DOI: https://doi.org/10.26642/ten-2025-2(96)-128-135
УДК 004.056.5:004.89:656.2(477)

Д.І. Прокопович-Ткаченко, к.т.н., доц.
Л.В. Рибальченко, к.е.н., доц.
Університет митної справи та фінансів
І.М. Козаченко, начальник підрозділу
Державний центр кіберзахисту
Державної служби спеціального зв'язку та захисту інформації
В.Г. Бушков, аспірант
Державний торговельно-економічний університет
Б.С. Хрушков, аспірант
Університет митної справи та фінансів

Когнітивні методи протидії інсайдерським і складним кібератакам: аналіз інциденту в ІТ-інфраструктурі АТ «Укрзалізниця»

23 березня 2025 року в ІТ-системі АТ «Укрзалізниця» було зафіксовано масштабний технічний збій, що призвів до тимчасової недоступності онлайн-сервісів з продажу квитків, блокування сервісних каналів комунікації та втрати доступу до критичних операційних даних.

Досліджено, що цей інцидент має характеристики складеної кібератаки, яка враховує традиційні вектори зовнішнього втручання (наприклад, атак на вебдодатки та платформи електронного обслуговування), а також потенційний інсайдерський компонент, що підсилює руйнівний ефект. Актуальність дослідження пов'язана з необхідністю виявлення та протидії подібним комплексним загрозам, де традиційні засоби моніторингу й реагування виявляються недостатньо ефективними. У статті запропоновано когнітивні методи індикації інсайдерських і складених кібератак, зокрема гібридні системи штучного інтелекту, що поєднують символічні та нейромережеві методи аналізу подій. Розкрито можливості поведінкової аналітики, Bayesian Belief Networks, Graph Neural Networks та інших моделей, спрямованих на інтеграцію фрагментарних сигналів та онтологічну реконструкцію атаки. Обґрунтовано необхідність вбудовувати когнітивні агенти у процеси збору та обробки даних з різноманітних інформаційних каналів, щоб своєчасно виявляти аномальні шаблони у діяльності співробітників, контрагентів і зовнішніх підключень.

Зроблено висновок про доцільність формування єдиного національного когнітивного центру реагування на інциденти в критичній ІТ-інфраструктурі, який би інтегрував поведінковий, статистичний та онтологічний аналіз подій. Окреслено перспективи застосування таких систем у реальному масштабі критично важливих об'єктів, а також можливі обмеження і напрями подальших наукових досліджень у галузі кібербезпеки.

Ключові слова: *кібератака; штучний інтелект; інсайдерські загрози втручання; багатомірний аналіз; когнітивні агенти.*

Актуальність теми. Сучасні дослідники в галузі кібербезпеки наголошують на зростанні кількості інсайдерських загроз, зумовлених як недбалими діями персоналу, так і навмисним шкідливим втручанням [3]. У поєднанні з поширеними методами зовнішнього зламування такі загрози можуть утворювати складні (композитні) атаки, що підвищує складність їхнього виявлення [4]. Традиційні системи моніторингу (наприклад, SIEM-рішення) переважно зосереджені на потоці подій рівня мережевих протоколів або лог-файлів, але не завжди враховують глибинні поведінкові чи контекстуальні індикатори [5].

Аналіз останніх досліджень та публікацій, на які спираються автори. Тема інсайдерських загроз глибоко досліджена у працях [7–9], де розглядаються переважно поведінкові моделі персоналу та психометричні маркери ризику. Пропонується методологія когнітивної аналітики, що містить ймовірнісні графові моделі (Bayesian Belief Networks) і гібридні системи штучного інтелекту, які активно розвиваються у дослідженнях [10–12]. Відомо, що на теоретичному рівні сформувався підхід до поєднання різних джерел даних (лог-файлів, телеметрії, HR-метрик, соціальної інженерії) у єдиний багатовимірний простір аналізу [13]. Це дозволяє розширити горизонти та глибину детектування загроз.

Метою статті є аналіз інциденту в ІТ-інфраструктурі АТ «Укрзалізниця» із застосуванням когнітивних методів для дослідження зовнішніх факторів, які впливають на інсайдерські дії. Важливо проілюструвати ефективність когнітивних агентів та інтегрованих когнітивних систем для детекції аномальної поведінки. Практичною цінністю варто вважати можливість оцінити, наскільки впровадження штучного інтелекту й онтологічних підходів покращує виявлення інцидентів у режимі реального часу.

А також запропонувати рекомендації щодо розвитку національного сегмента центрів реагування на інциденти, орієнтованих на когнітивний аналіз загроз.

