УДК 004.8+65.05+681.5 DOI: 10.31673/2786-8362.2025.016252

Катков Ю.І., д.т.н.; **Березовська Ю.В.,** PhD;
Клюєва В.В.; Вишнівський О.В.;
Заднепрянець О.Ю.; Рищиковець І.О.

АНАЛІЗ СПОСОБІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОКРАЩЕННЯ МОНІТОРИНГУ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ

Katkov Yu.I., Berezovska Yu.V., Kliuieva V.V., Vyshnivskyi O.V., Zadneprianets O.Yu., Ryshchykovets I.O. Analysis of ways to use artificial intelligence to improve monitoring of secure IT-infrastructure. The article is dedicated to the analysis of various ways of applying artificial intelligence for monitoring the protected IT infrastructure. The modern world is undergoing rapid technological transformation, where information technologies play a key role in the functioning of almost all aspects of our lives. Information technology infrastructure becomes not only critically important for supporting businesses and organizations but also determines the convenience and efficiency of using and developing digital services in the modern world. Ensuring the continuity and optimal functioning of IT infrastructure is of paramount importance for businesses, organizations, and society as a whole. In this regard, the application of artificial intelligence for monitoring and supporting IT infrastructure proves to be a powerful tool for predicting, detecting, and resolving issues before they strengthen and affect efficiency. Today's IT infrastructure is becoming increasingly complex and voluminous, requiring constant monitoring to timely respond to possible failures or malfunctions that may lead to disruptions in work, financial losses, or even threats to data security. In this context, the application of artificial intelligence becomes crucial as it can provide fast, accurate, and forecasted solutions based on the analysis of a vast amount of data and previous patterns of failures.

Keywords: vulnerabilities, IT infrastructure monitoring, cybersecurity, artificial intelligence

Катков Ю.І., Березовська Ю.В., Клюєва В.В., Вишнівський О.В., Заднепрянець О.Ю., Рищиковець І.О. Аналіз способів застосування штучного інтелекту для покращення моніторингу захищеної ІТ-інфраструктури. Стаття присвячена питанню аналізу різноманітних способів застосування штучного інтелекту для покращення моніторингу захищеної ІТ-інфраструктури. Сучасний світ переживає стрімке технологічне перетворення, де інформаційні технології відіграють ключову роль у функціонуванні практично всіх аспектів нашого життя. ІТ-інфраструктура сьогодення стає все більш складною та об'ємною, вимагаючи постійного моніторингу, щоб вчасно реагувати на можливі збої чи неполадки, які можуть призвести до перерв у роботі, фінансових втрат та загроз для безпеки даних. Тому ІТ-інфраструктура стає не тільки критично важливою для підтримки бізнесу та організацій, але й визначає зручність й ефективність використання та розвиток цифрових послуг у сучасному світі. Забезпечення безперебійності та оптимального функціонування ІТ-інфраструктури стає завданням надзвичайної важливості для бізнесу та організацій, а також для суспільства в цілому. У зв'язку з цим, застосування штучного інтелекту для покращення моніторингу та підтримки ІТ-інфраструктури виявляється потужним інструментом для передбачення, виявлення та вирішення проблем погіршення ефективності. У цьому контексті застосування штучного інтелекту набуває великого значення, тому що саме він може надати швидкі, точні та прогнозовані рішення на основі аналізу величезної кількості даних та попередніх патернів збоїв.

Ключові слова: вразливості, моніторинг ІТ-інфраструктури, кібербезпека, штучний інтелект

Вступ

Сьогодні існує багато практичних прикладів успішного впровадженні систем моніторингу захищеної ІТ-інфраструктури на основі штучного інтелекту (ШІ). Наприклад, автоматизований моніторинг мережі Cisco Stealthwatch [1]; детектор загроз Darktrace [2], детектор загроз Vectra AI [3] та інші. Також сьогодні відомо програмне забезпечення для моніторингу ІТ-інфраструктури, наприклад, Nagios, Zabbix, Checkmk, OpenNMS, Icinga, Netdata, LibreNMS та інші. Ці приклади показують, як успішно ШІ використовується для постійного моніторингу мережевої активності та виявлення загроз, допомагає компаніям захищати свою ІТ-інфраструктуру в реальному часі. Але багато питань ще не визначено, тому існує проблема застосування ШІ для покращення моніторингу захищеної ІТ-інфраструктури з метою забезпечення безперебійності та оптимального функціонування ІТ-інфраструктури.

