ҒТАХР 81.93.29

10.51889/2959-5894.2026.93.1.018

Н.А. Капалова[1], Н.С.Ергеш[2*]

[1]ҚР ҒЖБМ ҒК Ақпараттық және есептеу технологиялары институты, Алматы қ., Қазақстан
[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан
[*]e-mail: yergesh.nursultan@almatyedu.kz

ҚОРҒАЛҒАН АУТЕНТИФИКАЦИЯ СХЕМАЛАРЫ: ӘДІСТЕРІ ЖӘНЕ ҚАУІПСІЗДІК ТАЛДАУЫ

Аңдатпа

Бұл мақалада ақпараттық жүйелердегі қорғалған аутентификация схемаларының негізгі әдістері жүйелендіріліп, олардың қауіпсіздік қасиеттері теориялық және қолданбалы тұрғыдан талданады. Зерттеудің мақсаты - құпиясөзге негізделген, көпфакторлы және парольсіз аутентификация тәсілдерінің қауіп-қатер моделін айқындап, қарсыластың мүмкіндіктерін ескере отырып салыстырмалы бағалау жүргізу. Талдау барысында шабуыл векторлары (онлайн және офлайн іріктеу, тіркелгі деректерін қайта қолдану, фишинг, сеансты басып алу) жіктеліп, бұзылу ықтималдығын бағалауға арналған ықтималдықтық модельдер және факторларды біріктірудің композициялық қағидалары қарастырылады. Құпиясөздік схемалар үшін табыстылық ықтималдығы құпиясөз кеңістігінің тиімді көлеміне, тексеру құнына және әрекет санын шектеу механизмдеріне тәуелді екені көрсетіледі. Көпфакторлы аутентификацияда қауіпсіздіктің артуы факторлардың тәуелсіздігі жағдайында жалпы бұзылу ықтималдығының көбейтінді түрінде төмендеуімен негізделеді. Парольсіз схемаларда ашық кілтке негізделген шақыру-жауап (challenge–response) протоколдары фишингке төзімділікті күшейтіп, тіркелгі деректерін қайта қолдану тәуекелін азайтатыны сипатталады. Нәтижесінде тәуекел деңгейіне сәйкес аутентификаторларды таңдау, әрекеттерді шектеу, құрылғыға байлау және контекстік тәуекелді бағалау бойынша практикалық ұсынымдар беріледі. Ұсынылған қорытындылар қауіпсіздігі күшейтілген аутентификация шешімдерін жобалау және эксперименттік тексеру үшін әдістемелік негіз қалыптастырады.

Түйін сөздер: аутентификация; қорғалған аутентификация; көпфакторлы аутентификация; парольсіз аутентификация; қауіп-қатер моделі; ықтималдықтық талдау; фишингке төзімділік; шақыру-жауап протоколы.

Н.А. Капалова[1], Н.С. Ергеш [2]
[1]Институт информационных и вычислительных технологий КН МНВО РК, г.Алматы, Казахстан
[2]Казахский национальный университет имени аль-Фараби, г.Алматы, Казахстан

ЗАЩИЩЁННЫЕ СХЕМЫ АУТЕНТИФИКАЦИИ: МЕТОДЫ И АНАЛИЗ БЕЗОПАСНОСТИ

Аннотация

В статье систематизированы основные методы построения защищённых схем аутентификации в информационных системах и выполнен теоретико-прикладной анализ их свойств безопасности. Цель исследования заключается в определении модели угроз и сравнительной оценке парольной, многофакторной и безпарольной аутентификации с учётом возможностей противника. В рамках анализа классифицируются ключевые векторы атак (онлайн и офлайн перебор, повторное использование учётных данных, фишинг, захват сеанса), рассматриваются вероятностные модели оценки успешности компрометации и композиционные принципы объединения факторов. Для парольных схем показано, что вероятность успешной атаки определяется эффективным размером пространства паролей, вычислительной стоимостью проверки гипотез и механизмами ограничения числа попыток. Для многофакторной аутентификации рост устойчивости обосновывается мультипликативным снижением вероятности компрометации при независимости факторов. Для безпарольных подходов описываются публично-ключевые протоколы типа «вызов–ответ» (challenge–response), повышающие устойчивость к фишингу и уменьшающие риск повторного использования учётных данных. В результате сформулированы практические рекомендации по выбору

аутентификаторов в зависимости от уровня риска, ограничению попыток входа, привязке к устройству и контекстной оценке риска. Полученные выводы могут служить методологической основой для проектирования и экспериментальной проверки усиленных решений аутентификации.

Ключевые слова: аутентификация; защищённая аутентификация; многофакторная аутентификация; безпарольная аутентификация; модель угроз; вероятностный анализ; устойчивость к фишингу; протокол вызов–ответ.

N.A. Kapalova[1], N.S. Yergesh[2]
[1]Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan
[2]Al-Farabi Kazakh National University, Almaty, Kazakhstan

SECURE AUTHENTICATION SCHEMES: METHODS AND SECURITY ANALYSIS

Abstract

This paper systematizes key methods for designing secure authentication schemes in information systems and provides a combined theoretical and practical analysis of their security properties. The study aims to define a unified threat model and to comparatively evaluate password-based, multi-factor, and passwordless authentication approaches under realistic adversary capabilities. The analysis classifies major attack vectors (online and offline guessing, credential reuse, phishing, and session takeover) and considers probabilistic models for estimating compromise success as well as compositional principles for combining factors. For password-based schemes, we show that attack success probability depends on the effective password search space, the computational cost of verifying guesses, and attempt-limiting controls. For multi-factor authentication, improved robustness is explained by a multiplicative decrease in compromise probability under factor independence. For passwordless approaches, we describe public-key challenge–response protocols that increase phishing resistance and reduce credential reuse risks. Finally, we provide practical recommendations on selecting authenticators by risk level, enforcing strict attempt limiting, enabling device binding, and applying context-aware risk assessment. The presented results can serve as a methodological basis for designing and experimentally validating strengthened authentication solutions.

Keywords: authentication; secure authentication; multi-factor authentication; passwordless authentication; threat model; probabilistic analysis; phishing resistance; challenge–response protocol.

Кіріспе

Қазіргі ақпараттық жүйелерде - бұлттық сервистерде, электрондық қызметтерде, корпоративтік порталдар мен білім беру платформаларында - қол жеткізуді басқарудың негізгі буыны аутентификация механизмі болып табылады. Аутентификация пайдаланушының заңды екендігін растауға арналған. Егер бұл механизм әлсіз болса, авторизация, аудит және бақылау құралдары өз тиімділігін жоғалтады. Себебі қауіп көбінесе «кім кірді?» деген бастапқы кезеңде-ақ іске асады. Сондықтан халықаралық стандарттарда аутентификацияны тәуекелге сай деңгейлеу, аутентификатор сенімділігі және протоколдың фишингке төзімділік қасиеті жеке талап ретінде қарастырылады [1-3].

