията е успешно обсъдена и насочена за защита пред научно жури.

Не познавам лично Рахели Менда-Шабат, но от предоставените ми документи автобиографията (CV) мога да отбележа нейното активно присъствие и участие в областта на разглежданата тематика в дисертационния труд като практически експерт и специалист.

Докторантът заявява, че участва в сертифицирането по киберсигурност над 30 години на проекти с полупроводници и повече от 20 години в разработването, тестването и сертифицирането на продукти за киберсигурност. В момента е вицепрезидент „Сертифициране по киберсигурност“ в корпорация Winbond, ръководейки програми за сертифициране на продукти в съответствието с глобалните стандарти и регулаторните изисквания за сигурност и безопасност. Тя е активен сътрудник в международните стандарти и регулаторни рамки (ISO/IEC), участвайки в комитети и работни групи, оформящи разпоредбите за киберсигурност, сигурна свързаност и устойчивост на продуктите.

Докторантът участва като технически експертен член на **Европейския комитет** за стандартизация (CEN: European Committee for Standardization) и **Европейския комитет** за стандартизация в електротехниката (CENELEC: European Committee for Electrotechnical Standardization), **допринасяйки за определянето на изискванията за сигурност за Директивата за радиосъоръженията (RED) и Закона за киберустойчивост (CRA)**. От 2000 г. участва в стандартизацията на сигурността, включително ранни дефиниции на модули за надеждна платформа (TPM – Trusted Platform Module). Заема също ръководни позиции в Eurosmart и GlobalPlatform, ръководейки технически групи, които усъвършенстват стандартите за киберсигурност и регулаторната готовност.

2. Актуалност и значимост на темата

Темата е изключително актуална за IoT (**Internet of Things** - Интернет на нещата) сектора, който експоненциално нараства с всяка година с включването на много нови устройства за умните домове, градове и машини. Международният стандарт **ISO/IEC 15408** е известен като **Общи критерии за оценка на сигурността на информационните технологии**, по който се прави оценка на сигурността на продуктите им, като се проверява дали отговарят на специфични, признати критерии за сигурност. Стандартът среща затруднения при обслужването на този мащабен пазар поради зависимостта си само от публични органи. Изследването в дисертацията акцентира на критичната празнота в литературата относно интегрирането на **частни органи за оценяване на съответствието (CABs)** съгласно новата регулаторна архитектура на ЕС (CSA, RED, CRA).

Споменатият по-рано експертен опит „от първа ръка“ на докторанта превръща анализа на стандарти като **EN 18031** в дисертацията от теоретичен обзор в професионална оценка с висока приложна стойност.

3. Обща характеристика и структура на труда

Дисертацията е в обем от **218 страници**, структурирана в увод, три глави, заключение и приложения. Научният апарат включва **29 таблици, 21 фигури и библиография от 187 литературни източника**. Структурата е логична и последователна, водеща от теоретичен анализ към разработване на иновативни модели и тяхната емпирична проверка.

4. Методология на изследването

Авторът прилага мултидисциплинарна методология, съчетаваща регулаторен анализ, казусни изследвания и напредничаво количествено моделиране. Избраните методи – **многофазно сценарийно моделиране** (за макрониво) и **Метод на размито приоритизиране (FPM - Fuzzy Prioritization Method)** за микрониво са високотехнологични инструменти, адекватни за управление на несигурността и субективността в сложните системи за киберсигурност.

5. Аналитична оценка на съдържанието на труда

Глава първа разглежда регулаторната среда и стандарти, при което е извършена детайлна класификация на **20 международни и регионални стандарта** (вкл. SESIP и EN 18031).

Направеният анализ за включването на частни схеми в европейската рамка за сертифициране на киберсигурността бележи ключова и спорна регулаторна промяна. Това е обусловено от необходимостта за мащабируемост, гъвкавост и съгласуваност с индустрията на бързо развиващи се сектори какъвто е IoT. Анализирани са основните предизвикателства и са показани начини за тяхното решаване. Основният извод е, че ЕС преминава към **хибридна екосистема**, в която частните Органи за оценка на съответствието (CABs - Conformity Assessment Bodies) стават жизненоважни поради капацитетните ограничения на държавните

структури. Ценността тук е в идентифицирането на доверието и легитимността като централни проблеми при тяхното установяване.

Глава втора е озаглавена: Модел за успешен прием на микро- и макроравнище при частни схеми – оценка на алтернативни модели и разработване на нов модел. Предложени са два оригинални инструмента. **PSF (Private Scheme Forecasting - Прогнозиране на частни схеми)** представлява значителна иновация на макрониво в дисертационния труд, предлагаща научно обоснована рамка за прогнозиране на системния успех при възприемането на частни сертификационни схеми в IoT екосистемата. Прогностичната стойност на PSF модела се изразява в няколко критични направления, които са от съществено значение за индустрията и регулаторите: **идентифициране на жизнеспособни сертификационни пътища** при който анализът на кръстосаната съвместимост (CCM) показва, че около 20% (65 сценария) от теоретично възможните комбинации са практически правдоподобни; **технологично приоритизиране** където моделът прогнозира, че високите нива на сигурност изискват преход към хардуерно ориентирани архитектури като nanotechnology - нанотехнологии и вграден софтуер, подкрепени от независима оценка от трета страна; **разкриване на скритите рискове** чрез 3D моделирането на измеренията при „Защита на ключове“ и „Сигурно съхранение“ са идентифицирани като попадащи в „критичната зона“ и **валидиране на пазарната жизнеспособност.**

Моделът **PSS (Private Scheme Selection - Избор на частна схема)** реформира възприемането на сертификацията, като я представя не като пречка пред конкурентоспособността, а като инструмент за изграждане на доверие, което е валидирано чрез реални продукти (Winbond W75F и др.) и потвърждава прогностичните допускания – сертифицираните продукти постигат по-висока сигурност без влошаване на производителността.

