ИКОНОМИЧЕСКИ УНИВЕРСИТЕТ – ВАРНА
ФАКУЛТЕТ „ИНФОРМАТИКА“
КАТЕДРА „ИНФОРМАТИКА“

Петър Димитров Димитров

Универсална двуфакторна автентикация за защита на уеб базирани информационни системи

А В Т О Р Е Ф Е Р А Т

на дисертационен труд
за присъждане на образователна и научна степен „доктор“
по докторска програма „Информатика“
професионално направление
4.6. „Информатика и компютърни науки“

Научен ръководител:
проф. д.н. Павел Петров

Варна
2026

Дисертационният труд е в обем 167 страници, в това число 26 фигури и 5 таблици. Книгописът обхваща 129 литературни източника.
Основните резултати от изследванията са представени в научни публикации – 3 научни статии и 4 научни доклада.
Дисертационният труд е обсъден и насочен за защита пред научно жури на заседание на катедра „Информатика" при факултет „Информатика" на Икономически университет – Варна на 21.01.2026 г.

Научно жури:
1. Вътрешни членове
проф. д-р Силвия Стоянова Парушева, ИУ-Варна, parusheva@ue-varna.bg
доц. д-р Иван Огнянов Куюмджиев, ИУ-Варна, ivan_ognyanov@ue-varna.bg

2. Външни членове
проф. д-р Георги Петров Димитров, УниБИТ, g.dimitrov@unibit.bg
доц. д-р Боян Колев Жеков, УниБИТ, b.jekov@unibit.bg
проф. д-р Евдокия Николаева Сотирова, Бургаски държавен университет „Проф. д-р Асен Златаров", esotirova@btu.bg

Защитата на дисертационния труд ще се състои на ..... от ……. часа в зала ……. на Икономически университет – Варна на заседание на Научно жури, назначено със Заповед No ..... на Ректора на Икономически университет – Варна.
Материалите по защитата са на разположение на интересуващите се на интернет страницата на Икономически университет – Варна, https://www.ue-varna.bg

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Актуалност на изследването

През последното десетилетие дигитализацията се утвърди като основен двигател на икономическото и социалното развитие, при което уеб базираните информационни системи се прилагат в значителен брой обществени сфери – електронно управление, здравеопазване, банкиране, образование и електронна търговия. Нарастващото значение на тези системи е съпроводено от увеличаване на киберзаплахите, насочени към компрометиране на потребителската идентичност и достъпа до чувствителна информация.

Най-уязвимият елемент в сигурността на уеб системите традиционно остава паролата и въпреки дългогодишната ѝ употреба като основен метод за автентикация, нейното използване има редица недостатъци:

- лесно може да бъде откраднатa чрез различни видове атаки, включително фишинг и използване на зловреден софтуер;
- често се използват лесни и широко разпространени пароли, които подлежат на различни видове атаки (напр. brute force и dictionary);
- потребителите често преизползват една и съща парола в множество системи, което повишава риска от масови пробиви чрез атаки, основани на повторно използване на удостоверителни данни (credential stuffing).

Според Verizon Data Breach Investigations Report 2023 злоупотребата с компрометирани удостоверения е в основата на над 40 % от успешните пробиви – като се прави разлика между общите инциденти и специфичните уеб-атаки. За по-широк контекст, в отчета за 2024 година „човешкият елемент“ (грешки, фишинг, компрометирани пароли) е бил фактор в приблизително 68% от пробивите. Множество изследвания показват, че традиционната автентикация с потребителско име (или имейл адрес) и парола демонстрира ниска надеждност като средство за защита на чувствителни данни и достъп до услуги в съвременната дигитална среда. Традиционните методи за

удостоверяване, базирани на пароли, са идентифицирани като критична уязвимост в сигурността, тъй като слабите, повторно използвани или компрометирани пароли са сред основните вектори за атаки. Паролите са доказано недостатъчна защита срещу киберпрестъпления, което води до заключението, че много потребители приоритизират използваемостта пред сигурността.

В опит за преодоляване на този проблем се внедряват допълнителни механизми за защита, наречени двуфакторна автентикация (2FA) – обикновено чрез еднократни кодове (било то чрез SMS или чрез мобилно приложение). Макар и повишаващи сигурността и правейки достъпът до чувствителна информация или услуги по-сигурен, тези механизми също имат недостатъци:

- SMS-съобщенията могат да бъдат прихванати чрез специфични видове атаки върху мобилната инфраструктура;
- потребителските устройства от своя страна са уязвими на атаки чрез подмяна на SIM карта (SIM swapping), при които нападателят успява да прехвърли телефонния номер на жертвата върху собствена SIM карта и така получава достъп до еднократни кодове за автентикация, изпращани чрез SMS;
- въвеждането на допълнителни кодове създава значително неудобство за потребителите.

С цел решаване на посочените проблеми се създава организацията FIDO Alliance, която чрез стандартите FIDO2, WebAuthn и CTAP2 формулира подход за въвеждане на безпаролна автентикация, насочен към повишаване на сигурността и намаляване на зависимостта от традиционните пароли. Предложени е подход, при който потребителите се автентикират с криптографски ключове, защитени в хардуерни или софтуерни автентикатори, без необходимост от запомняне и въвеждане на пароли. Това значително повишава сигурността, като елиминира риска от фишинг и кражба на пароли, и в същото време подобрява потребителското изживяване.

Терминът „универсална двуфакторна автентикация“ (U2F) се използва в съответствие с първоначалната концепция на FIDO Alliance от периода 2014-2018 г. и в дисертацията служи като основа за последващото изследване и интеграция на разширения стандарт FIDO2/WebAuthn. В контекста на дисертацията понятието „универсална двуфакторна автентикация“ се отнася до унифицирания модел на автентикация, основан на криптография чрез публични и частни ключове и стандартизирани протоколи, а не до конкретна реализация, ограничена в рамките на една-единствена система.

2. Изследователска теза

Изследователската теза на дисертационния труд е, че стандартите FIDO2/WebAuthn позволяват изграждане на универсален и практически приложим модел за силна автентикация в уеб базирани информационни системи, който едновременно повишава сигурността и запазва висока степен на използваемост. Чрез криптографско удостоверяване с публични и частни ключове и други методи, специфични за стандарта, WebAuthn елиминира основни класове атаки (фишинг, credential stuffing и MitM), характерни за паролно-базираните решения, и позволява внедряване в реални институционални среди без фундаментална промяна на тяхната архитектура.

3. Цели и задачи на изследването

Целта на настоящата дисертация е да се разработи и обоснове концептуален и архитектурен модел за универсална двуфакторна автентикация в уеб-базирани информационни системи, основан на стандартите FIDO2 и WebAuthn, който да осигурява високо ниво на криптографска защита, устойчивост срещу съвременни атаки и практическа приложимост в реални институционални среди. В рамките на изследването се отделя специално внимание на използваемостта и достъпността за крайните потребители, така че предлаганият модел да бъде не само сигурен, но и приемлив в ежедневната практика.

За постигане на поставената цел в дисертационния труд се решават следните основни задачи:

- извършване на систематичен анализ на съществуващите подходи за потребителска автентикация и техните ограничения; изследване на архитектурните принципи и стандарти, свързани с FIDO2/WebAuthn и тяхната интеграция със съществуващи системи за управление на идентичности;
- проектиране и моделиране на архитектура на система за двуфакторна автентикация с ясно дефинирани логически, комуникационни и данни-ориентирани компоненти;
- анализ на рисковете, заплахите и бъдещите тенденции в сигурността на безпаролните системи, включително в контекста на пост-квантовата криптография, разгледана в аналитичен и прогностичен аспект.

