ВАРНЕНСКИ СВОБОДЕН УНИВЕРСИТЕТ
„ЧЕРНОРИЗЕЦ ХРАБЪР“
ФАКУЛТЕТ ПО СОЦИАЛНИ, СТОПАНСКИ И КОМПЮТЪРНИ НАУКИ
КАТЕДРА „КОМПЮТЪРНИ НАУКИ“

РАХЕЛИ МЕНДА ШАБАТ

ВЛИЯНИЕ НА РЕГЛАМЕНТ (ЕС) 2019/881 (АКТ ЗА КИБЕРСИГУРНОСТТА) ВЪРХУ РАЗШИРЯВАНЕТО НА СЕРТИФИКАЦИИТЕ ПО КИБЕРСИГУРНОСТ

АВТОРЕФЕРАТ

на дисертационен труд за присъждане на образователно и научна степен „ДОКТОР“, професионално направление 4.6. „Информатика и компютърни науки“, докторска програма „Информационни системи и технологии, информатика и компютърни науки“

Научен ръководител:
Доц. д-р Галина Милева
Доц. д-р Златогор Минчев

Варна, 2026

ВАРНЕНСКИ СВОБОДЕН УНИВЕРСИТЕТ
„ЧЕРНОРИЗЕЦ ХРАБЪР“
ФАКУЛТЕТ ПО СОЦИАЛНИ, СТОПАНСКИ И КОМПЮТЪРНИ НАУКИ
КАТЕДРА „КОМПЮТЪРНИ НАУКИ“

РАХЕЛИ МЕНДА ШАБАТ

ВЛИЯНИЕ НА РЕГЛАМЕНТ (ЕС) 2019/881 (АКТ ЗА КИБЕРСИГУРНОСТТА) ВЪРХУ РАЗШИРЯВАНЕТО НА СЕРТИФИКАЦИИТЕ ПО КИБЕРСИГУРНОСТ

АВТОРЕФЕРАТ

на дисертационен труд за присъждане на образователно и научна степен „ДОКТОР“, професионално направление 4.6. „Информатика и компютърни науки“, докторска програма „Информационни системи и технологии, информатика и компютърни науки“

Научен ръководител:
Доц. д-р Галина Милева
Доц. д-р Златогор Минчев

Рецензенти:
проф. д-р Теодора Бакърджиева
проф. д-р Найден Ненков

Варна, 2026

Дисертационният труд е структуриран в увод, три глави, заключение, библиография и приложения, с общ обем 213 страници. Основният текст съдържа 25 таблици и 21 фигури. Списъкът на използваната литература включва общо 187 източника.

Дисертационният труд е обсъден от членовете на катедра „Компютърни науки“ и е насочен за защита пред научно жури. Авторът на дисертационния труд е докторант на самостоятелна подготовка към катедра „Компютърни науки“, факултет „Социални, стопански и компютърни науки“ на Варненския свободен университет „Черноризец Храбър“.

Публичната защита на дисертационния труд ще се проведе на заседание на научното жури на 07.07.2026 г. от 11:00 ч. в заседателната зала на Варненския свободен университет „Черноризец Храбър“.

Материалите по защитата са на разположение в канцеларията на катедра „Компютърни науки“ към Факултета по социални, стопански и компютърни науки на Варненския свободен университет „Черноризец Храбър“ и на интернет адрес: www.vfu.bg, раздел "Докторанти".

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Въведение

В днешната хиперсвързана среда киберсигурността се разви от допълнителен аспект в критична необходимост. Нарастващата зависимост от цифровата инфраструктура изложи отделните лица, бизнеса и публичните институции на все по-сложни рискове за сигурността, вариращи от атаки срещу инфраструктурата и мащабни пробиви в данните до рансъмуер и финансови престъпления, извършвани чрез киберсредства.

Рамката на Общите критерии на ЕС (Common Criteria, CC) (ISO/IEC 15408) дълго време доминираше в сертифицирането на сигурността. Нейното изключително разчитане на публични сертифициращи органи обаче създаде структурни ограничения, които възпрепятстваха мащабируемостта, повишаваха разходите и забавяха навлизането на пазара, особено в бързо разрастващия се сектор на Интернет на нещата (IoT).

Актът на ЕС за киберсигурността (CSA) 2019/881 отбеляза съществена промяна, като отвори процесите на сертифициране за частни органи за оценяване на съответствието (CABs). Това бе последвано от задължителни изисквания съгласно Делегирания акт към Директивата за радиосъоръженията (EU) 2022/30 и Акта за киберустойчивостта (CRA) (EU) 2024/2847. Тази хибридна среда поставя основни въпроси относно ролята, надеждността и легитимността на частните CABs в рамките на европейската система за сертифициране.

Освен това е необходимо да се провери въздействието от навлизането на частните CABs в екосистемата върху тенденциите за пазарно възприемане на сертификациите за сигурност.

2. Актуалност и значимост на изследователската тема

Актуалността на настоящия дисертационен труд се определя от неотложната необходимост от мащабиране на сертифицирането на киберсигурността за IoT устройства в отговор на бързото разпространение на свързани продукти, развиващата се регулаторна рамка на ЕС и структурните ограничения на традиционното сертифициране, ръководено от публични органи. Повечето IoT устройства остават несертифицирани, главно поради разходи, време

и процедурна сложност. В същото време те все по-често обработват чувствителни или критични данни.
Наред с това липсват научно обосновани изследвания, които да разглеждат условията, при които частните CABs могат надеждно да бъдат интегрирани в област, исторически управлявана от публични органи. Настоящият дисертационен труд разглежда тази празнота, като предлага както теоретична рамка, така и емпирична валидация. По този начин той отговаря на съществена потребност на създателите на политики, производителите и сертифициращите органи.

3. Обект и предмет на изследването

Обект на настоящия дисертационен труд е европейската рамка за сертифициране на киберсигурността на IoT устройства, с акцент върху механизмите, чрез които CABs, както публични, така и частни, оценяват и валидират сигурността на свързаните продукти.
Предметът на изследването се фокусира върху влиянието на три ключови регулаторни инструмента на ЕС: Акта за киберсигурността (CSA) 2019/881, Делегирания акт към Директивата за радиосъоръженията 2022/30 и Акта за киберустойчивостта 2024/2847. По-конкретно, дисертационният труд изследва как тези регламенти формират възприемането и легитимността на частните схеми за сертифициране на киберсигурността и как влияят върху доверието, осигуряването на качеството, хармонизацията и пазарното приемане.

4. Изследван проблем

Изследваният проблем представлява шестизмерно несъответствие между бързо нарастващата необходимост от мащабируемо и икономически ефективно сертифициране на киберсигурността на IoT устройства и капацитета на настоящата рамка да го осигури:
(1) Могат ли частните CABs да гарантират същото качество на оценяване като публичните схеми?
(2) Създава ли тяхното участие риск от регулаторно несъответствие?
(3) Как могат частните и публичните схеми да бъдат хармонизирани с оглед на взаимно признаване?
(4) Как могат частните схеми да придобият легитимност, без да подкопават държавния авторитет?