Тәжірибеде ең кең тараған тәсіл – құпиясөзге негізделген бір факторлы схема. Бұл тәсіл қолдануға ыңғайлы болғанымен, қазіргі қауіп-қатер ортасында елеулі шектеулерге ие. Пайдаланушылардың құпиясөзді бірнеше сервисте қайталап қолдануы және әлсіз комбинацияларды таңдауы тіркелгі деректерін толтыру (credential stuffing), құпиясөзді жаппай сынау (password spraying) және офлайн іріктеу (brute-force) шабуылдарының сәтті болу ықтималдығын арттырады [4-5]. Фишинг пен әлеуметтік инженерия техникалық қорғаныс жоқ болған жағдайда бірнеше қорғаныс қабатын бір уақытта айналып өтуге қабілетті. Сонымен қатар, дерекқор бұзылған кезде хэш-қорғаныс дұрыс таңдалмаса, шабуылдаушының офлайн есептеу ресурстары қауіпті практикалық деңгейге көтереді [5]. Осыған байланысты «қорғалған аутентификация» ұғымы тек құпиясөз саясатын ғана емес, көпқабатты және дәлелденетін қауіпсіздік қасиеттері бар схемаларды таңдауды талап етеді.

Осы шолу мақаланың мақсаты - қорғалған аутентификация схемаларының қазіргі әдістерін жүйелеп, олардың қауіпсіздігін қауіп-қатер моделі тұрғысынан талдау.

Міндеттері:

1) құпиясөзді күшейту тәсілдерін (хэштеу, есептеу құнын арттыру, әрекетті шектеу) жинақтау;

2) көпфакторлы аутентификацияның (бір реттік кодтар, аппараттық токендер, биометрия) қауіпсіздік артықшылықтарын және тәуелсіздік шарттарының рөлін түсіндіру;

3) ашық кілтке негізделген парольсіз шақыру–жауап (challenge–response) протоколдарының фишингке төзімділік қасиеттерін сипаттау;

4) қауіпсіздік–қолданушылық компромисін ескере отырып, тәуекел деңгейіне сәйкес практикалық ұсынымдар ұсыну [1-2], [6-7].

Зерттеу әдістемесі ретінде бірнеше бағыттағы материалдар жүйелі талданады: халықаралық стандарттар мен нұсқаулықтардың талаптары (аутентификация сенімділігі деңгейлері, фишингке төзімділік), қолданбалы қауіпсіздік ұйымдарының ұсынымдары (онлайн шабуылдарға қарсы бақылаулар), сондай-ақ веб-аутентификацияның салалық стандарттары (WebAuthn, FIDO тәрізді) [1-7]. Мақаланың келесі бөлімдерінде алдымен қауіп-қатер моделі мен бағалау қағидалары беріледі. Одан кейін құпиясөзге негізделген тәсілдер, көпфакторлы схемалар және парольсіз протоколдар салыстырылады. Соңында қорытынды ұсынымдар жасалады [8].

Зерттеу әдіснамасы

Зерттеу жұмысы жүйелендіруші шолу (structured narrative review) ретінде орындалды. Аутентификация схемаларының қазіргі әдістері (құпиясөзге негізделген, көпфакторлы, парольсіз) ортақ қауіп-қатер моделі шеңберінде бірдей критерийлермен сипатталып, салыстырмалы синтез жүргізілді. Зерттеу келесі кезеңдерден тұрады:

1-кезең. Дереккөздерді іріктеу: нормативтік құжаттар (NIST SP 800-63B-4), протоколдық стандарттар (RFC 9106, RFC 6238), индустриялық нұсқаулықтар (OWASP) және ғылыми еңбектер жиналып, сәйкестік, сенімділік және техникалық мазмұн критерийлері бойынша іріктелді.

2-кезең. Формальдандыру: әр аутентификация механизмі «қолданылатын аутентификаторлар» және «верификация протоколы» тұрғысынан сипатталып, $\Pi=\langle Enroll, Auth, Verify, Recover\rangle$ төрттігімен модельденді.

3-кезең. Қауіп-қатерлерге сәйкестендіру: әр схема A1 (онлайн болжау), A2 (офлайн бұзу), A3 (тіркелгі деректерін толтыру), A4 (фишинг/прокси-фишинг) шабуыл кластарымен салыстырылып бағаланды.

4-кезең. Салыстырмалы синтез: қауіпсіздік, қолданушылық және енгізу күрделілігі өлшемдері бойынша интеграл баға есептелді және матрица/диаграмма түрінде берілді. Мұндай нормаланған сипаттау тәсілі аутентификация талаптарын тәуекелге негіздеп қоюға мүмкіндік береді [1-3].

Зерттеу сұрақтары (RQ):

RQ1. Қазіргі қорғалған аутентификацияда негізгі техникалық бағыттар қандай және олар қандай қауіп-қатерлерді жабады? [1-2]

RQ2. Құпиясөзді сақтау/тексеру (KDF, memory-hard функциялар) параметрлері офлайн шабуылға төзімділікке қалай әсер етеді? [7-8]

RQ3. OTP және MFA тәсілдерінің фишингке төзімділік шекарасы қандай және passwordless (WebAuthn/FIDO) шешімдері оны қалай өзгертеді? [2], [9-12], [13]

Шолуда дереккөздер төрт деңгейге бөлініп қаралады:

- нормативтік/ұсыным құжаттар (Digital Identity Guidelines, assurance деңгейлері) [1-3];
- протоколдық стандарттар (IETF RFC: PBKDF2, Argon2, HOTP/TOTP) [7-10];
- веб-қолданба қауіпсіздігі бойынша индустриялық нұсқаулықтар (OWASP cheat sheet-тері) [4-6];
- салыстырмалы бағалау қаңқаларын ұсынатын ғылыми еңбектер (қауіпсіздік-қолданушылық-ендіру компромисі) [13].

Іріктеу критерийлері:

- Сәйкестік: аутентификация, аутентификатор, протокол қауіпсіздігі, шабуыл модельдері;
- Қайнар сенімділігі: ресми стандарттар/спецификациялар және кең танылған қауіпсіздік нұсқаулықтары;
- Тексерілетін техникалық мазмұн: анықтамалар, талаптар, протокол ағымы, параметрлер, қауіпсіздік талдауы.