4. Обект и предмет на изследване

Обектът на изследването е защитата на уеб базирани информационни системи, които обработват чувствителни данни и изискват надеждна автентикация на потребителите.

В рамките на настоящия труд под „уеб базирана информационна система“ се разбира многослойно приложение, достъпно чрез уеб браузър или уеб клиент, което използва HTTP(S) като транспортен протокол, централизирана сървърна логика и база данни за съхранение и обработка на информацията. Характерно за този тип системи е, че достъпът до функционалностите им се осъществява чрез стандартни уеб технологии (HTML, CSS, JavaScript) и те често обслужват голям брой отдалечени и разнородни потребители.

Разглеждането на уеб базираните информационни системи в изследването е обусловено от няколко фактора. На първо място, именно този тип системи са широко разпространени в контекста на електронното

управление, образованието и облачните услуги, като осигуряват дистанционен достъп до критични данни и функции за голям брой потребители. На второ място, уеб приложенията традиционно разчитат на паролно-базирана автентикация, което ги прави в значителна степен уязвими към множество видове атаки. На трето място, стандарти като FIDO2/WebAuthn са проектирани за уеб среда и предоставят вграден механизъм за замяна на паролите с криптографски ключове. В този контекст уеб базираните системи представляват най-подходящата и релевантна среда за анализ и внедряване на универсален модел за силна автентикация.

Предметът на изследването обхваща архитектурните решения, криптографските протоколи и технологиите за реализиране на универсална двуфакторна автентикация, базирана на FIDO2 и WebAuthn, както и интегрирането на съвременни методи за защита на уеб приложенията от актуални вектори на атака, като фишинг, replay атаки, компрометиране на сесии и злоупотреби с удостоверителни данни.

Целта на настоящата дисертация е да се разработи концептуален модел и архитектура за универсална двуфакторна автентикация на потребителите в уеб базирани информационни системи, основана на стандартите FIDO2/WebAuthn, който да осигурява високо ниво на криптографска защита чрез използване на съвременни алгоритми и протоколи, съобразени с най-добрите практики в информационната сигурност. Моделът е концептуално насочен към постигане на устойчивост на най-често срещаните кибератаки, включително фишинг, replay атаки и credential stuffing, чрез внедряване на механизми за сигурна верификация и управление на сесии. В контекста на стандартизацията и съвместимостта с различни платформи, в труда се предлага интеграционен подход, базиран на стандартите FIDO2 и WebAuthn, който осигурява приложимост на разработената архитектура към широк спектър от уеб системи и гарантира съвместимост с актуални браузъри и устройства. Отделя се специално внимание на използваемостта и достъпността за крайните потребители, като се разработват интерфейсни решения и

процедури, които минимизират бариерите при внедряване на двуфакторната автентикация и увеличават удовлетворението и безопасността на потребителите.

5. Методология на научното изследване

Методологичният апарат на изследването включва следните изследователски методи и техники:

- Сравнителен анализ – за оценка на традиционните 2FA методи спрямо WebAuthn по отношение на сигурност, удобство и внедряване.
- Системен подход – за моделиране на архитектурата и взаимодействието между компонентите.
- Моделиране и прототипиране – за изграждане на тестова среда и демонстрация на основни сценарии (регистрация, автентикация).
- Логически анализ и сценарии – за описание на потоци на данни, атаки и механизми за защита.

Методиката включва както теоретичен анализ, така и практическа имплементация чрез изграждане на прототип на система за двуфакторна автентикация с интегриран WebAuthn сървър и реална база данни.

Настоящото изследване се реализира в рамките на определени ограничения, които следва да бъдат отчетени при интерпретацията на резултатите и направените изводи. На първо място, дисертационният труд е фокусиран върху уеб базирани информационни системи и стандартите FIDO2/WebAuthn в контекста на уеб среда, което означава, че анализът и предложената архитектура не обхващат в пълнота специфичните особености на други видове системи.

На второ място, практическата реализация и експерименталната част на изследването са ограничени до конкретна технологична платформа (PHP/MySQL и стандартни уеб браузъри), което позволява детайлен анализ на интеграцията на WebAuthn, но не претендира за изчерпателност по отношение

на всички възможни програмни езици и среди. Направените изводи относно приложимостта и ефективността на модела следва да се разглеждат като валидни в рамките на избраната технологична конфигурация.

Изследването не цели изчерпателна формална верификация на използваните криптографски протоколи, а се базира на утвърдени стандарти и съществуващи формални анализи, публикувани от W3C, FIDO Alliance и академичната общност. По тази причина трудът се концентрира върху архитектурните, интеграционните и приложните аспекти на FIDO2/WebAuthn, а не върху разработване на нови криптографски примитиви. По отношение на използваемостта и потребителското изживяване, анализът се опира основно на съществуващи емпирични изследвания и ограничени наблюдения в рамките на прототипната реализация, без да се провеждат мащабни потребителски експерименти с представителна извадка. В този смисъл направените заключения за UX следва да се разглеждат като индикативни и като основа за бъдещи по-задълбочени изследвания. Разглеждането на бъдещи тенденции, включително пост-квантовата криптография, има предимно прогностичен и аналитичен характер и не включва експериментална оценка на реални пост-квантови реализации в рамките на WebAuthn, тъй като подобни стандартизирани решения към момента на изследването все още са в процес на разработване и оценка.

5. Апробация

Апробацията на получените резултати е осъществена чрез разработване и внедряване на работещ прототип за WebAuthn автентикация в университетската система WSDB на ИУ–Варна, както и чрез публикуване и представяне на резултати в 3 научни статии и 4 научни доклада. Практическата реализация включва сценарии за регистрация на автентикатор, двуфакторна автентикация и използване на криптографския ключ за подписване на академични данни.

II. СТРУКТУРА НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд се състои от въведение, три глави и заключение и е в обем 167 страници, в това число 26 фигури и 5 таблици. Книгописът обхваща 129 литературни източника.

Съдържание:

III. КРАТКО СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Глава I. Теоретични и практически предпоставки за въвеждането на WebAuthn

Използването на все повече информационни системи, платформи и приложения както в личния живот, така и в професионалния контекст разширява възможностите за дистанционна работа, електронни услуги и обработка на данни, но едновременно с това увеличава експозицията към киберрискове. В дисертационния труд тази реалност се разглежда като отправна точка за изследване на автентикацията като критичен механизъм за контрол на достъпа, от който зависи защитата на чувствителна информация и надеждността на уеб базираните информационни системи. Организациите са изправени пред необходимост едновременно да поддържат висока използваемост и едновременно с това да прилагат механизми за сигурност, които са устойчиви на актуалните атаки срещу чувствителни и удостоверителни данни.

Един от най-ранните и най-разпространени методи за ограничаване на достъпа е паролата. В дисертационния труд се проследява историческото ѝ възприемане като средство за удостоверяване, включително навлизането ѝ в многопотребителските компютърни системи и формирането на модела за централизирана автентикация. Изведено е, че макар паролата да е технологично проста и лесна за внедряване, тя поставя сигурността в зависимост от човешки фактори и от качеството на организационните практики за нейното създаване, съхранение и използване.

С течение на времето паролите започват да демонстрират ограниченията си. В дисертационния труд се акцентира, че в реални условия множество потребители използват кратки или предвидими пароли и често ги използват повторно в други системи. Това създава предпоставки за редица атаки, както и за мащабни компрометирания на акаунти при изтичане на данни от една услуга и последващо „пренасяне“ на риска към други услуги. Именно този

комплекс от уязвимости мотивира преминаването към механизми, които намаляват или елиминират зависимостта от „споделени тайни“ и ограничават възможността за фишинг и повторно използване на компрометирани удостоверения.