(5) Може ли съответствието с изискванията за киберсигурност да бъде постигнато, без да се влошава производителността на IoT продуктите или тяхното пазарно възприемане?
(6) Кои критерии и методологически подходи следва да насочват избора на CAB, за да се осигури успешно сертифициране?

5. Авторова теза

Основната защитавана теза е двуаспектна:
Първо, признаването на частните CABs като легитимни субекти в рамките на системата на ЕС за сертифициране на киберсигурността, регулирани чрез стандарти за акредитация, механизми за прозрачност и регулаторната архитектура на CSA/RED/CRA, може значително да повиши мащабируемостта и ефективността на сертифицирането на сигурността на IoT, без да компрометира качеството или хармонизацията.
Второ, IoT продуктите, сертифицирани по признати схеми за киберсигурност, показват измеримо по-високи нива на внедрени функции за сигурност в сравнение с еквивалентни несертифицирани продукти, без това да води до значими загуби в производителността.
Тези тези се операционализират чрез два нови модела: модел за прогнозиране на частни схеми (Private Scheme Forecasting, PSF), който осигурява макониво на системна прогноза относно възприемането на сертификацията, и модел за избор на частна схема (Private Scheme Selection, PSS), който предлага структуриран инструмент за вземане на решения на микониво при избора на CAB.

6. Цел и задачи на дисертационния труд

Основната цел на настоящия дисертационен труд е да разработи научно обосновани, хармонизирани модели, които улесняват прогнозиране на успешното интегриране на частни сертификационни схеми в по-широката сертификационна екосистема, както и да формализира тези модели в надеждна рамка за вземане на решения при избора на CAB.
За постигането на тази цел са формулирани следните шест задачи:
Задача 1: Оценяване на качеството и ефективността.
Задача 2: Анализ на регулаторното въздействие.
Задача 3: Разработване на стратегии за хармонизация.
Задача 4: Изследване на механизмите за доверие.
Задача 5: Оценяване на пазарното възприемане и мащабируемостта.

Задача 6: Формулиране на модел за вземане на решения при избора на САВ.

7. Методология на изследването

Настоящият дисертационен труд използва мултидисциплинарна методология, която съчетава регулаторен анализ, сравнителни изследвания, казусни изследвания и количествено моделиране в рамките на два интегрирани подхода:

Теоретико-аналитичен: задълбочен преглед на законодателството; сравнителен анализ на сертификационни рамки; и казусни изследвания от сектори, в които частни схеми допълват публичния надзор.

Емпирико-моделиращ: модел за прогнозиране на частни схеми (PSF), използващ многофазно сценарийно моделиране, което включва морфологичен анализ, матрица за кръстосана съвместимост, прогностично аналитично моделиране и анализ на чувствителността за оценка на динамиката на възприемане на макониво; и модел за избор на частна схема (PSS), основан на метода на размито приоритизиране (Fuzzy Prioritization Method, FPM) за структурирано вземане на решения при избора на САВ. И двата модела са валидирани чрез емпирична оценка.

8. Ограничения на проблемния обхват на докторския труд

Ограниченията на настоящото изследване включват: разчитане на публично достъпна техническа документация при емпиричното сравнение на продуктите; ограничаване на експерименталната валидация до три представителни категории IoT продукти; изключване на собственически данни за разходите, свързани със сертификационните процедури; и фокус предимно върху регулаторния контекст на ЕС. Бързо развиващият се характер на заплахите и регулациите в областта на киберсигурността също означава, че част от резултатите може да изискват актуализиране с развитието на новите законодателни инструменти, особено CRA, който към момента на написване все още е в ранен етап на прилагане.

II. РАЗМЕР И СТРУКТУРА НА ДИСЕРТАЦИЯТА

Дисертационният труд е структуриран в увод, три глави, заключение, библиография и приложения, с общ обем 213 страници. Основният текст съдържа 25 таблици и 21 фигури. Списъкът на използваната литература включва 187 източника, включително международни и интернет източници. Освен това са включени 2 приложения (списък на акронимите и таблици за класификация на стандартите за киберсигурност):

СЪДЪРЖАНИЕ

III. ОБОБЩЕНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

УВОД

В увода се обосновават актуалността и значимостта на изследователския проблем, като се проследява развитието на киберсигурността от тясно технически въпрос, запазен предимно за отбранителни и правителствени системи, до критична обществена необходимост, засягаща всяко измерение на съвременния икономически, политически и социален живот. Нарастващата зависимост от цифровата инфраструктура съществено трансформира средата на заплахите: цифрови атаки като мащабни пробиви в данните, инциденти с рансъмуер, саботаж на инфраструктура, индустриален шпионаж и финансови престъпления, извършвани чрез киберсредства, стават все по-чести, по-сложни и с по-сериозни последици в различни сектори, сред които банковото дело, здравеопазването, енергетиката и публичната администрация. Централно място в тази трансформация заема безпрецедентното разпространение на устройствата от Интернет на нещата (IoT). Прогнозира се глобалният IoT сектор да достигне сложен годишен темп на растеж (CAGR), надхвърлящ 25% за периода 2020-2025 г., като генерира милиарди взаимосвързани устройства, които обработват и обменят огромни обеми чувствителни данни. Въпреки това значителна част от тези устройства навлизат на пазара без надеждни функции за сигурност, а повечето остават несертифицирани, главно поради факта, че доминиращата сертификационна рамка, Common Criteria (ISO/IEC 15408), е разработена за правителствени и отбранителни контексти и разчита изключително на публични сертифициращи органи дори при ниски нива на увереност.

Това структурно несъответствие между мащаба на IoT екосистемата и капацитета на сертификационния апарат формира основното напрежение, което мотивира настоящото изследване.

В увода се определят обектът и предметът на дисертационния труд: европейската рамка за сертифициране на киберсигурността на IoT устройства и по-конкретно влиянието на три ключови регулаторни инструмента на ЕС, Акта за киберсигурността (CSA) 2019/881, Делегирания акт към Директивата за радиосъоръженията 2022/30 и Акта за киберустойчивостта (CRA) 2024/2847, върху възприемането

и легитимността на частните органи за оценяване на съответствието (CABs).
Изследователският проблем е формулиран като шестизмерно предизвикателство: осигуряване на качеството, регулаторно съответствие, хармонизация, легитимност и доверие, пазарно възприемане и мащабируемост, както и структурирано вземане на решения при избора на CAB.
Представена е двуаспектната изследователска теза, че частните CABs могат да осигурят сертифициране със съпоставимо или по-високо качество в сравнение с публичните схеми, както и че сертифицираните IoT продукти показват измеримо по-високи нива на внедрени функции за сигурност, без това да води до загуби в производителността.
В увода се конкретизират шестте изследователски задачи, съотнесени към тези измерения, описва се мултидисциплинарната методология, която съчетава законодателен анализ, сравнителни казусни изследвания, математическо прогнозиране и емпирична оценка на продукти, и се очертава триглавната структура на дисертационния труд, завършваща с два оригинални модела, модел за прогнозиране на частни схеми (Private Scheme Forecasting, PSF) на макониво и модел за избор на частна схема (Private Scheme Selection, PSS) на микониво, като основни научни приноси на дисертационния труд.

