Інтелектуальні системи аналізу та прогнозування кіберінцидентів у корпоративних мережах

УДК 004.056.53:004.89:004.732

Євгенія Іванченко[1], Тетяна Берестяна[2], Володимир Дубровський[3]

Державний університет інформаційно-комунікаційних технологій,
[1] e.ivancenko@duikt.edu.ua, [2] t.berestiana@duikt.edu.ua,
[3] v.dybrovskyi@stud.duikt.edu.ua

У сучасних умовах цифрової трансформації корпоративних інфраструктур питання забезпечення кібербезпеки набуває стратегічного значення для стабільного функціонування організацій різних секторів економіки. Розширення корпоративних мереж за рахунок хмарних середовищ, мобільних пристроїв, IoT-інфраструктур та розподілених сервісів суттєво збільшує поверхню атаки й ускладнює процес моніторингу інформаційної безпеки [1]. Одночасно з цим спостерігається зростання складності та адаптивності кіберзагроз, що дедалі частіше реалізуються у вигляді багатоступеневих APT-кампаній, zero-day-атак та скоординованих групових вторгнень [2].

Традиційні системи кіберзахисту, зокрема SIEM та IDS/IPS, побудовані переважно на сигнатурних або rule-based підходах, демонструють обмежену ефективність у виявленні невідомих та адаптивних загроз через залежність від попередньо визначених шаблонів атак [3]. У таких умовах особливої актуальності набуває впровадження методів штучного інтелекту та машинного навчання, які дозволяють автоматизувати аналіз великих обсягів телеметричних даних, виявляти приховані закономірності у поведінці суб'єктів мережевої взаємодії та прогнозувати потенційні кіберінциденти ще до моменту їх повного розгортання [4].

Аналіз сучасних наукових досліджень показує, що застосування алгоритмів машинного навчання у системах виявлення вторгнень забезпечує значне підвищення точності ідентифікації аномалій порівняно з класичними сигнатурними методами [5]. Найбільш поширеними підходами є використання Random Forest, Support Vector Machines, XGBoost, а також методів глибинного навчання – згорткових нейронних мереж (CNN), рекурентних мереж (RNN, LSTM) та автоенкодерів [6]. Такі моделі дозволяють аналізувати як статичні ознаки мережевого трафіку, так і часові послідовності подій, що особливо важливо при виявленні повільних або розподілених атак.

Водночас використання ізольованих AI-based IDS не забезпечує повноцінного контексту для аналізу складних скоординованих кіберінцидентів. У зв'язку з цим найбільш перспективним напрямом розвитку корпоративних систем кіберзахисту є впровадження XDR-платформ (Extended Detection and Response), які поєднують телеметрію з мережевого, хостового, хмарного та прикладного рівнів в єдиному аналітичному середовищі [7]. Інтеграція XDR з алгоритмами машинного навчання дозволяє реалізувати крос-доменну кореляцію подій, зменшити кількість хибнопозитивних спрацювань та підвищити ефективність виявлення багатоступеневих атак [8].

Узагальнену архітектуру перспективної інтелектуальної системи аналізу та прогнозування кіберінцидентів наведено на рисунку 1.

На рисунку 1 представлено узагальнену архітектуру інтелектуальної системи аналізу та прогнозування кіберінцидентів у корпоративних мережах, побудовану на основі інтеграції XDR-платформи, AI/ML/DL-модулів аналізу та SOAR-механізмів автоматизованого реагування. Запропонована архітектура відображає послідовність обробки телеметричних даних – від централізованого збору та нормалізації інформації з різних джерел до інтелектуального аналізу, крос-доменної кореляції подій, оцінки ризиків і реалізації автоматизованих сценаріїв реагування. Такий підхід забезпечує комплексний контекстний аналіз кіберподій та створює основу для побудови проактивних адаптивних систем кіберзахисту нового покоління.

У межах дослідження проаналізовано функціональні можливості сучасних класів систем виявлення та реагування на кіберінциденти: SIEM, IDS/IPS, UEBA, SOAR, AI-based IDS, DL-based IDS та XDR. Встановлено, що традиційні SIEM- та IDS/IPS-рішення забезпечують ефективне виявлення відомих шаблонів атак і централізований збір подій безпеки, однак не демонструють достатньої стійкості до zero-day загроз та складних скоординованих атак. Системи UEBA покращують виявлення внутрішніх загроз за рахунок поведінкового аналізу, проте без інтеграції з іншими джерелами телеметрії мають обмежений аналітичний контекст [9].

Рис. 1. Архітектура інтелектуальної системи аналізу та прогнозування кіберінцидентів у корпоративних мережах

Для формалізації результатів порівняльного аналізу сучасних систем виявлення та реагування на кіберінциденти узагальнено їх ключові функціональні характеристики за критеріями стійкості до zero-day загроз, здатності до прогнозування, рівня автоматизації та ефективності виявлення групових атак (табл. 1).

