

А. В. Грицак
А. С. Камінська

ВИКОРИСТАННЯ АНАЛІЗУ ДАНИХ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ І АНОМАЛЬНОЇ ПОВЕДІНКИ КОРИСТУВАЧІВ

Вінницький національний технічний університет

Анотація

У тезах розглядається аналіз методів Data Analysis та Machine Learning (ML) для проактивного виявлення кіберзагроз і аномальної поведінки користувачів. Акцент зроблено на архітектурі User and Entity Behavior Analytics (UEBA), яка використовує неконтрольоване навчання (Isolation Forest, Автоенкодеру) для побудови динамічних поведінкових профілів. Доведено, що для мінімізації операційних ризиків (хибних спрацювань) критично важливою є інтеграція контекстуального Feature Engineering (S-A-O). Робота також підкреслює необхідність впровадження Пояснюваного Штучного Інтелекту (XAI) для забезпечення прозорості алгоритмів, довіри до системи та дотримання етичних і правових норм конфіденційності.

Ключові слова: аналіз даних, кіберзагрози, аномальна поведінка, UEBA, машинне навчання, XAI.

Abstract

The thesis examines the analysis of Data Analysis and Machine Learning (ML) methods for proactive detection of cyber threats and anomalous user behavior. The focus is on the User and Entity Behavior Analytics (UEBA) architecture, which employs unsupervised learning techniques (such as Isolation Forest and Autoencoders) to build dynamic behavioral profiles. It is demonstrated that minimizing operational risks (false positives) critically depends on the integration of contextual Feature Engineering (S-A-O). The work also highlights the necessity of implementing Explainable Artificial Intelligence (XAI) to ensure algorithmic transparency, system trust, and compliance with ethical and legal privacy standards.

Keywords: Data Analysis, Cyber Threats, Anomalous Behavior, UEBA, Machine Learning, XAI.

Вступ

Нестримне зростання кіберзлочинності, посилене широкою інформатизацією, активним використанням хмарних сервісів та геополітичними конфліктами, зумовлює необхідність кардинального перегляду традиційних стратегій кіберзахисту. Класичні сигнатурні методи виявлення поступово втрачають ефективність у боротьбі з постійно адаптивними, цільовими атаками та загрозами нульового дня. У сучасних умовах безпеки ключовим імперативом стає перехід до проактивних систем, здатних ідентифікувати загрози ще до того, як вони спричинять шкоду.

Одним із найважливіших інструментів досягнення проактивності виступає аналіз даних (Data Analysis, DA) у поєднанні з технологіями машинного навчання (Machine Learning, ML). Застосування ML дає змогу автоматизувати процеси запобігання, класифікації та прогнозування подій безпеки шляхом обробки та інтерпретації великих обсягів інформації. Якщо традиційні підходи орієнтовані на виявлення вже відомих шаблонів (сигнатур), то методи, засновані на аналізі даних, фокусуються на виявленні відхилень у поведінці користувачів та мережевих об'єктів, що дає змогу фіксувати нові, невідомі загрози.

Разом з тим, впровадження технологій машинного навчання у сферу кібербезпеки залишається складним завданням. Наукові дослідження підтверджують, що швидкий розвиток ML відкриває значні можливості, однак водночас створює труднощі у виборі найбільш ефективних методів та засобів прийняття рішень. Крім того, технологія має двосторонній характер – зловмисники також застосовують алгоритми ML та генеративні моделі для створення більш витончених і замаскованих кібератак.

Отже, актуальність дослідження полягає у систематизації та вдосконаленні методів Data Analysis, Machine Learning, здатних ефективно протидіяти як відомим, так і невідомим (аномальним) кіберзагрозам, забезпечуючи підвищення рівня адаптивності та стійкості інформаційних систем.

Результати дослідження

Використання машинного навчання у кібербезпеці зараз тримається передусім на алгоритмах для класифікації типів загроз[1]. Однією з основних технологій тут стали штучні нейронні мережі - особливо моделі багатоваріантного перцептрону (MLP) з інверсним поширенням помилки. Вони добре навчаються на складних шаблонах і використовуються для автоматизованих систем, які "знають", на що слід звертати увагу, базуючись на індикаторах компрометації (IoC)[2]. Для роботи з такими моделями системи моніторингу збирають цілу купу різних даних: журнали мережевого трафіку, історію входів в систему, дані про місцезнаходження або незвичайний спосіб доступу, журнали по роботі з файлами та інформацію з кінцевих точок, серверів і застосунків[3]. Наприклад, ці класифікаційні моделі реально допомагають відділити DDoS-атаки від звичайного трафіку чи знаходять фішингові листи по підозрілих URL та аномальних заголовках[4].