Постановка завдання. Проблема застосування штучного інтелекту для покращення моніторингу захищеної ІТ-інфраструктури з метою забезпечення безперебійності та оптимального функціонування ІТ-інфраструктури стає надзвичайно важливою для бізнесу та організацій. ІТ-інфраструктура сьогодення стає все більш складною та об'ємною, вимагаючи постійного моніторингу. Вважається, що застосування ШІ для покращення моніторингу захищеної ІТ-інфраструктури виявляється потужним інструментом для передбачення, виявлення та вирішення проблем до погіршення її ефективності. Отже, визначення способів застосування ШІ для покращення моніторингу захищеної ІТ-інфраструктури є надзвичайно актуальним завданням. Для цього треба виконати аналіз способів застосування штучного інтелекту для покращення моніторингу ІТ-інфраструктури.

Аналіз останніх досліджень. Дослідження проблеми застосування ШІ для моніторингу захищеної ІТ-інфраструктури з метою забезпечення безперебійності та оптимального функціонування ІТ-інфраструктури розглянуто в [4-9]. Ці приклади показують, як ШІ успішно впроваджується для покращення ефективності ІТ-інфраструктури за рахунок моніторингу. Але у результаті аналізу останніх наукових досліджень у даній області можна зазначити, що стрімкий розвиток різноманітних технологій із застосуванням ШІ вимагає постійного аналізу способів покращення застосування систем моніторингу захищеної ІТ-інфраструктури, щоб впроваджувати найбільш перспективні.

Метою роботи є підвищення ефективності практичного застосування сучасних методів моніторингу ІТ-інфраструктури шляхом впровадження найбільш перспективних систем моніторингу захищеної ІТ-інфраструктури.

Виклад основного матеріалу дослідження

Для досягнення цієї мети треба систематизація та оцінка основних способів застосування ШІ для покращення моніторингу захищеної ІТ-інфраструктури.

ІТ-інфраструктура (Information Technology) – комплексна система, яка застосовує інформаційні технології в апаратних та програмних засобах мережевих з'єднань, які допомагають створювати та підтримувати функціонування інформаційної системи в організації або компанії. ІТ-інфраструктура є фундаментом для забезпечення оптимальної роботи інформаційних систем у будь-якій сфері, оскільки вона відповідає за стабільність, безпеку та доступність всіх технологічних ресурсів, необхідних для успішної діяльності сучасних організацій.

ІТ-інфраструктура включає в себе всі необхідні елементи для збору, обробки, зберігання та передачі інформації, що є необхідними для функціонування сучасного бізнесу та організацій, а саме: апаратну складову (сервери, комп'ютери, мережеве обладнання, сховища даних, периферійні пристрої та інше обладнання), програмну складову (операційні системи, програмне забезпечення, системи управління базами даних, додатки та інструменти, що використовуються для управління та обробки даних), мережеву складову (локальні мережі, веб-сервери, VPN-з'єднання, хмарні сервіси та інші технології для забезпечення доступу до даних та ресурсів) та людські ресурси (системні адміністратори, інженери з підтримки, програмісти та користувачі).

Моніторинг в інформаційних технологіях відіграє важливу роль у забезпеченні працездатності, безпеки та ефективності ІТ-інфраструктури. Моніторинг є ключовим елементом для забезпечення надійності, безпеки та ефективності ІТ-інфраструктури, дозволяючи вчасно реагувати на проблеми, оптимізувати процеси та підтримувати високий рівень продуктивності.