Таблиця 1

Порівняльна характеристика сучасних систем виявлення та реагування на кіберінциденти

Тип системи	Zero-day	Прогнозування	Автоматизація	Групові атаки
SIEM	Низька	Ні	Часткова	Низька
IDS/IPS	Низька	Ні	Низька	Низька
UEBA	Середня	Частково	Середня	Середня
XDR	Висока	Так	Висока	Висока

Наведені у таблиці 1 результати демонструють, що інтегровані XDR-рішення забезпечують найвищий рівень функціональної ефективності серед розглянутих класів систем, що обґрунтовує доцільність їх використання як базового елемента інтелектуальних платформ аналізу та прогнозування кіберінцидентів.

На відміну від зазначених підходів, інтегровані XDR-рішення забезпечують найвищий рівень ефективності при виявленні складних кіберінцидентів завдяки централізованій телеметрії, машинному навчанню та можливостям крос-доменної кореляції [8]. Додаткове поєднання XDR з SOAR-платформами дозволяє автоматизувати сценарії реагування, скоротити середній час реагування на інциденти та знизити навантаження на аналітиків SOC.

Таким чином, результати проведеного дослідження підтверджують доцільність і необхідність переходу від ізольованих реактивних систем кіберзахисту до інтегрованих інтелектуальних платформ аналізу, виявлення та прогнозування кіберінцидентів, здатних забезпечувати комплексну обробку телеметричних даних, крос-доменну кореляцію подій та проактивне реагування на сучасні багатоступеневі кіберзагрози. Встановлено, що інтеграція XDR-платформ із алгоритмами машинного та глибинного навчання дозволяє суттєво підвищити точність детектування аномалій, зменшити кількість хибнопозитивних спрацювань, скоротити час реагування на інциденти та забезпечити стійкість корпоративних інформаційних систем до складних і раніше невідомих типів атак.

Отримані результати свідчать про формування нової парадигми побудови систем кіберзахисту, у межах якої ключову роль відіграють адаптивність, самонавчання та автоматизація процесів виявлення і реагування на загрози. Перспективним напрямом подальших досліджень є розробка гібридних архітектур виявлення загроз із підтримкою пояснюваного штучного інтелекту (XAI), адаптивних механізмів перенавчання моделей, захисту від adversarial-атак, а також методів забезпечення стійкості інтелектуальних моделей до концептуального дрейфу в умовах динамічної зміни ландшафту кіберзагроз. Реалізація зазначених підходів сприятиме створенню кіберзахисних систем

нового покоління, здатних функціонувати в умовах високої невизначеності та постійної еволюції кіберпростору.

1. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, 2024.
2. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity, 2023.
3. NIST. Cybersecurity Framework 2.0. National Institute of Standards and Technology, 2024.
4. Artificial Intelligence and Cybersecurity Research. ENISA, 2023.
5. Котенко Д. та ін. Штучний інтелект у системах виявлення і запобігання кібератакам. Управління розвитком складних систем. 2024.
6. Mohamed N. Artificial Intelligence and Machine Learning in Cybersecurity: State-of-the-Art Techniques and Future Paradigms. Knowledge and Information Systems. 2025.
7. Integrating AI/ML in Cybersecurity: Analysis of Open XDR Technology and its Application in Intrusion Detection. 2023.
8. ENISA. Artificial Intelligence Cybersecurity Challenges. 2023.
9. Lavrenchuk A. Майбутнє кібербезпеки: виклики штучного інтелекту та машинного навчання. Молодий вчений. 2024.

Дослідження використання штучного інтелекту для ідентифікації джерел радіоелектронної боротьби

УДК 004.89:621.396

Роман Бибик[1], Іван Опірський[2]

Національний університет "Львівська політехніка",
[1]roman.t.bybyk@lpnu.ua [2]ivan.r.opirskyi@lpnu.ua

Метою роботи є дослідження можливостей використання методів штучного інтелекту для підвищення ефективності ідентифікації джерел радіоелектронної боротьби на основі просторово-частотного аналізу сигналів. Актуальність дослідження обумовлена зростанням кількості електромагнітних загроз та необхідністю створення адаптивних систем протидії РЕБ, здатних функціонувати в умовах динамічної електромагнітної обстановки. Наукова новизна роботи полягає у поєднанні методів просторово-частотного орієнтування з алгоритмами машинного навчання для автоматизованої класифікації сигналів джерел РЕБ та підвищення точності їх локалізації.

Сучасні умови ведення бойових дій характеризуються активним застосуванням засобів радіоелектронної боротьби, які здійснюють вплив на системи зв'язку, навігації, управління та засоби ураження. Зростання кількості електромагнітних загроз зумовлює необхідність удосконалення методів виявлення та ідентифікації джерел радіоелектронного випромінювання. Особливої актуальності набуває використання технологій штучного інтелекту, здатних забезпечити автоматизований аналіз електромагнітного середовища та адаптацію до змін параметрів сигналів у реальному масштабі часу.Одним із