В първата подточка „**Начини за съхранение на данните за автентикация**“ се установява, че сигурността на автентикацията не зависи единствено от избрания механизъм за вход, а и от начина, по който системата съхранява и обработва автентикационните данни. Представени са основните подходи за съхранение на потребителски идентификатори и пароли и се анализират рисковете, свързани с тях. Подчертано е, че историческият преход от съхранение в открит вид към хеширане и засоляване е ключов за намаляване на последиците от пробиви, но не решава фундаменталните слабости на самия паролен модел.

Описан е ранният подход за съхранение на пароли в текстов вид, характерен за първите многопотребителски системи. Показано е, че централизираното съхранение на пароли в четим формат води до критични уязвимости като например това, че при минимална грешка в конфигурацията или при неправилен контрол на достъпа може да се постигне масово компрометиране на потребителски акаунти. На тази основа се формулира важен принцип, разгърнат и в следващите глави на дисертационния труд, а именно функцията по съхранение и функцията по проверка на удостоверителни данни следва да бъдат реализирани така, че дори при частична компрометация да не се разкриват тайни низове, които биха могли да доведат до неоторизиран достъп. Отбелязано е, че макар този подход да се счита за несъвместим със съвременните практики, и днес се срещат системи, в които поради технически и организационни пропуски се допуска съхранение на пароли без адекватна криптографска защита, което в контекста на дисертационния труд се разглежда като високорисков фактор.

Анализира се въвеждането на криптографски подходи за защита на паролите и се аргументира ролята на хеш функциите и посоляването за

намаляване на риска от офлайн разбиване при изтичане на бази данни. Представени са и исторически примери, които показват, че алгоритми, считани за надеждни в един период, могат да бъдат непрепоръчвани за използване при нарастване на изчислителната мощ и появата на специализиран хардуер. Този анализ подготвя логическия преход към тезата на дисертационния труд, че дори при коректно хеширане и посоляване паролният модел остава структурно уязвим към различни по рода си атаки, което налага търсене на подходи, заменящи паролите с криптографски удостоверения.

В подточката „**Квалифициран електронен подпис като средство за автентикация**“ на дисертационния труд е разгледан квалифицираният електронен подпис като технологичен инструмент с най-висока правна стойност в рамките на Европейския съюз и в частност в българската правна рамка. Анализът акцентира върху това, че КЕП се основава на класическа инфраструктура на публични ключове (PKI) и асиметрична криптография и осигурява не само автентикация, но и неотменимост при юридически значими действия. В същото време е аргументирано, че използването на КЕП като масов механизъм за ежедневна автентикация в уеб приложения има и недостатъци като например зависимост от специализирани устройства/носители, процедури по издаване и поддръжка, както и специфични потребителски и организационни изисквания. Този сравнителен анализ служи като междинна стъпка в дисертационния труд за обосноваване на необходимостта от решения, които комбинират висока криптографска сигурност с по-добра използваемост и оперативна приложимост в широки потребителски среди.

В подточката „**Критичен анализ на уязвимостите и еволюцията на автентикационните технологии**“ на дисертационния труд е разгледана еволюцията на сигурността като постоянна динамика между защитни мерки и техники за тяхното заобикаляне. Подчертано е, че защитата трябва да бъде системна и да покрива целия спектър от вектори на атака. На тази основа са

представени примери за мащабни пробиви и изтичания на пароли и хешове, които демонстрират последствията от зависимостта от статични удостоверителни данни. Изведен е ключов извод, който е водещ за дисертационния труд, а именно че повторната употреба на пароли, недостатъците в съхранението и атаките базирани на социално инженерство водят до „верижен“ риск, при който компрометиране на една услуга може да доведе до компрометиране на множество други.

Систематизирани са актуалните вектори на атака срещу механизми за удостоверяване, като се подчертава, че атакуващите комбинират технически и социални подходи. Разгледани са атаки чрез груба сила (brute force), речникови (dictionary) атаки, атаки чрез повторно използване на компрометирани удостоверения, фишинг кампании, както и сценарии за компрометиране на сесии и междинни компоненти. Анализът показва, че увеличената изчислителна мощ и наличието на масиви от вече изтекли пароли значително снижават практическата бариера за атака, което отново насочва към необходимост от механизми, които по дизайн намаляват ползата от откраднати удостоверения и ограничават възможността за подмяна на контекста на автентикация.

В подточката „**Аспекти на внедряването и приемането на FIDO2/WebAuthn от потребителите**“ на дисертационния труд е разгледано, че безпаролните и фишинг-устойчиви подходи, базирани на FIDO2/WebAuthn, предлагат значително по-висока степен на сигурност спрямо традиционните методи, но внедряването им в реална среда се обуславя от архитектурни, организационни и човешки фактори. Анализирани са въпроси като избор на автентикатори (платформени и външни), потребителско изживяване, политики за регистрация на устройства, управление на множество устройства, както и възстановяване на достъп при загуба или подмяна на автентикатор. Отделено е внимание на тенденцията към широкомащабна поддръжка на passkeys в съвременните платформи и браузъри, което създава благоприятни предпоставки за масова употреба. Тези аспекти се използват като основа за

последващите глави на дисертационния труд, в които се разработва модел за интеграция на WebAuthn и се демонстрира практическото му внедряване в реална университетска уеб базирана информационна система.

Глава II. Модел за автентикация, базиран на стандартите FIDO2 и WebAuthn

Във втора глава на дисертационния труд е разработен и аргументиран модел за силна двуфакторна автентикация за уеб-базирани информационни системи, базиран на FIDO2 и WebAuthn, като фокусът е поставен върху баланса между три взаимно обусловени изисквания, а именно сигурност, мащабируемост и удобство за потребителя. Показано е, че в реални институционални среди архитектурата за удостоверяване трябва едновременно да противодейства на фишинг, атаки чрез повторение и компрометиране на пароли, да обслужва висока едновременна активност без деградация на производителността, и да бъде достатъчно използваема, за да се приеме масово от потребителите. На тази основа са формулирани цели за имплементация на система за двуфакторна автентикация, а именно:

- гарантиране, че достъп получават единствено оторизирани потребители чрез защитена комуникация и криптографско удостоверяване с асиметрични методи;
- осигуряване на мащабируемост чрез ефективно съхранение и бърза верификация на публични ключове и оптимизирани операции върху базата данни;
- повишаване на удобството чрез редуциране на зависимостта от сложни пароли и чрез използване на интегрирани в потребителската екосистема средства за потвърждение, включително биометрични данни и локални механизми за верификация.

В първата подточка „**FIDO2/WebAuthn – роля в модела за силна автентикация**“ се обосновава изборът на FIDO2/WebAuthn като логичен отговор на системните слабости на паролно-базираната автентикация и на

традиционните 2FA подходи. Изведено е, че при паролите рискът се концентрира в статичен низ, чието качество зависи от потребителските навици и което може да бъде откраднато, преизползвано или компрометирано при пробив в хранилище. Показано е, че FIDO2 комбинира WebAuthn (браузърен API) и CTAP2 (протокол за комуникация между клиент и автентикатор), като заменя паролата и/или еднократните кодове с асиметрична криптография и модел „предизвикателство-подпис“. При регистрация на автентикатор се генерира двойка ключове за конкретната услуга (Relying Party), като частният ключ остава в защитена среда на устройството/автентикатора и не напуска тази среда, а на сървъра се съхранява единствено публичният ключ. При автентикация сървърът изпраща уникално криптографско предизвикателство, което се подписва локално и се валидира чрез публичния ключ. Аргументирано е, че тази архитектура променя модела на заплаха – компрометирането на базата данни не води до възможно офлайн разбиване на пароли, повторното използване на удостоверителни данни става практически неприложимо, а фишингът се ограничава по конструкция чрез обвързване на удостоверяването с произхода (origin) и идентификатора на услугата. В сравнителен план е посочено, че решения като SMS-OTP и TOTP, макар да добавят втори фактор към автентикацията, остават уязвими съответно към атаки върху телекомуникационния канал и към фишинг чрез пренасочване и социално инженерство, тъй като разчитат на пренасяне и/или въвеждане на кодове от потребителя.