Викладення основного матеріалу. Розбудова складних інформаційних систем та критичних інфраструктур, таких як мережа АТ «Укрзалізниця», неминуче супроводжується підвищеними ризиками кібератак. Сучасні атаки часто мають полівекторний та комбінований характер, коли застосовуються різні технічні вектори проникнення у поєднанні з соціально-інженерними техніками та потенційно інсайдерськими втручаннями [1, 2]. Інцидент, що стався 23 березня 2025 року, став показовим для аналізу: зупинка онлайн-сервісів та блокування функціоналу призвели до відчутних економічних втрат, а також до соціального резонансу.

Наукова та практична цінність цього дослідження полягає у застосуванні когнітивних підходів, що об’єднують методи штучного інтелекту та онтологічної аналітики, дають можливість створювати системи глибшого розуміння процесів, які відбуваються усередині складних IT-інфраструктур. Такі підходи дозволяють не лише реагувати на відомі патерни загроз, а й прогнозувати потенційно нові сценарії атаки та раніше невідомі вектори проникнення [6].

Інтерфейс сервіс-додатків АТ «Укрзалізниця» на момент фіксації інциденту наведено на рисунку 1.

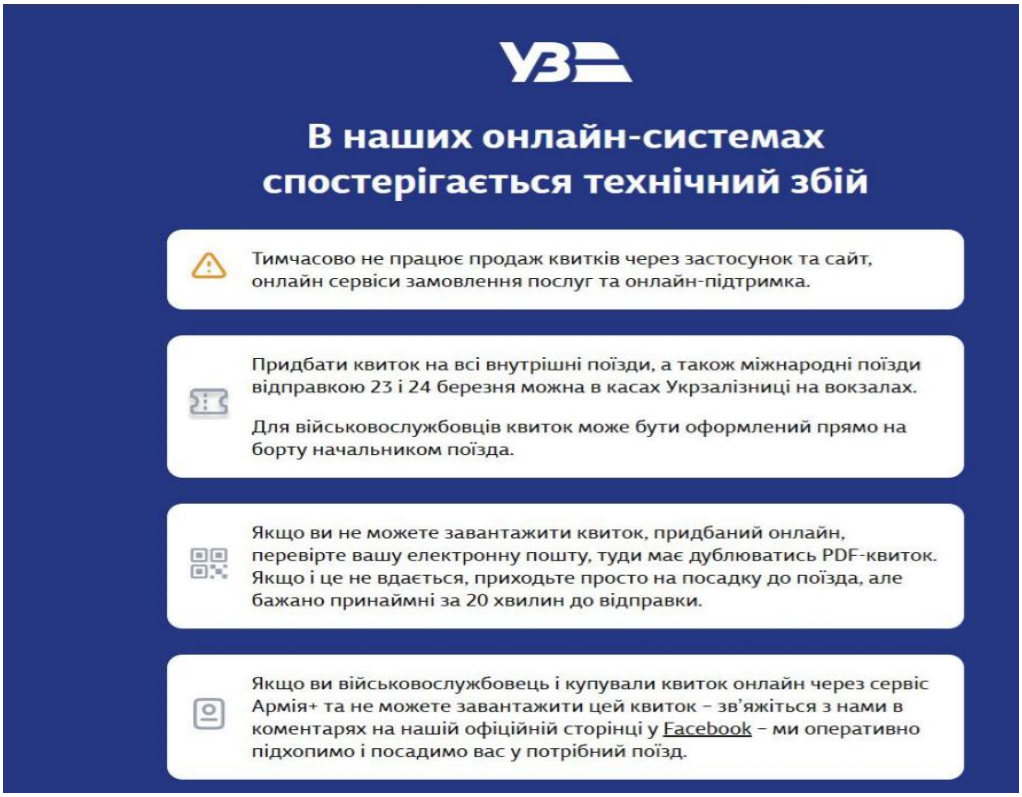

Рис. 1. Інтерфейс сервіс-додатків АТ «Укрзалізниця» на момент фіксації інциденту

У дослідженні застосовано когнітивні алгоритми та інтегровані статистичні методи, що ґрунтуються на підході, де об’єднуються дослідження у галузі поведінкової аналітики, ймовірнісних моделей та кібербезпеки.

