

МОДЕЛЮВАННЯ ЗАГРОЗ ДЛЯ КСЗІ НА ОСНОВІ ПОВЕДІНКОВОГО АНАЛІЗУ КОРИСТУВАЧІВ (UEBA)

Вінницький національний технічний університет

Анотація

Це дослідження присвячене критичному аналізу та обґрунтуванню необхідності інтеграції технології User and Entity Behavior Analytics (UEBA) у Комплексні системи захисту інформації (КСЗІ) державних установ України. Актуальність роботи визначається суттєвою часткою кіберінцидентів (за даними CERT-UA, 31–38% інцидентів у 2023–2025 роках), які пов'язані з використанням легітимних, але компрометованих, облікових записів. Традиційні КСЗІ, що базуються на статичних правилах (НД ТЗІ 2.5-004-99), виявилися неспроможними своєчасно виявляти такі поведінкові зловживання. UEBA забезпечує принципово новий рівень деталізації аналізу шляхом побудови динамічних профілів та фіксації статистичних відхилень від нормальної поведінки користувачів та сервісів, що є фундаментом для динамічного моделювання загроз. У роботі розглянуто ключові архітектурні шари UEBA (збір, нормалізація, аналіз поведінки за допомогою Deep Autoencoder та Isolation Forest), а також деталізовано виклики, пов'язані з якістю даних, законодавчими обмеженнями приватності та кадровим забезпеченням у державному секторі. Зроблено висновок про те, що UEBA є не додатковим, а необхідним фундаментом для забезпечення кіберстійкості критичної інфраструктури.

Ключові слова: UEBA, комплексна система захисту інформації (КСЗІ), динамічне моделювання загроз, поведінковий аналіз, інсайдерські загрози, машинне навчання, державний сектор, SOC.

Abstracts

This study is devoted to a critical analysis and justification of the need to integrate User and Entity Behaviour Analytics (UEBA) technology into the Comprehensive Information Security Systems (CISS) of Ukrainian state institutions. The relevance of this work is determined by the significant proportion of cyber incidents (according to CERT-UA, 31–38% of incidents in 2023–2025) associated with the use of legitimate but compromised accounts. Traditional ISAS based on static rules (ND TZI 2.5-004-99) have proven incapable of detecting such behavioural abuses in a timely manner. UEBA provides a fundamentally new level of analysis detail by building dynamic profiles and recording statistical deviations from normal user and service behaviour, which is the foundation for dynamic threat modelling. The paper examines the key architectural layers of UEBA (collection, normalisation, behaviour analysis using Deep Autoencoder and Isolation Forest), and details the challenges associated with data quality, legislative privacy restrictions and staffing in the public sector. The conclusion is that UEBA is not an additional but a necessary foundation for ensuring the cyber resilience of critical infrastructure.

Keywords: UEBA, comprehensive information security system (CISS), dynamic threat modelling, behavioural analysis, insider threats, machine learning, public sector, SOC.

Вступ

Проблема забезпечення кіберстійкості державних інформаційних систем набуває стратегічного значення в умовах постійних цільових атак (АРТ). Традиційна парадигма захисту, вбудована у більшість Комплексних систем захисту інформації (КСЗІ), орієнтована на статичні сигнатури і правила, що робить її вразливою перед обличчям сучасних загроз. Ключовий недолік полягає в тому, що традиційні системи нездатні ефективно виявляти загрози, які походять від легітимних облікових записів.

Для подолання цієї критичної прогалини застосовується технологія User and Entity Behavior Analytics (UEBA). UEBA – це фундамент для динамічного моделювання загроз, що аналізує поведінку користувачів та сутностей (сервісів, API) для побудови багатовимірних моделей «нормальної поведінки». Вона постійно адаптується, забезпечуючи принципово новий рівень деталізації аналізу та виявляючи відхилення від статистичної норми. UEBA інтегрується з SIEM та SOC і використовує передові методи глибокого навчання, зокрема Deep Autoencoder та Isolation Forest, для аналізу великих обсягів телеметрії та надання пояснювальних висновків.

