**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**МІЖНАРОДНИЙ УНІВЕРСИТЕТ**

# ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

**МАТЕРІАЛИ КОНФЕРЕНЦІЇ**
**(зимовий форум)**

**Одеса, Україна, 14 листопада 2025 р.**

**Одеса**
**2025**

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
**INTERNATIONAL UNIVERSITY**

# International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025)

**Odesa, Ukraine, November 14, 2025**

**Conference Proceedings**
**(winter forum)**

**Odesa**
**2025**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
**МІЖНАРОДНИЙ УНІВЕРСИТЕТ**

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

**Одеса, Україна, 14 листопада 2025 р.**

**Матеріали конференції**
**(зимовий форум)**

**Одеса**
**2025**

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings (winter forum). Odesa : International university, 2025, 101 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції (зимовий форум). Одеса : Міжнародний університет, 2025, 101 с.

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.

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

## СЕКЦІЇ

## СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

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

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

МІРОШНИК М.А. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний 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 університет, Одеса, Україна.
МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний 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 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 університет, Одеса, Україна
ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

**СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА**



**СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ**

**УДК 004.056.53 : 004.021 : 519.85**

*Григор'єва Т.І., кандидат технічних наук, доцент,*
*Мельник В.В., здобувач вищої освіти ступеня доктора філософії*
*спеціальності F5 - Кібербезпека та захист інформації*
*Міжнародний університет, місто Одеса*
*tig15090808@gmail.com*
*valikysimys.melnyk@gmail.com*

# АНАЛІЗ МЕТОДІВ ОПТИМІЗАЦІЇ БЕЗПЕКИ БАЗ ДАНИХ

***Анотація.*** *В роботі представлено аналіз різноманітних математичних підходів до оптимізації безпеки баз даних. Розглянуто сильні та слабкі сторони графових, статистичних, ймовірнісних, матричних та тензорних методів. Визначено, що вибір конкретного підходу залежить від специфіки завдання, наприклад, моделювання зв'язків, виявлення аномалій, управління ризиками, компресія даних, та вимог до обчислювальної ефективності. Зроблено висновок про необхідність гібридизації цих методів для побудови високонадійних та адаптивних систем захисту даних.*

У сучасних інформаційних системах безпека баз даних є критичним чинником забезпечення цілісності, конфіденційності та доступності корпоративних даних. Зростання складності загроз, зокрема цілеспрямованих атак, внутрішніх інцидентів і багатовимірних аномалій у поведінці користувачів, потребує впровадження більш формалізованих методів аналізу. Тому дуже актуальними стають оптимізаційні підходи, що використовують графові, статистичні, матричні та тензорні моделі для оброблення великих обсягів даних і виявлення прихованих закономірностей, які неможливо розпізнати за допомогою традиційних засобів контролю доступу чи простого моніторингу активності.

Традиційні методи забезпечення безпеки баз даних зосереджуються на таких аспектах, як, по-перше, управління дозволами користувачів, по-друге, відстеження активності користувачів та системних подій. А також, використання систем виявлення вторгнень та забезпечення конфіденційності даних, як під час зберігання, так і під час передачі. Ці методи є необхідними, але їхня ефективність знижується, коли потрібно проаналізувати неочевидні, складні взаємозв'язки між різними елементами системи безпеки, що характерно для сучасних розподілених середовищ.

Графові моделі можуть бути ефективними для візуалізації складних взаємозв'язків, виявлення прихованих каналів витоку даних та аналізу поведінки користувачів у контексті доступу до критичних ресурсів. Представимо бази даних у вигляді орієнтованого або неорієнтованого графу, де вузли відповідають користувачам, таблицям, запитам або транзакціям, а ребра – зв'язкам між ними. Такий підхід дозволяє моделювати структуру доступу, виявляти циклічні залежності, а також застосовувати алгоритми пошуку аномалій.

