№ 4(58) 2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online
УДК 004.056.5:004.738
https://doi.org/10.52058/2786-6025-2026-4(58)-4335-4348

Рзаєва Світлана Леонідівна кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук, Київський столичний університет імені Бориса Грінченка, м. Київ, https://orcid.org/0000-0002-7589-2045

Костюк Юлія Володимирівна доктор філософії (PhD), доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, Київський столичний університет імені Бориса Грінченка, м. Київ, https://orcid.org/0000-0001-5423-0985

Рзаєв Дмитро Олександрович старший викладач кафедри інформатики та системології, Київський національний економічний університет імені Вадима Гетьмана, м. Київ, https://orcid.org/0000-0002-7149-4971

МЕТОД БАГАТОРІВНЕВОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Анотація. У статті розглянуто метод багаторівневої автентифікації користувачів в інформаційно-комунікаційних системах, орієнтований на підвищення рівня інформаційної безпеки в умовах зростання кіберзагроз та цифровізації суспільства. Проаналізовано сучасний стан і основні підходи до автентифікації, зокрема багатофакторні, безпарольні та адаптивні механізми, а також визначено їхні переваги, обмеження та вразливості. Обґрунтовано доцільність використання багаторівневої моделі автентифікації, яка поєднує кілька незалежних факторів перевірки користувача, включаючи фактор знання, фактор володіння та біометричні характеристики, із врахуванням контекстних параметрів доступу, таких як місцезнаходження, тип пристрою, час доступу та поведінкові особливості. Запропонований метод базується на інтеграції механізмів перевірки факторів, аналізу контексту та оцінювання ризику, що дозволяє формувати інтегральний показник довіри до користувача. Особливістю підходу є використання динамічного порогового значення прийняття рішення, яке змінюється залежно від рівня ризику та умов доступу, забезпечуючи адаптивність процесу автентифікації. Розроблено архітектуру багаторівневої системи автентифікації, що включає модулі перевірки факторів, контекстного аналізу, оцінювання ризику та прийняття рішення, а також формалізовано алгоритм її функціонування з можливістю дострокового завершення у випадку виявлення критичних відхилень або ініціювання додаткових перевірок.

ISSN 2786-6025 Online

Проведено оцінювання ефективності запропонованого методу за показниками швидкодії, надійності та стійкості до атак. Отримані результати підтверджують зниження ймовірності несанкціонованого доступу та підвищення точності автентифікації порівняно з традиційними підходами.

Запропонований метод забезпечує раціональний баланс між рівнем захисту та зручністю користування системою, що визначає його практичну цінність і доцільність впровадження в сучасних інформаційно-комунікаційних системах із підвищеними вимогами до безпеки.

Ключові слова: багаторівнева автентифікація, інформаційна безпека, інформаційно-комунікаційні системи, контекстний аналіз, оцінка ризику, контроль доступу, адаптивна автентифікація, багатофакторна автентифікація, кібербезпека.

Rzaeva Svitlana Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Science, Borys Grinchenko Kyiv Metropolitan University, Kyiv, https://orcid.org/0000-0002-7589-2045

Kostiuk Yuliia PhD in Computer Science Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok, Borys Grinchenko Kyiv Metropolitan University, Kyiv, https//orcid.org/0000-0001-5423-0985

Rzaev Dmytro Senior Lecturer of the Department of Informatics and Systemology Vadym Hetman Kyiv National University of Economics, Kyiv, , https://orcid.org/0000-0002-7149-4971

MULTI-LEVEL USER AUTHENTICATION METHOD IN INFORMATION AND COMMUNICATION SYSTEMS

Abstract. The article presents a multi-level user authentication method for information and communication systems aimed at enhancing information security in the context of increasing cyber threats and ongoing digital transformation. The current state of authentication approaches is analyzed, including multi-factor, passwordless, and adaptive authentication mechanisms, with identification of their advantages, limitations, and vulnerabilities. The feasibility of applying a multi-level authentication model is substantiated, combining several independent authentication factors such as knowledge-based, possession-based, and biometric factors, along with contextual access parameters including location, device type, time of access, and behavioral characteristics. The proposed method is based on the integration of authentication factor verification, context analysis, and risk assessment, enabling the

ISSN 2786-6025 Online
formation of an integral trust score for the user. A key feature of the approach is the use of a dynamic decision threshold that adapts depending on the risk level and access conditions, ensuring flexibility and adaptability of the authentication process. The architecture of the multi-level authentication system is developed, including modules for factor verification, context analysis, risk evaluation, and decision-making, and the operational algorithm is formalized with support for early termination in case of critical deviations or initiation of additional verification procedures.