Застосування ситуаційного аналізу (Situation Awareness) передбачає систематичний збір, обробку та інтерпретацію даних з різних джерел (логи подій, мережеві трафіки, журнали автентифікації, файлові активності, показники систем моніторингу тощо) з метою реконструкції загальної картини атаки [14]. Для цього використовується змішаний (Mixed Methods) підхід: якісний аналіз (виявлення нетипових поведінкових сценаріїв) поєднується з кількісною оцінкою ризиків та частоти інцидентів. Крім того, здійснюється порівняльний аналіз із попередніми кібератаками в організаціях залізничного сектору (дані за 2014–2024 роки), що дозволяє виокремити потенційні шаблони атаки, характерні саме для критичних транспортних систем [15].

Когнітивні системи можуть враховувати семантичні та контекстуальні індикатори (наприклад, аномальна поведінка користувача у нічний час або поза межами робочого приміщення) і поєднувати їх із логічними правилами, закладеними у систему [16]. При цьому проводиться онтологічний аналіз, а саме будується формальне уявлення (онтологія) про можливі сценарії атаки, зв’язки між учасниками процесу, типами ресурсів і вразливостей.

Важливо створити моделі виявлення інсайдерів. Наприклад, при інсайдерській загрозі часто застосовується підхід Bayesian Belief Network (BBN), де події (наприклад, багаторазове неправильне введення пароля, незвичайні операції з БД, використання USB-носіїв без дозволу) слугують вузлами в мережі, а ймовірності їх взаємозв'язків оновлюються в реальному часі.

Для детального аналізу авторами пропонується формальна модель (1), яка відображає сумарну апостеріорну ймовірність $P(\text{Insider})$ на основі сукупності ознак $E = \{e_1, e_2, \dots, e_n\}$:

$$P(\text{ Insider } \mid E) = \frac{P(E \mid \text{ Insider }) \cdot P(\text{ Insider })}{P(E)}. \quad (1)$$

Оскільки $P(E)$ може бути розкладено як $P(E) = (P(E \mid \text{Insider}) \cdot P(\text{Insider}))/P(\text{Insider} \mid E)$, система має змогу динамічно оновлювати оцінку ризику інсайдерської активності при надходженні нових даних [17, 18].

Використання Graph Neural Networks (GNN) для виявлення складених атак дозволило відобразити сукупність подій та взаємодій (включно з користувачами, системами, сервісами) у вигляді графа, де вершини – це суб'єкти чи об'єкти (користувач, сервер, база даних), а ребра – канали зв'язку та дії (HTTP-запити, SQL-запити, файлові операції тощо) [19].

У контексті складених атак кожна вершина чи ребро містить фічі (наприклад, час доби, тип операції, критичність даних), на основі яких GNN навчається визначати, чи є цей фрагмент графа підозрілим.

Для таких вихідних даних може бути побудована формальна модель (2), яка узагальнено демонструє функцію Γ, що оновлює векторний стан кожної вершини v_i на k-й ітерації, виходячи зі станів її сусідів $N(i)$:

$$h_i^{(k)} = \Gamma\left(h_i^{(k-1)}, \left\{h_j^{(k-1)} \mid j \in N(i)\right\}\right), \quad (2)$$

де $h_i^{(k)}$ – вектор стану (ембедінг) вершини і на ітерації k, а Γ – нелінійна функція, яку параметризує нейронна мережа.

Наприкінці процесу формується глобальна оцінка ризику для всього графа чи для окремих його підграфів, що відображає імовірність складеної атаки [20].

Для аналізу інциденту 23 березня 2025 року було сформовано вибірку з понад 12 мільйонів подій безпеки за період 01.03.2025–22.03.2025 включно із:

a) записами SIEM-системи (мережеві події, ідентифіковані можливі вразливості);
b) логами серверів вебдодатків і баз даних;
c) HR-даними про робочі графіки, зміни персоналу, доступи до ресурсів.

Також додатково було зібрано інформацію про аномальні входи та автентифікації з нетиповими IP-адресами і часовими поясами.

Результати емпіричного аналізу наведено в таблиці 1, відображено застосовані параметри та опис застосованих методів когнітивної детекції загроз.

Таблиця 1

Параметри та опис застосованих методів когнітивної детекції загроз

Параметр	**Опис**	**Джерело даних**
Період збору	01.03.2025–22.03.2025	Архівні логи, SIEM
Кількість подій	12000000 +	Сумарно за всі джерела
Типи даних	Мережеві, файлові, HR, записи доступів	Лог-файли, SIEM, дані контролю
Кількість підозрілих підмереж	18	Виявлено за допомогою IDS/IPS та ранньої аналітики
Метод виявлення інсайдерів	Bayesian Belief Networks, когнітивна аналітика	SIEM-агрегатори, платформи AI/ML
Метод виявлення складених атак	Graph Neural Networks, кореляційний аналіз	Власна реалізація + модулі Python

Довідка: розробка авторів

Усі методи дослідження реалізовано з використанням інструментарію мов програмування Python та *R* з додатковими бібліотеками для побудови Bayesian Networks (наприклад, pgmpy) та для моделювання GNN (бібліотеки PyTorch Geometric і DGL).