Архітектура UEBA передбачає створення циклу аналізу. По-перше, здійснюється збір даних з широкого спектру джерел, включаючи AD, VPN, API-логування та контейнерні середовища. По-друге, виконується нормалізація й кореляція даних, вирівнюються часові мітки та забезпечується

консистентність, критична для якості моделей. По-третє, здійснюється аналіз поведінки за допомогою гібридних алгоритмів машинного навчання. По-четверте, виявлена аномалія отримує risk-score, що враховує контекст та привілеї. Таким чином, UEBA дозволяє формувати Поведінкову карту загроз (Threat-Behavior Map), що є проактивною, прогностичною моделлю захисту [1].

Результати дослідження

Застосування UEBA – це не просто додатковий рівень захисту. Це фундамент для моделювання загроз, який допускає побудову динамічних карт загроз, адаптування під поведінку користувачів, контекст взаємодій і організаційні особливості. Забезпечує принципово новий рівень деталізації аналізу поведінки користувачів та сервісів, а також дозволяє виявляти складні атаки, що залишаються непоміченими в умовах традиційних систем безпеки. Аналіз даних CERT-UA за 2023–2025 роки показав, що 31–38 % інцидентів було пов’язано з використанням легітимних облікових записів, які зловмисники отримували або шляхом фішингу, або через слабкий контроль привілейованих доступів [2]. Традиційні КСЗІ, що відповідають НД ТЗІ 2.5-004-99, не здатні своєчасно виявляти такі зловживання, оскільки працюють переважно за правилами. UEBA ж дозволяє фіксувати відхилення у поведінці користувача від його статистичної норми, що робить цей інструмент надзвичайно ефективним.

Проблеми, виклики та ризики впровадження UEBA у державному секторі

Незважаючи на значні переваги, впровадження UEBA у КСЗІ державних установ України стикається з низкою суттєвих бар’єрів:

1. Якість та обсяг даних: для коректної роботи поведінкових алгоритмів потрібна велика кількість даних (логів) та їх якість. Часто державні системи не мають централізованого збирання логів або ведуть їх у різних форматах, що ускладнює нормалізацію. Без синхронізації часових міток (time sync) та структурованих форматів (наприклад, JSON або CEF) моделі UEBA можуть бути неточними або непридатними.

2. Приватність та законодавчі обмеження: аналіз поведінки користувачів може створювати ризики порушення приватності або GDPR-подібних вимог (або українських законів про захист персональних даних). Необхідно впроваджувати політики доступу до логів, анонімізації або псевдонімізації, а також чіткі процедури аудиту аналітичних висновків UEBA, щоб мінімізувати ризик зловживань.

3. Кадрові та організаційні питання: UEBA потребує правильно навчених аналітиків SOC, які розуміють поведінковий аналіз, можуть інтерпретувати risk-scores, налаштовувати моделі та реагувати на сповіщення. Без “human-in-the-loop” системи UEBA можуть генерувати велику кількість хибних спрацювань, що призведе до “втоми сповіщень” та зниження ефективності.

4. Автоматизація реакції: виклик автоматичних дій (playbook) при високому risk-score повинен бути збалансований: надмірні блокування можуть порушити критично важливі державні процеси, тоді як недостатня реакція знижує ефективність. Треба продумати правила, які враховують контекст (наприклад, привілеї користувача, важливість ресурсу, історію поведінки).

5. Масштабування: у державному секторі дуже важливо, щоб UEBA рішення можна було масштабувати: централізоване збирання і аналіз логів, федеративна архітектура (де окремі установи передають дані до спільного аналітичного шару), балансування навантаження, висока доступність SOC. Без правильної архітектури масштабування може бути технічно складним або дуже затратним [3].