Для підвищення ефективності моніторингу захищеної ІТ-інфраструктури передбачається, що застосування різноманітних способів штучного інтелекту (ШІ). Сьогодні існує багато прикладів реалізації різноманітних способів ШІ для моніторингу. Тому для систематизації та оцінки основних цих способів моніторингу необхідно виконати збір, обробку та аналіз інформації про ці способи.

Сьогодні основним джерелом інформації є Інтернет. Для пошуку інформації в Інтернеті

використовуються пошукові системи, наприклад, багатофункціональні типу Google, Bing, Yahoo Search та інші, або спеціалізовані типу Google Scholar, Wikipedia та інші. В цих пошукових системах використовують OSINT.

OSINT (Open Source Intelligence) або розвідка на основі відкритих джерел – це методологія роботи з інформацією, яка включає принципи, методи і підходи, що використовуються для збору, обробки, аналізу та представлення інформації [11-14]. Для реалізації цей методології використовуються різноманітні технології та інструменти для збору, аналізу та використання публічно доступної інформації для отримання корисних відомостей, наприклад, скрипти, програмне забезпечення, фреймворки, реєстри та бази даних, що автоматизують збір даних, аналіз метаданих, геолокацію, розпізнавання обличь тощо. Також застосовуються методи аналізу з використанням штучного інтелект (ШІ), машинного навчання (МН) для обробки великих обсягів даних, виявлення закономірностей та зав'язків. Отже, OSINT – це не просто "технологія" в сенсі конкретного пристрою чи програми. Це ширша концепція, яка передбачає методологію роботи з інформацією, а технології є інструментами, що допомагають цю методологію втілювати в життя [14-20]. Приклади популярних OSINT-інструментів надані в таблиці 1.

Таблиця 1

Популярні OSINT-інструменти [21]

Інструмент / платформа	Призначення
Shodan	Пошук відкритих пристроїв і сервісів у мережі
Censys	Альтернатива Shodan, глибший аналіз SSL/сертифікатів
Have I Been Pwned	Перевірка витоків паролів та email-адрес
Maltego	Візуальна розвідка зв'язків (доменів, IP, організацій)
SpiderFoot	Автоматичний збір інформації про ціль
Google Dorks	Цільові запити до Google (наприклад, filetype:xls site:)
theHarvester	Збір email-адрес, доменів, IP
BuiltWith	Технології на сайті конкурента
Social Searcher	Моніторинг згадок у соцмережах
DNSdumpster	Визначення DNS-записів, субдоменів

Для отримання в Інтернеті достовірної інформації OSINT базується на репрезентативної виборці. З точки зору теорії ймовірності та статистиці репрезентативна вибірка – це така, яка достатньо точно відображає основні характеристики генеральної сукупності пошуку інформації, тобто є: випадковою, має достатній обсяг, відображає основні характеристики потрібної інформації, забезпечує мінімізацію похибки в оцінках. Пошук інформації в інтернеті здійснюється за допомогою пошукових запитів (ключових слів).

В OSINT-пошуку вибір ключових слів напряму впливає на репрезентативність ключових слів вибірки даних, повноту охоплення релевантних джерел, баланс між синонімами/варіаціями термінів. На відміну від класичної статистики похибка (margin of error) і довірчий рівень (confidence level) прямо не розраховуються так, як у вибіркових опитуваннях [22]. Проте, можна наблизитися до статистичного підходу, якщо OSINT-процес базується на вибірці великих обсягів текстових даних, новин, постів тощо. Тобто на відміну від класичної статистики, тут не існує "жорсткого числа", але є практичні підходи.

Практичний підхід у тому, що передбачається наявність наближеної математичної моделі репрезентативності вибірки. Ця модель може застосовуватися, якщо розглядати популяцію як всю інформацію в Інтернеті з певної теми; вибірку – як результати, отримані за запитами з N ключових слів/фраз; об'єкти дослідження – пости, новини, згадки тощо. Тобто можна застосувати модель наближеного довірчого інтервалу похибки для пропорцій:

$$MOE = z * \sqrt{\frac{p(1-p)}{n}}, \quad (1)$$

де MOE – похибка (Margin of Error),

z –коефіцієнт довіри (1.96 для 95% рівня),

p –частка позитивних згадок / релевантності,

n –кількість знайдених документів.