Във втората подточка „**Концептуален модел**“ се формализират участниците, функционалните граници и логическите взаимовръзки в системата за универсална двуфакторна автентикация, като се подчертава, че целта на концептуалното ниво не е описание на конкретни формати и протоколни полета, а ясно разграничаване на роли и отговорности. Дефинирани са основните логически единици, а именно потребител, клиентско приложение (браузър/мобилно приложение), автентикатор, сървър (Relying Party) и хранилище на публични ключове. Потребителят инициира

регистрация и автентикация като потвърждава операциите чрез действие, което гарантира осъзнато участие (например натискане на бутон, биометрия или въвеждане на PIN). Клиентското приложение посредничи между уеб приложението и автентикатора, като управлява WebAuthn интерфейса и пренася данните към сървъра. Автентикаторът съхранява частния ключ в защитена среда и извършва криптографските операции, като отказва подписване без изрично участие на потребителя като при необходимост предоставя и т.нар. атестация, която позволява на сървъра да установи характеристики и доверие към използваните устройства/автентикатори. Сървърът генерира уникални криптографски предизвикателства, съхранява публичните ключове и валидира подписи, а базата данни съдържа публични ключове и метаданни, така че дори при компрометирането ѝ да не се рдопусне компрометиране на чувствителни данни. Връзката с нива на гаранция е разгледана чрез рамка, в която се дефинират нива на достоверност на автентикацията, като при най-високото ниво се изискват фишинг-устойчиви автентикатори и непредаваем частен ключ – изискване, което се постига именно чрез FIDO2/WebAuthn. В рамките на концептуалния модел са посочени и използваните криптографски примитиви и роли на алгоритмите – цифрови подписи (напр. ECDSA или RSA), хеширане (напр. SHA-256) и генериране на случайни стойности за криптографските предизвикателства.

В третата подточка „**Логически модел**“ се преминава от абстрактното описание към формализиране на данните и зависимостите между тях, като ER представянето се използва като основа за релационна структура, независима от конкретна СУБД. Показано е минималистично, но функционално достатъчно разделение на данните в две основни таблици:

- таблица за потребители (идентификатор, уникално потребителско име и контактна информация)
- таблица за FIDO удостоверителни записи, свързани с конкретен потребител.

Описани са ключовите реквизити за всеки автентикатор, а именно:

- идентификатор на устройството/удостоверителните данни
- връзка към потребителя
- идентификатор на ключа (keyHandle/credential идентификатор)
- публичен ключ
- сертификат/атестационни данни (когато се използват)
- брояч (signCount/counter) за откриване на повторение или клониране.

Подчертано е, че структурата поддържа сценарии с множество устройства, като един потребител може да има повече от един регистриран автентикатор, което е критично за устойчивост на механизма по автентикация при загуба на един от автентикаторите. Допълнително са очертани възможности за по-висока управляемост и сигурност сред които водене на логове за успешни/неуспешни опити за автентикация с времеви отпечатък и IP адрес, реквизити и приоритизация на резервни устройства, история на ключове и сертификати, обвързване с IP/геолокация за анализ на риск, както и механизми за логическо изтриване (soft-delete), които ограничават опасни операции и подпомагат одита на базата данни.

В четвъртата подточка „**Комуникационен модел**“ се описва семантиката и редът на обмен на съобщения между участниците, като се разглежда кога и как сървърът създава предизвикателство, как клиентът го предава към автентикатора, как автентикаторът връща подписан отговор (assertion) и как сървърът валидира подписа чрез публичния ключ от хранилището. Показано е, че моделът комбинира протоколните изисквания на WebAuthn/CTAP2 (формати за представяне на данни, атестация, потребителска верификация) с инфраструктурни изисквания като работа през HTTPS/TLS, коректно генериране на криптографски предизвикателства и управление на сесии. Регистрационният поток е описан като последователност, при която автентикатора локално генерира ключова двойка, публичният ключ се предава през защитен канал, сървърът го валидира и съхранява, връща потвърждение за успешна регистрация, като при множество устройства публичният ключ се асоциира към потребителя като отделен запис.

Потокът на данни при автентикация е описан чрез избор на регистрирано устройство/автентикатор, подписване на предизвикателство с частния ключ и верификация от сървъра спрямо съответния публичен ключ, като паралелно се поддържат механизми за логване на устройство, време и IP за последващи анализи. Отделено е внимание на това, че защитата на комуникацията чрез TLS/HTTPS е задължително условие, тъй като протоколът осигурява конфиденциалност, интегритет, предотвратява подслушване и подмяна на данни в канала и е предпоставка WebAuthn да се изпълнява в защитен контекст. Подчертано е, че некоректната TLS конфигурация (остарели версии, слаби шифри, невалидни сертификати) може да компрометира цялата сигурност на решението, независимо от надеждността на автентикатора.

В петата подточка „**Структура и механизми на протоколите WebAuthn и CTAP2**“ се разглежда вътрешната структура на протоколните данни и взаимодействието между уеб слоя и устройството за автентикация. Показано е, че WebAuthn дефинира стандартизирания интерфейс за уеб приложенията и браузърите, докато реалната комуникация към автентикатора се осъществява чрез CTAP2, като браузърът изпълнява ролята на посредник между приложението и хардуера/платформата. Посочено е, че CTAP2 използва компактен бинарен формат за сериализация (CBOR) и поддържа множество транспортни механизми (USB, NFC и Bluetooth Low Energy), което е ключово за универсалната приложимост на подхода в различни клиентски среди. Описани са и основни CTAP2 операции, които управляват регистрацията и удостоверяването, включително създаване на удостоверителни данни (makeCredential), получаване на доказателство за вход (getAssertion), защита с локален PIN и извличане на възможности на устройството. От страна на WebAuthn са разгледани ключовите структури от данни, които осигуряват контекстна обвързаност и проверимост:

- данни от клиента, които включват предизвикателство, произход и тип операция;

- данни от автентикатора, които съдържат хеш на идентификатора на услугата (rpIdHash), флагове за състояния като потребителска верификация, брояч на подписванията (signCount) и удостоверителни данни при регистрация;
- и атестационен обект, който позволява на сървъра да валидира характеристики и доверие към устройството, когато политиките изискват това.

Подчертано е, че именно комбинацията от „origin binding“ и обвързване към RP-ID прави подписа неизползваем извън реалната система, а атестацията е особено релевантна за среди с високи изисквания за контрол върху типовете допустими автентикатори.