An evaluation of the proposed method is conducted using performance, reliability and attack. The results demonstrate a reduction in the probability of unauthorized access and improved authentication accuracy compared to traditional approaches. The proposed method provides a balanced trade-off between security and usability, which determines its practical applicability and effectiveness in modern information and communication systems with enhanced security requirements.

Keywords: multi-level authentication, information security, information and communication systems, contextual analysis, risk assessment, access control, adaptive authentication, multi-factor authentication, cybersecurity.

Постановка проблеми. Сучасні інформаційно-комунікаційні системи (ІКС) функціонують в умовах постійного зростання кількості та складності кіберзагроз, що спрямовані насамперед на механізми автентифікації користувачів як первинний бар'єр доступу до ресурсів. Аналіз традиційних підходів показує, що однофакторна та навіть двофакторна автентифікація вже не забезпечують достатнього рівня захисту через вразливість до фішингових атак, компрометації облікових даних, атак повторного відтворення та використання соціальної інженерії. Особливо критичною є ситуація в системах із підвищеними вимогами до безпеки, де несанкціонований доступ може призвести до втрати або викривлення конфіденційної інформації. Додатковою проблемою є те, що більшість існуючих механізмів автентифікації є статичними та не враховують контекстні умови доступу користувача, такі як геолокація, тип пристрою, часові характеристики та поведінкові патерни. Це призводить до недостатньої адаптивності систем захисту та високого рівня як хибнопозитивних, так і хибнонегативних рішень. Водночас, підвищення рівня безпеки шляхом ускладнення процедур автентифікації часто негативно впливає на зручність користування системою, що створює необхідність пошуку балансу між безпекою та ергономічністю.

Таким чином, актуальною науково-практичною задачею є розроблення методу багаторівневої автентифікації користувачів, який би поєднував використання кількох незалежних факторів перевірки, інтегральну оцінку довіри та адаптивне врахування контексту доступу. Такий підхід повинен забезпечувати підвищення стійкості до сучасних кіберзагроз без суттєвого

ISSN 2786-6025 Online

погіршення швидкодії та зручності роботи користувачів у інформаційно-комунікаційних системах.

Аналіз останніх досліджень і публікацій. Сучасні дослідження у сфері багатофакторної автентифікації демонструють перехід від класичних статичних підходів до адаптивних і контекстно-залежних моделей захисту. У науковому дослідженні [1] розглядається розвиток безпарольних та адаптивних механізмів автентифікації, зокрема інтеграція підходів risk-based authentication і стандарту FIDO2, що дозволяє підвищити рівень безпеки завдяки усуненню залежності від традиційних паролів. Автори статті підкреслюють, що використання криптографічних методів автентифікації значно знижує ризик компрометації облікових даних. У статті [2] здійснено комплексний аналіз сучасних багатофакторних систем автентифікації, в якій наголошується на необхідності поєднання кількох незалежних факторів (знання, володіння, біометрія) для підвищення стійкості до атак. Сучасні MFA-рішення мають забезпечувати баланс між високим рівнем безпеки та зручністю для користувачів, що передбачає оптимізацію процесів автентифікації та зниження їхньої складності без погіршення захисних властивостей системи. Автори в роботі [3] систематизують основні підходи до багатофакторної автентифікації, аналізуючи вимоги до таких систем, типові атаки та проблеми їх практичної реалізації.

У дослідженні зазначається, що до найбільш поширених загроз належать фішингові атаки, атаки повторного відтворення та методи соціальної інженерії, що зумовлює необхідність переходу до динамічніших моделей автентифікації, які враховують контекстні умови виконання автентифікації.

Окремий напрям досліджень представлено в роботі [5], де запропоновано адаптивну модель ризик-орієнтованої автентифікації та авторизації (RAD-AA). Автори акцентують увагу на використанні контекстних параметрів та динамічній оцінки ризику при прийнятті рішень щодо доступу до інформації, тим самим підвищуючи рівень безпеки системи без істотного зниження її швидкодії.

Узагальнюючи результати наведених досліджень, можна зробити висновок, що сучасні підходи до автентифікації поступово еволюціонують у бік адаптивних, контекстно-орієнтованих та ризик-орієнтованих моделей, що, в свою чергу, створює підґрунтя для подальшого розвитку багаторівневих методів автентифікації, які поєднують різні механізми перевірки користувача в єдину інтегровану систему захисту.

Мета статті – розроблення методу багаторівневої автентифікації користувачів в інформаційно-комунікаційних системах, що підвищує рівень інформаційної безпеки завдяки поєднання незалежних факторів перевірки, контекстного аналізу та адаптивного прийняття рішення про доступ.