Бұл бөлімде сандық PRISMA-санақ (қанша материал табылды т.б.) берілмейді, өйткені мақаланың мақсаты - санақтан гөрі әдістерді жүйелеу және дәлелдік қауіпсіздік талдау логикасын көрсету.

Әр схема төмендегі төрттікпен сипатталады: П=⟨Enroll, Auth, Verify, Recover⟩, мұнда Enroll- тіркеу/байлау (аутентификаторды аккаунтқа бекіту), Auth-дәлелді ұсыну (пароль енгізу, OTP, қолтаңба), Verify- верификация (сервер/IdP тексеруі), Recover- қалпына келтіру/өмірлік цикл (reset, rebind) [2], [11].

Таксономия (классификация):

Password-based: пароль + KDF/хэштеу + онлайн қорғаныс бақылаулары [4], [7].

MFA/2FA: кемінде 2 фактор (“білім-иелік-инеренция”), факторлар тәуелсіздігі және басқару талаптары [2].

Passwordless (public-key challenge–response): криптографиялық дәлел (қолтаңба) және relying party-ге/origin-ге байлау (scoped credentials) [11-12].

Талдау қолданба деңгейіндегі қарсыласқа негізделеді: қарсылас желіні бақылай алады, фишинг бет жасай алады, бот арқылы көптеген сұраным жібере алады; кей сценарийде пароль хэш-дерекқоры алынуы мүмкін. OWASP материалдары credential stuffing және password spraying сияқты автоматтандырылған шабуылдарды нақтылайды [5-6].

Шабуыл кластары:

A1: Онлайн болжау (online guessing/brute-force).

A2: Офлайн болжау (offline cracking) - KDF параметрлеріне тәуелді.

A3: Credential stuffing / spraying (қайта қолданылған парольдер).

A4: Фишинг және прокси-фишинг (реал-тайм делдал).

NIST нұсқаулығында assurance деңгейлері (AAL) және “phishing-resistant” талаптарының логикасы көрсетіледі: жоғары сенімділік үшін криптографиялық, экспортталмайтын кілтке негізделген аутентификаторлар талап етіледі [2].

Онлайн болжаудың табыстылық ықтималдығы. Егер қарсылас бір аккаунтқа qрет әрекет жасаса, ал құпия кеңістігі тиімді түрде N_{eff}болса (идеалдандырылған бірқалыпты жорамал), онда:

$$P_{\text{online}} = 1 - \left(1 - \frac{1}{N_{\text{eff}}}\right)^{q} \approx \min\left(1, \frac{q}{N_{\text{eff}}}\right).$$

Мұнда q- rate limiting/lockout/кідіріс саясатымен шектеледі (OWASP-та осы бақылаулардың практикалық нұсқаулары берілген) [4-5].

Ал парольдер бірқалыпты емес таралған жағдайда (тәжірибеде жиі), ең дұрысы -болжамдар ықтималдығын кему ретімен $p_{(i)}$деп алып:

$$P_{\text{online}}(q) = \sum_{i=1}^{q} p_{(i)}\,.$$

Бұл формула “ең ықтимал парольдер алдымен тексеріледі” деген рационалды қарсылас моделін береді және credential stuffing/төмен энтропия мәселесін түсіндіруге ыңғайлы [13].

Офлайнда қарсылас парольді тексеру функциясын жылдам қайталай алады. Сондықтан негізгі көрсеткіш - бір тексерудің есептеу құны C_{verify}және шабуылшының есептеу ресурсы R(тексеру/сек).

Жуық уақыт:

$$T_{\text{crack}} \approx \frac{G \cdot C_{\text{verify}}}{R},$$

мұнда G- болжам саны.

PBKDF2 үшін C_{verify}итерация саны cарқылы өседі:

$$C_{\text{PBKDF2}} \propto c \cdot C_{\text{PRF}},$$

өйткені PBKDF2 негізгі PRF-ті (әдетте HMAC) көп рет қолданады [7].

Argon2 типті memory-hard функцияларда қарсыласқа тек CPU емес, жад ресурсы да керек. RFC 9106 Argon2-нің қолданбалы сипаттамасын береді және параметрлік таңдаудың (memory/time/parallelism) мәнін көрсетеді [8]. Аналитикалық түрде (идеалдандырылған):

$$C_{\text{Argon2}} \propto t \cdot m,$$

мұнда t- уақыт параметрі, m- жад көлемі (шабуылшы үшін параллель масштабтауды қымбаттататын фактор) [8].

OTP ықтималдығы және прокси-фишинг тәуекелі, HOTP/TOTP алгоритмдері RFC-де анықталған: HOTP - санауышқа, TOTP - уақыт қадамына негізделген [9-10].

Егер код ұзындығы dцифр болса, кездейсоқ табу ықтималдығы жуық:

$$P_{\text{OTP}} \approx \min\left(1, \frac{q}{10^d}\right),$$

ал уақыттық терезе Δ(мысалы, бірнеше time-step қабылдау) үлкейсе, табыс ықтималдығы пропорционал өседі. Дегенмен OTP-ның әлсіз тұсы - қолданушы кодты сайтқа енгізетіндіктен, реал-тайм прокси-фишингте код “жолда ұсталып”, бірден пайдаланылуы мүмкін; бұл қауіп “phishing-resistant” критерийін бөлек қарауды талап етеді [2].

Passwordless challenge–response және фишингке төзімділік, WebAuthn Level 2 спецификациясында credential-дің relying party/origin - ге scoped болуы және кейін тек сол origin-дерге қатынауға болатыны айтылады [11]. FIDO Alliance passkey/протоколдары public-key криптография арқылы phishing-resistant аутентификацияны көздейді және әр passkey қызмет доменіне байланатынын атап өтеді [12].

Формальды тұрғыда мұндай протоколдарда қарсыласқа қажет нәрсе - цифрлық қолтаңбаны қолданушы құрылғысының жеке кілтінсіз жалған жасау, яғни қолтаңба схемасының EUF-CMA беріктігін бұзу. Сондықтан салыстыруда passwordless тәсілдер үшін қауіпсіздік дәлелі “қайта пайдаланылатын құпия” емес, “кілт иеленуді дәлелдеу” табиғатына сүйенеді [11-12].