ГЛАВА ПЪРВА: СЕРТИФИКАЦИИ ЗА КИБЕРСИГУРНОСТ - ИЗСЛЕДВАНЕ НА РЕГУЛАТОРНАТА СРЕДА, СТАНДАРТИТЕ И CABs ПРЕЗ ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД ВЪЗПРИЕМАНЕТО НА ЧАСТНИ СХЕМИ И ПРЕЗ ПРИЗМАТА НА ТЕОРИЯТА ЗА ЛЕГИТИМНОСТТА

Първа глава изгражда регулаторната, теоретичната и институционалната основа на целия дисертационен труд чрез цялостен и систематичен анализ на средата на сертифициране в областта на киберсигурността.
Главата започва с проследяване на историческите корени на сертифицирането на киберсигурността: от Trusted Computer System Evaluation Criteria на Министерството на отбраната на САЩ (TCSEC,

„Orange Book“, 1983), през европейската ITSEC и канадската CTCPEC, до тяхното обединяване в глобално признатата рамка Common Criteria (CC, ISO/IEC 15408) през 1999 г. Първоначално насочени към правителствени, отбранителни и финансови системи, сертификационните схеми по-късно се разширяват към телекомуникациите, управлението на идентичността и платежните инфраструктури.

Индустриално ориентирани стандарти като ISO/IEC 27001 за управление на информационната сигурност и FIPS 140-2 за криптографски модули също придобиват значимост, като засилват ролята на сертифицирането за изграждане на доверие и постигане на регулаторно съответствие.

До 2010-те години сертифицирането на киберсигурността се утвърждава като ключов инструмент в сектори, които обработват чувствителни данни или управляват критична инфраструктура, но достъпността му остава ограничена поради сложност, разходи и структурното ограничение, произтичащо от изключителната роля на публичния сектор.

Извършена е цялостна класификация и анализ на стандартите за киберсигурност по четири основни измерения.

Първо, вид на обхвата, като се разграничават средови стандарти, насочени към сигурността на средата за разработване, тестване и производство, например ISO/IEC 27001, и функционални стандарти, насочени към възможностите за сигурност, вградени в самия продукт, например Common Criteria и FIPS 140-3, при признаване на дълбоката взаимозависимост между тези две области: функционалните характеристики за сигурност на даден продукт могат да бъдат обезсилени, ако средата за разработване е компрометирана.

Второ, управленско ниво, като се разграничават международни стандарти, разработени от глобално признати органи като ISO/IEC, регионални стандарти като тези, разработвани в рамките на ЕС, и национални стандарти, съобразени със специфичната инфраструктура, среда на заплахи и регулаторни приоритети на отделните държави.

Трето, приложимост, като се разграничават хоризонтални стандарти, предназначени за универсално междусекторно приложение чрез

подходи, основани на оценка на риска, например ISO/IEC 27001 и ISO/IEC 15408, от вертикални стандарти, адаптирани към конкретни пазарни сегменти като автомобилната индустрия (ISO/SAE 21434, UNECE R155), индустриалните системи за управление (IEC 62443) и IoT (ETSI EN 303 645, SESIP).

Четвърто, методология за оценяване, като стандартите се категоризират според това дали изискват самооценка, формална декларация за съответствие (Declaration of Conformity, DoC) или независима оценка от трета страна.

Чрез тази рамка са анализирани и класифицирани двадесет стандарта, включително ISO/IEC 27001, ISO/IEC 15408 (Common Criteria), ISO/IEC 19790, FIPS 140-3, IEC 62443, EN 18031, ETSI EN 303 645, SESIP (EN 17927:2023), ISO/SAE 21434, UNECE R155, PSA Certified, както и национални схеми от Япония (JC-STAR), Сингапур (CLS IoT), САЩ (NIST IR 8259, NIST IR 8425A), Германия (BSI TR-03109-1), Испания (LINCE), Китай (GB/T 18336.1) и Тайван (SSIPS).

Тази класификация разкрива значително разнообразие в методологиите за оценяване и управленските подходи и, което е особено важно, потвърждава съществени празноти в специфичните за IoT сертификационни пътища на международно равнище. Тази констатация пряко мотивира фокуса на дисертационния труд върху частните CABs като решение за постигане на мащабируемост. Систематично са очертани съществените фактори, които обуславят сертификационното предизвикателство при IoT устройствата. Разчитането на рамката Common Criteria на публични сертифициращи органи (CBs) дори при оценки с ниско ниво на увереност EAL1 създава структурни затруднения, които ограничават мащабируемостта, увеличават разходите и забавят навлизането на пазара на бързо развиващи се потребителски IoT продукти. Анализът на празнотите, извършен от ENISA през 2019 г., потвърждава липсата на адекватни стандарти, специфични за IoT. Същевременно сложността на IoT сектора, обхващащ хардуерни компоненти, инфраструктурни устройства и потребителска електроника, изисква експертиза за оценяване, която публичните органи, функциониращи в рамките на правителствени структури и ресурсни ограничения, често не могат да осигурят с необходимата скорост и детайлност, изисквани от пазара.

Регулаторният отговор на ЕС чрез три допълващи се законодателни инструмента е разгледан като възможност за мащабиране на сертифицирането на киберсигурността. Актът за киберсигурността (CSA) 2019/881 въвежда структурирана общоевропейска рамка, която установява три доброволни нива на увереност, базово, съществено и високо, и, което е от ключово значение, за първи път отваря процесите на сертифициране за частни CABs, като по този начин дава възможност за по-широко участие на пазара и за по-гъвкави сертификационни екосистеми.
Делегираният акт към Директивата за радиосъоръженията (EU) 2022/30 установява задължителни изисквания за киберсигурност за определени класове радиосъоръжения, основно чрез декларация за съответствие от производителя съгласно хармонизирани стандарти като EN 18031, като създава задължение за съответствие, без да изисква оценка от трета страна за повечето продукти. Актът за киберустойчивостта (CRA) (EU) 2024/2847 разширява обхвата на задължителното съответствие с изискванията за киберсигурност към много по-широк кръг цифрови продукти с мрежова свързаност, като изисква оценка от трета страна за високорискови категории и значително разширява оперативната роля на CABs в рамките на сертификационната екосистема. Взети заедно, тези три акта създават многопластова регулаторна архитектура, която преминава от доброволност (CSA), през задължителна самооценка и декларация за съответствие (RED), към задължителна оценка от трета страна (CRA), като формира хибридна среда с нарастващо структурно търсене на капацитет от страна на частните CABs.
Теоретичният контекст на публичните спрямо частните регулаторни схеми е анализиран през призмата на теорията за легитимността, като се изследва как организациите и регулаторните актьори придобиват социално приемане и авторитет. Особено релевантни са три измерения на легитимността: прагматична легитимност, произтичаща от практическите ползи, които частните CABs предоставят на производителите и пазарите; морална легитимност, произтичаща от придържането към признати стандарти на поведение и безпристрастност; и когнитивна легитимност, произтичаща от

