МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ATICE'2025)

ОДЕСА, УКРАЇНА, 18 ЛИПНЯ 2025 Р.

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

ОДЕСА

2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

INTERNATIONAL HUMANITARIAN UNIVERSITY

INTERNATIONAL CONFERENCE

ADVANCED TECHNOLOGY IN INFORMATION AND COMMUNICATION ENGINEERING

(ATICE'2025)

ODESA, UKRAINE, JULY 18, 2025

CONFERENCE PROCEEDINGS

ODESA

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

Одеса, Україна, 18 липня 2025 р.

Видавничий дім
«Гельветика»
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL HUMANITARIAN UNIVERSITY

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2025)

Odesa, Ukraine, July 18, 2025

Conference Proceedings

Видавничий дім
«Гельветика»
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 18 липня 2025 р.

Матеріали конференції

Видавничий дім
«Гельветика»
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings. Odesa : International humanitarian university, 2025, 123 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції. Міжнародний гуманітарний університет, 2025. – Одеса: Видавничий дім «Гельветика», 2025. – 123 с.

ISBN 978-617-554-582-9

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний 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

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний 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.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

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

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

РУСУ О.П. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.

ЙОНА Л.Г. – к.т.н., доц., Міжнародний гуманітарний університет, Одеса, Україна.

МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.

ПЕДЯШ В.В. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.

ЖИГУЛІН О.А. – д.е.н., проф., Міжнародний гуманітарний університет, Одеса, Україна

ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

централізований контроль і меншу кількість точок входу, але вразливість в одній частині може поставити під загрозу всю систему. Натомість мікросервіси дають гнучкість та ізоляцію компонентів, проте вимагають ретельного підходу до захисту міжсервісної комунікації, автентифікації та моніторингу. У результаті, ефективна безпека додатку значною мірою залежить від правильного балансу між архітектурним підходом і впровадженими механізмами захисту.

Література:

1. Архітектура програмного забезпечення: як правильне проєктування забезпечує ефективність та безпеку. Березень 2025 року. [Електронний ресурс] URL: https://wezom.com.ua/ua/blog/arhitektura-programnogo-zabezpechennya (дата звернення 30.06.2025)

2. The Importance of Microservices Architecture and Security Challenges. Березень 2025 року. [Електронний ресурс] URL: https://www.hostragons.com/en/blog/security-challenges-in-microservices-architecture (дата звернення: 30.06.2025).

3. Microservices vs. Monoliths: Why Every Developer Must Also Be a Cybersecurity Professional. Березень 2023 року. [Електронний ресурс] URL: https://vfunction.com/blog/microservices-vs-monoliths-why-every-developer-must-be-cybersecurity-professional (дата звернення: 30.06.2025).

Пахолюк Олег Ігорович
Аспірант, спеціальність 125 «Кібербезпека та захист інформації»,
Науковий керівник
Йона Лариса Григорівна, к.т.н., доцент
Міжнародний гуманітарний університет
yonalarisa66@gmail.com

ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ОПТИМІЗАЦІЇ ПРОЦЕДУР ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

Анотація*. У статті запропоновано підхід до виявлення вразливостей інформаційних систем, що базується на вдосконаленні процедур ідентифікації та автентифікації. Розглянуто основні недоліки існуючих методів захисту, які можуть призводити до компрометації безпеки. Наведено математичну модель, яка дозволяє прогнозувати потенційні вразливості на ранніх етапах і забезпечувати високий рівень кіберзахисту.*

Вступ

Інформаційні системи є основою багатьох бізнесових, адміністративних і технологічних процесів та охоплюють етапи збереження, оброблення, видалення та передавання даних.

Проте кіберзлочинці постійно вдосконалюють свої методи атак та здатні обходити традиційні заходи безпеки, тобто загрози розвиваються так само швидко, як і технології

захисту. Серед найпоширеніших способів атак виділяються фішинг, атаки методом перебору паролів (brute force), експлуатація вразливостей програмного забезпечення, а також атаки соціальної інженерії.

