МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ПТІКІ'2026)

Одеса, Україна, 16 липня 2026 р.

Матеріали конференції

ОДЕСА

2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

«Передові технології в інформаційно-комунікаційній інженерії»

(ПТІКІ'2026)

Одеса, Україна, 16 липня 2026 р.

Матеріали конференції

Одеса

2026

УДК 004.9
ББК 32

Проведення заходу зареєстровано в Державній науковій установі «Український інститут науково-технічної експертизи та інформації» (Реєстраційний номер: 3326U000765 від 01-07-2026 р.).

Рецензенти:
Надія КАЗАКОВА – д.т.н., професор, завідувач кафедри інформаційних технологій Одеського національного університету ім. І.І. Мечнікова
Віктор СТРЕЛЬБИЦЬКИЙ – к.т.н., доцент, доцент кафедри підйомно-транспортні машини та інжиніринг портового технологічного обладнання Одеського національного морського університету

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2026): Conference Proceedings. Odesa: International university, 2026, 145 p**.**
DOI: https://doi.org/10.32837/11300.33747

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2026): Матеріали конференції. Одеса: Міжнародний університет, 2026, 145 с.

У збірнику подано результати наукових досліджень, висвітлено обговорення актуальних проблем, викликів і тенденцій з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами у різних галузях народного господарства. Матеріали охоплюють інноваційні підходи, досвід упровадження сучасних рішень і приклади успішних практик трансформації різних галузях народного господарства .

Видання призначене для науково-педагогічних працівників, здобувачів освіти, науковців і фахівців ІТ галузі.

Відповідальні за випуск:
к.т.н., доцент Пунченко Наталія,
к.т.н., доцент Розенвассер Денис.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова

КІВАЛОВ С.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.

Співголови

ГРОМОВЕНКО К.В. – д.ю.н., проф., Міжнародний університет, м. Одеса, Україна.
ЛЕФТЕРОВ В.О. – д.п.н., проф., Міжнародний університет, Одеса, Україна
СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., НТУ України "КПІ імені Ігоря Сікорського", Київ, Україна.

Члени організаційного комітету

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ВАКАРЧУК А.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРІБОВА В.В. – к.ф.-м.н., доц., Міжнародний університет, Одеса, Україна.

РЕДАКЦІЙНИЙ КОМІТЕТ

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л. С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЗМІСТ

УДК 004.056.53

DOI: https://doi.org/10.32837/11300.33765

СИСТЕМНИЙ МЕТОД ОЦІНЮВАННЯ СТІЙКОСТІ АВТЕНТИФІКАЦІЇ МЕХАНІЗМІВ У ІНФОРМАЦІЙНИХ СИСТЕМАХ

Пахолюк Олег Ігорович
Аспірант, спеціальність 125
"Кібербезпека та захист інформації",
Міжнародний університет, м. Одеса, Україна
Olegpah@proton.me
Науковий керівник,
Йона Лариса Григорівна, к.т.н.,
Завідувач, доцент кафедри Комп'ютерної інженерії та інноваційних технологій
Факультету Кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародного університету
yonalarisa66@gmail.com

Анотація. *В дослідженні пропонується метод комплексного аналізу автентифікаційних механізмів інформаційних систем та виявлення вразливостей. Запропонований метод поєднує систематизацію загроз із практичними інструментами ідентифікації, що узгоджується з сучасними стандартами безпеки. Результати підтверджують його ефективність у підвищенні захисту інформаційних ресурсів.*

Для забезпечення інформаційної безпеки основну роль виконують протоколи автентифікації, адже вона визначає, чи має користувач право доступу до ресурсів системи. За даними ENISA (Агентство Європейського Союзу з кібербезпеки), понад 40% інцидентів у сфері кібербезпеки пов'язані саме з компрометацією автентифікаційних процедур [1]. Це зумовлює необхідність розробки комплексних методів аналізу та виявлення вразливостей, які поєднують теоретичні моделі та практичні інструменти.

Серед основних вразливостей протоколів автентифікації можна виділити кілька категорій, кожна з яких має власні характеристики та методи виявлення.

Найчастіше відбуваються випадки слабких чи повторно використаних паролів, що є найпоширенішою причиною компроментації облікових записів. Цей факт створює умови для атак типу «brute force» та «credential stuffing».

Крім того, часто паролі зберігаються у відкритому вигляді або використовуються застарілі алгоритми хешування, які не відповідають сучасним вимогам криптографічної стійкості. Це надає можливості зловмисникам отримати доступ до баз даних та відновити автентифікаційні дані користувачів.

Також серйозну загрозу становить використання застарілих протоколів автентифікації, таких як NTLM чи PAP. До того ж, багатофакторна автентифікація (MFA), яка розглядається як більш надійний механізм, має

власні слабкі місця. Використання SMS-кодів як другого фактору може бути небезпечним через можливість їх перехоплення або здійснення атак «SIM swapping», що вже неодноразово фіксувалося у звітах міжнародних агентств [1]. Це свідчить про необхідність переходу до більш захищених методів, таких як апаратні токени чи мобільні додатки-генератори кодів.