ISSN 2786-6025 Online

Методи дослідження. Теоретичну основу дослідження становлять методи системного аналізу, які дозволили дослідити структуру інформаційно-комунікаційних систем як цілісного об'єкта з урахуванням взаємодії підсистем автентифікації, контролю доступу та обробки контекстної інформації. Для побудови архітектури методу та опису його логічної структури застосовано методи моделювання складних систем, зокрема структурне та UML-моделювання. При розробці алгоритму багаторівневої автентифікації використано методи алгоритмізації та формалізації процесів прийняття рішень, що забезпечило опис послідовності перевірок та умов переходу між рівнями автентифікації. Для оцінювання ефективності запропонованого підходу застосовано методи порівняльного аналізу, які передбачають зіставлення показників (швидкодія, FAR, FRR, EER, стійкість до атак) із традиційними методами автентифікації.

Також використано методи теорії ймовірностей та ризик-аналізу для формування інтегральної оцінки довіри до користувача та моделювання ймовірності несанкціонованого доступу, що дозволило обґрунтувати доцільність використання динамічного порогового механізму прийняття рішень у багаторівневих системах автентифікації.

Виклад основного матеріалу. Автентифікація користувачів є одним з етапів захисту інформаційно-комунікаційних систем, оскільки саме на цьому етапі система визначає, чи відповідає користувач заявленій ідентичності. Спочатку відбувається ідентифікація – введення логіна або іншого унікального ідентифікатора. Далі здійснюється автентифікація, тобто перевірка особи користувача, після чого визначається рівень доступу (авторизація). Наявність вразливостей на етапі автентифікації може призвести до несанкціонованого доступу, тому її надійність є критично важливою. Існує кілька підходів до автентифікації залежно від кількості факторів перевірки. Найпростішим є однофакторний підхід (наприклад, пароль), який є зручним, але недостатньо безпечним. Більш надійним є двофакторний підхід, що передбачає додаткове підтвердження, зокрема за допомогою одноразового коду. Найвищий рівень захисту забезпечує багатофакторна автентифікація, яка поєднує кілька незалежних факторів: фактор знання, фактор володіння та біометричні характеристики.

Сучасні інформаційно-комунікаційні системи залишаються вразливими до широкого спектра кіберзагроз. До найпоширеніших належать атаки підбору паролів (brute force), фішингові атаки та атаки повторного відтворення (replay attack). Окрему небезпеку становлять загрози, пов'язані з компрометацією облікових даних унаслідок витоків, використання слабких паролів або шкідливого програмного забезпечення. У таких умовах навіть двофакторна автентифікація може бути недостатньо ефективною. З огляду на це виникає

ISSN 2786-6025 Online

необхідність застосування більш надійних підходів, зокрема багаторівневої автентифікації, яка поєднує кілька незалежних механізмів перевірки та враховує умови доступу, такі як місцезнаходження користувача, тип пристрою, час входу та поведінкові характеристики. Такий підхід дозволяє підвищити рівень захисту системи та зменшити ризик несанкціонованого доступу.

З урахуванням наведених загроз застосування одно- та двофакторної автентифікації є недостатнім для критичних систем, що обумовлює доцільність впровадження багаторівневих методів. У загальному вигляді така архітектура розглядається як ієрархія рівнів перевірки, де кожен рівень формує часткову оцінку достовірності користувача.

Архітектура багаторівневої автентифікації передбачає послідовне або частково паралельне проходження кількох рівнів перевірки, кожен із яких відповідає окремому фактору. Зазвичай виділяють базовий рівень (логін/пароль), додатковий рівень (одноразовий код або токен) та розширений рівень (біометрія або поведінковий аналіз), кожен з яких формує часткове рішення щодо автентичності користувача. Формально процес можна описати як послідовність функцій перевірки:

$$A_i(u) \in [0, 1],\ i = 1, 2, \ldots, n, \tag{1}$$

де $A_i(u)$ – оцінка проходження *u-м* користувачем і-го рівня автентифікації (0 – відмова, 1 – повне підтвердження).

Інтегральна оцінка автентичності формується як агрегована функція:

$$A(u) = \prod_{i=1}^{n} A_i(u), \tag{2}$$

У випадку жорсткої політики (Strict Authentication) доступ надається лише тоді, коли всі рівні пройдено успішно ($A(u) = 1$), тоді як у гнучких системах допускається часткова компенсація між рівнями.

Ефективність багаторівневої автентифікації значною мірою визначається тим, наскільки коректно поєднані різні методи перевірки користувача. Ключовою вимогою є незалежність факторів автентифікації: знання (наприклад, пароль), володіння (пристрій або токен) та притаманність (біометричні характеристики) повинні функціонувати автономно та не залежати один від одного.