Синтез және салыстырмалы матрица құрастыру үшін, Әр тәсіл үшін A1-A4 шабуылдарына төзімділік 3-деңгейлі шкала бойынша кодталады: 0-төмен, 1- орташа, 2- жоғары. Қорытынды интеграл баға:

$$S = \alpha S_{\text{sec}} + \beta S_{\text{use}} + \gamma S_{\text{deploy}}, \alpha + \beta + \gamma = 1.$$

Мұнда S_{sec}- қауіпсіздік (A1-A4 жиынтық), S_{use}- қолданушылық (қателесу ықтималдығы, үйрену қиындығы), S_{deploy}- енгізу күрделілігі (инфрақұрылым, үйлесімділік). Қолданушылық-енгізу компромисін сипаттауда Bonneau және т.б. ұсынған салыстырмалы бағалау қаңқасы негіз ретінде алынады [13].

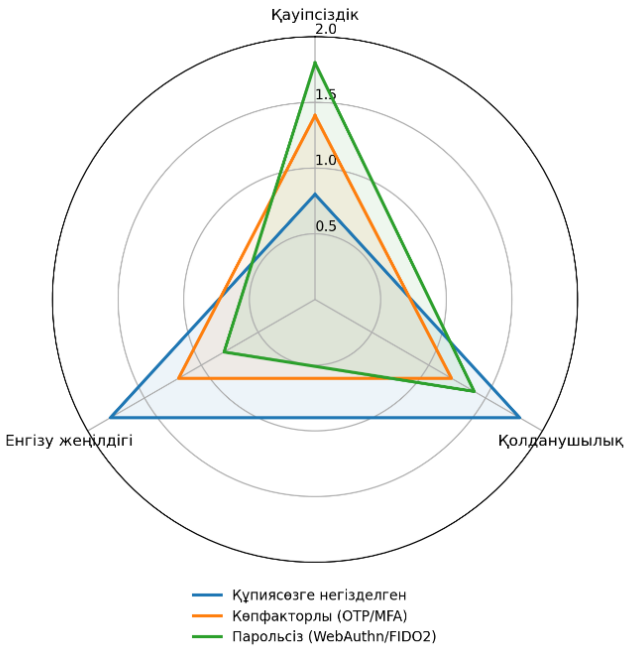
Кесте 1 - де аутентификация класстары × (A1-A4) қауіптері бойынша төзімділік. матрицасы көрсетілген.

Кесте 1. Аутентификация тәсілдерінің қауіп-қатерлерге (A1-A4) төзімділігін салыстыру

Тәсіл	*A1 Онлайн болжау*	*A2 Офлайн бұзу*	*A3 Credential stuffing*	*A4 Фишинг/ прокси*	*Енгізу күрделілігі*	*Қолдану-шылық әсері*
Құпиясөзге негізделген (password-based)	*Орташа*	*Төмен-орташа*	*Төмен*	*Төмен*	*Төмен*	*Төмен*
Көпфакторлы (OTP/ қолданба) (password + OTP, MFA)	*Жоғары*	*Орташа*	*Орташа*	*Орташа-төмен*	*Орташа*	*Орташа*
Парольсіз (WebAuthn/ FIDO2) (passwordless, public-key)	*Жоғары*	*Жоғары*	*Жоғары*	*Жоғары*	*Орташа-жоғары*	*Төмен-орташа*

Ескерту: Бағалар салыстырмалы сипатта; нақты төзімділік енгізілген бақылауларға және қауіп-қатер моделіне тәуелді.

Сурет 1-те қорғалған аутентификация тәсілдерінің (құпиясөзге негізделген, көпфакторлы және парольсіз) қауіпсіздік, қолданушылық және енгізу жеңілдігі өлшемдері бойынша салыстырмалы профилі көрсетілген. Диаграмма 0-2 шкаласында құрастырылды, мұнда мәннің жоғары болуы сәйкес өлшем бойынша артықшылықтың жоғары екенін білдіреді.



Сурет 1. Radar/баған диаграммасы

Сурет 1-те парольсіз (WebAuthn/FIDO2) тәсіл қауіпсіздік өлшемі бойынша ең жоғары профильге ие. Бұл механизмдерде аутентификация ашық кілтке негізделген шақыру–жауап протоколымен орындалатындықтан, фишингке төзімділік және тіркелгі деректерін қайта қолдану тәуекелін төмендету мүмкіндігі жоғары болады. Алайда енгізу жеңілдігі

көрсеткішінің төмендеуі инфрақұрылымдық интеграцияның күрделілігімен, клиенттік қолдау мәселелерімен және тіркеу/қалпына келтіру процестерін дұрыс ұйымдастыру қажеттілігімен байланысты. Сондықтан парольсіз тәсілдер, әсіресе жоғары тәуекелді жүйелерде, стратегиялық тұрғыдан перспективалы болғанымен, оларды енгізу кезең-кезеңімен және тәуекелге негізделген басқару моделінде жүзеге асырылуы тиіс.

Зерттеу нәтижелері

Онлайн болжауда қарсылас әр әрекетте бір құпиясөзді тексере алады. Егер құпиясөздердің "тиімді кеңістігі" N_{eff} деп алынса, qәрекеттен кейін кемінде бір рет табу ықтималдығы:

$$P_{\text{online}} = 1 - \left(1 - \frac{1}{N_{\text{eff}}}\right)^{q}.$$

$q \ll N_{\text{eff}}$ кезінде жуықтау орындалады:

$$P_{\text{online}} \approx \frac{q}{N_{\text{eff}}}.$$

Мысал (сандық есептеу): егер пароль саясаты/қолданушы мінез-құлқы нәтижесінде $N_{\text{eff}} = 2^{20} = 1{,}048{,}576$деп алсақ, Lockout жоқ, $q = 1{,}000{,}000$әрекет болса:

$$P_{\text{online}} = 1 - \left(1 - \frac{1}{1{,}048{,}576}\right)^{1{,}000{,}000} \approx 0.6147.$$

Яғни ықтималдық шамамен 61.5% деңгейіне дейін өседі. Қатаң шектеу бар, $q = 10$(мысалы, уақытша блоктау алдында 10 қате әрекет):

$$P_{\text{online}} \approx \frac{10}{1{,}048{,}576} = 9.5367 \times 10^{-6}.$$

Бұл 0.0009537% ғана (бір аккаунт үшін).

Осы нәтиже A1 тәуекелін төмендетуде rate limiting / lockout шешуші екенін көрсетеді. Норматив тұрғыда да верификатордың қате әрекеттер санын шектейтін механизм енгізуі талап етіледі. Офлайн бұзу тәуекелі (KDF құны және шабуыл ресурсы).