Якщо говорити відверто, якість результатів таких ML-моделей дуже залежить від того, наскільки добре підготували вхідні дані. Ось чому попередній аналіз (Exploratory Data Analysis, EDA) стає буквально критичним у цій справі. Тут треба попрацювати з викидами, подивитися на розподіл даних через box plot'и чи діаграми розсіювання, збудувати кореляційні матриці, щоб краще зрозуміти структуру даних і підлаштувати модель[1]. EDA фактично допомагає одразу втримати під контролем ризики. Якщо неправильно знайти або обробити викиди, "нормальне" поведінка системи може вийти зовсім не такою, як треба: у підсумку купа нерелевантних тривог і жодної довіри до системи від команди безпеки[5]. Після цього, коли моделі вже працюють, їхню ефективність зазвичай оцінюють через Матрицю хибних спрацювань (Confusion Matrix). Це корисний інструмент, щоб зрозуміти, наскільки модель одночасно і точна (Accuracy), і достатньо чутлива (Recall), бо для швидкого реагування - як на ті ж DDoS - обидва показники важливі[1].

Аналітика поведінки користувачів та об'єктів (UEBA) - зараз це, мабуть, найбільш стратегічний підхід у кібербезпеці. Тут вже не шукають підписи чи відбитки відомих атак, а дивляться на поведінку користувача чи пристрою всередині мережі, щоб помітити підозрілі дії. Основна задача - побачити внутрішні загрози, зламані акаунти та інші дивні речі, які зазвичай передують інциденту[6]. UEBA-системи починають із масового збору всієї можливої інформації з різних джерел - мережеві логи, входи, дії з файлами[5]. Далі алгоритми визначають, як виглядає звичайна поведінка для кожного користувача або пристрою. Цей "нормальний" шаблон весь час оновлюється разом із новими даними[6]. UEBA - це вже база для наступного етапу: систем Виявлення та Реагування на Загрози Ідентифікації (ITDR), що особливо працюють проти атак на облікові записи та зловживань правами доступу. UEBA якраз дозволяє вчасно помітити такі речі, як спроби підвищити свої привілеї чи рухатися по мережі в обхід захистів - це якраз ті сигнали, на які і треба реагувати[7].

Для перетворення статистичної аномалії, виявленої алгоритмами неконтрольованого навчання, у підтверджену загрозу необхідне вдосконалення етапу Feature Engineering, що вимагає інтеграції семантичного та контекстуального аналізу, який виходить за межі лише обробки статистичних показників [8]. Ключовим підходом для зменшення FPR є використання архітектури «Суб'єкт-Дія-Об'єкт» (Subject-Action-Object, S-A-O), яка забезпечує контекстуальну узгодженість подій і дозволяє розрізняти технічні збої або випадкові відхилення від цілеспрямованих кібератак. Подія оцінюється за трьома основними параметрами: прогностичною узгодженістю – через аналіз розбіжності між очікуваною (прогнозованою моделлю) та фактичною послідовністю подій; контекстуальною узгодженістю (S-A-O) – через перевірку відповідності дії, виконаної суб'єктом щодо об'єкта, його історичному базовому профілю; та зміною стану ІКС – шляхом оцінювання змін у стані інформаційно-комунікаційної системи до і після виявлення аномалії [8]. Такий підхід підвищує операційну точність, оскільки збагачення сирих логів контекстом S-A-O перетворює статистичне попередження з високим FPR у високовірогідний інцидент безпеки, що суттєво зменшує операційне навантаження на команди SecOps.

Ефективність UEBA значно підвищується при його інтеграції з ширшим набором рішень кіберзахисту. Співпраця UEBA з інструментами, такими як Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) та Managed Detection and Response (MDR), дозволяє організаціям формувати уніфіковану платформу безпеки (Unified SecOps) [5]. Хоча EDR моніторить та реагує на інциденти на рівні індивідуальної кінцевої точки, UEBA аналізує поведінку користувачів та об'єктів у масштабі всієї мережі, включаючи ці кінцеві точки. Таке поєднання забезпечує більш надійний захист та повніше розуміння контексту загроз. Глибокий та постійний аналіз поведінки