Тобто, компрометація одного фактору не повинна автоматично призводити до компрометації інших, що суттєво підвищує загальний рівень безпеки системи. Комбінована модель може бути представлена як зважена сума:

ISSN 2786-6025 Online

$$S(u)=\sum_{i=1}^{n} w_i \cdot A_i(u), \quad \sum_{i=1}^{n} w_i = 1, \tag{3}$$

де w_i – ваги факторів, що відображають їхню надійність. Наприклад, біометрія може мати більшу вагу, ніж пароль. Такий підхід дозволяє підвищити гнучкість системи: навіть якщо один фактор має нижчу достовірність, інші можуть компенсувати цей ризик.

Політика доступу визначає правила, за якими приймається рішення про надання доступу. У традиційних системах використовується фіксований поріг автентифікації, проте в сучасних умовах доцільно застосовувати адаптивні механізми, які враховують рівень ризику. Рішення про доступ можна подати як:

$$Access(u) = \begin{cases} 1, & A(u) \geq \theta(R) \\ 0, & A(u) < \theta(R)' \end{cases} \tag{4}$$

де $\theta(R)$ – порогове значення, що залежить від оцінки ризику R. Таким чином, при зростанні ризику (наприклад, незвична локація або пристрій) значення порогу θ підвищується, що вимагає від користувача проходження більшої кількості або більш надійних рівнів автентифікації. У випадку низького ризику поріг знижується, що дозволяє спростити процедуру входу без втрати безпеки.

Контекстні фактори дозволяють оцінити умови здійснення доступу, що значно підвищує точність виявлення аномалій. До них належать геолокація, характеристики пристрою, часові параметри та поведінкові патерни користувача. Інтегральну оцінку ризику доцільно визначати як нормалізовану міру відхилення поточних параметрів від типових значень:

$$R(u) = \sum_{j=1}^{m} \beta_j \cdot \frac{|x_j - \mu_j|}{\sigma_j}, \tag{5}$$

де x_j – поточне значення j-го контекстного параметра, μ_j – середнє (нормальне) значення для користувача, σ_j – стандартне відхилення, β_j – ваговий коефіцієнт важливості параметра; m – кількість контекстних факторів. Така модель дозволяє оцінити ступінь відхилення поведінки користувача від його типового профілю. Зі збільшенням значення $R(u)$ система автоматично підвищує рівень вимог до автентифікації, забезпечуючи баланс між безпекою та зручністю використання.

Враховуючи зростання кількості та складності кіберзагроз виникає необхідність переходу від окремих механізмів автентифікації до цілісного

ISSN 2786-6025 Online

методу, який забезпечує комплексну перевірку користувача. Метод багаторівневої автентифікації ґрунтується на інтеграції кількох незалежних факторів перевірки з урахуванням контексту доступу та подальшою узагальненою оцінкою достовірності користувача. Застосування даного методу полягає не лише у використанні декількох факторів автентифікації, а у побудові узгодженої логічної структури, де кожен етап перевірки формує частковий внесок у загальне рішення. Такий підхід дозволяє підвищити стійкість системи до компрометації окремих факторів та забезпечити гнучке реагування на зміну умов доступу. Логічно метод складається з чотирьох основних компонентів: модуля збору облікових та контекстних даних, модуля багаторівневої перевірки, модуля оцінки ризику та довіри, а також модуля прийняття рішення.

Структуру методу подано за допомогою UML-моделювання (рис. 1), що відображає взаємодію основних елементів системи.