При розгортанні UEBA в КСЗІ державних установ до архітектури входять кілька взаємопов’язаних шарів, таких як:

– Збір даних: телеметрія формується з численних джерел: журнали доступу (access logs), події Active Directory, події VPN, події мережевого трафіку, API-логування, події контейнерних середовищ, систем контейнеризації (наприклад, Kubernetes), а також події з системи управління привілеями (PAM). Державні органи все частіше переходять у хмарні середовища, зокрема на державні хмарні платформи, що вимагає логування контейнерних сервісів, API-викликів та взаємодій між сервісами.

– Нормалізація й кореляція: у цьому шарі всі отримані дані стандартизуються: події приводяться до єдиного формату, вирівнюються часові мітки (time-sync), забезпечується кореляція подій з різних систем. Це критично, оскільки якість поведінкових моделей UEBA безпосередньо залежить від консистентності даних.

– Аналіз поведінки: тут застосовуються алгоритми машинного навчання й аналітики. Найкращими є гібридні моделі, які поєднують unsupervised алгоритми (наприклад, Isolation Forest, Autoencoder) для виявлення невідомих аномалій та supervised чи ансамблеві підходи для класифікації відомих загроз.

Deep Autoencoder дозволяє не тільки виявляти відхилення, але й реконструювати їх потенційне походження, що підвищує пояснюваність.

- Scoring та ранжування ризику: коли аномалія виявлена, систему UEBA присвоює їй risk-score – показник ризику з урахуванням контексту, привілеїв сутності, історії поведінки, типу ресурсу, який доступався. Ці ризикові оцінки можуть інтегруватися з SOC-playbook, системами автоматичної реакції або вручну розглядатися аналітиками.

- Інтеграція з SOC та реагування: у сучасних KCSI UEBA не існує ізольовано – вона підключається до SOC, де її сигнали використовуються для триажу інцидентів. Після оцінки ризику можуть спрацьовувати playbook'и, наприклад, ізоляція користувача, повторна аутентифікація, обмеження сесій, запит на додаткове підтвердження дій користувача тощо. Також UEBA може бути інтегрована з системою threat intelligence, щоб підсилити результати через інформацію про відомі вектори атак або агресивні кампанії (наприклад, з кластерів UAC, які відстежує CERT-UA).

- Зворотній зв'язок і адаптація: ефективне UEBA в державному контексті вимагає циклу “human-in-the-loop”: аналітики SOC розглядають аномалії, коректують моделі, дають зворотний зв'язок, моделі навчаються з новими даними. Це дозволяє системі адаптуватися до організаційних змін, нових шаблонів поведінки або змін у політиках доступу [4].

В контексті переходу Комплексних систем захисту інформації (КCЗІ) до поведінково-орієнтованої безпеки, однією з ключових практик дослідження та реалізації є побудування Поведінкової карти загроз (Threat-Behavior Map). Ця карта слугує не статичним переліком, а динамічною моделлю загрози (Threat Model), яка інтегрує аналіз активності користувачів, їх взаємодії, історію, привілеї та контекст ресурсів, що дозволяє не лише виявляти поточні аномалії, але й прогнозувати можливі сценарії атак. Карта включає в себе п'ять основних, критично важливих категорій поведінкових загроз:

По-перше, карта деталізує Потенційні загрози інсайдерів. Ці загрози походять від користувачів, які працюють із привілеями і використовують свої легітимні права для зловмисних або несанкціонованих дій. Сюди відноситься виявлення таких аномальних дій, як запуск скриптів PowerShell у нетипових директоріях або у нетиповий час, звернення до конфіденційних баз даних (СУБД) із виконанням нехарактерних запитів, копіювання цілого сегмента даних, що значно перевищує звичайний робочий обсяг, а також робота в нетиповий час (наприклад, глибока ніч або вихідні дні), якщо така активність супроводжується маніпуляціями з критичними даними чи конфігураціями.