користувачів, необхідний для функціонування UEBA (включаючи моніторинг часу входу, локації, доступу до даних), неминуче породжує серйозні етичні та правові ризики [5]. Зростання ролі кібербезпеки вимагає збереження тонкого балансу між забезпеченням захисту та дотриманням цифрових прав людини. Важливо, щоб політика безпеки включала забезпечення права на анонімність та конфіденційність [9]. Системи, що збирають і аналізують дані користувачів, повинні гарантувати належну згоду та застосування необхідних заходів приватності. Крім прямого ризику конфіденційності, використання складних алгоритмів AI створює проблему непрозорості (algorithmic opacity) та ризику упередженості навчальних моделей. Якщо алгоритми приймають рішення на основі упереджених даних, це може призвести до дискримінації або неправильного делегування відповідальності, що ускладнює етичне управління автоматизованими системами. Для вирішення проблем непрозорості та упередженості критично важливим є впровадження Пояснюваного Штучного Інтелекту (Explainable AI, XAI) [10]. XAI – це набір методик і інструментів, розроблених для того, щоб зробити процеси прийняття рішень AI-системами зрозумілими для людей [11]. XAI має подвійне значення. По-перше, він встановлює довіру до системи безпеки. Це дозволяє користувачам, клієнтам та особливо регуляторним органам сприймати та підтримувати прозорі AI-системи. По-друге, XAI є необхідним для команд безпеки (SecOps) для швидкого та якісного розслідування інцидентів. Якщо система UEBA повідомляє про аномалію, але не може пояснити логіку цього рішення, команді SecOps доводиться витрачати значно більше часу на ручний аналіз, щоб підтвердити, чи є оповіщення справжньою загрозою чи хибним спрацюванням. Таким чином, XAI безпосередньо сприяє скороченню часу реагування (Mean Time to Resolution, MTTR) та підвищує операційну ефективність. Очікується, що жорсткіші закони щодо прозорості AI, особливо у критичній інфраструктурі та фінансах, стануть головним стимулом для подальшого впровадження XAI [11]. Впровадження XAI вимагає ретельної оцінки компромісу між прозорістю та операційною ефективністю [12]. Хоча прозорість є етичною та операційною необхідністю, додавання механізмів пояснюваності може підвищувати обчислювальне навантаження та впливати на продуктивність системи. У кібербезпеці, де швидкість виявлення DDoS-атак та інших загроз у реальному часі є критичною, будь-яка затримка (Latency) може бути неприпустимою [12]. Необхідна розробка пояснюваних моделей, які є достатньо легкими для інтеграції, щоб не створювати значного уповільнення.

Після розгляду різних існуючих рішень запропонована багаторівнева адаптивна модель для перевірки контексту - ACVM (Адаптивна модель контекстуальної валідації). Основна її ідея: не просто знаходити кіберзагрози заздалегідь і з мінімумом помилкових спрацювань, а й пояснити кожне рішення, якого в багатьох сучасних системах бракує. Система працює без етапу ручного маркування - вона постійно збирає дані та автоматично створює "живий" шаблон поведінки для кожного користувача, пристрою чи сервісу. У процесі пошуку відхилень від норми система використовує неконтрольоване навчання, зокрема алгоритми Isolation Forest та автоенкодера, і швидко ловить дивні чи підозрілі дії у мережевих та поведінкових логах [13]. Виявлені підозрілі події далі одразу передаються на глибший аналіз за принципом "Суб'єкт-Дія-Об'єкт" (S-A-O) [8]. Це серце ACVM. Саме ця логіка допомагає не сплутати цілеспрямовану атаку - наприклад, коли хтось ізловив шкідливу програму і отримав прямий доступ до системи - із банальним технічним збоєм чи просто нестандартною легітимною поведінкою користувача. Після такого фільтрування залишається вже не просто сигнал, а інцидент, схожий на справжню загрозу, і більшість зайвих системних тривог відсіюється [11]. Тільки ті інциденти, які пройшли цей S-A-O аналіз, потрапляють до аналітиків (SecOps). До кожного попередження система додає пояснювальні дані за принципами XAI, тобто пояснює, чому саме спрацювало попередження. Це допомагає зрозуміти причину тривоги, швидше реагувати і, що важливо, довіряти системі більше.

Для швидкої реакції та цілісної картини ACVM найкраще реалізувати як частину одного середовища безпеки (Unified SecOps) - тут її модуль UEBA працює разом із SIEM та EDR. Така збірка дозволяє бачити все, що відбувається в режимі реального часу, і частково автоматизувати відповідь на небезпечні події [5].