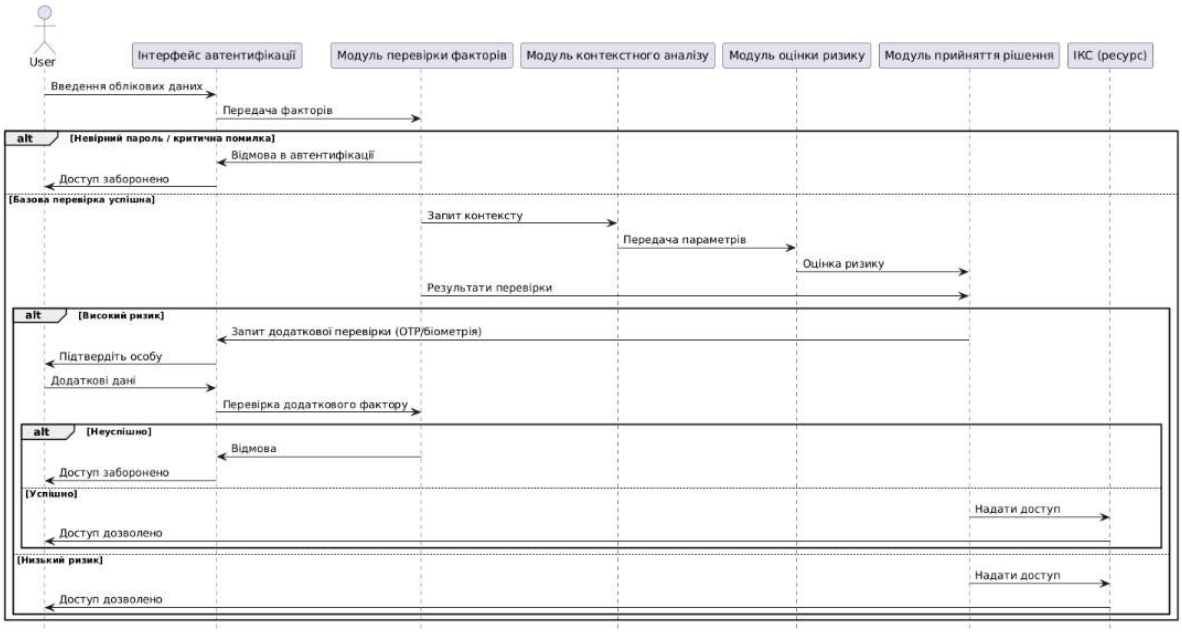

Рис. 1. *Структура методу багаторівневої автентифікації*
Джерело: побудовано авторами

Алгоритм перевірки користувача передбачає поетапну обробку як облікових, так і контекстних даних. На першому етапі здійснюється первинна ідентифікація за логіном або унікальним ідентифікатором, після чого виконується перевірка пароля або PIN-коду (фактор знання). У разі успішного проходження активується наступний рівень – перевірка фактора володіння (одноразовий код, push-підтвердження або апаратний токен), а також може додатково виконуватися біометрична перевірка. Паралельно система збирає контекстні параметри (IP-адреса, геолокація, тип пристрою, час входу,

ISSN 2786-6025 Online

поведінкові характеристики). Кожен етап формує часткову оцінку достовірності, яка передається до модуля прийняття рішення. У разі виявлення критичних відхилень (наприклад, некоректні облікові дані або підозрілий пристрій) алгоритм може бути достроково завершений із відмовою у доступі або переходом до додаткових перевірок. Механізм прийняття рішення базується на агрегуванні результатів усіх рівнів автентифікації та формуванні інтегральної оцінки довіри, яка порівнюється з пороговим значенням, визначеним політикою безпеки.

Інтеграція запропонованого методу з існуючими інформаційно-комунікаційними системами здійснюється шляхом його впровадження як окремого сервісного модуля або додаткового рівня безпеки. Такий підхід може бути реалізований через API, middleware або механізми єдиного входу (SSO). Метод не потребує повної перебудови існуючої інфраструктури, оскільки взаємодіє з нею через стандартні інтерфейси автентифікації. При цьому забезпечується сумісність із наявними базами користувачів, системами управління доступом (IAM) та журналами подій безпеки, що дозволяє ефективно впроваджувати його в існуюче інформаційне середовище.

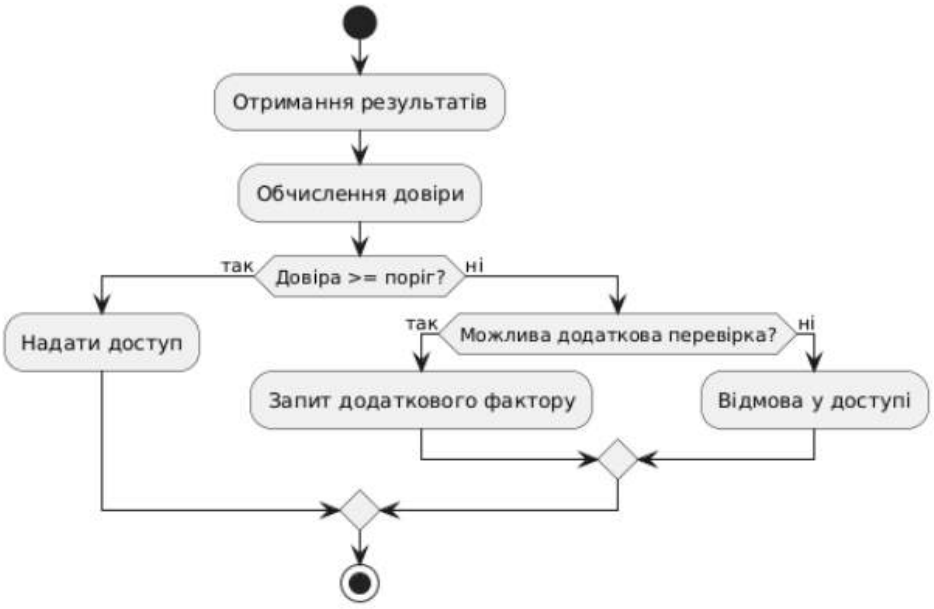

Рис. 2. *Алгоритм механізму прийняття рішення про доступ*
Джерело: побудовано авторами