В шестата подточка „**Анализ на сигурността и производителността**“ се извършва систематична оценка на контрамерките, заложени в протокола, както и на ефектите върху латентността, пропускателната способност и натоварването на сървърната инфраструктура. От гледна точка на сигурността е изведено, че WebAuthn елиминира споделените тайни и ограничава последствията от пробиви в хранилища, тъй като на сървъра се съхраняват публични ключове и метаданни, а не пароли или еквивалентни тайни. Показано е как фишингът се адресира чрез криптографско обвързване към домейна и идентификатора на услугата, replay атаките се ограничават чрез еднократни предизвикателства и броячи, а MitM атаките се редуцират чрез комбинация от защитен транспортен слой (HTTPS/TLS) и подписване на контекстни параметри на операцията. Разгледани са сценарии като кражба/клониране на устройство и е посочено, че протоколът изисква непредаваем частен ключ и допуска локална верификация на потребителя (биометрични данни или въвеждане на PIN), която не се пренася към приложния слой. Акцентирано е и върху организационната страна на сигурността, а именно че устойчивостта в реална среда зависи от политики за допустими автентикатори, управление на жизнения цикъл на устройствата, мониторинг и реакция при инциденти. Наред с това са обсъдени и бъдещи

предизвикателства, като например възможни усъвършенствани атаки, при които компрометиране на взаимодействието клиент-автентикатор може да доведе до кражба на сесия, както и рисковете, които квантовите изчисления поставят пред алгоритми като RSA и ECDSA, което налага планиране на преход към пост-квантови или хибридни схеми за подписване на низове.

По отношение на производителността е показано, че оценката е тясно свързана с прототипа, разработен в дисертационния труд, и че резултатите от измерванията се използват за калибриране на параметри като избор на алгоритъм, конфигурация на TLS/HTTPS и оптимизации на базата данни. Разгледана е процесната последователност на WebAuthn (генерация и изпращане на предизвикателство, взаимодействие браузър-автентикатор чрез CTAP2, верификация на подпис на сървъра) и е уточнено, че различните транспортни механизми имат различен принос към латентността (USB с най-ниско забавяне, NFC и BLE с допълнителни закъснения поради инициализация и поддържане на връзка). Акцентирано е, че изборът на криптографски алгоритъм има пряко отражение върху натоварването при масови едновременни автентикации, като по-ефективни конфигурации позволяват по-добра скалируемост в среди с множество активни потребители. В рамките на оптимизацията и мащабируемостта са описани инженерни подходи за ускоряване на хранилището и криптографските операции като например индексиране по потребител и идентификатор на автентикатор, логическо разделяне на таблици (partitioning), кеширане на статични елементи като публични ключове и метаданни, паралелизация и асинхронност при проверка на подписи и валидиране на съобщения, предварителна проверка на структурата преди криптографска обработка, както и инфраструктурни решения като клъстеризация и балансиране на натоварването, репликация на база данни и използване на кеширане за статични компоненти на клиента.

В седмата подточка „**Избор на подходящ автентикатор**“ се анализира влиянието на типа автентикатор върху скоростта, удобството и нивото на сигурност. Направено е разграничение между хардуерни автентикатори (USB,

NFC, Bluetooth) и платформени/биометрични решения, като е подчертано, че изборът следва да се базира на изискваното ниво на гаранция, контекста на използване и профила на потребителите. Посочено е, че USB автентикаторите осигуряват най-ниски времена за реакция и висока степен на контрол, NFC решенията добавят закъснение поради безконтактния канал, а BLE сценарии включват допълнителна латентност за установяване на сесия. Биометричните сензори предоставят бърза и интуитивна автентикация, като съществено е, че сравняването на биометричните шаблони се извършва локално, а ключът остава в защитена среда. Аргументира се твърдението, че в институционални среди често е целесъобразен хибриден модел, при който критични профили и административен достъп използват хардуерни автентикатори, а масовите потребители – платформени/биометрични автентикатори, като се осигуряват резервни средства за възстановяване на достъп.

В осмата подточка „**Интеграционни и оперативни проблеми при внедряване на FIDO/WebAuthn в големи институционални среди**“ се показва, че успешното внедряване изисква не само технологична интеграция, но и организационна рамка за управление, поддръжка и приемане от потребителите. Подчертано е, че институционалната среда се характеризира с хетерогенни устройства, различна техническа грамотност и необходимост от съвместимост между уеб и мобилни платформи, което налага управляеми политики и устойчиви процеси. Разгледан е подходът за интеграция със съществуващи системи за управление на идентичности и достъп, включително централизирани схеми за удостоверяване, директории с потребители и федеративни модели, като е аргументирано, че оптимален ефект се постига при добавяне на WebAuthn на ниво доставчик на идентичност, а не като изолирана функционалност в отделно приложение, тъй като това осигурява единна точка на автентикация, унифицирано управление на ключове и съвместимост между множество услуги.

Интеграцията следва да предвиди защитено и производително съхранение на публичните ключове и метаданните на автентикаторите,

индексиране по потребител и идентификатор на удостоверителните данни, както и механизми за кеширане и логическо структуриране на данните при голям мащаб. Отделено е внимание на жизнения цикъл на автентикаторите като ключово оперативно предизвикателство, тъй като са необходими ясни процедури за регистрация, отмяна (revocation), временно блокиране и възстановяване на достъп, като се препоръчва задължителна регистрация на резервен автентикатор и възможност за дистанционно деактивиране чрез системите за управление на идентичности. За сценарии с дистанционни потребители са очертани гъвкави методи за повторно удостоверяване на самоличността, които да съчетават сигурност и оперативна ефективност.

Показано е още, че приемането от потребителите зависи от качеството на потребителското изживяване. Необходима е интуитивна регистрация, ясни указания на всяка стъпка и безпроблемна употреба на различни платформи, като могат да се използват измерими метрики (време за регистрация, време за автентикация, процент успешни входове без техническа помощ). Подчертано е значението на постоянния мониторинг и одит на събитията по автентикация, включително регистриране на успешни и неуспешни опити, използвани устройства, локация и ниво на доверие на сесията, както и възможност за интеграция със системи за анализ и ранно откриване на аномалии. Дефинирани са и оперативни показатели за управление на внедряването (процент успешно регистрирани устройства, средно време за възстановяване на достъп, инциденти с изгубени/компрометирани автентикатори, честота на използване на резервни методи), като е аргументирано, че редовното им отчитане подпомага оптимизацията на процесите. В заключение е изведено, че внедряването в големи институции изисква балансиран подход между технологична надеждност, оперативна ефективност и достъпност за потребителя, а успехът зависи както от правилния избор на протоколи и устройства, така и от способността на организацията да управлява жизнения цикъл на автентикаторите, да провежда обучения и да поддържа висока степен на приемане. Като логическо продължение е посочено, че следващата глава

представя практическото внедряване на FIDO/WebAuthn в университетска информационна система, включително интеграцията с текущата инфраструктура, процесите по регистрация и управление на автентикаторите и постигнатите резултати от внедряването.

Глава III. Внедряване на WebAuthn в уеб-базираната информационна система на Икономически университет – Варна

В трета глава на дисертационния труд е представено практическото внедряване на WebAuthn в реална уеб-базирана институционална среда – информационната система на Икономически университет – Варна. Главата има приложен характер и показва как разработеният във втора глава модел за силна автентикация може да бъде интегриран в съществуваща инфраструктура с минимален риск, без прекъсване на услугата и при запазване на съвместимостта с наследени компоненти. Разгледани са организационният контекст и еволюцията на университетските системи, избраната архитектурна стратегия за интеграция в PHP/MySQL среда, ключовите технически компоненти и сървърни конфигурации, както и потребителските потоци по регистрация и автентикация. В заключителната част е демонстрирана възможността технологията да надгради автентикацията и да се използва като механизъм за криптографско удостоверяване на критични действия в учебния процес, с акцент върху защитата на данните, генерирани в академичната среда.