постепенното възприемане на дадена практика като саморазбираща се в рамките на сектора.
Съображенията при акредитирането на частни CABs за киберсигурност са анализирани задълбочено, като се подчертава специфичното предизвикателство, пред което са изправени CABs в областта на киберсигурността в сравнение с тези в други регулирани области: те работят с криптографски алгоритми и методологии за сигурност, които могат да бъдат класифицирани като активи от значение за националната сигурност и да попадат под действието на регулации за експортен контрол като U.S. EAR и Регламент (ЕО) № 428/2009 на ЕС. Това създава фундаментално напрежение между необходимостта от гъвкавост на частния сектор и държавния императив за защита на чувствителни знания в областта на сигурността.
Разгледани са казуси от аналогични регулирани сектори с цел извеждане на паралели и добри практики: секторът на безопасността на храните, в който частни акредитирани органи извършват продуктови инспекции и одити под регулаторен надзор с доказано високи резултати по отношение на съответствието; секторите на пожарната безопасност и екологичното съответствие, в които частни изпитвателни лаборатории функционират в рамките на задължителни акредитационни режими; и секторът на финансовите услуги, в който частни одиторски фирми извършват оценки със системно значение.
Във всички тези случаи се очертава последователен модел: добре регулирани частни актьори, функциониращи при задължителна акредитация и под въздействието на пазарна отчетност, могат да поддържат, а в много случаи и да надхвърлят регулаторните резултати, постигани чрез изцяло публични механизми. Представен е систематичен анализ на предимствата, секторно специфична експертиза, оперативна гъвкавост, по-бързи цикли на оценяване, отзивчивост към пазара, способност за привличане на специализиран експертен потенциал, и недостатъците, риск от търговски натиск върху стандартите, ограничена прозрачност при липса на надзор, потенциални конфликти на интереси, намален държавен контрол върху знанията, свързани с криптографската сигурност, на частните сертификационни схеми. Обоснована е

необходимостта от специализирани изисквания към CABs в областта на киберсигурността, които надхвърлят общата акредитация по ISO/IEC 17065 и включват безпристрастност в криптографски контексти, проверки за надеждност на персонала и управление на информационната сигурност в самия CAB.

ИЗВОДИ КЪМ ПЪРВА ГЛАВА

Въз основа на извършения анализ се установява, че регулаторната рамка за сертифициране на киберсигурността в ЕС се развива от изцяло публичен, централизиран модел към хибридна публично-частна екосистема, обусловена от съвпадането на пазарното търсене, регулаторната модернизация и технологичното развитие.

Класификацията на 20 стандарта за киберсигурност по четири измерения потвърждава значителното разнообразие от методологии за оценяване и управленски подходи, използвани понастоящем в световен мащаб, и откроява съществени празноти в специфичните за IoT сертификационни пътища на международно равнище.

Показано е, че сближаването между Акта за киберсигурността (CSA), Делегирания акт към Директивата за радиосъоръженията (RED Delegated Act) и Акта за киберустойчивостта (CRA) създава както възможности, така и структурни напрежения при интегрирането на частни CABs: CSA отваря възможност за тяхното участие, RED създава задължително търсене на съответствие, което натоварва капацитета на публичните органи, а CRA допълнително засилва това търсене, като изисква оценяване от трета страна за високорискови категории.

Идентифицирани са централните предизвикателства: доверие, легитимност, осигуряване на качеството, регулаторна хармонизация, пазарна мащабируемост и структуриран избор на CAB. Те са теоретично обосновани и формулирани като шест изследователски задачи, разгледани в следващите глави.

Анализът на казуси от различни сектори изгражда основната доказателствена база, че частните регулаторни актьори, когато са адекватно управлявани и подложени на ефективен надзор, могат да постигат регулаторни резултати, съпоставими с тези на публичните им аналози или дори по-добри от тях. Това осигурява теоретично основание за основната теза на дисертационния труд.

ГЛАВА ВТОРА: МИКРО-МАКРО МОДЕЛ ЗА УСПЕШНО ВЪЗПРИЕМАНЕ НА ЧАСТНИ СХЕМИ - ОЦЕНКА НА ВЪЗМОЖНИ МОДЕЛИ И РАЗРАБОТВАНЕ НА МОДЕЛ

Втора глава разработва теоретичната и методологическата рамка на двата оригинални модела в дисертационния труд, като преминава през три етапа: оценка на възможни подходи за моделиране, избор и обосновка на най-подходящите подходи и формално разработване на моделите PSF и PSS.

Главата започва с обосноваване на необходимостта от математическо моделиране в настоящото изследване. Решението за интегриране на частни схеми в сертифицирането на киберсигурността включва широк кръг променливи - институционална надеждност, възможности за стандартизация, пазарна динамика, техническа отзивчивост, регулаторно съответствие, които взаимодействат по сложен, нелинеен и динамично развиващ се начин.

Прекалено стеснен модел би довел до неточни изводи; недостатъчно строг модел не би могъл да обхване системните взаимозависимости, които определят реалните резултати от сертифицирането. Поради това изборът на подходящи рамки за моделиране представлява основно методологическо решение.

Задълбочено са оценени три възможни подхода за моделиране:

1. House of Quality (HoQ) - основан на Quality Function Deployment (QFD), предоставя структурирана матрична методология, която трансформира потребностите на клиентите или заинтересованите страни в технически проектни изисквания. Макар да е интуитивен и добре утвърден в контекста на продуктовото разработване, неговата

статична структура и ограничената му способност да отчита вероятностна несигурност или нелинейни взаимозависимости го правят недостатъчно гъвкав за динамичната и развиваща се среда на заплахи при сертифицирането на киберсигурността.
2. Размит аналитичен йерархичен процес (Fuzzy AHP) - съчетава йерархичното структуриране и приоритизирането на критерии от класическия AHP с теорията на размитите множества, като позволява на вземащите решения да изразяват преценките си чрез лингвистични променливи, например „умерено по-важен“, „значително по-важен“, които се преобразуват в триъгълни размити числа, вместо да се изискват точни числови стойности. Този подход повишава надеждността при групово вземане на решения в условия на несигурност и позволява приоритизиране на нематериални или качествени критерии, което го прави особено подходящ за многокритериалния проблем при избора на CAB. Въпреки това неговата изчислителна сложност и възможността за субективно влияние при дефинирането на размити скали го правят по-малко подходящ като инструмент за прогнозиране на макрониво.
3. Многофазно сценарийно моделиране - интегриращо морфологичен анализ, оценка чрез матрица за кръстосана съвместимост, прогностично аналитично моделиране и 3D анализ на чувствителността, е избрано като основен инструмент на макрониво поради по-високия му капацитет да отчита сложни, многоизмерни и развиващи се рискови среди. Извършено и представено е систематично сравнение по критерии като гъвкавост, отчитане на несигурността, многоизмерност, изчислителна приложимост и приложимост към сертифицирането на киберсигурността, което потвърждава основанията за избора.
Моделът за прогнозиране на частни схеми (Private Scheme Forecasting, PSF) е разработен като рамка на макрониво, използваща многофазно сценарийно моделиране за прогнозиране на системния успех при възприемането на частното сертифициране на киберсигурността в IoT екосистемата. PSF е структуриран около четири аналитични фази:
Във Фаза 1 проблемното поле е дефинирано чрез идентифициране на десет ключови измерения и фактора, които влияят върху резултатите от сертифицирането, като се излиза отвъд конвенционалните

технически показатели и се включват съображения, свързани с човешкия фактор, икономически и пазарни въздействия, междусекторни взаимозависимости и съгласуваност с глобалните стандарти - включително мерки за сигурност, сигурно съхранение, защита на ключове, защита на системи, интелигентни електропреносни мрежи, IoT, защита на комуникациите, защита на потребителските данни, човешки фактор и киберустойчивост.