В результаті виконання алгоритму отримані дані потребують узагальнення та інтерпретації, що реалізується у механізмі прийняття рішення про доступ. Саме цей етап забезпечує перехід від набору часткових результатів перевірки до фінального рішення щодо надання або відмови у доступі до

ISSN 2786-6025 Online

ресурсів системи. Основою механізму є формування інтегральної оцінки довіри до користувача, яка враховує як результати проходження рівнів автентифікації, так і оцінку ризику. На відміну від простих моделей запропонований підхід дозволяє враховувати часткову достовірність та невизначеність. Прийняття рішення здійснюється шляхом порівняння отриманої оцінки з пороговим значенням, яке може змінюватися залежно від рівня ризику. У випадку недостатньої довіри система може або відмовити у доступі, або ініціювати додаткову автентифікацію, що забезпечує гнучкість та зменшує кількість помилкових відмов.

Сформоване рішення передається до інформаційно-комунікаційної системи, що логічно приводить до питання інтеграції запропонованого методу в існуючу інфраструктуру.

Завершальним етапом реалізації методу є його інтеграція з існуючими інформаційно-комунікаційними системами, що забезпечує практичну цінність запропонованого підходу (рис. 3).

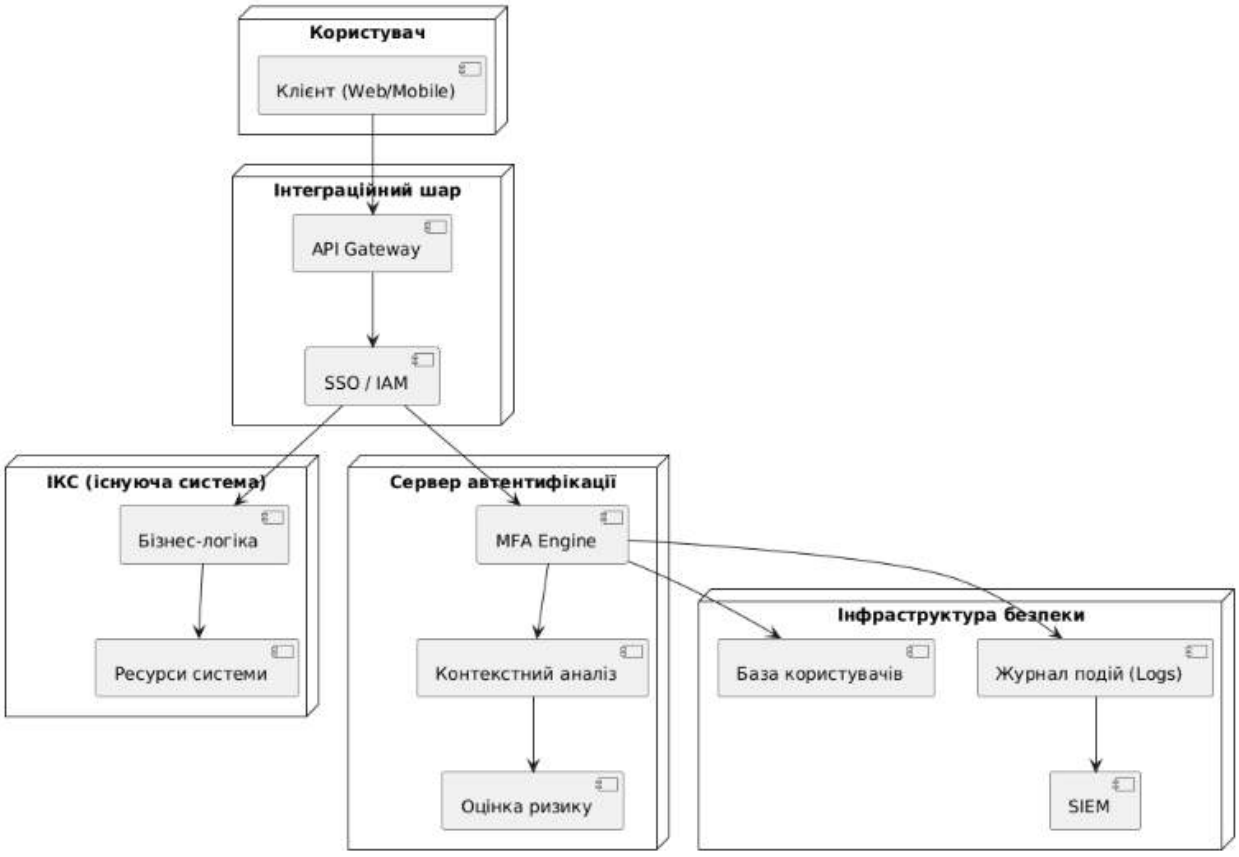

Рис. 3. *Структурно-функціональна модель інтеграції багаторівневої автентифікації в існуючу ІКС*
Джерело: побудовано авторами