В първата подточка „**Обща характеристика на ИУ–Варна**“ се описва институционалната среда, в която се реализира внедряването, и се аргументира защо именно университетска информационна система е подходяща за валидиране на WebAuthn в условията на разнообразни потребители и високи изисквания към наличност и сигурност. Икономически университет – Варна е висше училище с утвърдена практика в използването на цифрови технологии за управление на учебни и административни процеси, като профилът на потребителите включва хиляди студенти, международни обучаеми и значителен академичен и административен състав. Тази

хетерогенност поставя изисквания не само към защитата на достъпа, но и към удобството и надеждността на механизмите за удостоверяване, тъй като системата трябва да работи в широк спектър от устройства, браузъри и потребителски навици. В подточката е проследена еволюцията на информационните системи в университета през няколко технологични етапа, като се подчертава как стратегическите приоритети по дигитализация и развитието на интернет инфраструктурата постепенно трансформират модела на достъп – от локално ограничени решения към интернет-достъпни платформи. Представен е ранният етап, при който сървърната инфраструктура е базирана на една машина с операционна система Novell, която изпълнява функции по идентификация чрез потребителско име и парола и предоставя споделяне на файлове с програмен код и бази данни във формат dBase, като достъпът е ограничен до компютри в локалната мрежа на университета. Описан е и междинният организационен подход за информираност на студентите чрез терминали в сградата на университета, където те въвеждат факултетен номер (към този момент все още албумен номер) и ЕГН за извличане на оценки и лични данни, като зад всеки терминал стои отделен компютър с мрежова връзка към сървъра. Следващият етап е свързан с проект за конвертиране и модернизация на базата данни, чрез който се полагат основите на по-достъпна платформа, позволяваща на студентите да достигат до информация и през интернет. В този контекст се създава поддомейнът info.ue-varna.bg и се изгражда сървърна среда с Linux, уеб сървър с поддръжка на PHP и локална MySQL база данни, използвана и за ETL процеса. Тази еволюция е важна предпоставка за внедряване на WebAuthn, защото показва налична уеб архитектура, реални потребители и натоварване, както и ясно изразена необходимост от повишаване на сигурността в достъпна в интернет пространството услуга.

Във втората подточка „**Интеграция на WebAuthn в съществуващата PHP/MySQL среда**“ се разглежда стратегическият подход за надграждане на сигурността на системата WSDB без разрушаване на наличната логика и без

необходимост от пълно пренаписване на потребителския модул. Изходната среда е описана като стабилна PHP/MySQL инфраструктура в рамките на WHM/cPanel сървър, поддържана организационно от специализирана структура в университета, като системата е виртуализирана върху локална (self-hosted) инфраструктура. В дисертационния труд е изведено, че тази инфраструктура дава по-висока степен на контрол върху данните и конфигурацията, но изисква дисциплинирана поддръжка, стриктни актуализации и активни защитни механизми поради постоянната експозиция към външни атаки. Основната цел на интеграцията на WebAuthn е тя да се въведе като допълнителен слой за сигурност, работещ паралелно с класическата паролна автентикация, така че внедряването да бъде съвместимо и да позволи постепенна миграция, включително сценарии, при които WebAuthn постепенно замества паролата напълно или я допълва като втори фактор. Показано е, че от архитектурна гледна точка това се реализира чрез междинен слой (middleware), който посредничи между уеб приложението, базата данни и браузъра на клиента и изпълнява ключови функции като генериране на криптографски предизвикателства, верификация на подписи и публични ключове, обработка на атестационни данни, както и управление на сесии и отговори към клиента. В контекста на програмния езикт PHP е разгледано използването на специализирани софтуерни библиотеки, които реализират необходимите операции за регистрация и автентикация и позволяват коректна обработка на протоколните структури и сериализацията им. Подчертано е, че този модел гарантира фундаментално свойство на WebAuthn, а именно че сървърът работи единствено с публични ключове и подписани отговори и по дизайн няма достъп до частните ключове, които остават защитени в автентикатора на потребителя. На сървърно ниво като ключово условие е разгледана необходимостта цялата комуникация да се извършва през HTTPS с TLS, както и ограничаването на операциите до домейн, допустим в конфигурацията на WebAuthn. Това, комбинирано с обвързването на подписа към произхода, съществено редуцира риска от

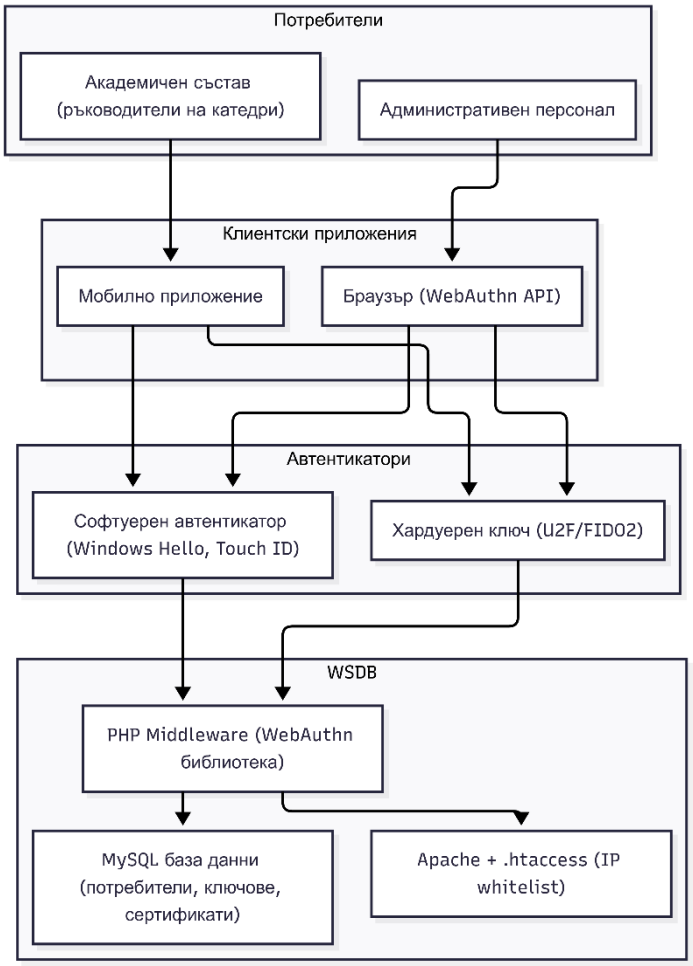
фишинг и атаки чрез повторение, тъй като генерираните подписи са валидни единствено в рамките на конкретния домейн и конкретния контекст на операцията.

В третата подточка „**Компоненти на системата**“ се описва архитектурата на внедреното решение като съвкупност от четири основни компонента, които в комбинация реализират универсална двуфакторна автентикация:

- клиентски уеб интерфейс,
- FIDO устройство (автентикатор),
- сървърна логика за автентикация
- и база данни за съхранение на необходимата информация.

Клиентският компонент е реализиран с HTML5, CSS и JavaScript, като основната точка на интеграция е WebAuthn API в браузъра. Показано е, че браузърът изпълнява ролята на доверен посредник между приложението и автентикатора, като стартира регистрацията чрез извикване на `navigator.credentials.create()` и стартира автентикацията чрез `navigator.credentials.get()`. В дисертационния труд е акцентирано, че освен чисто техническото извикване на API, клиентският слой е критичен и за качеството на потребителското изживяване. Клиентският слой управлява визуалните съобщения, инструкциите към потребителя и обработката на грешки и повторни опити, например когато устройството не е открито, когато потребителят прекъсне процеса или когато автентикацията е неуспешна. Обсъден е и практическият аспект на съвместимостта – необходимостта решението да работи в различни браузъри и мобилни операционни системи, което е ключово за институционална услуга с широк профил от потребители. Посочено е, че системата е конфигурирана така, че в първоначалния етап да не изисква конкретни модели на атестация на автентикатори, което намалява бариерите пред внедряването и улеснява първоначалното внедряване и експлоатация. Отделено е внимание и на параметри, които влияят на реалната използваемост, като например настройката на времевите прозорци за реакция,

тъй като прекомерно кратки стойности могат да доведат до неуспешни процеси при определени транспортни режими, например при Bluetooth автентикатори. В архитектурната част е включен и архитектурен модел за внедряване на WebAuthn във WSDB (Фигура 1), който визуализира взаимодействията между браузър, WebAuthn API, автентикатор, сървър и база данни и фиксира мястото на middleware слоя в общата схема.