Докторантът прави извод, че тези модели елиминират субективността на експертната преценка.

Глава трета е със заглавието - Модел за успешно приемане на частна схема в микро и макро-система – реализация на модела и имплементация на резултатите. Тук се представя постъпково описание на двата модела, предложени от докторанта: Модел за прогнозиране на частни схеми (PSF - Private Scheme Forecasting Model) и Моделът за избор на частна схема (**PSS - Private Scheme Selection Model**). Двата модела описват теоретичните им аспекти и много добро впечатление оставя математическата обосновка, използваща теорията на размитите множества (fuzzy sets) и релевантното ѝ приложение в този труд. При верификацията и валидацията на моделите се използват практически примери от добрата експериментална работа на докторанта с real IoT компоненти. Резултатите са показани с таблици и графики за всеки модел. **Сравнителният анализ на сертифицираните продукти (като например Winbond W75F) спрямо несертифицираните аналози в избраните три IoT категории показва, че тези резултати са статистически значими ($p < 0.001$) и доказват, че сертификацията повишава сигурността без влошаване на производителността.**

6. Основни научни и научно-приложни приноси

Разработване на PSF модел (Макрониво).

Моделът е базиран на 324 сценарийни комбинации, от които едва **20%** са идентифицирани като практически правдоподобни. **3D анализът на чувствителността** картографира рисковете, разкривайки скрити заплахи в зони като „Защита на ключове“ и „Сигурно съхранение“, които са критични за системната устойчивост.

Математическа обосновка на PSS модела (Микрониво).

Използването на триъгълни размити числа (Triangular Fuzzy Numbers - TFN) и метода на центроида позволява превръщане на субективни мнения

в конкретни тегла: **Доверие (38%)**, Правоприлагане (23%), Легитимност (16%), Качество (11%) и Ефективност (11%). Математическата надеждност е доказана с Коефициент на съгласуваност **CR = 0.0195** (значително под прага 0.10).

Интегрирана макро-микро рамка: Създадена е затворена система, в която стратегическото прогнозиране информира оперативните решения за избор на САВ, служеща като пътна карта за хармонизиране на частните и публичните схеми в ЕС.

7. Личен принос и публикационна дейност

Личният принос на Рахели Менда-Шабат е безспорен, базиран на лидерските ѝ роли в **Eurosmart** и **GlobalPlatform**. Публикационната дейност включва **7 публикации** в Springer, BISEC, AdComSys. Наукометричните показатели на докторанта напълно отговарят на минималните национални и университетски изисквания.

8. Оценка на автореферата

Авторефератът е изготвен съгласно изискванията и вярно и точно отразява основното съдържание и приносите на дисертационния труд. Възможно е да бъде допълнен с малко повече **фактология, отразяваща самите теоретични модели** и тяхната връзка с показаните резултати.

9. Критични бележки и въпроси

Бележката ми към автореферата е, че има възможност по-подробно да се покажат и част от теоретичните обосновки на разработените модели и връзката им с резултатите. Според мен така пред четящите тази кратка форма още по-убедително ще се обосноват и защитят тезите на докторанта в дисертационния труд.

Може да се избегнат и някои неточности при оформление на таблиците и текста при пренасянето между страниците.

Препоръчвам в бъдещата работа докторантът да изследва по-детайлно въздействието на **изкуствения интелект** върху автоматизираните процеси за сертифициране, идентифициран в труда като потенциална заплаха или възможност.

Въпрос към докторанта: Как предложените модели PSF и PSS могат да се адаптират към концепцията за „**постоянно наблюдение на сигурността**“ през целия жизнен цикъл на продукта, изисквано от Закона за киберустойчивост (CRA- Cyber Resilience Act) ?

10. Становище по наличието на плагиатство

В дисертационния труд по моето мнение **не установявам наличие на плагиатство**. Авторът е спазил стриктно етичните норми и е цитирал коректно използваните източници.

11. Заключение

Дисертационният труд на **Рахели Менда-Шабат** представлява самостоятелно, завършено, иновативно и научно издържано изследване със значим приложен ефект за европейската сертификационна практика. Критичните бележки не омаловажават постигнатите резултати и тяхната актуалност.

Всичко това ми дава пълно основание да предложа на уважаемото научно жури да оцени дисертацията с **ПОЛОЖИТЕЛНА ОЦЕНКА** и да присъди на Рахели Менда-Шабат образователната и научна степен „**ДОКТОР**“ в професионално направление 4.6 „Информатика и компютърни науки“.

Дата: 05.06.2026 г.

Рецензент:

проф. д-р инж. Найден Ненков