Додатковим джерелом ризику виступають методи соціальної інженерії та фішингові атаки, спрямовані на викрадення автентифікаційних даних користувачів. Зловмисники активно застосовують електронну пошту, месенджери та підроблені веб-ресурси для введення користувачів в оману. За даними ENISA (2022), фішинг залишається одним із найпоширеніших способів компрометації автентифікаційних механізмів, що підтверджує необхідність комплексного підходу до їх захисту. Основні техніки соціальної інженерії та фішингових атак охоплюють фішинг, вішинг, смішинг, бейтінг, прітекстинг та інсайдерські загрози. Вони ґрунтуються на психологічних маніпуляціях, спрямованих на отримання доступу до конфіденційної інформації. Соціальна інженерія не передбачає технічного зламу систем, а базується на використанні людського фактору. Саме тому ключовими заходами протидії є навчання персоналу, застосування багатофакторної автентифікації та моніторинг поведінкових моделей користувачів [2].

Комплексний підхід ґрунтується на інтеграції різних методів оцінки безпеки. Використання автоматизованих сканерів (Nessus, OpenVAS) забезпечує виявлення некоректних конфігурацій системи. Аналіз мережевого трафіку дозволяє фіксувати випадки передачі незашифрованих автентифікаційних даних. Проведення тестів на проникнення моделює реальні сценарії атак з метою перевірки стійкості системи. Додатково аудит політик доступу та контроль журналів автентифікації сприяють своєчасному виявленню аномальних спроб входу.

Моделювання атак та аналіз каналів доставки кодів у багатофакторній автентифікації здійснюється не одним конкретним алгоритмом, а комплексом методологій і технік: STRIDE, DREAD, PASTA, LINDDUN, Attack Trees, Side-channel analysis. Вони дозволяють систематизувати загрози, оцінити ризики та перевірити стійкість каналів доставки кодів (SMS, push-сповіщення, токени).

Моделювання атак роблять для того, щоб перетворити потенційні загрози на контрольовані сценарії, які можна дослідити, оцінити та використати для вдосконалення системи захисту.

Комплексний метод аналізу реалізується поетапно. Спершу здійснюється систематизація загроз, що дозволяє класифікувати ключові вразливості автентифікаційних механізмів. Далі проводиться моделювання атак, яке забезпечує створення контрольованих сценаріїв для перевірки стійкості системи. Наступним етапом є аналіз каналів доставки автентифікаційних кодів, що дає змогу оцінити надійність SMS-повідомлень, push-сповіщень та апаратних токенів. Інструментальний аудит використовується для перевірки конфігурацій, політик доступу та виявлення технічних недоліків. На основі

отриманих результатів здійснюється оцінка ризиків із визначенням їх пріоритетності, що дозволяє виділити найбільш критичні загрози. Завершальний етап передбачає розробку заходів протидії, які включають впровадження сучасних криптографічних алгоритмів, оновлення протоколів автентифікації та підвищення рівня обізнаності персоналу.

Можна зробити висновок, що комплексний метод поєднує аналітичну, технічну та організаційну складові, що забезпечує проактивний підхід до захисту автентифікаційних механізмів. Його застосування дозволяє не лише підвищити рівень кіберзахисту, але й забезпечити відповідність сучасним міжнародним та національним вимогам у сфері інформаційної безпеки.

Висновки. У таблиці 1 представлено основні результати застосування комплексного методу аналізу автентифікаційних механізмів.

Запропонований комплексний метод аналізу та виявлення вразливостей автентифікаційних механізмів поєднує систематизацію загроз із практичними інструментами їх виявлення. Це дозволяє підвищити рівень захисту інформаційних систем та забезпечити відповідність сучасним міжнародним і національним стандартам.

Таблиця 1 - Результати експериментальної перевірки методу

№	Етап	Дія	Результат
1	Систематизація загроз	Класифікація основних вразливостей автентифікаційних механізмів	Визначено критичні точки ризику для подальшого аналізу
2	Моделювання атак	Створення контрольованих сценаріїв проникнення	Підтверджено здатність системи протидіяти реальним атакам
3	Аналіз доставки кодів	Оцінка надійності SMS, push-сповіщень та апаратних токенів	Виявлено слабкі та сильні сторони різних каналів автентифікації
4	Інструментальний аудит	Перевірка конфігурацій, політик доступу та технічних налаштувань	Виявлено помилки конфігурації та недоліки політик
5	Оцінка ризиків	Пріоритизація загроз на основі отриманих даних	Сформовано перелік найбільш критичних ризиків
6	Розробка заходів протидії	Впровадження сучасних криптографічних алгоритмів, оновлення протоколів, навчання персоналу	Підвищено рівень захисту інформаційних ресурсів та відповідність міжнародним стандартам

Література

1. Threat Landscape 2022. European Union Agency for Cybersecurity, 2022.
2. Hideez. Що таке соціальна інженерія в кібербезпеці? Реальні приклади та методи запобігання. Київ: Hideez, 2024.
   URL: https://hideez.com/uk-ua/blogs/news/social-engineering

3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, 2022.
4. NIST Special Publication 800-63-3. Digital Identity Guidelines. National Institute of Standards and Technology, 2017.
5. OWASP Authentication Cheat Sheet. OWASP Foundation, 2023.
6. Державна служба спеціального зв'язку та захисту інформації України. Методичні рекомендації щодо організації систем автентифікації та управління доступом. Київ, 2021.
7. Йона Л. Г., Пахолюк О.І. Методи виявлення слабких місць інформаційних систем у процесах підтвердження справжності користувача // Передові технології в інформаційно-комунікаційній інженерії (ATICE'2025) : зб. матеріалів міжнар. конф. (зимовий форум) / відп. ред. І. М. Соловська, Д. М. Розенвассер. – Одеса : Міжнародний університет, 2025. – С. 101-105. – Режим доступу: https://doi.org/10.32837/11300.31453