ISSN 2786-6025 Online

Інтеграція може здійснюватися шляхом впровадження окремого модуля або сервісу автентифікації, який взаємодіє з ІКС через стандартизовані інтерфейси (API). Такий підхід дозволяє централізувати процес автентифікації та забезпечити єдину політику безпеки для різних підсистем. Крім того, можливе використання технологій єдиного входу (SSO) та систем управління ідентифікацією (IAM), що дозволяє масштабувати метод на рівні організації. Це забезпечує не лише підвищення безпеки, але й покращення користувацького досвіду за рахунок зменшення кількості повторних автентифікацій.

Для реалізації багаторівневої автентифікації застосовується комплекс сучасних технологій, що забезпечують як безпеку, так і масштабованість системи. На рівні автентифікації широко використовуються стандарти генерації одноразових паролів, зокрема TOTP (Time-based One-Time Password), а також протоколи OAuth 2.0 та OpenID Connect для реалізації єдиного входу та федеративної автентифікації.

Серверна частина системи може бути реалізована з використанням сучасних фреймворків (наприклад, Node.js, Java Spring Boot або .NET), які дозволяють створювати мікросервісну архітектуру. Для зберігання облікових даних та журналів подій застосовуються реляційні або NoSQL бази даних, а для обробки подій безпеки – системи моніторингу та аналізу (SIEM).Для засобів контекстного аналізу, які реалізують збір і обробку параметрів середовища доступу (геолокація, IP-адреса, характеристики пристрою) використовуються бібліотеки *Device Fingerprinting* та сервіси визначення геолокації. Поведінковий аналіз може бути реалізований за допомогою алгоритмів машинного навчання, які формують профіль «нормальної» активності користувача.

З боку клієнта використовуються веб-технології або мобільні SDK, які підтримують багатофакторну автентифікацію, зокрема інтеграцію з біометричними сенсорами пристрою. У сукупності ці інструменти формують технологічну основу для реалізації ефективної системи багаторівневої автентифікації.

Оцінювання ефективності запропонованого методу багаторівневої автентифікації здійснюється на основі сукупності кількісних та якісних критеріїв, що відображають його здатність забезпечувати захист інформаційно-комунікаційної системи без суттєвого погіршення користувацького досвіду. Ключовими серед них є швидкість автентифікації, надійність ідентифікації користувача та стійкість до сучасних кіберзагроз. Комплексне врахування цих показників дозволяє оцінити не лише технічну ефективність методу, а й доцільність його практичного застосування.

Швидкість автентифікації характеризується часом виконання повного циклу перевірки користувача: від моменту введення облікових даних до прийняття рішення про доступ. Формально цей показник можна подати як суму часу виконання окремих етапів:

ISSN 2786-6025 Online

$$T_a = \sum_{i=1}^{n} T_i, \quad (6)$$

де T_i – час виконання і-го рівня автентифікації. У багаторівневих системах важливо мінімізувати T_a за рахунок адаптивного підходу, при якому додаткові перевірки активуються лише у випадку підвищеного ризику. Це дозволяє зберегти високу швидкість для більшості легітимних користувачів.

Для оцінювання надійності автентифікаційних систем використовуються стандартні метрики: ймовірність помилкового допуску користувача (False Acceptance Rate, FAR) та ймовірність помилкового відхилення легітимного користувача (False Rejection Rate, FRR). Вони визначаються як:

$$FAR = \frac{N_{FA}}{N_{IA}}, \quad FRR = \frac{N_{FR}}{N_{LA}}, \quad (7)$$

де N_{FA} – кількість помилкових допусків, N_{IA} – загальна кількість спроб несанкціонованого доступу, N_{FR} – кількість помилкових відмов, N_{LA} загальна кількість легітимних спроб входу. У практиці оцінювання біометричних та багатофакторних систем часто використовується інтегральний показник – рівень рівності помилок (Equal Error Rate, EER), який визначається як значення, при якому функції F_{AR} та F_{RR} перетинаються: $EER = FAR(\tau^*) = FRR(\tau^*)$, де τ^* – порогове значення системи, при якому обидві помилки є рівними.

Стійкість до атак характеризує здатність системи протистояти різним типам кіберзагроз, зокрема підбору паролів, фішингу, атакам повторного відтворення та компрометації факторів автентифікації. Формально її можна оцінити через ймовірність успішного несанкціонованого доступу:

$$P_a = \prod_{i=1}^{n} P_i,$$

де P_i – ймовірність компрометації окремого фактору. Використання незалежних факторів дозволяє експоненційно зменшити загальний ризик.