Базовими елементами безпеки інформаційних систем є процедури ідентифікації та автентифікації, тому більш уваги слід приділяти саме методам їх вдосконалення. Сучасні умови вимагають запровадження прогресивних підходів, що враховують поведінку користувачів, специфіку операційного контексту та здатність систем гнучко реагувати на загрози в реальному часі.

Такі підходи спрямовані на зниження ризиків, забезпечення більшої гнучкості систем безпеки та покращення користувацького досвіду.

Метою статті є розробка підходу, що поєднує аналіз поведінкових й контекстних характеристик користувачів із адаптивними механізмами безпеки для зниження ризику несанкціонованого доступу до інформаційних систем та побудова математичної моделі виявлення вразливостей на основі оптимізації процедур ідентифікації та автентифікації.

Аналіз існуючих підходів та пропонований підхід

Основними складовими безпеки інформаційних систем є методи ідентифікації та автентифікації. До найбільш поширених методів належать паролі, біометричні технології, двофакторна автентифікація та концепція довірчої мережі (Zero Trust). Проте навіть найсучасніші методи автентифікації мають свої обмеження, які зумовлюють необхідність розробки нових підходів. Оптимальне рішення має враховувати баланс між безпекою, зручністю для користувачів та можливістю адаптації до змінних умов сучасних кіберзагроз.

Запропонований підхід дозволяє знизити ризики компрометації системи за рахунок використання трьох основних компонентів: збору даних, поведінкового аналізу та контекстної автентифікації.

Збір даних передбачає постійний моніторинг дій користувача з використанням різних джерел інформації.

Поведінковий аналіз використовує алгоритми машинного навчання, які аналізують поведінкові шаблони користувачів і виявляють аномалії.

Контекстна автентифікація є основним етапом у забезпеченні балансу між безпекою та зручністю для користувачів. У разі виявлення підозрілої активності система застосовує додаткові перевірки. При цьому в разі підтвердження автентичності, система запам’ятовує контекст, що дозволяє зменшити кількість додаткових перевірок у майбутньому за подібних умов доступу.

Використання ризик-орієнтованого підходу передбачає застосування різних заходів перевірки або блокування доступу залежно від рівня загрози. Цей підхід активно застосовується в сферах управління безпекою інформаційних систем, фінансових операцій і банківської діяльності та дозволяє автоматизовано оцінювати ризики на основі заданих параметрів, таких як ймовірність загрози або її вплив на систему, і відповідно адаптувати заходи безпеки.

Запропонована математична модель аналізу ризиків є ключовим елементом адаптивної системи автентифікації, яка дозволяє динамічно оцінювати безпеку доступу на основі поведінкових і контекстних характеристик користувача. Модель ґрунтується на комбінованій оцінці двох основних параметрів:

- ймовірність аномальної поведінки користувача (P-показник, що відображає наскільки поточна активність відрізняється від звичайного поведінкового шаблону);
- критичність доступу до системи (C- рівень важливості ресурсів або даних, до яких запитується доступ, що визначає потенційні наслідки несанкціонованого проникнення).

Модель оцінки ризиків інтегрує ймовірність аномальної поведінки користувача та критичність доступу для визначення загального рівня ризику. Математичне представлення виглядає так:

$$R = \alpha P + \beta C, \quad (1)$$

де R — загальний рівень ризику; P — ймовірність аномальної поведінки, яка визначається моделями машинного навчання; C — критичність доступу, яка попередньо класифікується; α і β — вагові коефіцієнти, що враховують значущість відповідних факторів (наприклад, $\alpha+\beta=1$).

Класифікація критичності доступу C виконується наступним чином:

— низький рівень (C=1): доступ до загальнодоступної інформації, яка не потребує значного захисту;

— середній рівень (C=2): доступ до персональних чи корпоративних даних, що мають обмежений доступ;

— високий рівень (C=3): доступ до критично важливої інформації, зокрема конфіденційних даних чи систем управління.