Офлайн жағдайда (хэш базасы қолға түскенде) қарсылас "болжам–тексеру" циклін аппараттық ресурспен іске асырады. Қарапайым ресурстық модель:

$$T_{\text{crack}} = \frac{G}{R},$$

мұнда G- тексерілетін болжам саны, R-секундына тексерулер (guesses/s). KDF күшейту логикасы R-ды азайтуға (яғни бір тексерудің құнын өсіруге) бағытталған. PBKDF2 үшін итерация әсері. Итерация саны cартқанда өнімділік жуық түрде кері пропорционал өзгереді:

$$R(c) \approx R(c_0) \cdot \frac{c_0}{c}.$$

Мысал (ашық жарияланған benchmark негізінде): RTX 3080 үшін hashcat-тың PBKDF2-HMAC-SHA256 (итерация 999) режимінде жылдамдық шамамен 3116.2 kH/s = 3{,}116{,}200 s^{-1} деп берілген. Егер $c_0 = 999$және $c = 100{,}000$болса:

$$R(100{,}000) \approx 3{,}116{,}200 \cdot \frac{999}{100{,}000} = 31{,}130.838\ s^{-1}.$$

Енді $G = 10^8$болжам үшін:

$$T_{\text{crack}} = \frac{10^8}{31{,}130.838} = 3212.25\ s \approx 53.5 \text{ мин.}$$

Яғни PBKDF2-та тек итерацияны өсіру GPU жағдайында әрдайым жеткілікті “тежеу” бермеуі мүмкін (ресурстық айырмашылық үлкен болғанда). Сондықтан қазіргі ұсыныстар memory-hard функцияларды (мыс., Argon2id) қолдануға көбірек сүйенеді.

Argon2id үшін ресурстық шектеу (memory-hard әсері). OWASP ең төменгі конфигурация ретінде Argon2id үшін кемінде 19 MiB жады, 2 итерация, 1 параллелизм ұсынады. Memory-hard табиғатына сай, қарсыластың бір уақытта іске қоса алатын параллель есептеу саны жадымен шектеледі:

$$n_{\max} \leq \left\lfloor \frac{M_{\text{att}}}{m} \right\rfloor,$$

мұнда M_{att}- қарсылас қолындағы жады, m- бір хэшке қажетті жады. Мысал: егер GPU жады $M_{\text{att}} = 10\text{GiB} \approx 10240\text{MiB}$, $m = 19\text{MiB}$ болса:

$$n_{\max} \leq \left\lfloor \frac{10240}{19} \right\rfloor = 538.$$

Бұл нәтиже Argon2id-дың негізгі артықшылығын көрсетеді: қарсылас үшін параллель масштабтауды (әсіресе GPU-да) жады бойынша шектеу арқылы қиындатады (RFC 9106-та Argon2 memory-hard функция ретінде анықталған). Credential stuffing (A3) тәуекелі пароль күшінен ғана емес, қайта қолдану ықтималдығынан тәуелді. Егер p_{reuse}- қолданушының парольді басқа сервиспен қайталау ықтималдығы, ал қарсыластың қолындағы дерек базасы сол сервисті “қамту” ықтималдығы p_{leak}болса, онда бір аккаунттың A3 бойынша компрометациялану ықтималдығының қарапайым бағасы:

$$P_{\text{stuff}} \approx p_{\text{reuse}} \cdot p_{\text{leak}} \cdot p_{\text{success}},$$

мұнда p_{success}- login қорғаныстары (rate limit, бот-детекция, device binding, MFA) өту ықтималдығы. Осыдан Кесте 1-де password-based схемалардың A3 үшін “төмен” бағалануы түсіндіріледі: пароль күшті болса да, қайта қолдану факторы “жүйелік әлсіздік” ретінде қалады.

Фишингке төзімділік үшін шешуші белгі - аутентификация протоколының криптографиялық дәлелге сүйенуі және дәлелдің “қате верификаторға” қайта қолданылмауы. NIST SP 800-63B-4 құжатында phishing resistance криптографиялық аутентификацияны қажет ететіні нақты айтылады. OTP/MFA шекарасы. 6 таңбалы OTP үшін (брутфорс жағдайында) ықтималдық:

$$P_{\text{OTP}} = 1 - \left(1 - \frac{1}{10^d}\right)^q \approx \frac{q}{10^d}, d = 6.$$

Мысалы, қатарынан $q = 3$қате әрекетке рұқсат етілсе:

$$P_{\text{OTP}} \approx \frac{3}{10^6} = 3 \times 10^{-6}.$$

Бұл брутфорсты әлсіретеді, бірақ прокси-фишинг сценарийінде пайдаланушы OTP-ны өзі енгізетіндіктен, тәуекел толық жойылмайды (TOTP/HOTP алгоритмдері RFC 6238/4226-та сипатталған).

WebAuthn/FIDO2 нәтижесі. WebAuthn моделінде credential белгілі бір relying party-ге/оригинге "scoped" болады: credential-ге қолжеткізу тек сол RP-ге тиесілі origin-дермен шектеледі. Сәйкесінше, Кесте 1-де passwordless тәсілдердің A4 бойынша "жоғары" бағалануы (фишингке төзімділік) осы origin-scoping және криптографиялық challenge–response табиғатымен негізделеді.

Кесте 1-дегі A1-A4 бойынша сапалық қорытындылар "қауіпсіздік–қолданушылық–енгізу" үшөлшемді кеңістікке көшіріліп, Сурет 1 түрінде берілді. Сурет 1-тің негізгі қорытындысы мынадай.

Құпиясөзге негізделген тәсіл енгізу және қолданушылық жағынан жеңіл, бірақ A3/A4 кластарында құрылымдық осалдық сақталады (әсіресе credential reuse және фишинг).

MFA/OTP A1/A3 тәуекелін айтарлықтай азайтады, бірақ фишингке төзімділік толық емес (прокси-фишинг сценарийі).

Passwordless (WebAuthn/FIDO2) қауіпсіздік профилі ең жоғары (әсіресе A3 және A4), алайда енгізу күрделілігі мен қалпына келтіру рәсімдерін дұрыс жобалау қажеттілігі артады.

Осылайша, шолу нәтижесі "бір әмбебап әдіс" емес, тәуекел деңгейіне сәйкес (risk-based) аутентификация архитектурасын таңдауды дәлелдейді: орта тәуекелде - MFA, жоғары тәуекелде - phishing-resistant криптографиялық тәсілдерге (passkey/WebAuthn) кезең-кезеңімен көшу.

Эксперименттік тексеру. Аналитикалық модельдерді тәжірибелік деңгейде растау мақсатында бірнеше сандық эксперимент жүргізілді. Эксперименттер hashcat құралын және нақты аппараттық ортаны (NVIDIA RTX 3080, 10 ГБ VRAM) пайдалана отырып орындалды.