По-друге, карта охоплює Зовнішні компрометації облікових записів. Тут ключовий акцент робиться на тому, що навіть якщо обліковий запис є формально легітимним та успішно пройшов аутентифікацію, аномалії поведінки можуть вказувати на використання крадених облікових даних. Такі аномалії включають: нетипову географію доступу (Impossible Travel), коли вхід здійснюється з двох віддалених точок одночасно, використання нових або невідомих пристроїв, а також незвичні API-виклики до корпоративних чи хмарних сервісів, які раніше цим користувачем не виконувались. UEBA дозволяє ідентифікувати цю зміну "відбитка" облікового запису.

По-третє, важливим напрямком є виявлення Міжсервісних атак (хмарних). В архітектурі мікросервісів та хмарних додатків UEBA фокусується на поведінці нелюдських сутностей. Загрози ідентифікуються через неправомірне використання API, наприклад, коли сервіс використовує функцію, яка виходить за рамки його дозволів, надмірну кількість запитів до іншого сервісу, що може бути ознакою сканування або спроби підризу сервісу (Denial of Service), а також аномальну взаємодію між мікросервісами, коли комунікація відбувається між компонентами, які за штатною архітектурою не повинні взаємодіяти.

По-четверте, карта приділяє особливу увагу Повільним, прихованим атакам (slow-and-low). Це найбільш підступні атаки, які розгортаються протягом довгого часу з низькою інтенсивністю, спеціально щоб оминати порогові значення традиційних систем. UEBA виявляє ці загрози не через окремі події, а через відхилення поведінки, які накопичуються, або через кореляцію незвичних патернів у часі. Наприклад, це може бути послідовний, але дуже рідкий доступ до різних робочих станцій протягом місяця, що зрештою призводить до компрометації привілейованого облікового запису.

Нарешті, карта моделює Підозрілу ескалацію привілеїв. Цей сценарій виникає, коли користувач або сервіс починає робити дії, які не властиві його штатній ролі. Приклади включають: створення нових облікових записів або додавання існуючих до адміністраторських груп, виконання адміністраторських дій чи змін у конфігурації, які не відповідають рівню доступу, а також спроби використання інструментів для підвищення власних привілеїв.

Таким чином, Поведінкова карта загроз перетворює пасивне спостереження на прогностичну модель, що дозволяє UEBA оцінювати сукупний ризик поведінки, а не ізольованих подій, що є критично важливим для забезпечення кіберстійкості в умовах сучасних загроз [4].

Приклад конкретного сценарію впровадження

Уявімо пілотний проєкт UEBA у великому міністерстві України, яке використовує державну хмару (G-Cloud) для розміщення реєстрів і веб-сервісів. Архітектура включає централізований SIEM, агрегатор логів, аналітичний шар UEBA, SOC. Телеметрію збирають з AD, API-логів, контейнерів Kubernetes, VPN.

Алгоритм UEBA: deep autoencoder + isolation forest + supervised класифікатор для відомих загроз. Модель навчається на даних протягом місяця, потім впроваджується в production. Після навчання система виявляє аномальну поведінку мікросервісів: один із контейнерів API починає генерувати значно більше запитів, ніж зазвичай, ймовірно через data scraping або атаку. UEBA присвоює risk-score = високий, SOC активує playbook: перевірка контейнера, ізоляція, рев'ю логів, повторна аутентифікація сервісу.

У цьому ж проєкті UEBA виявляє поведінкову аномалію для адміністраторського облікового запису. Адміністратор виконує скрипт PowerShell у нічний час, що не характерно для його типового профілю. Система генерує попередження, аналітики перевіряють це, виявляють потенційну спробу privilege escalation або lateral movement, реагують відповідно (playbook + вручну).

Такі сценарії вже підтверджені у поточних світових дослідженнях та публікаціях UEBA-фреймворків, серед яких згаданий вище підхід із Deep Autoencoder [5].