Наприклад: якщо з 1000 документів за визначеними ключовими словами 600 є релевантними (p = 0.6), тоді:

$$MOE = 1{,}96 * \sqrt{\frac{0{,}6(1-0{,}4)}{1000}} \approx 0{,}03. \quad (2)$$

Це означає, що з імовірністю 95% реальна частка релевантних результатів лежить у межах ±3%.

Сьогодні вважається, що потрібне ***N*** ключових слів/фраз не менше 5-10 добре підібраних ключових слів або фраз на кожну тему/категорію. Сама цифра 5-10 – це загальноприйнята кліше-практика, випробувана в реальних OSINT-проєктах [24]. Це мінімум для того, щоб: охопити семантичне різноманіття (синоніми, скорочення, професійні терміни), зменшити інформаційне викривлення (bias) та шум, уніфікувати запити до різних джерел (Google, Shodan, Twitter, Pastebin, тощо) (табл. 2).

Таблиця 2

Визначення основних параметрів OSINT

Параметр	Значення
Кількість ключових слів	5-10 на кожну тему (мінімум)
Довірчий рівень	~90-95% (якщо вибірка зібрана правильно)
Похибка змістовна	~5-10% (за умови гарного підбору слів)
Статистична похибка	~2-5% (якщо результатів > 500)

Вважається, що репрезентативна основа для збору даних по цій темі буде, якщо враховані фактори, що вказані в таблиці 3.

Таблиця 3

Фактори, що впливають на кількість ключових слів

Фактор	Рекомендація
Тематика (IT, соцмережі, військове)	Чим складніша — тим більше варіантів потрібно (10-50)
Мова пошуку	Додайти запити кількома мовами (англ, укр, нем та інші)
Платформи пошуку	Підлаштовувати запити під особливості кожної (Google ≠ GitHub ≠ Telegram)
Синоніми, абревіатури	Наприклад: VPN breach, VPN cracked, VPN auth leak
Цільове джерело	Якщо моніторите darknet або paste-сайти — ключові слова мають бути більш "низькорівневі"

Рекомендований підхід для створення репрезентативності:

1. Скласти основне ядро з 5-10 ключових слів;
2. Додати до кожного 2-3 синоніми чи альтернативні написання;
3. Використовувати логічні оператори (AND, OR, site:, filetype:), щоб структурувати запити;
4. Тестувати пошукові результати: якщо результати починають повторюватися або не змінюються – семантичне покриття достатнє;
5. Застосовувати інструменти, які допомагають підібрати ключові слова: Google Trends, Keyword Tool, Semrush, Ahrefs (SEO-платформи), Maltego, SpiderFoot (для OSINT-автоматизації).

Таким чином, 10+ варіантів – це вже репрезентативна основа для збору даних по визначеної темі. Але для покращення репрезентативної вибірки в OSINT-пошуку доцільне мати більш 10-20 унікальних, контекстно релевантних ключових запитів, адаптованих до різних джерел і мов.

Реалізація аналізу способів застосування штучного інтелекту для покращення моніторингу ІТ-інфраструктури за допомогою технології та інструментів OSINT-пошуку.

Крок 1. Для вирішення завдання щодо визначення способів застосовування ШІ завдяки використанню технології та інструментів OSINT-пошуку було визначено ключові слова та відповідні пошукові запити для пошуку «Способів застосування ШІ для моніторингу захищеної ІТ-інфраструктури».

Для покращення репрезентативної вибірки в OSINT-пошуку було вибране 12 унікальних, контекстно релевантних ключових запитів, адаптованих до різних джерел і мов (табл. 4).

