ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської
науково-практичної конференції

27 листопада 2025 року

м. Львів

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ПРИВАТНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ «ІТ СТЕП УНІВЕРСИТЕТ»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

27 листопада 2025 року

Львів – 2025

ББК 32.81+78.362

Інформаційна безпека та інформаційні технології: збірник тез доповідей VII Всеукраїнської науково-практичної конференції, м. Львів, 27 листопада 2025 року. Львів, ЛДУ БЖД, 2025, 493 с.

РЕДКОЛЕГІЯ:

Василь ПОПОВИЧ – доктор технічних наук., професор, проректор з наукової роботи, Львівський державний університет безпеки життєдіяльності

Олександр ПРИДАТКО – кандидат технічних наук, доцент, проректор з навчально-методичної роботи Львівського державного університету безпеки життєдіяльності

Роман ЯКОВЧУК – доктор технічних наук, доцент, начальник навчально-наукового інституту цивільного захисту, Львівський державний університет безпеки життєдіяльності

Ольга МЕНЬШИКОВА – кандидат фізико-математичних наук, доцент, заступник начальника навчально-наукового інституту цивільного захисту, Львівський державний університет безпеки життєдіяльності

БУРАК Назарій Євгенович – кандидат технічних наук, доцент, начальник кафедри інформаційних технологій та систем електронних комунікацій, Львівський державний університет безпеки життєдіяльності

ІВАНУСА Андрій Іванович – кандидат технічних наук, доцент, начальник кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності

НАЗАР Юлія Сергіївна – доктор філософії, заступник начальника кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ХЛЕВНОЙ Олександр Вікторович – кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

СМОТР Ольга Олексіївна – кандидат технічних наук, доцент, професор кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

БОРЗОВ Юрій Олексійович – кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ГОЛОВАТИЙ Роман Русланович – кандидат технічних наук, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ПИЛИПЕНКО Володимир Миколайович – старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ЖЕЗЛО-ХЛЕВНА Наталія Володимирівна – викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

РАЙТА Діана Анатоліївна – старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ДОВБНЯК Віра Йосипівна викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ПОЛОТАЙ Орест Іванович – кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності

БАЛАЦЬКА Валерія Сергіївна – викладач кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності

ТКАЧУК Ростислав Львович – доктор технічних наук, професор, професор кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

© ЛДУ БЖД, 2025

УДК 004.056:004.412.2

ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У СКБД НА ОСНОВІ ПОВЕДІНКОВОЇ АНАЛІТИКИ ТА НЕКОНТРОЛЬОВАНОГО НАВЧАННЯ

Микола ЦІКО[1], Ростислав ТКАЧУК[1,2], Артур ТКАЧЕНКО[1]
[1]Львівський державний університет безпеки життєдіяльності
[2]Національний університет «Львівська політехніка»

Анотація. *У роботі представлено інтелектуальну систему виявлення аномальної активності в базах даних, спрямовану на підвищення інформаційної безпеки в умовах зростання обсягів даних та кіберзагроз. Проведено аналіз сучасних методів детекції аномалій, нормативних вимог і доступних рішень, що підтвердило потребу у створенні адаптивного та модульного програмного комплексу. Обґрунтовано вибір технологічного стеку (Python, FastAPI, Scikit-learn, PostgreSQL, React) і алгоритму Isolation Forest для обробки SQL-запитів у режимі реального часу. Система реалізована як мікросервісна архітектура, яка забезпечує збір, класифікацію та візуалізацію логів, підтримує перенавчання моделі та інтеграцію в корпоративну інфраструктуру.*

Ключові слова*: аномалії в базах даних, інформаційна безпека, поведінкова аналітика, машинне навчання, логування, детекція загроз, моніторинг активності, мікросервісна архітектура.*

Abstract. *The paper presents an intelligent system for detecting abnormal activity in databases, aimed at improving information security in the face of growing data volumes and cyber threats. An analysis of modern methods of anomaly detection, regulatory requirements and available solutions was conducted, which confirmed the need to create an adaptive and modular software package. The choice of a technology stack (Python, FastAPI, Scikit-learn, PostgreSQL, React) and the Isolation Forest algorithm for processing SQL queries in real time is justified. The system is implemented as a microservice architecture that provides collection, classification and visualization of logs, supports model retraining and integration into corporate infrastructure.*

Keywords: *anomalies in databases, information security, behavioral analytics, machine learning, logging, threat detection, activity monitoring, microservice architecture.*

У сучасному цифровому середовищі інформація є ключовим ресурсом для економіки, обороноздатності та суспільного функціонування, а обсяг даних, що перевищив 100 зетабайтів і подвоюється приблизно кожні два роки, створює серйозні виклики для кіберзахисту. Бази даних залишаються одними з найбільш вразливих елементів IT-інфраструктури: 44 % інцидентів безпеки пов'язані з неправомірним доступом до СКБД, з яких значна частка — внутрішні загрози [1]. Традиційні засоби захисту — автентифікація, контроль доступу, шифрування — не завжди виявляють нетипову активність користувачів, тому критично важливим стає впровадження систем виявлення аномалій (Anomaly Detection Systems), зокрема на основі алгоритму Isolation Forest. Нормативні вимоги GDPR та ISO/IEC 27001 [6] і резонансні витоки даних, як у Equifax [1], підкреслюють необхідність практичних, адаптивних і ефективних рішень на основі Python, PostgreSQL, FastAPI та сучасних веб-фреймворків.