Във Фаза 2 морфологичният анализ създава структурирана морфологична матрица, която картографира връзките между нивата на гарантиране на сигурността, технологичните области, методите за оценяване и видовете внедряване чрез принципите на размитата логика. Това позволява системно генериране на възможни сертификационни сценарии и оценка на тяхната вътрешна съгласуваност чрез кръстосана съвместимост.

Във Фаза 3 прогностичното аналитично моделиране надгражда морфологичния анализ чрез въвеждане на предиктивни техники - вероятностна симулация и размита логика, за оценяване на дългосрочните вероятности за успех на сертифицирането при различни сценарийни конфигурации, като използва представяния чрез насочени графи и разпределение на Дирихле за моделиране на развиващи се рискови профили.

Във Фаза 4 3D анализът на чувствителността използва триизмерно моделиране, за да определи чувствителността на сценариите и да идентифицира потенциални скрити заплахи, които биха могли да подкопаят сертификационните схеми, включително уязвимости във веригата на доставки, атаки, задвижвани от изкуствен интелект, и рискове, свързани с квантовите изчисления.

Моделът за избор на частна схема (Private Scheme Selection, PSS) е разработен като структуриран инструмент за вземане на решения на микониво, насочен към шестата изследователска задача: дефиниране на критериите и методологическия подход, които следва да насочват решението за ангажиране на частен CAB. Моделът е изграден върху метода на размитото приоритизиране (Fuzzy Prioritization Method, FPM), който преодолява ограниченията, присъщи на изцяло точните AHP подходи, чрез включване на експертната несигурност посредством преобразуване на лингвистични преценки.

Въз основа на теоретичния анализ в дисертационния труд са дефинирани пет критерия за избор:
• Легитимност - признание на CAB, обхват на акредитацията и доказана безпристрастност в различни региони и нива на увереност.
• Качество - яснота, последователност и надеждност на издаваните сертификационни доклади.
• Ефективност - оперативен капацитет, експертна задълбоченост, продължителност на оценяването и иновативни процеси на оценка.
• Правоприлагане - обхват на притежаваните акредитации и покритие в различни регулаторни сегменти.
• Доверие - доверие на заинтересованите страни, доказано чрез обема и разнообразието на издадените сертификации и оценените нива на сигурност.
Двойните сравнения между тези пет критерия са установени въз основа на теоретичен анализ и практически опит, преобразувани са в триъгълни размити числа (TFNs) чрез съответствието Saaty(k) → (k−1, k, k+1), изчислени са геометрични средни стойности за всеки критерий, размитите тегла са нормализирани и е извършена дефазификация чрез центроидния метод ($w_i = (L_i + M_i + U_i) / 3$). Получените нормализирани тегла на критериите - доверие (38%), правоприлагане (23%), легитимност (16%), качество (11%), ефективност (11%), отразяват водещото значение на доверието на заинтересованите страни и на регулаторния авторитет при избора на CAB в контекста на киберсигурността, където чувствителността на криптографските материали и последиците за националната сигурност превръщат доверието в основна предпоставка за легитимност.
Формализиран е шестстъпков инструмент PSS за практическо приложение, който позволява на всеки производител или собственик на схема да въведе оценки за представянето на CAB по скала от 1 до 10, да изчисли претеглени общи резултати, да ги нормализира в проценти и да получи класирана препоръка за избор.

ИЗВОДИ КЪМ ВТОРА ГЛАВА

Сравнителната оценка на моделите потвърждава, че многофазното сценарийно моделиране предлага най-строгата и гъвкава аналитична основа за прогнозиране на сложната, многоизмерна динамика при

възприемането на сертификационни схеми, докато Fuzzy AHP предоставя най-подходящата методология за структуриран избор на CAB в условия на експертна несигурност.
Разработването на модела PSF идентифицира три ключови условия за ефективно интегриране на частни схеми: иновативни стратегии за оценяване, основани на риска, които надхвърлят формалното съответствие по контролен списък; реалистично и вътрешно съгласувано конструиране на сценарии, което балансира между изчерпателност и правдоподобност; и системна интеграция между технологични, регулаторни и методологически измерения, вместо стеснен фокус върху отделни сертификационни пътища.
Формализирането на модела PSS показва, че размитата логика успешно отчита присъщата субективност и неточност на експертната преценка при многокритериалното оценяване на CAB, като генерира стабилни, защитими и прозрачни приоритетни тегла, които могат да насочват както отделни сертификационни решения, така и по-широко разработване на политики.
Взети заедно, моделите PSF и PSS изграждат допълваща се макро-микро система: PSF осигурява прогностична перспектива относно цялостната системна роля и стойност на частните сертификационни схеми, докато PSS предоставя оперативна методология за прилагане на тези изводи чрез структуриран, основан на доказателства избор на CAB.

ГЛАВА ТРЕТА: МИКРО-МАКРО МОДЕЛ ЗА УСПЕШНО ВЪЗПРИЕМАНЕ НА ЧАСТНИ СХЕМИ - ПРИЛОЖЕНИЕ НА МОДЕЛА И ВАЛИДИРАНЕ НА РЕЗУЛТАТИТЕ

Трета глава прилага и емпирично валидира двата модела, като превежда теоретичните и методологическите рамки, разработени във втора глава, в конкретни аналитични резултати и практически приложими изводи. Главата преминава през цялостното прилагане и валидиране на модела PSF, последвано от прилагането и валидирането на модела PSS, и завършва с интегриран анализ, свързващ макро- и микроперспективата.
Прилагането на модела PSF е осъществено в четири аналитични фази. Във фазата на морфологичния анализ е конструирана морфологична матрица, която съотнася десет ключови измерения на

сертифицирането към техните възможни състояния, като генерира общо 324 сценарийни комбинации.
Анализът на кръстосаната съвместимост чрез матрица за кръстосана съвместимост (Cross-Consistency Matrix, CCM) оценява вътрешната правдоподобност на всяка комбинация, като присвоява сценарийни тегла въз основа на съгласуваността и взаимната съвместимост на състоянията по отделните измерения. Само приблизително една пета от 324-те комбинации, около 65 сценария, са определени като правдоподобни и вътрешно съгласувани.
Доминиращите сценарии с високи тегла от 210 или повече са идентифицирани като стратегически съгласувани пътища за внедряване на сертифицирани продукти. Те се характеризират с хардуерно ориентирани архитектури за защита, регулаторно съответствие, основано на спазване на изискванията, интегриране на нанотехнологии и методология за оценяване от трета страна. Тази констатация ясно показва сложността при конструирането на съгласувани сертификационни пътища в целия спектър от технически и регулаторни области: преобладаващата част от теоретичните сценарийни комбинации са практически несъвместими, което подчертава необходимостта от структурирани аналитични инструменти като PSF за идентифициране на жизнеспособни пътища.
Фазата на прогностичното аналитично моделиране използва насочени графи и вероятностни връзки, за да разкрие системните взаимозависимости между десетте ключови измерения на сертифицирането. Моделирането показва, че малки промени в съображенията, свързани с човешкия фактор или практиките за защита на потребителските данни, се разпространяват значимо в системата и влияят върху цялостното състояние на сигурността по начин, който чисто техническите сертификационни оценки биха пропуснали.
Анализът идентифицира силни взаимозависимости между сигурното съхранение, защитата на ключове, системната защита и киберустойчивостта, като потвърждава, че сертификационните подходи трябва да разглеждат динамичната системна устойчивост, а не само статичното техническо съответствие.