Використання графових алгоритмів, наприклад, пошуку шляху, таких як BFS або DFS [1] дозволяє швидко перевірити наявність несанкціонованого або опосередкованого доступу користувача до критичних даних. Графові алгоритми можуть бути застосовані для ідентифікації неочікуваних шаблонів поведінки або аномальних зв'язків. Наприклад, алгоритм PageRank [1] може допомогти виявити аномальні вузли, що сприяє швидшому виявленню інцидентів. Графові моделі дозволяють проводити системний аналіз інформаційної безпеки, моделювати граф атак та оцінювати потенційні ризики, що допомагає приймати обґрунтовані управлінські рішення щодо пріоритезації заходів захисту.

Порівняно з традиційними реляційними підходами, графові методи забезпечують вищу швидкість та гнучкість при аналізі зв'язків, що критично важливо в умовах реального часу для систем кібербезпеки. Інтеграція графових методів у системи захисту баз даних є перспективним напрямом оптимізації кібербезпеки. Вони не замінюють традиційні заходи, а доповнюють їх, надаючи потужний інструмент для моделювання, аналізу та візуалізації складних взаємозв'язків у великих обсягах даних. Графові методи ідеально підходять для завдань, де ключовим є аналіз топології мережі доступу, прав користувачів та потенційних шляхів атак.

Статистичні методи орієнтовані на аналіз агрегованих характеристик даних, таких як середнє значення, дисперсія, кореляція та гістограми частот. Вони дозволяють швидко оцінити нормальність поведінки користувачів, виявити пікові навантаження, а також побудувати профілі активності. У поєднанні з ймовірнісними моделями, такими як байєсівські мережі, марковські процеси або моделі прихованих марковських ланцюгів, статистичні методи забезпечують прогнозування ризиків, оцінку ймовірності порушення політик безпеки та адаптивне реагування на зміну поведінки користувачів.

Описова статистика застосовується для узагальнення даних, розрахунку середніх значень, дисперсії, частоти подій. Це допомагає адміністраторам безпеки швидко оцінити загальний стан системи та виявити відхилення від типових параметрів, наприклад, незвичайно велика кількість невдалих спроб входу за короткий проміжок часу. Статистичні та ймовірнісні методи є основою для систем виявлення аномалій та прогнозування загроз. Вони використовуються для аналізу поведінки користувачів, де на основі історичних даних формується "нормальна" базова лінія активності [2]. Ці методи ефективні там, де потрібна кількісна оцінка відхилень та мінімізація хибних спрацьовувань. Ймовірнісні моделі, зокрема Байєсівські мережі, застосовуються для управління ризиками та діагностики першопричин інцидентів, забезпечуючи роботу з невизначеністю та неповними даними.

Інференційна статистика дозволяє робити висновки про генеральну сукупність на основі вибіркових даних. Методи перевірки гіпотез використовуються для підтвердження або спростування припущень про загрози.

Регресійний аналіз використовується для прогнозування майбутньої поведінки системи або виявлення залежностей між різними змінними, наприклад, залежність між часом доби та типом виконуваних запитів, що може вказувати на аномалії. Перевага статистичних методів полягає в математичній строгості та можливості кількісної оцінки відхилень, що забезпечує об'єктивну основу для прийняття рішень.

Ймовірнісні методи розширюють можливості статистики, інтегруючи елементи невизначеності та ризику безпосередньо в моделі безпеки. Байєсівські моделі є потужним інструментом для представлення ймовірнісних залежностей між різними подіями безпеки. Вони дозволяють оновлювати ймовірності загроз в режимі реального часу на основі нових даних (свідчень), що надходять від систем моніторингу. Байєсівські мережі використовуються для діагностики першопричин інцидентів та прогнозування розвитку атак. Ймовірнісні моделі лежать в основі кількісної оцінки ризиків інформаційної безпеки. Використання ймовірнісних моделей дозволяє обчислити очікувані збитки від потенційних загроз. Марковські моделі застосовуються для моделювання послідовностей подій, наприклад, етапів багатоланкової атаки. Аналіз переходів між станами дозволяє ідентифікувати найбільш ймовірні шляхи проникнення та розробити контрзаходи.