Таблиця 4

Ключові слова та відповідні пошукові запити для теми «Способи застосування ШІ для моніторингу захищеної ІТ-інфраструктури»

Категорія	Ключове слово / фраза	Приклад запиту (Google)
Штучний інтелект	AI-based monitoring	"AI-based monitoring" cybersecurity site:researchgate.net
Штучний інтелект	anomaly detection	"anomaly detection" log analysis filetype:pdf
Кібербезпека	IT infrastructure protection	"IT infrastructure protection" AND AI
Кібербезпека	network security monitoring	"network security monitoring" AND ML
Моніторинг	log analysis AI	"log analysis AI" site:github.com
Моніторинг	real-time monitoring	"real-time monitoring" AI site:medium.com
Загрози	ransomware detection AI	"ransomware detection AI" site:arxiv.org
Загрози	insider threat detection	"insider threat detection" AI cybersecurity
Інструменти	MITRE ATT&CK AI	"MITRE ATT&CK AI" filetype:pdf
Інструменти	Darktrace	Darktrace AI threat detection site:techcrunch.com
Способи	Способи (укр)	https://itedu.center/ua/blog/ratings/monitoring_tools/?srsltid=AfmBOorBpJFuLuLrTM02n-AdYB5tK8_-f8kA5AAyinH25U2tHRSfbLgA
Способи	Ways (англ)	https://www.toladata.com/blog/types-of-monitoring-and-evaluation/

Це позволило визначити способи застосування ШІ для покращення моніторингу захищеної ІТ-інфраструктури з імовірністю 95% релевантних результатів, що лежить у межах ±3% (табл. 5).

Були також визначені сучасні інструменти з AI для моніторингу ІТ-безпеки: Darktrace – виявлення загроз у реальному часі на основі поведінкових моделей; IBM QRadar з Watson – AI-аналітика в SIEM-системі; CrowdStrike Falcon – інтелектуальний агент для моніторингу кінцевих точок; Microsoft Defender for Endpoint – AI для захисту пристроїв на Windows.

Крім того незважаючи на значні переваги від впровадження ШІ в моніторинг захищеної ІТ-інфраструктури були визначені виклики:

– якість даних: Ефективність ШІ значною мірою залежить від якості та обсягу вхідних даних;

– складність інтеграції: Інтеграція ШІ-рішень з існуючими системами безпеки може бути складною;

– потреба в кваліфікованих кадрах: Для налаштування, моніторингу та інтерпретації результатів ШІ потрібні фахівці з відповідними знаннями;

– етичні аспекти та конфіденційність: Використання ШІ для моніторингу поведінки користувачів вимагає ретельного розгляду питань конфіденційності та відповідності нормативним вимогам.

Таблиця 5

Способи застосування ШІ для покращення моніторингу захищеної ІТ-інфраструктури

	Спосіб	Пояснення
1.	Інтелектуальний моніторинг мережевого трафіку	Аналіз поведінки: AI-системи вивчають типову поведінку користувачів і пристроїв та виявляють аномалії (наприклад, раптові великі обсяги переданих даних). Deep Packet Inspection (DPI) з використанням ML дозволяє аналізувати вміст трафіку для виявлення шкідливих шаблонів.
2.	Виявлення вторгнень (IDS/IPS) з AI	Моделі машинного навчання навчаються на великих наборах даних атак і можуть виявляти нові, раніше невідомі загрози. Self-learning IDS постійно оновлюють правила виявлення без людського втручання.
3	SIEM-системи з AI-підтримкою	ШІ оптимізує кореляцію подій із різних джерел логів. Забезпечує пріоритезацію інцидентів, автоматично розрізняючи критичні та неважливі загрози.
4.	Безперервне сканування вразливостей	AI дозволяє динамічно адаптувати сканування, враховуючи зміни в інфраструктурі. Системи ранжують вразливості за реальним ризиком, а не лише за CVSS-оцінкою
5.	Передбачувальна аналітика (Predictive Analytics)	AI прогнозує ймовірність інцидентів на основі історичних даних та трендів. Застосовується для превентивних дій – наприклад, закриття портів або обмеження доступу до серверів.
6.	Автоматизоване реагування на інциденти	SOAR-платформи (Security Orchestration, Automation and Response) з AI приймають рішення без участі людини, що: блокують IP-адреси; відключають підозрілі пристрої; оновлюють правила фаєрвола.
7.	Інтелектуальна аутентифікація та контроль доступу	AI аналізує поведінкову біометрію користувачів (наприклад, як вони друкують, рухають мишкою). Динамічний рівень довіри для доступу до ресурсів (zero trust model).
8.	AI у хмарній безпеці	Виявлення аномалій у хмарних середовищах (AWS, Azure, GCP). Моніторинг активності API-запитів та автоматичне виявлення зловживань

