11. Framework for Teachers' Cyber Literacy in Digital Age. UNESCO. Paris: UNESCO, 2023. 178 p.

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В OSINT ДЛЯ ПОПЕРЕДЖЕННЯ КІБЕРЗАГРОЗ

Ганна СКРИПКА, Олександр СКРИПКА

Сучасний світ зазнає швидких змін завдяки стрімкому розвитку штучного інтелекту (ШІ), який проникає в усі сфери життя, трансформуючи нашу щоденну діяльність, робочі процеси та спосіб взаємодії з технологіями. Кібербезпека також відчуває на собі ці зміни, зокрема, знижується ефективність традиційних засобів захисту і постає питання розробки інноваційних рішень для захисту цифрового простору. Таким рішенням може стати ШІ, оскільки він вже перетворився на ключовий інструмент у боротьбі з кіберзагрозами нового покоління завдяки своїй здатності аналізувати величезні обсяги даних, виявляти аномалії та прогнозувати дії зловмисників.

З метою боротьби з кіберзагрозами, для забезпечення безпеки користувачів в інтернеті сьогодні, з-поміж інших, використовується методологія OSINT. **Розвідка на основі відкритих джерел** (англ. Open source intelligence, **OSINT**) – концепція, методологія й технологія добування та використання військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів. Використовується для ухвалення рішень у сфері національної оборони та безпеки, розслідувань тощо [1]. Таким чином, OSINT дозволяє правоохоронним органам отримувати інформацію з відкритих джерел, що може бути корисним для виявлення та розслідування злочинів, пов’язаних з дітьми та їх діяльністю в інтернеті, а також кібератак, кіберінцидентів, кіберзагроз на об’єктах критичної інфраструктури, установах і підприємствах, державних електронних інформаційних ресурсах і, як наслідок, у прийнятті рішень щодо захисту інформаційних систем.

На сучасному етапі розвитку технологій OSINT не може застосовуватись без використання ШІ, оскільки ця технологія спрощує та прискорює процес

збору, аналізу й обробки даних із відкритих джерел. Штучний інтелект допомагає:

- ідентифікувати ключові об’єкти, як-от люди, місця, організації;
- виявляти аномалії та маніпуляції у текстах, зображеннях або відео;
- збирати дані в реальному часі з різноманітних джерел;
- аналізувати природну мову (NLP) для виявлення трендів, емоцій та ключових фраз;
- визначати зв’язки та закономірності у даних та, як наслідок – отримувати інформацію про тенденції, взаємозв’язки та потенційні загрози;
- виявляти кіберзагрози, зокрема, для оновлення даних систем виявлення вторгнень (IDS), що дозволяє виявляти різні форми шкідливої активності в реальному часі, такі як комунікації з C&C серверами ботнетів, атаки грубої сили та фішингові події [2].

ШІ-інструменти та методи виявлення кіберзагроз.

- Платформи обміну та аналізу інформації про загрози.

Платформи, такі як Malware Information Sharing Platform (MISP), сприяють обміну інформацією про загрози, що допомагає у запобіганні та виявленні кібератак [3]. Усі дані, які з’являються на платформі MISP – це ексклюзивні дані з першоджерел. Користувач отримує доступ до мережі, якою користуються провідні кіберфахівці світу, й має змогу бути у курсі найсвіжіших та найгарячіших подій. MISP є потужним агрегатором і сховищем – різноманітної інформації, оскільки містить енциклопедичну, довідкову, хронологічну інформацію по кіберзагрозам. Ще однією перевагою цієї платформи є те, що вона дає можливість не тільки читати, а й самому активно брати участь, ділитися власними спостереженнями, створювати нові події про загрози та відправляти їх через MISP у спільноту кіберфахівців усього світу [4].

Таблиця 1

Порівняльна таблиця платформ на основі штучного інтелекту для OSINT та виявлення кіберзагроз