Ймовірнісні методи забезпечують гнучкість у роботі з неповними або зашумленими даними та дозволяють інтегрувати експертні знання в кількісні моделі. Таким чином, статистичні та ймовірнісні методи є потужними інструментами оптимізації безпеки баз даних. Використання статистичних та ймовірнісних методів дозволяє виявляти загрози та управляти

ризиками. Інтеграція цих методів у сучасні архітектури безпеки забезпечує більш високий рівень стійкості інформаційних систем до сучасних кіберзагроз, що робить їх ключовим компонентом комплексного захисту даних.

Матричні методи, зокрема сингулярне розкладання матриці (SVD), аналіз головних компонент (PCA) та негативне матричне факторизування (NMF), дозволяють виявляти латентні структури у даних доступу [3]. Наприклад, SVD може бути використане для побудови матриці доступу, де кожен елемент відображає силу зв’язку між користувачем і ресурсом, а низькорівневі сингулярні значення – потенційні аномалії. PCA дозволяє зменшити розмірність логів доступу, зберігаючи найбільш значущі компоненти, що сприяє швидкому виявленню відхилень. NMF, завдяки своїй інтерпретованості, дозволяє класифікувати запити за темами доступу та побудувати поведінкові шаблони користувачів.

Матриці суміжності використовуються для моделювання мережевих з'єднань між серверами баз даних та клієнтами. Аналіз власних значень цих матриць може допомогти виявити аномальну мережеву активність або несанкціоновані з'єднання.

Тензорні методи є узагальненням матричних моделей на багатовимірні дані, що включають часові, контекстні та структурні виміри. Вони дозволяють моделювати складні залежності між запитами, користувачами, типами доступу та часовими інтервалами. Тензорна факторизація, зокрема CP або Tucker розкладання [4], забезпечує виявлення багатовимірних патернів, що не доступні при двовимірному аналізі. Це особливо корисно для побудови адаптивних систем моніторингу, які враховують контекст доступу, історію взаємодій та динаміку змін у поведінці користувачів.

Матричні та тензорні підходи є перспективними напрямами оптимізації безпеки баз даних. Використання матричних та тензорних методів дозволяє ефективно моделювати, аналізувати та стискати великі обсяги даних безпеки, виявляючи приховані патерни та аномалії. Впровадження цих методів, особливо тензорного аналізу для багатовимірних даних, забезпечує значне підвищення рівня захисту інформаційних систем.

**Висновки**

1. Жоден із розглянутих підходів не є універсальним рішенням для всіх завдань безпеки баз даних. Графові методи чудово підходять для аналізу зв'язків, статистичні та ймовірнісні – для виявлення аномалій та оцінки ризиків, а матричні та тензорні – для ефективної обробки та компресії великих масивів даних.
2. Оптимізація безпеки баз даних майбутнього полягає в інтеграції цих методів у гібридні системи, які можуть використовувати сильні сторони кожного підходу для побудови багаторівневого, проактивного та інтелектуального захисту інформації.
3. Математичне моделювання в контексті безпеки баз даних є фундаментом для побудови інтелектуальних систем захисту, які здатні адаптуватися до нових загроз, масштабуватися відповідно до обсягів даних та забезпечувати стійкість цифрових екосистем.

**Література**

1. Pushap Goyal. (2025). The Role of Databases in Cybersecurity and Threat Detection: Advancements through Spanner Graph Technology. Journal of Computer Science and Technology Studies, 7(5), 544-557. https://doi.org/10.32996/jcsts.2025.7.5.61.

2. Habeeb Omotunde, & Maryam Ahmed. (2023). A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and

Beyond. Mesopotamian Journal of CyberSecurity, 2023, 115-133. https://doi.org/10.58496/MJCSC/2023/016.

3. Martin Stoll (2020) A literature survey of matrix methods for data science: GAMM - Mitteilungen published by Wiley-VCH GmbH on behalf of Gesellschaft f\xFCr Angewandte Mathematik und Mechanik. https://doi.org/10.1002/gamm.202000013.

4. Kolda, T.G. and Bader, B.W. (2009) Tensor Decompositions and Applications. SIAM Review, 51, 455-500. https://doi.org/10.1137/07070111X.