Зростання обсягів і критичності даних у фінансових, медичних та державних сервісах актуалізує застосування поведінкової аналітики. Понад 80 % інцидентів у СКБД пов'язані з компрометацією доступу, а приклад Equifax (2017) демонструє наслідки відсутності ефективного автоматичного моніторингу [1]. Традиційні механізми захисту не здатні розпізнавати інсайдерські атаки чи поступові відхилення поведінки користувачів, тому машинне навчання для аналізу SQL-запитів, аутентифікаційних подій і логів у реальному часі стає найбільш ефективним способом виявлення загроз.

Предметна область дослідження охоплює широкий спектр об'єктів контролю — SQL-запити, процедури автентифікації, зміну прав доступу, мережеві транзакції — та різноманітні джерела даних, такі як transaction logs, query logs, audit logs і системні журнали. Для виявлення аномалій застосовуються статистичні підходи, методи кластеризації, outlier-детекція та нейромережеві моделі. У контексті практичних систем безпеки особливо цінними є неконтрольовані алгоритми, здатні самостійно формувати модель «норми» та виявляти відхилення без потреби у великих мічених вибірках [2, 3]. Алгоритм Isolation Forest, на якому базується створений модуль, має низку переваг — лінійну складність, стійкість до викидів, здатність працювати зі стримінговими даними, а також сумісність із Python-екосистемою, що робить його одним із найефективніших методів для систем реального часу [2, 4].

Аналіз сучасних промислових рішень (IBM Guardium, Oracle Audit Vault, McAfee DAM) показав їх високу технічну надійність та масштабованість, однак водночас — значну вартість, складність налаштування та обмежену адаптивність для малих і середніх організацій. Open-source платформи (OpenDLP, Apache Spot) є економічно доступними, але нерідко обмежені функціонально або потребують значних інженерних доопрацювань. Це підтвердило необхідність створення програмного рішення, яке поєднує надійність, доступність, модульність і адаптивність, та є реалістичним в умовах корпоративних IT-інфраструктур.

На підставі порівняльного аналізу методів детекції аномалій обрано Isolation Forest як найбільш збалансований підхід. Він дозволяє працювати без мічених даних, забезпечує масштабованість для опрацювання потоків логів, підтримує аналіз у режимі реального часу та має низькі вимоги до ресурсів. Інтеграція цього алгоритму з FastAPI, PostgreSQL і Python-модулями забезпечує високу продуктивність та стабільність роботи [5, 6], що підтверджує практичну доцільність його застосування у створеній системі.

Розроблена система виявлення аномальної активності має модульну багаторівневу архітектуру, що включає клієнтську частину на React, серверну логіку на FastAPI, модуль машинного навчання з Isolation Forest, PostgreSQL та допоміжні сервіси. Така структура забезпечує масштабованість, незалежний розвиток компонентів та можливість гнучкого розширення. Взаємодія між модулями реалізована через REST API, що дозволяє інтегрувати систему у різні корпоративні середовища без потреби у глибокій перебудові їхньої інфраструктури.

Модуль машинного навчання завантажує попередньо треновану модель Isolation Forest, аналізує нові лог-події в режимі реального часу та записує результати класифікації у таблицю query_logs PostgreSQL, з активацією системи сповіщень при виявленні критичних відхилень. Функція адаптивного перенавчання через endpoint /retrain-model підтримує актуальність моделі та стійкість системи до змін поведінки користувачів. Центральна таблиця query_logs оптимізована індексами та денормалізацією для швидкого виконання запитів і побудови аналітичних візуалізацій, а логічна модель дозволяє додавати сутності users, roles або alerts для подальшого розширення. Інтерфейс користувача реалізовано як адаптивний дашборд з таблицями логів, графіками, фільтрами, мультимовністю, темною/світлою темою та експортом PDF, що забезпечує оперативне оновлення даних і швидке реагування аналітиків на загрози.

Система демонструє високу практичну цінність, забезпечує автоматизований моніторинг поведінки користувачів та дозволяє значно зменшити ризики порушення безпеки даних, що робить її актуальним та надійним інструментом у сучасних умовах зростаючих кіберзагроз.

Література

1. World Economic Forum. The Global Risks Report 2023: 18th edition [Електронний ресурс]. – Режим доступу: https://www.weforum.org/reports/global-risks-report-2023.

2. Ahmed M., Mahmood A. N., Hu J. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. – 2016. – Т. 60. – С. 19–31.

3. Ящук В. І., Івануса А. І., Маслова Н. О., Ткачук Р. Л., Брич Т. Б. Інтеграція баз даних вразливостей у СУІБ – шлях до підвищення кіберстійкості критичних систем, Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference. Drohobych: Donetsk National Technical University, 2025. pp. 60–65.

4. Ткачук Р. Л., Ткаченко А. М., Андріїв Р. Р. Розроблення та застосування експлойтів з подальшою інтеграцією в ботнет. Безпека інформаційних технологій : матеріали XIII Міжнародної науково-технічної конференції ITSec-2024 (Львів, 9–11 травня 2024 р.). Львів : ЛНУ ім. І. Франка, 2024. С. 200–202.

5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. – Geneva: ISO, 2022. – 33 p.

6. Ящук В.І., Івануса А.І., Маслова Н.О., Ткачук Р.Л., Брич Т.Б. Концептуалізація інтегративного використання баз даних вразливостей у контексті системного менеджменту інформаційної безпеки. Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. пр. Львів : ЛДУ БЖД, 2025. № 31. С. 126–139. DOI: https://doi.org/10.32447/20784643.31.2025.13

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

Відповідальні за випуск **Назарій БУРАК**
Олександр ХЛЕВНОЙ

Оригінал-макет **Юлія НАЗАР, Ольга СМОТР, Роман ГОЛОВАТИЙ, Діана РАЙТА, Віра ДОВБНЯК, Іван РОВЕЦЬКИЙ, Наталія ЖЕЗЛО-ХЛЕВНА**

Підписано до друку 12.11.2025 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 30.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.