На основі викладеного дослідження, проведено багатовимірний аналіз інциденту в IT-інфраструктурі АТ «Укрзалізниця», що стався 23 березня 2025 року.

Виявлено, що за тиждень до інциденту значно зросла кількість несанкціонованих спроб доступу до внутрішніх серверів (приблизно на 40 % проти середньомісячних показників). При цьому одночасно зареєстровано збільшення внутрішньомережевих перенаправлень даних з маркетингового підрозділу до

віддалених IP-адрес, які належать незареєстрованим партнерам. В цілому система BBN продемонструвала зростання апостеріорної вірогідності сценарію «інсайдерська загроза» від початкових 0,02 до 0,25 (у день перед інцидентом), що є суттєвим сигналом підвищеного ризику.

Впроваджені когнітивні агенти аналізували поведінку користувачів у контексті операційних ролей: виявлено ряд аномалій (наприклад, робітники технічного відділу здійснювали доступ до маркетингової CRM-системи без узгодженого дозволу). Побудована система дозволила об'єднати логічні правила (як-от: «доступ до високочутливих сегментів повинен здійснюватися лише у робочий час, окрім випадків аварійного обслуговування») із шаблонами з машинного навчання (наприклад, «аудитор ідентифіковано у системі у нетиповий день»).

Моделювання складених атак за допомогою GNN дало можливість проаналізувати граф взаємодій (події за 20.03.2025–22.03.2025) та виявити кілька щільно пов'язаних підграфів, у яких вирішальну роль відігравали два внутрішні вузли (працівники з ідентифікаторами EMP_5543 та EMP_6621). Підраховано, що коефіцієнт центральності за метрикою betweenness centrality для цих двох вузлів зріс у 7–9 разів за 48 годин до інциденту порівняно з попередніми періодами. Результати GNN-класифікації свідчать про високу ймовірність (~ 0,82) того, що атака мала складений характер (поєднання технічної експлуатації вразливостей та інсайдерських дій).

Виконано порівняння ефективності різних методів детекції. На рисунку 2 наведено графік точності (Precision) та повноти (Recall) для трьох методів детектування: традиційні SIEM, когнітивні агенти +BBN, когнітивна система + GNN. При цьому по осі X відкладено значення Recall (від 0,0 до 1,0), по осі Y відкладено значення Precision (від 0,0 до 1,0), а кожна крива відображає взаємозв'язок Precision-Recall для відповідного методу детекції. Аналіз результатів на діаграмі демонструє, що традиційний SIEM має нижчі показники Precision і Recall порівняно з іншими, особливо при високій кількості малопомітних подій. При цьому когнітивні агенти $+BBN$ демонструють кращі результати, підвищуючи Recall майже до 0,75 при збереженні достатнього рівня Precision (близько 0,7). Для визначених параметрів когнітивна система $+GNN$ дає змогу досягти ще вищого рівня Precision (0,85) при високому Recall (0,80), що вказує на більш ефективне виявлення складених атак.