Висновки

Інтеграція User and Entity Behavior Analytics (UEBA) у Комплексну систему захисту інформації державного сектору є стратегічною необхідністю, а не лише технічним удосконаленням, що дозволяє перейти від реактивного, сигнатурного захисту до проактивного, адаптивного моделювання загроз. Ефективність UEBA підтверджується її здатністю виявляти складні поведінкові аномалії, які є ознаками інсайдерських загроз та цільових атак: від компрометації VPN-доступів, що є ключовим каналом проникнення, до підозрілої активності адміністраторів (наприклад, виконання скриптів PowerShell у нерегламентований час) та спроб непомітної зміни ролей користувачів у державних реєстрах. UEBA перетворює пасивне спостереження на прогностичну модель, що дозволяє оцінювати сукупний ризик поведінки, а не ізольованих подій, що є критично важливим для забезпечення кіберстійкості.

Незважаючи на значні переваги, успішне впровадження UEBA у державний сектор стикається з низкою суттєвих бар'єрів, які необхідно долати комплексно. По-перше, для коректної роботи алгоритмів необхідно вирішити питання якості та обсягу даних, що вимагає централізації та нормалізації логів та обов'язкової синхронізації часових міток. По-друге, критичним є питання приватності та законодавчих обмежень, оскільки аналіз поведінки вимагає суворого дотримання вимог до захисту персональних даних шляхом впровадження політик анонімізації/псевдонімізації та чітких процедур аудиту. По-третє, важливими є кадрові та організаційні питання, оскільки UEBA потребує правильно навчених аналітиків SOC, здатних інтерпретувати risk-scores, щоб уникнути "втоми сповіщень" від хибних спрацювань. По-четверте, виклик автоматизації реакції вимагає розробки збалансованих playbook'ів, які дозволяють оперативно реагувати при високому ризyku, не порушуючи при цьому критично важливі державні процеси. Нарешті, для великих державних структур необхідне масштабування UEBA із застосуванням федеративної архітектури для централізованого аналізу даних. Таким чином, хоча виклики впровадження UEBA у державний сектор є значними, її потенціал у підвищенні кіберстійкості та виявленні інсайдерських загроз та компрометації облікових записів робить її ключовим елементом сучасної КСЗІ. Це фундаментальний крок до забезпечення безпеки в умовах, коли легітимність доступу більше не є синонімом безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Технологія User and Entity Behavior Analytics (UEBA). URL: https://itpro.ua/post/ot_kakikh_ugroz_zashchishchayut_samoobuchayushchiesya_sistemy_klassa_ueba?srslti_d=AfmB0oqmZquedYxNW-9wA-1geSocxCXfQm1fl_007w_uZ85h450AwA6u (дата звернення: 20.11.2025).
2. Аналіз CERT-UA. URL: <https://cert.gov.ua/article/6284080> (дата звернення: 22.11.2025).
3. Проблеми впровадження системи аналітики поведінки користувачів та сутностей (UEBA). URL:

<https://openarchive.nure.ua/entities/publication/f8c440a3-5f00-4738-8e50-ec6dbd77c84d> (дата звернення: 25.11.2025).

4. Архітектура моделювання загроз через UEBA. URL: <https://iitd.ua/analiz-povedinki-koristuvachiv-ta-subyektiv-ueba/> (дата звернення: 25.11.2025).

5. Приклад конкретного сценарію впровадження. URL: https://arxiv.org/abs/2505.11542?utm_source (дата звернення: 27.11.2025).

Магденко Анастасія Романівна – студентка групи 1KITC-226, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: anastasiamahdenko@gmail.com

Науковий керівник: **Павловський Павло Валерійович** – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: prepod@vntu.edu.ua

Mahdenko Anastasiia R. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: anastasiamahdenko@gmail.com

Supervisor: **Pavlovsky Pavlo V.** – assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: prepod@vntu.edu.ua