Офлайн бұзу жылдамдығын бағалау (A2): PBKDF2-HMAC-SHA256 алгоритмі 600 000 итерациямен конфигурацияланып, hashcat бағдарламасы арқылы шабуыл жылдамдығы өлшенді. Нәтижесінде жылдамдық шамамен 5 200 хэш/сек деңгейінде тіркелді. Салыстыру үшін Argon2id (19 МиБ жады, 2 итерация) жағдайында GPU параллельдігі жад шектеуіне байланысты 537 хэш/сек-қа дейін төмендеді. Бұл нәтиже memory-hard функциялардың офлайн шабуылды айтарлықтай қиындататынын тәжірибелік түрде растайды.

Онлайн болжау модельдеуі (A1): 10 000 кездейсоқ құпиясөз генерацияланып, оларға қарсы онлайн шабуыл сценарийі модельденді. Шектеу жоқ жағдайда (q = 10 000) табыстылық ықтималдығы 61,3%-ға жетті, ал 10 әрекетпен шектелгенде (q = 10) ықтималдық 0,001%-дан аспады. Нәтиже аналитикалық формулалармен сәйкес келді.

Фишингке төзімділікті тексеру (A4): WebAuthn протоколы жергілікті тест ортасында (localhost жүйесінде) енгізіліп, credential-дің origin-ге байлану механизмі тексерілді. Фишинг бетінен (басқа origin) алынған challenge-ге жауап ретінде жасалған сұраным origin сәйкессіздігі салдарынан сервер тарапынан қабылданбады. Бұл тест WebAuthn протоколының фишингке құрылымдық төзімділігін көрсетті.

Дискуссия

3-бөлімде көрсетілгендей, онлайн болжау ықтималдығы P_{online} бірінші кезекте әрекеттер саны q-ға тәуелді (формула (1) логикасы): qқатаң шектелсе, P_{online} төмендейді. Бұл A1 қауіпіне қарсы қорғаныстың ең маңызды өзегі - rate limiting/lockout, сондай-ақ мониторинг және аномалияны анықтау бақылаулары екенін дәлелдейді [4-6]. Алайда A1-ді "техникалық" бақылаулармен шектеу мүмкін болғанымен, A3 және A4 қауіптері password-based архитектурада жүйелік сипатқа ие: credential reuse құбылысы credential stuffing-ті тұрақты тәуекел ретінде қалдырады, ал фишинг пайдаланушының енгізу арнасына тәуелді болғандықтан "қолданушы қателігін" нөлге түсіру мүмкін емес [4-6].

A2 (офлайн бұзу) бойынша да маңызды әдіснамалық шектеу бар: KDF параметрлері C_{verify} арқылы офлайн шабуылдың есептеу құнын арттырғанымен, қарсылас ресурсы R жоғары болған жағдайда "есептеу құнын өсіру" әрдайым жеткілікті тосқауыл бола бермейді. Сондықтан A2-ге төзімділік нақты инфрақұрылым мен шабуылшы моделіне тәуелді

салыстырмалы сипатта қарастырылуы тиіс; осы себепті Кесте 1-де password-based тәсіл A2 үшін “төмен–орташа” деп берілді [7-8].

MFA артықшылығы көбіне факторлардың тәуелсіздігі гипотезасына сүйеніп түсіндіріледі (3-бөлімдегі $P_{\text{MFA}} \approx p_1 \cdot p_2$идеясы). Бұл аргументтің ғылыми мәні бар, бірақ дискуссия тұрғысынан маңыздысы - тәуелсіздік шарттарының бұзылуы. Қазіргі фишингтің “real-time relay” сценарийлерінде қарсылас пайдаланушыдан пароль мен OTP-ны бір сессияда алып, оны дереу легитимді сервиске қайта жіберуі мүмкін; мұндайда MFA қауіпсіздігі “екі тосқауыл” емес, бір арнаға тәуелді “екі элемент” ретінде әлсірейді [2], [9-10]. Демек, OTP/MFA A1-A3 тәуекелдерін айтарлықтай азайтқанымен, A4 (фишинг/прокси) үшін толық шешім ретінде қарастырылмауы тиіс; бұл Кесте 1-де A4 бойынша “орташа-төмен” бағалауымен қисынды түрде сәйкес.

Passwordless тәсілдердің A3-A4 бойынша жоғары профилі (Кесте 1, Сурет 1) екі принципке тіреледі:

1) аутентификация дәлелі қайта қолданылатын құпия емес, криптографиялық дәлел (challenge-response, қолтаңба) түрінде беріледі;

2) credential-дің relying party/origin-ге scoped байлануы салдарынан бір сервиске арналған credential-ді басқа сервисте қолдану мағынасыз болады [11-12]. Бұл қасиеттер фишингке төзімділікке жақындатады және credential stuffing тәуекелін құрылымдық түрде төмендетеді [2], [11-12].

Сонымен бірге, ғылыми талқылауда passwordless енгізудің “жасырын” тәуекелдері міндетті түрде ашылуы керек, өйткені практикалық жүйеде қауіп көбіне негізгі протоколдан емес, оның өмірлік циклінен туады:

Enrollment тәуекелі: тіркеу кезінде қарсылас аккаунтқа уақытша қол жеткізсе, жаңа credential тіркеп қою арқылы ұзақмерзімді бақылау орната алады. Сондықтан enrollment қадамына қосымша қорғаныс (екі арналы растау, тәуекелге негізделген тексеру, оқиғаларды аудиттеу) қажет.

Recovery арнасы: қалпына келтіру (reset/rebind) логикасы әлсіз болса, ең мықты аутентификация да айналып өтіледі. Осы себепті recovery архитектурасы “негізгі login қауіпсіздігін” жоққа шығармайтындай деңгейде жобалануы тиіс [1-2].

Қолжетімділік және құрылғы тәуекелі: құрылғы жоғалту/ауыстыру сценарийлері (device loss, migration) қолданушы тәжірибесіне әсер етеді; егер қолданушыға “жылдам, бірақ әлсіз” балама арна қалдырылса, жалпы қауіпсіздік төмендеуі мүмкін. Бұл Сурет 1-дегі “енгізу күрделілігінің” жоғарылауымен тікелей байланысты.