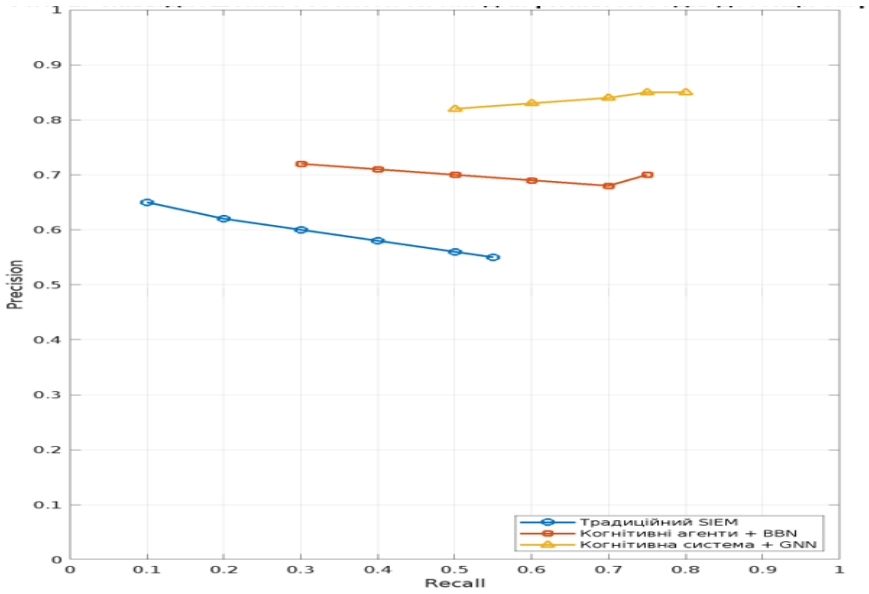

Рис. 2. Співвідношення Precision-Recall для різних методів детекції загроз

У таблиці 2 наведено порівняння основних показників ефективності (AUC, Precision, Recall, F1-score) та приблизних обчислювальних витрат (час обробки, використання пам'яті) для кожного з методів. В таблиці 1 та рисунку 2 вказано нормовані величини із діапазоном від 0 до 1. Нуль означає мінімальне значення, одиниця – максимальне.

Таблиця 2

Порівняння основних показників ефективності

Метод	AUC	Precision	Recall	F1-score
Традиційний SIEM	0,69	0,65	0,55	0,59
Когнітивні агенти + BBN	0,78	0,70	0,75	0,72
Когнітивна система + GNN	0,88	0,85	0,80	0,82

Довідка: розробка авторів

Таким чином, когнітивна система $+GNN$ виявилася найбільш результативною, хоча і вимагала більш суттєвих обчислювальних ресурсів. Як показали перші експерименти, графові моделі краще вловлюють структуру та динаміку взаємодій, що є вирішальним для детектування складених атак.

Отримані результати підтверджують гіпотези про наявність інсайдерського компоненту в розглянутому інциденті та доцільність використання когнітивних підходів для його виявлення. Аналізуючи співвідношення з висунутими гіпотезами та завданнями, маємо результати, які чітко вказують, що традиційні засоби (SIEM) недооцінювали складені загрози з інсайдерською компонентою, гіпотеза про потребу когнітивних рішень підтверджена. Важливо зауважити, що застосування когнітивних агентів і графових моделей (GNN) дозволило досягти вищої точності та повноти детекції, що відповідає цілі дослідження – створити концептуальну модель ефективнішого виявлення. За результатами експертизи подій виявлені двоє підозрюваних працівників із нестандартною поведінкою (EMP_5543 і EMP_6621), що свідчить про високий рівень поведінкового ризику, що збігається з завданням верифікувати наявність інсайдерів.

Якщо порівнювати отримані результати з іншими публікаціями, то наші результати корелюють із твердженнями в [8, 9], де також показано, що ефективність традиційних підходів обмежена без урахування людського чинника. Важливість цього дослідження [10, 16] підтверджують переваги Bayesian Belief Networks щодо раннього виявлення інсайдерських загроз. Аналогічним чином недавні праці [19, 20] демонструють, що GNN дають значний приріст якості класифікації складних взаємодій у кіберпросторі.

Запропоновані дослідження проводилися в умовах обмежень. У дослідженні здебільшого розглядався один конкретний інцидент (АТ «Укрзалізниця»). Хоча обсяг даних був значним, генералізація результатів на інші галузі потребує додаткових експериментів. Налаштування та підтримка когнітивних систем (особливо GNN) вимагають кваліфікованих фахівців й обчислювальних ресурсів, що може обмежити масове впровадження на середніх і малих підприємствах. У питанні повноцінної інтеграції поведінкових і контекстуальних чинників часто виникають проблеми із конфіденційністю та легітимністю збирання таких даних.

Незважаючи на певні абстракції та обмеження, ми звертаємо увагу на перспективні напрями для майбутніх робіт. В першу чергу таких як розширення моделі за рахунок включення більш детальних психологічних та соціальних показників, пов’язаних із профілями працівників (з урахуванням GDPR та інших норм захисту персональних даних). Наступним фактором може стати мультионтологічний підхід, а саме побудова кількох взаємопов’язаних взаємодій (IT-інфраструктури, бізнес-процесів, поведінки персоналу) та їх інтеграція у спільну когнітивну платформу. При побудові моделі важливим є автоматизація оновлення Bayesian Belief Networks та GNN у реальному часі шляхом активного навчання (active learning) та самоадаптивних механізмів, дозволяє зменшити залежність від ручних налаштувань.