Крок 2. Для вирішення завдання оцінки способів завдяки використанню технології та інструментів OSINT-пошуку було визначено ключові слова та відповідні пошукові запити для визначення основних «Ключових показників ефективності (KPI) для порівняння способів моніторингу захищеної ІТ-інфраструктури (включаючи традиційні та на основі ШІ)» з імовірністю 95% релевантних результатів, що лежить у межах ±3% (табл. 6).

Крок 3. Для вирішення завдання порівняння способів завдяки використанню технології та інструментів OSINT-пошуку було визначено ключові слова та відповідні пошукові запити для теми «Порівняння ефективності традиційних способів моніторингу ІТ-інфраструктури та методів на основі штучного інтелекту» (табл. 7).

Таким чином, визначено попередня оцінка ефективності способів моніторингу ІТ-інфраструктури за рахунок використання ШІ. З таблиці 7 умовно бачимо, які способи доцільні для покращення моніторингу захищеної ІТ-інфраструктури. Для визначення більш точної оцінки треба продовжити дослідження з використанням інших методів. Більш точна оцінка ефективності способів моніторингу захищеної ІТ-інфраструктури потребує системного підходу та застосування методів, які поєднують кількісні метрики (KPI) з якісним SWOT-аналізом, аналізом ризиків, порівняльним аналізом, методом Red/Blue Team Testing та методами моделювання.

Таблиця 6

Ключові показники ефективності (KPI) для порівняння способів моніторингу захищеної IT-інфраструктури (включаючи традиційні та на основі ШІ

	Показник	Пояснення
1.	Точність виявлення загроз (Detection Accuracy)	Відсоток правильно виявлених реальних атак. Показує, наскільки метод здатен розрізняти загрозу і нормальну активність. Чим вище – тим краще.
2.	Кількість хибнопозитивних спрацьовувань (False Positives Rate)	Відсоток помилкових сигналів про загрозу. Високе значення призводить до "інформаційного шуму" і втоми операторів. Чим нижче – тим ефективніше.
3.	Швидкість виявлення інциденту (Mean Time to Detect, MTTD)	Середній час між початком атаки і її виявленням. Визначає, наскільки оперативно система реагує на загрозу.
4.	Швидкість реагування (Mean Time to Respond, MTTR)	Час від виявлення до завершення дій із нейтралізації інциденту. Високий MTTR = високий ризик витоку або пошкодження даних.
5.	Масштабованість (Scalability)	Здатність системи підтримувати ефективний моніторинг при зростанні обсягу даних або кількості користувачів.
6.	Автоматизація (Automation Level)	Рівень, на якому система може працювати без втручання людини: виявляти, аналізувати, реагувати.
7.	Адаптивність (Adaptability)	Можливість системи самостійно вчитися на нових типах загроз і підлаштовувати свої правила та моделі.
8.	Інтеграційна сумісність (Integration Capability)	Наскільки легко система може бути інтегрована з існуючими IT-ресурсами (SIEM, фаєрволами, API).
9.	Споживання ресурсів (Resource Consumption)	Обчислювальні потужності, які потрібні системі для ефективної роботи (ЦП, пам’ять, мережа).
10.	Вартість впровадження та обслуговування (TCO – Total Cost of Ownership)	Загальна вартість, включаючи ліцензії, апаратне забезпечення, налаштування, персонал і оновлення.