Фазата на 3D анализа на чувствителността картографира всяко от десетте измерения в триизмерно рисково пространство, дефинирано чрез пряк риск (ос X), непряк риск (ос Y) и управляемо ниво на риск (ос Z), като класифицира компонентите в критични и некритични зони. Мерките за сигурност (0.8, 0.69, 0.86), защитата на ключове (0.42, 0.59, 0.71) и системната защита (0.25, 0.22, 0.88) са позиционирани в или близо до критичната зона, докато сигурността на данните и защитата на ключове са идентифицирани като области на скрити заплахи, тоест измерения, при които уязвимостите може да не бъдат непосредствено видими при стандартни сертификационни оценки, но носят значими системни рискови последици. Валидирането на модела PSF е проведено чрез систематична емпирична оценка на три представителни категории IoT продукти, избрани така, че да обхващат хардуерни компоненти, инфраструктурни устройства и потребителска електроника.

Категорията Flash Memory IC е представена чрез Winbond TrustME W75F Secure Serial Flash Memory, сертифицирана на ниво EAL5+ по Common Criteria. Това е продукт с високо ниво на увереност, предназначен за вградени системи, изискващи поверителност и интегритет на данните, който поддържа сигурно зареждане, сигурно обновяване на фърмуера и хардуерно базирано криптиране. Категорията инфраструктурни устройства е представена чрез EFR GmbH Secure SGH-S Smart Grid Hub, сертифициран на ниво EAL4+, който осигурява сигурен и надежден пренос на данни между потребители на енергия, оператори на мрежи и доставчици на услуги. Категорията потребителска електроника е представена чрез Dahua Network Camera IPC-HDBW4200E, сертифицирана на ниво EAL2+, предназначена за видеонаблюдение с основни функции за сигурност, включително криптирано видеопредаване и контрол на потребителските акаунти.

Всеки сертифициран продукт е сравнен с еквивалентен несертифициран продукт от същата функционална категория, като идентичността на несертифицираните устройства е запазена, за да се избегнат репутационни рискове.

За всяка продуктова двойка са оценени шест параметъра на киберсигурността: криптиране на данни, сигурни пароли по подразбиране, мрежови защити/сигурен канал, откриване на

манипулации, защита на потребителски акаунти и системна защита/инициализация.
Оценяването е проведено на относителна основа чрез използване на публично достъпна техническа документация и документация за целите на сигурността, като оценките на функциите за киберсигурност отразяват силата и дълбочината на внедряване спрямо съответното ниво EAL.
Сертифицираните продукти последователно показват значително по-високи нива на внедряване по всички шест параметъра и във всички три продуктови категории: устройството Secure Flash (W75F) получава оценки между 90% и 100% по всички критерии, като криптирането на данни и защитата на потребителски акаунти достигат 100%, мрежовите защити и откриването на манипулации са оценени на 95%, сигурните пароли по подразбиране на 90%, а системната защита/инициализацията на 95%. За сравнение, оценките на несертифицирания Flash аналог са трайно на равнища от 40% или по-ниски: криптиране на данни 5%, сигурни пароли по подразбиране 5%, мрежови защити 5%, откриване на манипулации 20%, защита на потребителски акаунти 35% и системна инициализация 40%.
Статистическият анализ чрез t-тест потвърждава, че тези разлики са с висока статистическа значимост ($p < 0.001$).
Сертифицираният Smart Grid Hub показва разлики от 30 до 75 процентни пункта спрямо несертифицираната версия по шестте параметъра, като статистическата значимост е потвърдена при $p < 0.01$.
IP камерата показва подобрения в сигурността при пет от шестте параметъра, като изключение е откриването на манипулации, при което и сертифицираният, и несертифицираният модел получават минимална оценка от 5%. Това отразява секторна празнота в откриването на физическо проникване при този продуктов клас на оценяваното ниво на увереност.
Оценяването на производителността е проведено чрез количествени показатели (време за четене/програмиране, цикли на изтриване/запис, запазване на данните, енергийна ефективност при Flash Memory; латентност при събиране на данни в реално време, отзивчивост при дистанционно управление, мащабируемост, надеждност и резервираност, управление на енергията при Smart Grid

Hub; качество на изображението, мегапиксели, клас на защита, кадрова честота при IP камера) и чрез качествени измерения в случаите, когато не е налично пряко числово сравнение. Резултатите потвърждават, че сертифицирането на киберсигурността не води универсално до влошаване на производителността. При Flash Memory не е установена статистически значима разлика в производителността между сертифицирания и несертифицирания вариант ($p > 0.05$), като сертифицираният модел показва умерени подобрения в енергийната ефективност в режим deep power-down (40% спрямо 30%) и еквивалентни или малко по-добри показатели за издръжливост. При Smart Grid Hub сертифицираният продукт се представя еднакво добре или по-добре от несертифицираната версия по всички пет измерения на производителността, с особено отчетливо предимство при надеждност и резервираност (95% спрямо 60%), като агрегираното представяне показва статистически значимо предимство за сертифицирания продукт ($p < 0.05$). При IP камерата не е установена статистически значима обща разлика в производителността ($p = 0.0943$), като единственото по-съществено различие е предимството на несертифицирания модел по отношение на мегапикселите (80% спрямо 40%), компенсирано от по-добрата архитектура за сигурност на сертифицирания модел. Тази констатация съответства на пазарното приоритизиране на спецификациите на изображението пред вградената архитектура за сигурност в сегмента на потребителското видеонаблюдение. Прилагането на модела PSS преминава през шестте формализирани стъпки. Дефинирането на критериите установява петте измерения за избор: легитимност, качество, ефективност, правоприлагане и доверие, обосновани чрез теоретичните изводи от първа глава. Двойните сравнения, отразяващи практически опит и теоретични приоритети, са установени чрез скалата на Saaty, като доверието получава най-висока сравнителна значимост спрямо всички останали критерии, следвано от правоприлагането.

Размитите сравнения преобразуват точните стойности по Saaty в триъгълни размити числа съгласно формулата за съответствие, като генерират пълна размита матрица за двойно сравнение. Изчислени са геометрични средни за всеки критерий, като са получени размити вектори на геометричните средни (L, M, U): доверие (1.516, 2.221,

2.862), правоприлагане (0.803, 1.320, 1.933), легитимност (0.608, 0.922, 1.351), качество (0.488, 0.608, 0.871), ефективност (0.488, 0.608, 0.871).