Висновки та перспективи подальших досліджень. Проведене дослідження показало, що інцидент 23 березня 2025 року в IT-інфраструктурі АТ «Укрзалізниця» має високу ймовірність бути складеною кібератакою із суттєвим інсайдерським елементом. Продемонстровано, що класичні підходи (SIEM) не дозволили вчасно й повно виявити латентні шаблони взаємодій, які вказували на відхилення у поведінці працівників і зовнішні втручання.

Рекомендаціями авторів щодо подальшого розвитку досліджень виявлення шкідливих інцидентів є застосування когнітивних технологій зокрема гібридних систем штучного інтелекту, що поєднують символічні (онтологічні) та нейромережеві (графові) методи аналізу. Це дало змогу не тільки інтегрувати різнорідні дані (лог-файли, мережеві трафіки, поведінкові профілі персоналу) у єдиний багатовимірний простір та визначати складені (гібридні) сценарії, де внутрішні фактори взаємодіють із зовнішніми вразливостями, а також оцінювати ризики за допомогою ймовірнісних та графових моделей з більшою точністю й повнотою (Recall до 0,80).

Практичне застосування отриманих результатів полягає у вдосконаленні систем моніторингу в критичних інфраструктурах (транспорт, енергетика, банківський сектор). Зокрема, при розгортанні когнітивних SIEM необхідно застосовувати практичні кейси впровадження інтелектуальних модулів, що обробляють поведінкові, контекстуальні та онтологічні дані й виявляють ознаки інсайдерських аномалій, більш широко використовуючи адаптивні політики доступу, що має на меті відслідковування нетипових транзакцій у реальному часі та внесення динамічних змін у привілеї користувачів (role-based і attribute-based підходи), а також створення профілів довіри, які містять процедури формування індивідуальних профілів довіри та ризику для кожного працівника на основі аналізу історії поведінки, що уможливлює раннє виявлення потенційних інсайдерів.

Рекомендаціями подальшого дослідження та протидії інсайдерським і складним кібератакам, є необхідність створення Національного когнітивного центру реагування на базі централізованої платформи, що об’єднує відомості про загрози з різних секторів, дозволяючи швидше і точніше виявляти багатовекторні атаки. Такою структурою на першому етапі може стати Національний координаційний центр кібербезпеки при РНБО України для сектору безпеки і оборони держави та Антикризовий центр кіберзахисту бізнесу при ТПП України для приватного сектору економіки. Варто зазначити про

необхідність міжнародної кооперації через розвиток партнерства у сфері обміну досвідом та даними про атаки, зокрема з європейськими та американськими центрами реагування, щоб підвищити глобальну обізнаність про нові методи зловмисників. І важливим компонентом практичних рекомендацій є науково-дослідна робота, поглиблене вивчення інтеграції когнітивних систем із квантово-стійкими криптографічними методами захисту, оскільки технологічний розвиток вимагає проактивної протидії майбутнім загрозам.

Впровадження когнітивних рішень потребує значних фінансових та кадрових ресурсів, тому їх тиражування на середні та малі підприємства залишається складним питанням. Безумовно, етичні та юридичні аспекти збору персональних даних для поведінкового аналізу можуть стати перешкодою при масштабуванні систем на різні галузі. Проте успішна адаптація таких систем у критичній інфраструктурі (як-от залізничний транспорт) може значно зменшити ризик катастрофічних наслідків від інцидентів, подібних до того, що трапився 23 березня 2025 року.

Таким чином, запропоновані методи та результати експериментальних досліджень підкреслюють доцільність та ефективність когнітивних підходів для виявлення та протидії складеним кібератакам, зокрема з інсайдерською складовою.

References:

1. Ahmad, A., Maynard, S.B. and Park, S. (2014), «Information security strategies: towards an organizational multi-strategy perspective», *Journal of Intelligent Manufacturing*, doi: 10.1007/s10845-014-0929-y.
2. Anderson, R. (2020), *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed., John Wiley & Sons, 1232 p., [Online], available at: https://www.wiley.com/en-us/Security+Engineering%3A+A+Guide+to+Building+ Dependable+Distributed+Systems%2C+3rd+Edition-p-9781119642787
3. Probst, C.W. and Hunker, J. (2010), «The risk of insider threats in corporate networks», *Computers & Security*, Vol. 29, No. 4, pp. 333–341, doi: 10.1016/j.cose.2009.12.001.
4. Silowash, G.J., Cappelli, D.M., Moore, A.P. et al. (2012), *Common sense guide to mitigating insider threats*, 4th ed., CERT Division, Carnegie Mellon University, [Online], available at: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_51946.pdf
5. Zhou, X., Zhang, X., Luo, X. and Hu, H. (2017), «SIEM-oriented detection approach for advanced persistent threats», *Security and Communication Network*s, doi: 10.1155/2017/3272890.
6. Greitzer, F.L., Kangas, L.J., Noonan, C.F. et al. (2012), «Psychosocial modeling of insider threat risk based on behavioral and word use analysis», *e-Service Journal*, Vol. 9, No. 1, pp. 106–138, doi: 10.2979/eservicej.9.1.106.
7. Costa, D.L., Albrethsen, M.J., Collins, M.L. et al. (2016), «Insider threat research: merging quantitative and qualitative data», CERT Division, Software Engineering Institute, Carnegie Mellon University, [Online], available at: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2016_004_001_484758.pdf
8. Shaw, E.D., Post, J.M. and Ruby, K.G. (1998), «Inside the mind of the insider», *Security Awareness Bulletin*, No. 2, pp. 1–10, [Online], available at: https://apps.dtic.mil/sti/pdfs/ADA367627.pdf
9. Kandias, M., Mylonas, A., Virvilis, N. et al. (2010), «An insider threat prediction model», *Trust, Privacy and Security in Digital Business*, Springer, pp. 26–37, doi: 10.1007/978-3-642-15152-1_3.
10. Carbone, R., Legay, A., Schaus, P. and Spoletini, P. (2021), «Bayesian networks for threat detection: A systematic literature review», *Information Systems*, Vol. 99, doi: 10.1016/j.is.2021.101722.
11. Taddeo, M. and Floridi, L. (2018), «How AI can be a force for good», *Science*, Vol. 361, No. 6404, pp. 751–752, doi: 10.1126/science.aat5991.
12. Bhatt, S., Manadhata, P.K. and Zomlot, L. (2014), «The operational role of security information and event management systems», *IEEE Security & Privacy*, Vol. 12, No. 5, pp. 35–41, doi: 10.1109/MSP.2014.84.
13. Endsley, M.R. (2015), «Final Reflections: Situation Awareness Models and Measures», *Journal of Cognitive Engineering and Decision Making*, Vol. 9, No. 1, pp. 101–111, doi: 10.1177/1555343415573911.
14. Berg, G.A. (2022), «Exploring vulnerabilities in railway critical infrastructures», *Transportation Research*. Part. *Policy and Practice*, Vol. 159, pp. 243–256, doi: 10.1016/j.tra.2022.03.016.
15. Chen, H., Chou, T.C. and Chen, R. (2017), «An intelligent system for insider threat detection», *Expert Systems with Applications*, Vol. 91, pp. 117–129, doi: 10.1016/j.eswa.2017.08.041.
16. Sarkar, K. (2010), «Assessing insider threats to information security using technical, behavioural and organisational measures», *Information Security Technical Report*, Vol. 15, No. 3, pp. 112–133, doi: 10.1016/j.istr.2010.11.002.
17. Scarselli, F., Gori, M., Tsoi, A.C. et al. (2009), «The graph neural network model», *IEEE Transactions on Neural Networks*, Vol. 20, No. 1, pp. 61–80, doi: 10.1109/TNN.2008.2005605.
18. Wu, Z., Pan, S., Chen, F. et al. (2021), «A comprehensive survey on graph neural networks», *IEEE Transactions on Neural Networks and Learning Systems*, Vol. 32, No. 1, pp. 4–24, doi: 10.1109/TNNLS.2020.2978386.
19. Rowe, D.C., Lunt, T.F. and Uribe, T.E. (2007), «Adaptive insider threat detection system», *Proceedings of the 2007 IEEE Conference on Technologies for Homeland Security*, pp. 144–149, doi: 10.1109/THS.2007.370032.
20. He, D., Chan, S. and Guizani, N. (2015), «User privacy and data trustworthiness in mobile crowd sensing», *IEEE Wireless Communications*, Vol. 22, No. 1, pp. 28–34, doi: 10.1109/MWC.2015.7054721.
21. Do, Q., Martini, B. and Choo, K.-K.R. (2018), «Is the data sharing economy a new breed of cyber insider threat?», *Computers & Security*, Vol. 81, pp. 90–100, doi: 10.1016/j.cose.2018.01.008.