Таблиця 7

Порівняння ефективності традиційних способів моніторингу IT-інфраструктури та методів на основі штучного інтелекту

Показник	Традиційний моніторинг	Моніторинг із використанням ШІ
1. Точність виявлення загроз	Середня (залежить від фільтрів і сигнатур)	Висока (за рахунок навчання моделей)
2. Хибнопозитивні спрацьовування	Високі	Низькі (завдяки поведінковому аналізу)
3. Швидкість виявлення (MTTD)	Від хвилин до годин	У реальному часі або майже миттєво
4. Швидкість реагування (MTTR)	Від годин до днів	Автоматизована реакція за секунди/хвилини
5. Масштабованість	Обмежена	Висока, особливо в хмарних середовищах
6. Рівень автоматизації	Низький (багато ручних процесів)	Високий (SOAR, auto-response, auto-tuning)

Продовження таблиці 7

Порівняння ефективності традиційних способів моніторингу ІТ-інфраструктури та методів на основі штучного інтелекту

Показник	Традиційний моніторинг	Моніторинг із використанням ШІ
7. Адаптивність	Обмежена (оновлення вручну)	Висока (самонавчання моделей)
8. Інтеграція з ІТ-системами	Може вимагати додаткових модулів	Широка підтримка API та хмарних платформ
9. Споживання ресурсів	Помірне	Залежить від складності моделі (може бути високе)
10. Загальна вартість (ТСО)	Нижча на старті, але дорожча у підтримці	Вища початкова, але ефективніше у довгостроковій перспективі

Висновки

Таким чином, для вирішення проблеми застосування ШІ для покращення моніторингу захищеної ІТ-інфраструктури з метою забезпечення безперебійності та оптимального функціонування ІТ-інфраструктури можливе використання технології та інструментів OSINT-пошуку, які дають попередню оцінку ефективності.

Майбутньою перспективою використання ШІ для покращення моніторингу захищеної ІТ-інфраструктури може бути створення автономних систем моніторингу, які здатні самостійно адаптуватися до змін та виявляти проблеми без людської участі. Розвиток автономних систем є одним із ключових напрямків у сфері ШІ. Ці системи мають значний потенціал у різних галузях, наприклад, самокеровані автомобілі, автономні роботи (дрони), розрахункові системи зі збільшеною точністю та швидкістю тощо.

Список використаної літератури:

1. Cisco Secure Network Analytics (formerly Stealthwatch) At-a-Glance. URL: https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/ secure-network-analytics-aag.html

2. Darktrace DETECT | Autonomous Threat Detection. Darktrace | The Essential AI Cybersecurity Platform. URL: https://www.darktrace.com/products/detect

3. Vectra AI | Cybersecurity AI That Stops Attacks Others Canâ□□t. Vectra AI | Cybersecurity AI That Stops Attacks Others Canâ™t. URL: https://www.vectra.ai

4. Uraikul V., Chan C. W., Tontiwachwuthikul P. Artificial intelligence for monitoring and supervisory control of process systems. Engineering Applications of Artificial Intelligence. 2007. Vol. 20, no. 2. P. 115–131. URL: https://doi.org/10.1016/j.engappai.2006.07.002

5. Using a multi-agent system and artificial intelligence for monitoring and improving the cloud performance and security / D. Grzonka et al. Future Generation Computer Systems. 2018. Vol. 86. P. 1106–1117. URL: https://doi.org/10.1016/j.future.2017.05.046

6. US9886955B1 - Artificial intelligence for infrastructure management - Google Patents. Google Patents. URL: https://patents.google.com/patent/US9886955B1/en

7. Reddy Yeruva A. Monitoring Data Center Site Infrastructure Using AIOPS Architecture. Eduvest – Journal of Universal Studies. 2023. Vol. 3, no. 1. P. 265–277. URL: https://doi.org/10.36418/eduvest.v3i1.732

8. Dong W. AIOps Architecture in Data Center Site Infrastructure Monitoring. Computational Intelligence and Neuroscience. 2022. Vol. 2022. P. 1–12. URL: https://doi.org/10.1155/2022/1988990

9. McMillan L., Varga L. A review of the use of artificial intelligence methods in infrastructure systems. Engineering Applications of Artificial Intelligence. 2022. Vol. 116. P. 105472. URL: https://doi.org/10.1016/j.engappai.2022.105472

10. Катков Ю. І., Березовська Ю. В., Заднепрянець О. Ю. Дослідження способів застосування штучного інтелекту для моніторингу ІТ-інфраструктури. Актуальні проблеми кібербезпеки: матеріали Всеукр. науково-практ. конф., м. Київ, 27 жовтня 2023. Київ, 2023. С. 121–122.