След нормализация и центроидна дефазификация крайните нормализирани приоритетни тегла са: доверие 38.1%, правоприлагане 22.8%, легитимност 16.3%, качество 11.4%, ефективност 11.4%. Инструментът PSS е демонстриран чрез три хипотетични CABs, на които са присвоени оценки за представяне по скала от 1 до 10 за всеки критерий, като са получени претеглени общи резултати от 6.47 (CAB A), 5.11 (CAB B) и 7.43 (CAB C), нормализирани проценти съответно 34.0%, 26.9% и 39.1%, като CAB C е класиран на първо място.

Валидирането на модела PSS е проведено в две стъпки:

1. Коефициентът на съгласуваност (Consistency Ratio, CR) е изчислен върху дефазифицираната точна матрица за двойно сравнение съгласно класическата AHP процедура на Saaty: изчисляване на геометричната средна на всеки ред от матрицата, нормализиране за получаване на точни AHP тегла, умножаване по първоначалната матрица за изчисляване на вектора на претеглените суми, извеждане на λ_i за всеки критерий и осредняване за получаване на $\lambda\_max = 5.087$. Индексът на съгласуваност $CI = (\lambda\_max - n)/(n - 1) = 0.0218$, а коефициентът на съгласуваност $CR = CI/RI = 0.0218/1.12 = 0.0195$, което е значително под прага от 0.10 и потвърждава, че експертните двойни преценки са логически съгласувани и моделът е валидиран.

2. Анализът на чувствителността в шест предварително дефинирани сценария (базов сценарий, доверие +5%, доверие −5%, правоприлагане +5%, правоприлагане −5%, качество +5%, ефективност +5% и изравнени равни тегла) потвърждава, че класирането на CABs остава напълно стабилно при ±5% вариации в теглата във всички сценарии, като CAB C последователно е класиран на първо място, CAB A на второ, а CAB B на трето. Доверието и правоприлагането са потвърдени като най-влиятелните критерии: вариациите в техните тегла водят до най-големите промени в общите резултати на CABs, докато качеството и ефективността, и двете с тегло 11%, оказват минимално влияние. Изравненият сценарий, при който всички критерии са принудително поставени с еднакво тегло от 20%, дава резултати, идентични с базовия случай по отношение на

класирането, което показва, че претегленият модел подсилва, а не изкривява основната оценка.

ИЗВОДИ КЪМ ТРЕТА ГЛАВА

Емпиричното валидиране потвърждава с необходимата статистическа строгост основните допускания на модела PSF: сертифицираните IoT продукти последователно и значимо превъзхождат несертифицираните си аналози по критични показатели за сигурност във всички продуктови категории и по всички шест параметъра на киберсигурността, без да се наблюдават статистически значими загуби в производителността в нито една от трите изследвани продуктови категории. Морфологичното и основаното на риска моделиране потвърждават жизнеспособността на целеви поднабор от съгласувани сценарии за частно сертифициране, приблизително една пета от всички възможни комбинации, като същевременно идентифицират системни слаби места в защитата на ключовете и сигурността на данните, които изискват изрично внимание при проектирането на сертификационни схеми.

Моделът PSS демонстрира практическа приложимост като структуриран, прозрачен, статистически валидиран и устойчив инструмент за избор на CAB, който генерира последователни класирания при всички тествани сценарии на вариации в теглата. Взети заедно, моделите PSF и PSS формират затворена макро-микро система, в която системното прогнозиране на макониво предоставя стратегическата обосновка и граничните условия за възприемане на частни схеми, докато структурираното вземане на решения на микониво операционализира тази стратегия в конкретни, защитими и релевантни за пазара резултати при избора на CAB, като преодолява разрива между теоретичното моделиране и приложното управление в сертифицирането на киберсигурността.

ЗАКЛЮЧЕНИЕ

Извършен е анализ на перспективите за интегриране на частни CABs в сертифицирането на киберсигурността в ЕС, като изводите са следните:

• Актуалността е обоснована - бързото разширяване на IoT пазара (CAGR >25%, 2020–2025 г.), структурните ограничения на сертифицирането, осъществявано само от публични органи по Common Criteria, и ключовата регулаторна промяна в ЕС чрез CSA, Делегирания акт към Директивата за радиосъоръженията и CRA заедно потвърждават неотложността и значимостта на изследването на интегрирането на частни CABs в екосистемата за сертифициране на киберсигурността.

• Качеството и ефективността на частните CABs са потвърдени - обратно на първоначалните опасения, частните CABs не компрометират качеството на оценяването. Тяхната секторно специфична експертиза, оперативна гъвкавост и пазарно обусловена отчетност, управлявани чрез акредитация по ISO/IEC 17065, водят до сертификации, които са съответстващи, строги и в много случаи по-отзивчиви към възникващи заплахи в сравнение с традиционните публични механизми.

• Регулаторният риск е ограничен - участието на частни CABs не увеличава риска от несъответствие. Задължителните стандарти за акредитация, текущите одити, партньорските прегледи и конкурентният натиск на пазара заедно функционират като надеждни гаранции срещу влошаване на качеството или отслабване на регулаторния контрол.

• Хармонизацията се поддържа от правото - триактната рамка на ЕС (CSA, RED, CRA), координирана от ENISA, запазва регулаторната съгласуваност между държавите членки. Взаимното признаване между публични и частни CABs има правна основа и е практически осъществимо, както се потвърждава от анализа на казуси от различни сектори.

• Доверието е идентифицирано и разгледано като централно предизвикателство - понастоящем частните CABs са ограничени до базови и съществени нива на увереност. Доверието трябва да се изгражда целенасочено чрез акредитация по ISO/IEC 17065,

механизми за контрол на безпристрастността, прозрачност и доказана история на извършени сертификации. Този процес вече е в ход и се ускорява с нарастващото участие на пазара.
• Подобряване на сигурността без загуба на производителност - емпирично доказано - във всички три изследвани категории IoT продукти (Flash Memory IC на ниво EAL5+, Smart Grid Hub на ниво EAL4+, IP Camera на ниво EAL2+) сертифицираните продукти последователно превъзхождат несертифицираните си аналози по всички шест параметъра на киберсигурността (криптиране на данни, сигурни пароли по подразбиране, мрежови защити, откриване на манипулации, защита на потребителски акаунти, системна инициализация), със статистически значими разлики ($p < 0.05$ до $p < 0.001$), без да показват статистически значимо влошаване на производителността.
• Пазарното възприемане е подкрепено - експерименталните резултати пряко адресират и отхвърлят опасението, че съответствието с изискванията за киберсигурност намалява пазарната привлекателност на продуктите. Сертифицираните продукти запазват съпоставима оперативна производителност, като по този начин се премахва основната пазарна бариера пред възприемането на сертификацията от производителите на IoT устройства.
• Модел PSF - реализирана иновация на макониво - моделът за прогнозиране на частни схеми (Private Scheme Forecasting), изграден върху многофазно сценарийно моделиране, предоставя нова системна рамка за прогнозиране на възприемането на частното сертифициране. От 324 морфологични сценарийни комбинации моделът идентифицира приблизително 20% правдоподобни пътища с високи тегла, като потвърждава, че хардуерно ориентираните, основани на съответствие и съгласувани с нанотехнологиите сценарии водят до най-жизнеспособни и сигурни сертификационни резултати.
• Модел PSS - реализирана иновация на микониво - моделът за избор на частна схема (Private Scheme Selection), изграден върху метода на размитото приоритизиране, операционализира избора на CAB в шестстъпков структуриран процес за вземане на решения. Моделът генерира стабилни и валидирани тегла на критериите (доверие 38%,

правоприлагане 23%, легитимност 16%, качество 11%, ефективност 11%) с коефициент на съгласуваност 0.0195, който е в допустимите граници, а класираниятa са потвърдени като устойчиви при ±5% вариации в анализа на чувствителността.