Фигура 1. Архитектура на системата за автентикация в WSDB

Разработка на автора

В четвъртата подточка „**Сървърна конфигурация и реализация на системата**“ се аргументира изборът на уеб сървър и конкретната конфигурация като част от изискванията за съвместимост и минимален риск при интеграция. В дисертационния труд е прието, че Apache HTTP Server е най-подходящото решение в конкретния контекст, тъй като вече е внедрен и поддържан в рамките на WHM/cPanel средата, в която функционира

университетската система. Представено е, че Apache предлага дългогодишна стабилност, широка екосистемна поддръжка и естествена съвместимост с традиционни PHP приложения, включително такива, които разчитат на .htaccess и модулни директиви. Направено е сравнение с алтернативи, като е уточнено, че макар някои от тях да имат предимства при обслужване на статично съдържание, в контекста на динамично PHP/MySQL приложение и при необходимост от минимални архитектурни промени, Apache в комбинация с PHP-FPM представлява практично и нискорисково решение. Подчертано е, че критично условие за WebAuthn е наличието на HTTPS, което се осигурява чрез модул за TLS/SSL и подходяща поддръжка на сертификати, като това може да се управлява ефективно в cPanel среда. Разгледана е и възможността чрез конфигурационни механизми да се запазят и надградят текущи политики за ограничаване на достъпа (например вече налични IP ограничения), така че WebAuthn да не замени съществуващия контрол, а да го допълни със съвременен протокол за автентикация.

В петата подточка „**Регистрация и автентикация на потребител**“ се описват потребителските потоци и инженерните решения при внедряването им в WSDB, като се разглеждат два подхода за регистрация на FIDO автентикатор към потребителски профил. Първият, по-разпространен подход, разделя регистрацията на две логически стъпки – първо се създава базов запис за потребителя в базата данни с цел генериране на уникален идентификатор (user ID), а след това, при успешното подписване от страна на автентикатора, към този запис се добавят данните за новосъздадения публичен ключ и идентификатора на удостоверителните данни. Аргументирано е, че това улеснява коректното обвързване на предизвикателството с конкретен потребител и поддържа ясна транзакционна логика при съхранение. Вторият подход реализира регистрация в една стъпка, при която въведените потребителско име и парола се прихващат и валидират преди заявката за генериране на предизвикателство, като след това се извършва допълнителна сървърна проверка за уникалност на потребителското име и се продължава с

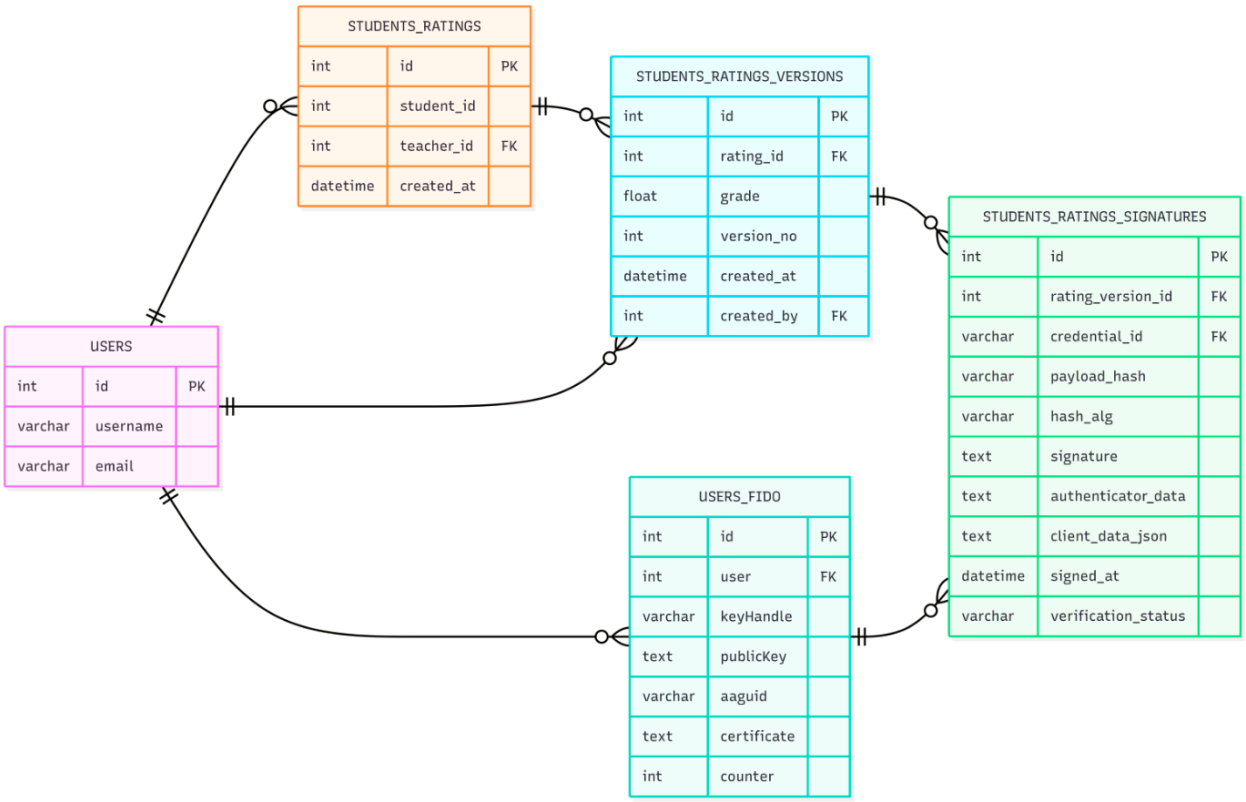
регистрацията. В дисертационния труд е посочено, че този подход може да намали броя на стъпките за потребителя, но изисква по-строга валидация и внимателно управление на данните. От клиентска страна регистрационният процес е описан като последователност, при която след въвеждане на потребителски идентификатор клиентът заявява от RP сървъра параметрите за регистрация, включително криптографско предизвикателство, идентификатор на услугата, данни за потребителя, допустими криптографски параметри и политики. След това браузърът инициира създаването на удостоверителни данни чрез WebAuthn API, а получените структури се сериализират в подходящ формат за пренос и се изпращат към сървъра за валидация и запис. От сървърна страна процесът е описан като двустъпков – генериране и временно съхранение на предизвикателство за корелация между заявка и отговор (например в сесийна променлива), последвано от приемане на отговора от автентикатора, верификация на подписа и (при наличие) атестационните данни и финално записване на публичния ключ, идентификатора на удостоверителните данни и брояча (signCount), който подпомага защитата срещу повторение и откриване на потенциално клониране.