Висновки

Проведене дослідження підтверджує, що сучасний кіберзахист не може ефективно функціонувати без широкого використання Data Analysis та Machine Learning. Технології ML, зокрема штучні нейронні мережі та багатошарові перцептрони, відіграють фундаментальну роль, забезпечуючи проактивне виявлення та класифікацію загроз на основі динамічних поведінкових патернів. Особливу ефективність демонструють системи UEBA, які завдяки алгоритмам неконтрольованого навчання, таким як Isolation Forest та автоенкодера, формують базові моделі поведінки та виявляють внутрішні загрози й скомпрометовані облікові записи. Водночас мінімізація операційного навантаження, спричиненого високим рівнем хибних спрацювань, потребує вдосконаленого Feature Engineering, що інтегрує прогностичну та контекстуальну узгодженість подій за архітектурою «Суб'єкт-Дія-Об'єкт» (S-A-O). Також критично важливим є впровадження Explainable AI (XAI), яке забезпечує етичну відповідність, прозорість та довіру команд SecOps до автоматизованих механізмів захисту.

Перспективи подальших досліджень включають поглиблене вивчення впливу XAI на продуктивність систем у режимі реального часу та розробку оптимізованих моделей пояснюваності, здатних працювати без значного збільшення затримок виявлення. Актуальним завданням залишається протидія Adversarial ML-технікам, де зловмисники використовують ML для приховування шкідливої активності, що потребує створення стійких до обману моделей. Крім того, важливо розробити стандартизовану архітектуру інтеграції, яка забезпечуватиме узгоджене впровадження контекстуального Feature Engineering (S-A-O) в екосистемі SecOps, такі як SIEM та EDR, що дозволить підвищити точність, знизити рівень хибних спрацювань і забезпечити високу швидкість реагування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A New Approach to Data Analysis Using Machine Learning for Cybersecurity URL: <https://www.mdpi.com/2504-2289/7/4/176> (дата звернення: 03.11.2025)
2. USE OF MACHINE LEARNING IN CYBER SECURITY URL: https://www.researchgate.net/publication/363292124_USE_OF_MACHINE_LEARNING_IN_CYBER_SECURITY (дата звернення: 03.11.2025)
3. UEBA (User and Entity Behavior Analytics) URL: <https://www.vpnunlimited.com/help/cybersecurity/ueba> (дата звернення: 05.11.2025)
4. Виявлення DDOS атак за допомогою машинного навчання URL: <https://ela.kpi.ua/server/api/core/bitstreams/12bad7f7-d715-445c-81fd-2fb091915b2e/content> (дата звернення: 05.11.2025)
5. What is user behavior analytics (UBA)? URL: <https://www.elastic.co/what-is/user-behavior-analytics> (дата звернення: 06.11.2025)
6. Що таке аналітика поведінки користувачів і сутностей (АПКС)? URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-user-entity-behavior-analytics-ueba> (дата звернення: 06.11.2025)
7. Що таке виявлення та реагування на загрози ідентифікаційним особам (ITDR)? URL: <https://stellarcyber.ai/uk/learn/what-is-identity-threat-detection-and-response/> (дата звернення: 06.11.2025)
8. Аналіз підходів до мінімізації хибних результатів у процесі виявлення аномалій системами кіберзахисту URL: https://www.researchgate.net/publication/395767696_Analiz_pidhodiv_do_minimizacii_hibnih_rezultativ_u_procesi_viyavlennja_anomalij_sistemami_kiberzahistu (дата звернення: 07.11.2025)
9. ІНФОРМАЦІЙНА БЕЗПЕКА: НОВІ ВИКЛИКИ ТА СТРАТЕГІЇ ЗАХИСТУ URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/09/60-2.pdf> (дата звернення 07.11.2025)
10. МОЖЛИВОСТІ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АУДИТУ ТА УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/872> (дата звернення: 07.11.2025)
11. Using Explainable AI (XAI) to Build Trust in Autonomous Cyber Defense Mechanisms URL: <https://medium.com/@RocketMeUpCybersecurity/using-explainable-ai-xai-to-build-trust-in-autonomous-cyber-defense-mechanisms-52be487127b7> (дата звернення: 08.11.2025)
12. Explainable AI (XAI) in Cybersecurity: Understanding AI-based Security Decisions URL: <https://akitra.com/explainable-ai-xai-in-cybersecurity/> (дата звернення: 08.11.2025)
13. How to perform anomaly detection with the Isolation Forest algorithm URL: <https://towardsdatascience.com/how-to-perform-anomaly-detection-with-the-isolation-forest-algorithm-e8c8372520bc/> (дата звернення: 08.11.2025)

Камінська Анна Сергіївна – студентка групи ІКІТС-226, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: akaanyaa@gmail.com

Науковий керівник: **Грицак Анатолій Васильович** – кандидат технічних наук, доцент, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: grytsak.a.v@gmail.com

Kaminska Anna S. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: akaanyaa@gmail.com

Supervisor: **Hrytsak Anatoly V.** – Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, e-mail: grytsak.a.v@gmail.com