• Интегрирана рамка PSF–PSS - оригинален научен принос - съвместната макро-микро система представлява основния принос на дисертационния труд към научната област: PSF осигурява системна прогноза относно възприемането на частни схеми, PSS предоставя оперативната методология за прилагане, а заедно те формират затворена, основана на доказателства пътна карта, която за първи път свързва теоретичното моделиране и приложното вземане на решения в сертифицирането на киберсигурността.

IV. ПРИНОСИ НА ДИСЕРТАЦИОННИЯ ТРУД

Принос на макониво: модел за прогнозиране на частни схеми (Private Scheme Forecasting, PSF)

1. **Разработен е оригинален модел за оценяване на надеждността на частните схеми за сертифициране на киберсигурността.** Чрез теоретично валидиране на ефективността на сертифицирането и чрез емпиричните резултати моделът потвърждава, че сертифицираните продукти последователно превъзхождат несертифицираните си аналози по ключови мерки за сигурност и в трите категории IoT продукти, без това да води до загуби в производителността. Това предоставя убедителни доказателства, че сертифицирането повишава устойчивостта, като същевременно запазва оперативната ефективност.
2. **Системни детерминанти на успеха.** Моделът PSF идентифицира три ключови условия за ефективно частно сертифициране: иновативни стратегии за оценяване, основани на риска; реалистично изграждане на сценарии, което балансира между обхватност и правдоподобност; и системна интеграция на технологичните и методологическите компоненти.
3. **Пазарни последици.** Като показва, че високото равнище на съответствие не е необходимо да подкопава конкурентоспособността, моделът PSF представя сертифицирането като едновременен фактор за изграждане на доверие и за поддържане на пазарна жизнеспособност.

Принос на микониво: модел за избор на частна схема (Private Scheme Selection, PSS)

4. **Разработен е алгоритмичен модел за подпомагане на производителите на IoT устройства при избора на орган за оценяване на съответствието (CAB).** Като

методологична иновация моделът PSS интегрира размита логика и я оптимизира чрез метода на размито приоритизиране (Fuzzy Prioritization Method, FPM), за да преобразува експертните лингвистични оценки в устойчиви количествени приоритети. По този начин моделът отчита несигурността и субективността по-ефективно от конвенционалните методи на аналитичния йерархичен процес (AHP).

5. **Операционна строгост.** Чрез шест структурирани стъпки, дефиниране на критерии, попарни сравнения, размито преобразуване, оптимизация чрез геометрична средна, дефъззификация и приложение при вземане на решение, моделът PSS създава прозрачен, възпроизводим и валидиран процес за избор на CAB, като доверието и правоприлагането се очертават като доминиращи критерии.
6. С цел улесняване на практическото приложение моделът PSS е реализиран чрез опростен инструмент, базиран на Excel. Тази реализация операционализира критериите за избор и съществено опростява вземането на решения относно избора на CAB, като по този начин повишава приложимостта на модела за практикуващите специалисти.

Интегриран принос: свързване на PSF и PSS

7. **Предложена е стратегия за хармонизиране на частните и публичните схеми в рамката на Европейския съюз.** Чрез двуперспективна рамка, която свързва стратегическото прогнозиране (PSF) с оперативното изпълнение (PSS), се формира затворена система, в която прогнозирането на макониво подпомага вземането на решения на микониво, а методологията на микониво валидира допусканията на макониво. По този начин се предлага оригинална, емпирично обоснована пътна карта за развитие на

частните схеми за сертифициране на киберсигурността, които укрепват устойчивостта на сигурността, запазват ефективността на производителността и поддържат пазарната жизнеспособност.

V. ПУБЛИКАЦИИ, СВЪРЗАНИ С ДИСЕРТАЦИЯТА

1. Menda-Shabat-More, R., & Veselina, S. (2026). Private schemes for cybersecurity certifications: Experimental modelling and forecasting for success. In W. Ding, A. Chakrabarti, M. Chakraborty, & S. Chakraborty (Eds.), *Proceedings of the Second International Conference on Advanced Computing and Systems. AdComSys 2025*. *Lecture Notes in Networks and Systems, 1887*. Springer, Cham. https://doi.org/10.1007/978-3-032-20253-6_15
2. Menda-Shabat-More, R. (2023). *Private schemes for cybersecurity certifications: An experimental modeling and forecasting for success*. BISEC 2023 Conference, Belgrade Metropolitan University, Serbia, 24 November 2023. https://bisec.metropolitan.ac.rs/agenda-2023/
3. Menda-Shabat-More, R. (2023). *IoT cybersecurity certification: A multicriteria assessment approach*. 18th Annual Meeting of the Bulgarian Section of SIAM, BGSIAM'23, 11-13 December 2023, Sofia, Bulgaria. http://www.math.bas.bg/bgsiam/docs/bgsiam_2023_program.pdf
4. Menda-Shabat-More, R. (2024). *Cybersecurity regulations and standards: Best practices and the future challenges of the cybersecurity regulations evolvement*. International Conference: Technological Challenges to Security, Defence and Innovations in the New Digital Age. https://securedfuture21.org/int_sec_conf_iict_aora_apr_26_27_2024/int_sec_conf_iict_aora_apr_24_files/Int_Conf_PC_Sofia_April_26_27_2024.pdf
5. Menda-Shabat-More, R. (2024). *Private schemes for cybersecurity certifications: An experimental modeling and*

forecasting for success. International Conference: Technological Challenges to Security, Defence and Innovations in the New Digital Age. https://securedfuture21.org/int_sec_conf_iict_aora_apr_26_27_2024/int_sec_conf_iict_aora_apr_24_files/Int_Conf_PC_Sofia_April_26_27_2024.pdf

6. Menda-Shabat-More, R. (2026). *Designing secure-by-default IoT products: What will actually change under the CRA?* EU Cyber Act Conference, March 2026; GlobalPlatform CRA Summit, April 2026.

7. Menda-Shabat-More, R., & Veselina, S. (2025). *Private schemes for cybersecurity certifications: Experimental modelling and forecasting for success*. AdComSys 2025, 2nd International Conference on Advanced Computing and Systems, 26-27 June 2025. https://adcomsys.uemkcstcsit.in/past-editions