Платформа	**Основне призначення**	**Основні функції**	**Ключова аудиторія**	**Унікальні особливості**
Maltego https://www.maltego.com/	Аналіз OSINT	Візуалізація зв'язків, збір метаданих	Аналітики, слідчі	Інтеграція з багатьма джерелами даних
SpiderFoot (складова дистрибутива Kali Linux)	Автоматизація збору OSINT	Аналіз доменів, IP-адрес, контактних даних	Фахівці з безпеки	200+ модулів для глибокого аналізу
Mantis Analytics https://mantisanalytics.com/	Виявлення інформаційних атак	Відстеження соціальних медіа, розпізнавання фейків	Державні структури, бізнес	Спеціалізація на боротьбі з ІПСО (інформаційно-психологічними операціями)
HARVESTER https://t.me/zedigital/4502, відкритого доступу для користувачів немає	Обробка великих масивів даних	Пошук у текстах, відео, аудіо, зображеннях	Державна розвідка	Обробка багатьох форматів даних
SentinelOne https://www.sentinelone.com/	Реагування на кіберзагрози	Виявлення атак, автоматична обробка	Корпорації, бізнес	Захист у реальному часі на базі ШІ
ThreatCloud AI https://www.checkpoint.com/ai/threatcloud/	Виявлення нових кіберзагроз	Аналіз загроз, шкідливих програм	Корпорації, IT-спеціалісти	Машинне навчання для прогнозування атак
Strider https://www.striderintel.com/	Моніторинг активності кіберактрів	Оцінка загроз від державних і комерційних суб'єктів	Уряди, великі компанії	Фокус на діяльність державних хакерів
MISP (Malware Information Sharing Platform) https://www.misp-project.org/	Обмін інформацією про загрози	Збір і поширення інформації про шкідливе програмне забезпечення та індикатори загроз	Кібербезпека, аналітики	Відкрите джерело, підтримка співпраці між організаціями

- Аналітичні методи, засновані на ШІ.

Для обробки даних OSINT використовуються методи глибинного аналізу даних, лінгвістичні та статистичні методи, а також методи кластерного аналізу для виявлення та візуалізації концепцій, пов'язаних з кібербезпекою. Інтеграція таких методів допомагає покращити виявлення та реакцію на кіберзагрози в реальному часі.

Таблиця 2

Аналітичні методи на основі ШІ для OSINT у виявленні кіберзагроз

Метод	Призначення	Приклади використання	Переваги
Машинне навчання (Machine Learning)	Аналіз великих обсягів даних, виявлення аномалій	• Виявлення аномалій у поведінці користувачів. • Прогнозування кіберзагроз на основі історичних даних.	Швидке адаптування до нових загроз
Обробка природної мови (NLP)	Аналіз текстів, отриманих із відкритих джерел	• Виявлення фраз на форумах кіберзлочинців. • Аналіз тональності для виявлення загроз.	Швидкий аналіз великих текстових даних
Аналіз графів і зв'язків	Візуалізація зв'язків між об'єктами	• Побудова зв'язків між IP, доменами та поштовими скриньками. • Виявлення взаємодії в кіберзлочинних групах.	Відкриття складних зв'язків між об'єктами
Автоматизований моніторинг соцмереж	Аналіз активності в соціальних мережах	• Виявлення підозрілих акаунтів або ботів. • Виявлення фішингових повідомлень у реальному часі.	Прискорений збір даних із соцмереж
Аналіз часових рядів	Відстеження трендів і аномалій у даних	• Моніторинг росту шкідливих DNS-запитів. • Виявлення тенденцій атак у певні періоди.	Забезпечення прогнозування загроз
Інструменти візуалізації даних	Інтерактивне представлення великих масивів даних	• Створення теплових карт атак (http://surl.li/ugzjew). • Графічний аналіз даних про мережевий трафік або загрози.	Покращена зрозумілість складних даних
Інтелектуальний аналіз зображень	Аналіз графічних файлів для виявлення загроз	• Розпізнавання шкідливих зображень (QR-кодів, логотипів). • Виявлення активності в медіаконтенті.	Високоточний аналіз візуального контенту

Ці методи дають змогу ефективно виявляти кіберзагрози у реальному часі, обробляти великі обсяги даних і адаптуватися до нових викликів кібербезпеки.

Разом з тим, використання OSINT для виявлення кіберзагроз вимагає суворого **дотримання етичних норм і законодавства про захист даних**. Оскільки OSINT працює з відкритими джерелами, можуть виникнути ситуації, де межа між легальним збором інформації та порушенням конфіденційності є нечіткою. Наприклад, якщо компанія проводить моніторинг соціальних мереж на предмет підозрілих активностей, і для цього зберігає та аналізує особисті дані користувачів без їх згоди, це може порушувати нормативні акти, такі як Закон про захист персональних даних [5], GDPR (General Data Protection Regulation) [6] у країнах ЄС або аналогічні закони в інших країнах. Також подібний аналіз відкритих даних може вплинути на репутацію конкретних людей чи компаній, якщо в ході пошуку кіберзагроз було виявлено акаунт як потенційне джерело загрози і оприлюднено результати дослідження, висунуто публічні звинувачення тощо. Попри те, що в Україні подібний досвід поки що незначний, важливо, щоб організації чітко визначали межі між дозволеним і забороненим під час використання інструментів OSINT. Також робота з OSINT з використанням штучного інтелекту потребує дотримання норм про конфіденційність даних та регулювання ШІ, як це визначено Європейським Законом про штучний інтелект AI Act [7]. Не зважаючи на те, що в Україні поки що немає подібного закону, який би чітко регламентував ступені ризику використанні ШІ в різних сферах, застосування методології OSINT з використанням ШІ має бути законним та прозорим, щоб уникнути репутаційних, правових і, як наслідок, фінансових ризиків. Особливо актуальними етичні аспекти стають у випадках міжнаціонального використання OSINT, оскільки законодавчі норми різних країн можуть суттєво відрізнятися.