В шестата подточка „**Хардуерни устройства**“ се разглеждат хардуерните автентикатори като физически носители на криптографски ключове и като практическа опция за потребители с повишени нива на достъп в университетска и институционална среда. Показано е, че основното им предимство е изолираната среда за генериране и съхранение на частния ключ, която минимизира риска от зловреден софтуер и от компрометиране през операционната система и мрежовите слоеве. В дисертационния труд е обяснено, че съвременните FIDO2 автентикатори работят чрез протокола CTAP2, който дефинира комуникацията между браузъра/приложението и физическото устройство, като устройствата могат да използват различни интерфейси – USB за настолни компютри и административни станции, NFC и Bluetooth при сценарии с мобилни устройства и потребители, които работят с

лаптопи и смартфони. Описано е, че хардуерните автентикатори разчитат на защитени елементи като Secure Element или TPM за съхранение на частния ключ и за извършване на криптографски операции вътрешно в устройството, така че частният ключ да не се разкрива и да не напуска защитената среда; към сървъра се изпраща единствено подпис върху уникално предизвикателство, генерирано от системата. Подчертано е, че този модел е особено подходящ за профили, при които компрометирането на достъпа би имало значими последици, например администратори, служители и преподаватели с разширени права.

В седмата подточка „**Възможности за внедряване на WebAuthn в учебния процес на висшите училища**“ се разширява приложният обхват на технологията отвъд автентикация в системата и се демонстрира как WebAuthn може да се използва като криптографски механизъм за удостоверяване и подписване на критични действия в учебния процес, с акцент върху оценяването на студентите от преподавателите. В дисертационния труд първо е описан базовият, „аналогов“ сценарий, при който процесът започва с явяване на студентите на изпит, преподавателят формира оценка по шестобалната система и я нанася в предварително изготвен списък на студентите, наречен „изпитен протокол“. След приключване на изпита преподавателят отразява оценките и в т.нар. „главна книга“, която представлява структурирана съвкупност от студентски данни, организирани по определен принцип, например по факултет или форма на обучение. Посочено е, че реквизитите и изискванията към главните книги са нормативно определени, а процесът логически приключва на етапа, в който студентът достигне до дипломиране, когато служител проверява наличието на всички оценки по учебен план и изготвя дипломата, като на практика пренася информацията от главната книга в дипломния документ. На тази основа е предложен модел за дигитализация, при който WebAuthn не служи единствено за автентикация, а се използва и за криптографско подписване на действията по въвеждане и потвърждаване на оценки и други академични записи. Описано е, че при въвеждане или

потвърждаване на оценка системата генерира уникално предизвикателство, което включва идентификатори на дисциплината, протокола, конкретния студент и времеви отпечатък, след което автентикаторът подписва предизвикателството, а сървърът валидира подписа спрямо публичния ключ, асоцииран с профила на преподавателя. Така всяка оценка се съпровожда от проверимо криптографско доказателство за авторство и целостта на записа, което повишава възможността за извършване на одити и намалява риска от неоторизирани промени и спорни ситуации при последващи проверки. В дисертационния труд е посочено, че моделът е приложим не само за оценки, но и за подписване на изпитни протоколи и главни книги, както и за други академични документи и действия, при които организационните правила изискват повишена надеждност и проследимост. Концептуалният модел за цифрово подписване на академични записи с WebAuthn е илюстриран с Фигура 2, която визуализира потока на предизвикателство-подпис-верификация и връзката му с регистрите на академични данни.



Фигура 2. Разширен релационен модел за целите на подписване на оценки

В заключение на главата в дисертационния труд е обобщено, че реализираното внедряване демонстрира практическата приложимост на WebAuthn като универсален механизъм за силна автентикация в уеб-базирани системи при реални организационни ограничения. Показано е, че избраният подход позволява надграждане на съществуваща PHP/MySQL среда с минимална инвазивност и поддържане на обратна съвместимост, като едновременно с това създава основа за разширяване към сценарии с по-висока степен на доказуемост и одитируемост на критични действия, включително в учебния процес.

IV. ПРИНОСИ

На база на проведените изследвания в дисертационния труд могат да бъдат формулирани следните научни и практико-приложни приноси:

1) Теоретично е обоснована концепцията за WebAuthn като нова парадигма за автентикация, преодоляваща основните уязвимости на паролно-базираните механизми за автентикация.

2) Разработен е архитектурен модел за внедряване на WebAuthn в университетска уеб-базирана информационна система, адаптиран към българския академичен контекст и към съществуваща PHP/MySQL инфраструктура.

3) Реализирана е практическа интеграция на WebAuthn в реална университетска информационна система (WSDB на ИУ–Варна), чрез която е демонстриран пълен и работещ цикъл на регистрация и автентикация с FIDO2 съвместими автентикатори.

4) Предложен и експериментално валидиран е механизъм за криптографско подписване на действия (в частност въвеждане и подписване на студентски оценки), базиран на WebAuthn, който осигурява обвързване на удостоверената идентичност с конкретно действие в рамките на университетската информационна система.

V. ПУБЛИКАЦИИ ПО ДИСЕРТАЦИОННИЯ ТРУД

Научни статии

1. Димитров, П. Методологични проблеми при използване на квалифициран електронен подпис и универсалната двуфакторна автентикация в уеб приложения. Известия на Съюза на учените – Варна, Сер. Икономически науки. Науката в служба на обществото: Научна конференция на СУБ – клон Варна, 7, 2018, 3, 287 – 293.

2. Dimitrov, P. & Petrov, P. (2025). Historiographical Study of Authentication Approaches in Computer Systems. *Izvestia Journal of the Union of Scientists - Varna. Economic Sciences Series, 14*(1) – под печат.

3. Dimitrov, P. & Simeonidis, D. (2025). Security Considerations Regarding Access to Information Systems. *Izvestia Journal of the Union of Scientists - Varna. Economic Sciences Series, 14*(1) – под печат.

Научни доклади

1. Димитров, П. Алгоритмични проблеми при внедряване на двуфакторна автентикация в уеб приложения. Научна конференция на младите научни работници – 2018: Сборник с доклади, Варна: Стено, 2018, с. 126 – 131.

2. Petrov, P., Dimitrov, P. Security Certificates in Public Web Sites of Banks from Balkan States. 9th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE – 2019), Oct. 24 – 26, 2019 : Conference Proceedings, Sofia : UNWE, 2019, 160 – 169.., ISSN(печатно) 2367-7635 , ISSN(онлайн) 2367-7643

3. Petrov, P., Buevich, A., Dimitrov, G., Kostadinova, I., Dimitrov, P. A Comparative Study on Web Security Technologies Used in Bulgarian and Serbian Banks. 19 International Multidisciplinary Scientific Geoconference SGEM 2019 : Conference Proceedings, 28 June – 7 July 2019, Albena, Bulgaria : Vol. 19. Informatics, Iss. 2.1, Sofia: STEF92 Technology Ltd., 2019, 3-10., ISSN(печатно) 13142704, ISBN(печатно) 978-619740876-8 / **Scopus**

4. Petrov, P., Dimitrov, P., Stoev, S., Dimitrov, G., Bulut, F. Using the Universal Two Factor Authentication Method in Web Applications by Software Emulated Device. 20th International Multidisciplinary Scientific Geoconference SGEM 2020 : Conference Proceedings, 18 – 24 Aug. 2020, Albena, Bulgaria : Vol. 20. Informatics, Geoinformatics and Remote Sensing. Iss. 2.1. Informatics, Geoinformatics, Sofia : STEF92 Technology DOI: https://doi.org/10.5593/sgem2020/2.1/s07.052, 20, 2020, 2.1, 403 – 410.., ISSN(печатно) 1314-2704, ISBN(печатно) 978-619-7603-06-4 / DOI 10.5593/sgem2020/2.1/s07.052 / **Scopus**