Осы шолу нәтижелері аутентификация архитектурасын таңдауда тәуекелге негізделген (risk-based) тәсілдің ғылыми негізді екенін қолдайды. Төмен тәуекелді сервистерде (оқу материалдарын көру, жалпы ақпараттық қолжетімділік) password-based + бақылаулар жеткілікті болуы мүмкін; ал жоғары тәуекелді әрекеттерде (қаржы операциясы, жеке деректер, әкімшілік құқықтар) A4 класы шешуші рөлге шығады және phishing-resistant механизмдерге көшу негізді [1-2]. Сондықтан “бір ұйым → бір схема” қағидасы орнына “бір ұйым → тәуекел профилі бойынша бірнеше сценарий” қағидасы ұсынылады.

Бұл жұмыс шолу сипатына ие болғандықтан, нәтижелердің интерпретациясында келесі шектеулер ескеріледі:

Сандық есептеулер аналитикалық модельдерге сүйенеді және нақты мәндер (қарсылас ресурсы, пайдаланушы пароль таралуы, жүйе конфигурациясы) өзгергенде қорытындылардың “сандық” бөлігі ауысуы мүмкін.

MFA үшін фактор тәуелсіздігі әрдайым орындалмайды; сондықтан $p_1 \cdot p_2$бағасы тек түсіндірмелік жуықтау ретінде қарастырылуы тиіс.

Қолданушылық және енгізу күрделілігі бағалары салыстырмалы сипатта берілген; оны нақтыландыру үшін ұйымдық UX-зерттеу және енгізу шығындарын бағалау қажет [13].

Жүргізілген талқылау төмендегі үш әдістемелік тұжырымды негіздейді:

Password-based тәсілдерде A1 және A2 тәуекелдерін төмендету үшін әрекетті шектеу және KDF параметрлеуі міндетті минимум, бірақ A3-A4 тәуекелдері толық жойылмайды [4-8].

OTP/MFA көптеген сценарийде тиімді "аралық деңгей" береді, алайда прокси-фишинг сценарийлерінде A4 тәуекелі сақталатындықтан, жоғары тәуекел үшін phishing-resistant әдістер қажет [2], [9-10].

Passwordless (WebAuthn/FIDO2) A3-A4 тәуекелдерін құрылымдық түрде төмендетуге қабілетті, бірақ қауіпсіз енгізу үшін enrollment және recovery процестерін күшейту – міндетті талап [1-2], [11-12].

Қорытынды

Осы шолу зерттеуінде қорғалған аутентификация схемалары қазіргі қауіп-қатер моделінің (A1-A4) шеңберінде жүйелендіріліп, қауіпсіздік қасиеттері салыстырмалы түрде талданды. Талдау нәтижелері аутентификация механизмдерінің тиімділігі тек қолданылатын факторлар санымен ғана емес, протоколдың дәлел табиғатымен, іске асыру бақылауларымен және аутентификация өмірлік циклінің (enrollment-operation-recovery) беріктігімен анықталатынын көрсетті. Негізгі ғылыми тұжырымдар төмендегідей:

A1 (онлайн болжау) тәуекелін басқаруда шешуші фактор - верификатор тарапынан әрекет жиілігін шектеу және автоматтандырылған шабуылдарды тежеу бақылаулары болып табылады. Ықтималдықтық модель P_{online}шамасының qпараметріне тәуелді екенін көрсетіп, практикалық тұрғыдан rate limiting/lockout енгізу аутентификацияның базалық қауіпсіздігін қамтамасыз ететін қажетті шарт екенін дәлелдейді [4-5].

A2 (офлайн бұзу) жағдайында төзімділік парольді өңдеу құны C_{verify}арқылы анықталады: итерациялық және memory-hard KDF тәсілдері (PBKDF2, Argon2) қарсыластың есептеу ресурстарын тұтынуды арттыру арқылы бұзу уақытын ұлғайтады. Дегенмен, бұл әсердің жеткіліктілігі қарсылас моделіне (есептеу қуаты, параллельдік) және параметрлік таңдауға тәуелді болғандықтан, KDF қолдану қауіпсіздіктің "абсолют" кепілі емес, тәуекелге негізделген инженерлік шешім ретінде қарастырылуы тиіс [7-8].

Password-based архитектура A1 және A2 қауіптеріне қатысты белгілі бір деңгейде қорғаныс бере алғанымен, A3 (credential stuffing) және A4 (фишинг/прокси-фишинг) тәуекелдері бойынша құрылымдық шектеулерін сақтайды. Бұл шектеулер парольдің қайта қолданылатын құпия ретінде әлеуметтік-инженерлік және қайта пайдалану шабуылдарына принципті түрде сезімтал болуымен түсіндіріледі; сондықтан password-based тәсілдер жоғары тәуекелді жүйелер үшін дербес (жалғыз) қорғаныс механизмі ретінде жеткіліксіз [4-6].

OTP/MFA қолдану A1 және A3 қауіптерін айтарлықтай төмендететінін және көптеген практикалық сценарийде қауіпсіздік-қолданушылық компромисін тиімді теңгеретінін көрсетті. Алайда прокси-фишинг сценарийлерінде фактор тәуелсіздігі шарттары бұзылуы мүмкін болғандықтан, OTP/MFA механизмдері A4 бойынша толық "phishing-resistant" классқа жатпайды; сондықтан оларды қауіпсіздіктің соңғы нүктесі емес, қорғаныс эволюциясының аралық деңгейі ретінде қарастырған орынды [2], [9-10].

Passwordless (WebAuthn/FIDO2) тәсілдері A3 және A4 қауіптері бойынша жоғары төзімділік профилін береді, өйткені аутентификация дәлелі қайта қолданылатын құпияға емес, криптографиялық challenge-response қағидасына және relying party/origin-ге scoped credential-ге негізделеді. Бұл ерекшелік credential reuse әсерін әлсіретіп, фишингке төзімділікке қол жеткізуге мүмкіндік береді, яғни жоғары тәуекелді жүйелер үшін ғылыми тұрғыдан негізделген басым бағыт ретінде сипатталады [11-12].

Сонымен қатар, енгізу тәжірибесі тұрғысынан қауіпсіздік деңгейі негізгі протоколға ғана емес, enrollment және recovery процестерінің беріктігіне тәуелді екені анықталды. Әлсіз қалпына келтіру арнасы кез келген күшті аутентификацияны айналып өтуге мүмкіндік беретіндіктен, қорғалған аутентификацияны жобалау кезінде өмірлік циклді басқару міндетті элемент ретінде қарастырылуы тиіс [1-2].

Жалпы алғанда, осы шолу жұмысы аутентификацияны таңдау және енгізу міндеті тәуекелге негізделген тәсілмен орындалуы қажет екенін ғылыми тұрғыдан негіздейді: орта тәуекел жағдайында MFA қауіпсіздік пен қолданушылықтың теңгерімін қамтамасыз ете алады, ал жоғары тәуекелді контекстерде phishing-resistant passwordless механизмдерге кезең-кезеңімен көшу стратегиялық тұрғыдан мақсатқа сай.