Отже, штучний інтелект відкриває нові горизонти у використанні OSINT для виявлення кіберзагроз, значно підвищуючи ефективність, точність і швидкість аналізу даних. Методи на основі машинного навчання, обробки природної мови, аналізу графів і часових рядів дають змогу аналізувати великі обсяги інформації з відкритих джерел у реальному часі, що є вирішальним для попередження атак і оцінки ризиків. Використання інструментів для візуалізації

та інтелектуального аналізу медіа дозволяє зробити процес роботи більш прозорим і зрозумілим для аналітиків.

Використання цих підходів у поєднанні з ретельно спланованою стратегією дозволить значно покращити кібербезпеку, дотримуючись при цьому етичних та юридичних норм.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Розвідка на основі відкритих джерел. *Вікіпедія*: URL: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D0%B2%D1%96%D0%B4%D0%BA%D0%B0_%D0%BD%D0%B0_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%96_%D0%B2%D1%96%D0%B4%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%85_%D0%B4%D0%B6%D0%B5%D1%80%D0%B5%D0%BB (дата звернення: 23.01.2025).

2. Vacas I., Medeiros I., & Neves N. Detecting Network Threats using OSINT Knowledge-Based IDS. 2018 14th European Dependable Computing Conference (EDCC). 2018. P. 128-135. https://doi.org/10.1109/EDCC.2018.00031.

3. Положення про порядок обміну інформацією з використанням адаптованого програмного продукту «Malware Information Sharing Platform and Threat Sharing «Ukrainian Advantage» (MISP-UA)»: Положення / Служба Безпеки України. URL: https://zakon.rada.gov.ua/laws/show/z2164-23#Text (дата звернення: 23.01.2025).

4. Що таке платформа MISP і як нею користуватися? KR. *LABORATORIES* : URL: https://kr-labs.com.ua/blog/shcho-take-platforma-misp (дата звернення: 23.01.2025).

5. Про захист персональних даних: Закон України від 01 черв. 2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 23.01.2025).

6. Need to learn more about the GDPR? *Usercentrics Cookiebot*: website. URL: https://www.cookiebot.com/en/uk-ie-gdpr-cookies/?utm_source=google&utm_medium=cpc&utm_term=gdpr%20web&utm_campaign=cb_dm_ww_eng_generic_cent-east-europe_search&utm_content=cent-eu-eng-

gdpr-website&campaign_id=1334729411&adset_id=57502227110&ad_id=591275250945&matchtype=p&utm_device=c&gad_source=1&gclid=Cj0KCQiAy8K8BhCZARIsAKJ8sfTYPAYDsZaySRx_3BhM8soROHMywH20k-6PDZytgA_XhRTW_iJOTuEaAoemEALw_wcB (Last accessed: 23.01.2025).

7. European Artificial Intelligence Act comes into force. *European Commission*: URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4123 (Last accessed: 23.01.2025).

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВОМУ СЕРЕДОВИЩІ ЯК СКЛАДОВА КІБЕРГРАМОТНОСТІ ПЕДАГОГА

Роман СТЕПАНЕНКО

Сучасний освітній процес все більше інтегрується в цифровий простір. Використання електронних журналів, дистанційного навчання, хмарних сервісів та соціальних мереж відкриває нові можливості для педагогів і учнів. Проте, разом із цим, зростають ризики витоку конфіденційної інформації, шахрайства та порушення прав використання особистої інформації.

Захист персональних даних є не лише правовою вимогою, а й важливим елементом цифрової грамотності сучасного педагога. Учителі повинні не тільки самі дотримуватися норм кібербезпеки, але й навчати цьому учнів.

Персональні дані – це будь-яка інформація, що дозволяє ідентифікувати конкретну особу. Вони поділяються на:

- Основні ідентифікаційні дані (ПІБ, дата народження, номер телефону, адреса).
- Фінансова інформація (банківські реквізити, паролі до платіжних систем).
- Освітні та професійні дані (місце роботи, освіта, сертифікати, дипломи).
- Цифрові сліди (історія пошуку, IP-адреси, активність у соцмережах).