22. Stallings, W. and Brown, L. (2018), *Computer Security: Principles and Practice*, 4th ed., Pearson, 800 p., [Online], available at: https://www.pearson.com/en-us/subject-catalog/p/computer-security-principles-and-practice/P200000005428
23. Von Solms, R. and van Niekerk, J. (2013), «From information security to cyber security», *Computers & Security*, Vol. 38, pp. 97–102, doi: 10.1016/j.cose.2013.04.004.
24. Gondree, M., Peterson, Z.N.J. and Denning, T. (2013), «Security through play», *IEEE Security & Privacy*, Vol. 11, No. 3, pp. 64–67, doi: 10.1109/MSP.2013.57.
25. Haque, A., Guo, M. and Alikhan, M.F. (2019), «Applying machine learning methods for structural health monitoring», *Structural Health Monitoring*, Vol. 18, No. 5–6, pp. 1495–1522, doi: 10.1177/1475921718786853.
26. Humayed, A., Lin, J., Li, F. and Luo, B. (2017), «Cyber-physical systems security: A survey», *IEEE Internet of Things Journal*, Vol. 4, No. 6, pp. 1802–1831, doi: 10.1109/JIOT.2017.2703172.
27. Trzeciak, R.F. et al. (2018), «The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes», *Addison-Wesley*, 432 p., [Online], available at: https://www.pearson.com/en-us/subject-catalog/p/the-cert-guide-to-insider-threats-how-to-prevent-detect-and-respond-to-information-technology-crimes/P200000002333
28. Zeadally, S., Isaac, J.T. and Baig, Z. (2020), «Security attacks and solutions in electronic health (e-health) systems», *Journal of Medical Systems*, Vol. 44, doi: 10.1007/s10916-020-01593-0.

Прокопович-Ткаченко Дмитро Ігорьович – доцент, кандидат технічних наук, завідувач кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів, Дніпро, Україна.
https://orcid.org/0000-0002-6590-3898.
Наукові інтереси:
- кібербезпека;
- управління ризиками;
- машинне навчання.

E-mail: omega2417@gmail.com.

Рибальченко Людмила Володимирівна – доцент, кандидат економічних наук, доцент кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів, Дніпро, Україна.
https://orcid.org/0000-0003-0413-8296.
Наукові інтереси:
- кібербезпека;
- інформаційна безпека;
- інформаційні технології.

E-mail: Luda_r@ukr.net.

Козаченко Ігор Миколайович – начальник підрозділу Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.
https://orcid.org/0000-0002-0774-7284.
Наукові інтереси:
- кібербезпека;
- захист інформації;
- управління ризиками.

Бушков Валерій Геннадійович – аспірант кафедри інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету.
http://orcid.org/0009-0005-5097-2689.
Наукові інтереси:
- кібербезпека;
- інформаційна безпека;
- захист даних.

Хрушков Борис Сергійович – аспірант кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів.
http://orcid.org/0009-0002-3978-5012.
Наукові інтереси:
- кібербезпека;
- інформаційна безпека;
- захист даних.

Prokopovych-Tkachenko D.I., Rybalchenko L.V., Kozachenko I.M., Bushkov V.H., Khrushkov B.S.

Cognitive methods of countering insider and sophisticated cyber attacks: analysis of an incident in the IT infrastructure of JSC «Ukrzaliznytsia»

On 23 March 2025, a large-scale technical failure was recorded in the IT system of JSC «Ukrzaliznytsia», which led to the temporary unavailability of online ticketing services, blocking of service communication channels and loss of access to critical operational data.

It is proved that this incident has the characteristics of a composite cyberattack, which includes traditional vectors of external interference (e.g., attacks on web applications and e-service platforms), as well as a potential insider component that enhances the destructive effect. The relevance of the study is related to the need to identify and counteract such complex threats, where traditional means of monitoring and response are not effective enough. The article proposes cognitive methods for indicating insider and composite cyberattacks, in particular, hybrid artificial intelligence systems that combine symbolic and neural network methods of event analysis. The possibilities of behavioural analytics, Bayesian Belief Networks, Graph Neural Networks and other models aimed at integrating fragmented signals and ontological reconstruction of the attack are revealed. The author substantiates the need to embed cognitive agents in the processes of collecting and processing data from various information channels in order to timely detect anomalous patterns in the activities of employees, contractors and external connections.

It is concluded that it is expedient to form a single national cognitive centre for responding to incidents in critical IT infrastructure, which would integrate behavioural, statistical and ontological analysis of events. The article outlines the prospects for the use of such systems on a real-world scale at critical facilities, as well as possible limitations and directions for further research in the field of cybersecurity.

Keywords: cyberattack; artificial intelligence; insider threats; multivariate analysis; cognitive agents.

Стаття надійшла до редакції 26.09.2025.