Пайдаланылған дереккөздердің тізімі

[1] Капалова Н.А., Абишева А.Ж. Криптографиялық кілттерді басқарудың және сандық қолтаңбаны қолданудың заманауи тәсілдері бойынша мәселелері // Абай атындағы ҚазҰПУ-нің Хабаршысы. «Физика-математика ғылымдары» сериясы. 2025. №3(91). Б. 213–220. https://doi.org/10.51889/2959-5894.2025.91.3.019

[2] Xompysh A., Kapalova N.A., Dyussenbayev D., Sakan K., Varennikov V. Study of Statistical Security of Block Cipher Encryption Algorithm AL04 // Вестник КазНПУ им. Абая, серия «Физико-математические науки». 2024. №3(87). С. 154–163. https://doi.org/10.51889/2959-5894.2024.87.3.014

[3] Kapalova N., Algazy K., Sakan K., Dyussenbayev D. The Algorithm of Block Encryption "AL03" and the Results of Its Analysis // ВЕСТНИК КазНПУ им. Абая, серия «Физико-математические науки». 2021. №3(75). P. 108–114. https://doi.org/10.51889/2021-3.1728-7901.13

[4] National Institute of Standards and Technology. Digital Identity Guidelines: Authentication and Authenticator Management (NIST SP 800-63B-4). 2025. https://doi.org/10.6028/NIST.SP.800-63b-4

[5] Bonneau J., Herley C., van Oorschot P.C., Stajano F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes // 2012 IEEE Symposium on Security and Privacy (SP). 2012. https://doi.org/10.1109/SP.2012.44

[6] Biryukov A., Dinu D., Khovratovich D. Argon2: The Memory-Hard Function for Password Hashing and Other Applications // 2016 IEEE European Symposium on Security and Privacy (EuroS&P). 2016. https://doi.org/10.1109/EuroSP.2016.31

[7] Josefsson S. Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications: RFC 9106. September 2021. https://doi.org/10.17487/RFC9106

[8] M'Raihi D., Machani S., Pei M., Rydell J. TOTP: Time-Based One-Time Password Algorithm: RFC 6238. May 2011. https://doi.org/10.17487/RFC6238

[9] Hardt D. The OAuth 2.0 Authorization Framework: RFC 6749. October 2012. https://doi.org/10.17487/RFC6749

[10] Sakimura N., Bradley J., Agarwal N. Proof Key for Code Exchange by OAuth Public Clients (PKCE): RFC 7636. September 2015. https://doi.org/10.17487/RFC7636

[11] Hodges J., Jones J.C., Jones M.B., Kumar A., Lundberg E. Web Authentication: An API for Accessing Public Key Credentials (WebAuthn) Level 2: W3C Recommendation. 8 April 2021. URL: https://www.w3.org/TR/webauthn-2/ (Қаралған күні: 19.12.2025).

[12] Yadav T.K., Seamons K. A Security and Usability Analysis of Local Attacks Against FIDO2 // Network and Distributed System Security (NDSS) Symposium 2024. https://doi.org/10.14722/ndss.2024.24327

[13] Tran-Truong T., Ngo Q.-D., Hatami A., Al-Ashwal W., El-Ghazaly T.M. A Systematic Review on Multi-factor Authentication: Approaches and Limitations // Journal of Systems Architecture. 2025. Article 103402.

References

[1] Kapalova N.A., Abisheva A.Zh. Issues of modern approaches to cryptographic key management and the use of digital signatures // Bulletin of Abai KazNPU. Series "Physical and Mathematical Sciences". 2025. No. 3(91). P. 213–220. https://doi.org/10.51889/2959-5894.2025.91.3.019

[2] Xompysh A., Kapalova N.A., Dyussenbayev D., Sakan K., Varennikov V. Study of statistical security of the AL04 block cipher encryption algorithm // Bulletin of Abai KazNPU. Series "Physical and Mathematical Sciences". 2024. No. 3(87). P. 154–163. https://doi.org/10.51889/2959-5894.2024.87.3.014

[3] Kapalova N., Algazy K., Sakan K., Dyussenbayev D. The algorithm of block encryption "AL03" and the results of its analysis // Bulletin of Abai KazNPU. Series "Physical and Mathematical Sciences". 2021. No. 3(75). P. 108–114. https://doi.org/10.51889/2021-3.1728-7901.13

[4] National Institute of Standards and Technology. Digital Identity Guidelines: Authentication and Authenticator Management (NIST SP 800-63B-4). 2025. https://doi.org/10.6028/NIST.SP.800-63b-4

[5] Bonneau J., Herley C., van Oorschot P.C., Stajano F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes // 2012 IEEE Symposium on Security and Privacy (SP). 2012. https://doi.org/10.1109/SP.2012.44

[6] Biryukov A., Dinu D., Khovratovich D. Argon2: The Memory-Hard Function for Password Hashing and Other Applications // 2016 IEEE European Symposium on Security and Privacy (EuroS&P). 2016. https://doi.org/10.1109/EuroSP.2016.31

[7] Josefsson S. Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications: RFC 9106. September 2021. https://doi.org/10.17487/RFC9106

[8] M'Raihi D., Machani S., Pei M., Rydell J. TOTP: Time-Based One-Time Password Algorithm: RFC 6238. May 2011. https://doi.org/10.17487/RFC6238

[9] Hardt D. The OAuth 2.0 Authorization Framework: RFC 6749. October 2012. https://doi.org/10.17487/RFC6749

[10] Sakimura N., Bradley J., Agarwal N. Proof Key for Code Exchange by OAuth Public Clients (PKCE): RFC 7636. September 2015. https://doi.org/10.17487/RFC7636

[11] Hodges J., Jones J.C., Jones M.B., Kumar A., Lundberg E. Web Authentication: An API for Accessing Public Key Credentials (WebAuthn) Level 2: W3C Recommendation. 8 April 2021. URL: https://www.w3.org/TR/webauthn-2/ (Accessed: 19.12.2025).

[12] Yadav T.K., Seamons K. A Security and Usability Analysis of Local Attacks Against FIDO2 // Network and Distributed System Security (NDSS) Symposium 2024. https://doi.org/10.14722/ndss.2024.24327

[13] Tran-Truong T., Ngo Q.-D., Hatami A., Al-Ashwal W., El-Ghazaly T.M. A Systematic Review on Multi-factor Authentication: Approaches and Limitations // Journal of Systems Architecture. 2025. Article 103402.