Ймовірність аномальної поведінки (P) визначається на основі аналізу дій користувача в реальному часі за допомогою моделей машинного навчання. Вхідні параметри для цих моделей включають: геолокацію користувача, час дії, типові дії у системі (запити до ресурсів, введення даних), попередні шаблони поведінки користувача.

Використання моделі виконується наступним чином:

— низький рівень ризику ($R<T_1$): система дозволяє доступ без додаткових перевірок;

— середній рівень ризику ($T_1 \leq R < T_2$): активується одноразова автентифікація;

— високий рівень ризику ($R \geq T_2$): доступ блокується до проведення повної багатофакторної автентифікації.

Налаштування вагових коефіцієнтів:

— α більше, якщо важливіша ймовірність аномальної поведінки;

— β більше, якщо критичність доступу має визначальне значення.

Запропонована модель дозволяє динамічно адаптувати рівень безпеки до ризиків, забезпечуючи баланс між зручністю доступу та захистом інформації.

Побудова математичної моделі дозволяє прогнозувати потенційні вразливості системи, оптимізувати процедури ідентифікації та автентифікації користувачів та знизити ймовірність реалізації атак за рахунок підвищення ефективності кіберзахисту.

Система представлена множиною об'єктів, які взаємодіють через канали зв'язку, і включає етапи ідентифікації та автентифікації.

Основними компонентами моделі є: множина об'єктів системи $S = \{s_1, s_2, \ldots, s_n\}$; характеристики ідентифікації $I = \{i_1, i_2, \ldots, i_m\}$ (логіни, паролі, біометричні дані); процедури автентифікації $A=\{a_1, a_2, \ldots, a_k\}$(однофакторні та багатофакторні); вразливості системи $V = \{v_1, v_2, \ldots, v_p\}$ (помилки програмного забезпечення, неправильно налаштовані політики

доступу); потенційні атаки $T = \{t_1, t_2, \ldots, t_q\}$(фішинг, перебір паролів, експлуатація вразливостей).

Для формалізації формули, що враховує оптимізацію процедур ідентифікації та автентифікації в рамках виявлення вразливостей інформаційних систем, можна запропонувати такий підхід: позначемо: V— загальний рівень вразливості системи; P_i— ефективність процедури ідентифікації; P_A— ефективність процедури автентифікації; C— критичність ресурсів, які захищає система (від 0 до 1); R_V— ризик відомих вразливостей (оцінка рівня загроз із бази CVE або подібної системи); E_{opt}— ефективність оптимізації захисних процедур (наприклад, використання двофакторної автентифікації або біометрії); F— частота виявлення нових вразливостей у системі (наприклад, кількість нових CVE на рік). Тоді оцінку вразливостей можна обчислити за формулою:

$$V = ((1 - P_i) + (1 - P_A)) / 2 \cdot C \cdot (R_v + F) \cdot (1 - E_{opt}), \qquad (2)$$

де $(1 - P_i)$ та $(1 - P_A)$ - враховують недостатню ефективність ідентифікації та автентифікації; C - підсилює вплив уразливостей залежно від важливості даних системи; $(R_v + F)$ описує загальну ймовірність появи вразливостей; $(1 - E_{opt})$ зменшує ризик вразливостей залежно від застосованих оптимізацій.

Формула (2) дозволяє оцінити загальний рівень вразливості системи та ефективність застосування різних методів оптимізації процедур ідентифікації й автентифікації. Вона може бути адаптована залежно від конкретних сценаріїв аналізу. Та надає можливість зробити висновки щодо:

— ефективності процедур: чим нижча ефективність процедур ідентифікації (P_i) і автентифікації (P_A), тим вищий загальний рівень вразливості;

— критичності: якщо система захищає важливі ресурси ($C \to 1$), то вразливості мають більший вплив;

— оптимізації: якщо впроваджено сучасні захисні механізми ($Eopt \to 1$), рівень вразливості знижується;

— ризиків вразливостей: чим більше ризиків (R_V) і частіше з'являються нові уразливості (F), тим більше зростає загальний ризик.