11. Bazzell, M. (2021). Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information (9th ed.). IntelTechniques.

12. Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.

13. Hulnick A. S. What's wrong with the Intelligence Cycle. Intelligence and National Security. 2006. Vol. 21, no. 6. P. 959–979. URL: https://doi.org/10.1080/02684520601046291

14. Salganik, M. J. (2018). Bit by Bit: Social Research in the Digital Age. Princeton University Press.

15. Monroe B. L., Colaresi M. P., Quinn K. M. Fightin' Words: Lexical Feature Selection and Evaluation for Identifying the Content of Political Conflict. Political Analysis. 2008. Vol. 16, no. 4. P. 372–403. URL: https://doi.org/10.1093/pan/mpn018

16. NATO. (2022). NATO Open Source Intelligence Handbook. NATO Intelligence Division. URL: https://www.nato.int

17. Kruschwitz, U., & Hull, R. (2017). Searching the Enterprise. Foundations and Trends® in Information Retrieval, 11(1), 1–142. URL: https://doi.org/10.1561/1500000050.

18. Lazer, D., Pentland, A. S., Adamic, L., Aral, S., Barabási, A.-L., Brewer, D., ... & Van Alstyne, M. (2009). Life in the network: The coming age of computational social science. Science, 323(5915), 721–723. URL: https://doi.org/10.1126/science.1167742

19. Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu

20. Graphika. (2023). Network Analysis Reports. URL: https://www.graphika.com

21. OSINT Framework. URL: https://osintframework.com/

22. Функціональна стійкість інформаційних мереж при наявності обмеженої апріорної інформації про надійність / Ю. Березовська та ін. Зв'язок. 2020. № 6(148). С. 42–46.

23. Березовська Ю. Інформаційні системи безперервного використання з часовим резервуванням. Сучасні досягнення компанії Hewlett Packard Enterprise в галузі ІТ та нові можливості їх вивчення і застосування : тези доп. Міжнар. науково-практ. конф., м. Київ, 16 груд. 2020 р. Київ, 2020. С. 6–8.

Автори статті

Катков Юрій – доктор технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0007-1194-4014

Березовська Юлія – PhD, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0002-9973-0497

Клюєва Вікторія – старший викладач, Київський національний університет будівництва і архітектури, Київ, Україна.

ORCID: 0000-0003-1267-0717

Вишнівський Олександр – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0008-0209-9549

Заднепрянець Олександр – магістр, Державний університет інформаційно-телекомунікаційних технологій, Київ, Україна.

ORCID: 0009-0000-6269-558X

Рищиковець Іванна – студент, Державний університет інформаційно-телекомунікаційних технологій, Київ, Україна.

ORCID: 0009-0004-0437-2546

Authors of the article:

Katkov Yuriy – Doctor of Sciences (technical), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0007-1194-4014

Berezovska Yuliia – PhD (technical), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0000-0002-9973-0497
Kliuieva Viktoriia – senior lecturer, Kyiv National University of Construction and Architecture, Kyiv, Ukraine.
ORCID: 0000-0003-1267-0717
Vyshnivskyi Oleksandr – postgraduate, State University of Information and Communication Technology, Kyiv, Ukraine.
ORCID: 0009-0008-0209-9549
Zadneprianets Oleksandr – master, State University of Information and Telecommunications Technologies, Kyiv, Ukraine.
ORCID: 0009-0000-6269-558X
Ryshchykovets Ivanna – student, State University of Information and Telecommunications Technologies, Kyiv, Ukraine.
ORCID: 0009-0004-0437-2546