Результати оцінювання показують, що запропонований метод багаторівневої автентифікації підвищує рівень безпеки порівняно з традиційними підходами за рахунок використання кількох незалежних факторів перевірки та врахування контексту доступу, що зменшує ризик несанкціонованого входу навіть у разі компрометації окремих елементів. При цьому адаптивний механізм перевірки дозволяє не перевантажувати користувача зайвими

ISSN 2786-6025 Online

етапами, оскільки додаткові рівні автентифікації активуються лише при підвищеному ризику, що зберігає прийнятну швидкодію системи. Крім того, застосування контекстного та поведінкового аналізу зменшує кількість помилкових рішень системи та забезпечує більш збалансоване поєднання безпеки й зручності використання в інформаційно-комунікаційних системах.

Висновки. У результаті проведеного дослідження було розроблено та формалізовано метод багаторівневої автентифікації користувачів для інформаційно-комунікаційних систем із підвищеними вимогами до безпеки. Запропонований підхід базується на поєднанні кількох незалежних факторів автентифікації, контекстного аналізу та інтегральної оцінки рівня довіри користувача. Побудована архітектура методу, алгоритм перевірки та механізм прийняття рішення дозволяють забезпечити адаптивний процес автентифікації, у якому рівень перевірки змінюється залежно від контексту доступу та оціненого ризику, що підвищує загальну ефективність захисту інформаційних ресурсів.

Оцінювання ефективності підтвердили доцільність використання багаторівневої автентифікації в сучасних ІКС. Використання контекстних параметрів, адаптивних політик доступу та комбінування різних методів перевірки користувача дозволяє знизити ймовірність несанкціонованого доступу, зменшити кількість помилкових рішень системи та забезпечити баланс між рівнем безпеки і зручністю користування. Отримані результати свідчать про перспективність подальшого розвитку запропонованого підходу, зокрема в напрямі інтеграції методів машинного навчання для більш точного аналізу поведінки користувачів та прогнозування ризиків доступу.

Література:

1. Al Kabir M. A., Elmedany W. (2024). Adaptive risk-based passwordless authentication: A FIDO2 integrated approach for enhanced security and usability. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4795401.

2. Chennuri, K. M. R. (2024). Adaptive multi-factor authentication systems: A comprehensive analysis of modern security approaches. *International Journal of Computer Engineering and Technology*, 15(6), 787–795.

3. Yassir Mohammed, A. H., & Dziyauddin, R. A. (2023). Current multi-factor authentication: Approaches, requirements, attacks and challenges. *International Journal of Advanced Computer Science and Applications,* 14(1), 1–10.

4. Singh, J., Patel, C., & Chaudhary, N. K. (2022). Resilient risk-based adaptive authentication and authorization (RAD-AA) framework. *arXiv preprint arXiv*:2208.02592. https://arxiv.org/abs/2208.02592.

5. Рзаєва, Світлана Леонідівна, et al. "Адаптивне управління інформаційною безпекою в хмарно-орієнтованих інтелектуальних транспортних системах." *Безпека інформації 31.1* (2025): 23-36.

ISSN 2786-6025 Online

6. Рзаєва, Світлана Леонідівна, et al. "Модель реалізації керування доступом на основі ролей (RBAC) у багаторівневій архітектурі сховища даних." *Сучасний захист інформації* 3 (2025): 137-149.

7. Rzaeva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, 31(1), 23-36.

References:

1. Al Kabir M. A., Elmedany W. (2024). Adaptive risk-based passwordless authentication: A FIDO2 integrated approach for enhanced security and usability. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4795401.

2. Chennuri, K. M. R. (2024). Adaptive multi-factor authentication systems: A comprehensive analysis of modern security approaches. *International Journal of Computer Engineering and Technology*, 15(6), 787–795.

3. Yassir Mohammed, A. H., & Dziyauddin, R. A. (2023). Current multi-factor authentication: Approaches, requirements, attacks and challenges. *International Journal of Advanced Computer Science and Applications*, 14(1), 1–10.

4. Singh, J., Patel, C., & Chaudhary, N. K. (2022). Resilient risk-based adaptive authentication and authorization (RAD-AA) framework. *arXiv preprint arXiv*:2208.02592. https://arxiv.org/abs/2208.02592.

5. Rzaieva, Svitlana Leonidivna, et al. "Adaptive management of information security in cloud-oriented intelligent transport systems." *Information Security*, 31(1), 2025, pp. 23–36.

6. Rzaieva, Svitlana Leonidivna, et al. "Model of role-based access control (RBAC) implementation in a multi-level data warehouse architecture." *Modern Information Protection*, 3, 2025, pp. 137–149.

7. Rzaeva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, 31(1), 23-36.

Дата першого надходження статті до видання: 12.04.2026
Дата прийняття статті до друку після рецензування: 26.04.2026