Висновки щодо переваг математичної моделі:

— модель дозволяє налаштовувати параметри і вагові коефіцієнти відповідно до потреб конкретної системи, тобто є гнучкою;

— аналіз здійснюється у реальному часі, що забезпечує оперативну реакцію на потенційні загрози, тобто є динамічною;

— використання алгоритмів машинного навчання дозволяє адаптувати модель до змін поведінки користувачів, тобто є інтеграція з сучасними технологіями;

— застосування додаткових заходів лише в разі потреби, що знижує ризики, не створюючи надмірних незручностей для користувачів.

Таким чином, запропонована математична модель є ефективним інструментом для підвищення рівня безпеки інформаційних систем та забезпечує оптимальний баланс між захистом і зручністю доступу.

У подальших дослідженнях планується розширити модель, додавши механізми інтеграції з технологіями штучного інтелекту та блокчейну для ще більшої безпеки.

Література

1. Гришко, С.М. Інформаційна безпека та захист інформації: Навчальний посібник. Київ: Видавничий дім «Кондор», 2020.

2. Лаптєв, В.М., Євдокименко, В.К., Рибалко, О.Ю. Комплексний підхід до захисту інформації: Підручник. Харків: ХНУРЕ, 2018.

3. Шахов, В.В. Основи кібербезпеки. Київ: Академія, 2019

4. Bishop, M. Computer Security: Art and Science. Boston: Addison-Wesley, 2003.

5. Stallings, W. Cryptography and Network Security: Principles and Practice. 7th edition. Upper Saddle River: Pearson, 2017.

6. Alpaydin, E. Introduction to Machine Learning. 4th edition. Cambridge: MIT Press, 2020.

7. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd edition. New York: Wiley, 2020.

Димов Максим Віталійович
Студент факультету Кібербезпеки, програмної інженерії та комп'ютерних наук,
Спеціальність: 125 Кібербезпека
Міжнародний гуманітарний університет
mak.dymov@gmail.com
Керівник: к.т.н.,доцент Йона Лариса Григорівна,
yonalarisa66@gmail.com

РИЗИКИ ДЛЯ БЕЗПЕКИ В ЦИФРОВОМУ ПРОСТОРІ

Анотація. Досліджуються сучасні ризики кібербезпеки, пов'язані з використанням штучного інтелекту для створення фішингового контенту. Проаналізовано класифікацію AI-підсилених атак, методи генерації синтетичного контенту та їх застосування в дезінформаційних кампаніях. Запропоновано підходи до виявлення та протидії таким загрозам в умовах гібридних конфліктів.

Ключові слова: кібербезпека, штучний інтелект, фішинг, синтетичний контент, дезінформація, цифрові загрози.

Сучасне цифрове середовище характеризується швидким зростанням технологій розумних комп'ютерів що відкриває нові шанси як для розвитку суспільства так і для зловмисних осіб. Використання AI-технологій для створення підробленого контенту стала однією з найбільших загроз безпеки Інтернету у останніх роках [1]. Звичайні способи обману урізноманітнилися від простих текстових повідомлень та до складних мультимедійний атак із використанням deepfake-технології, AI-створеними картинками та фальшивими текстами.

Актуальність роботи пов'язана із зростанням кількості кібер-інцидентів з використанням контенту, який було створено AI, особливо під час змішаних конфліктів та боїв за інформацію [2]. По даним аналізу цифр, більше 75% організацій зустрічали нові типи фішингових атак, що використовують елементи штучного уміння для покращення соціальної інженерії.

Дослідження показує, що атаки на основі штучного інтелекту можна розділити на три головні групи згідно з типом контенту: