заборони не працюють, працює лише зрозуміла логіка. Запропонований алгоритм прийняття рішень може бути інтегрований у навчальний процес, зокрема у вигляді рекомендацій для студентів і викладачів. Він дозволяє швидко визначити, чи є використання штучного інтелекту допустимим у конкретній ситуації.

Практична цінність результатів полягає у можливості створення систем підтримки прийняття рішень, які автоматизують контроль за використанням ШІ. У перспективі це може перерости у повноцінні освітні платформи нового типу.

Висновки. Проведене дослідження показало, що генеративні моделі штучного інтелекту не є ні абсолютним благом, ні абсолютною загрозою. Вони — інструмент. І питання лише в тому, як саме ми його використовуємо.

Було визначено основні етичні ризики, пов'язані з використанням ШІ в освіті, та доведено необхідність їх системного регулювання. Запропонована модель дозволяє формалізувати правила використання генеративних технологій і може бути застосована в освітніх установах. Ключовий висновок полягає в тому, що освіта повинна адаптуватися до нових реалій, не втрачаючи своїх базових принципів. Штучний інтелект може підсилювати навчання, але не повинен замінювати мислення.

УДК 004.6:343.98

OSINT-ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ КРИМІНАЛЬНОГО АНАЛІЗУ: ПРОБЛЕМИ ВЕРИФІКАЦІЇ ТА ОБРОБКИ ВЕЛИКИХ МАСИВІВ ДАНИХ

ЛУНГОЛ О.М., ВОЛОБОЄВА З.О.
(olyalungol@gmail.com; ordtaib@dnuvs.ukr.education)
Донецький державний університет внутрішніх справ

У тезах досліджується роль розвідки на основі відкритих джерел (OSINT) у сучасному кримінальному аналізі. Виокремлено основні проблеми, з якими стикаються підрозділи поліції під час збору цифрових доказів: обробка великих масивів даних (Big Data) та верифікація інформації в умовах поширення дезінформації. Запропоновано шляхи оптимізації аналітичної роботи через автоматизацію процесів.

Постановка проблеми. В епоху тотальної цифровізації та в умовах воєнного стану злочинна діяльність залишає значний цифровий слід. Відповідно до завдань оперативно-розшукової діяльності [1], правоохоронні органи потребують ефективних інструментів для збору та аналізу інформації. Технології OSINT (Open Source Intelligence) стали невід'ємною складовою кримінального аналізу. Проте ефективність їх застосування критично знижується через дві ключові проблеми: експоненційне зростання обсягів даних (Big Data) та складність підтвердження їхньої достовірності (верифікації).

Виклад основного матеріалу. Сучасний кримінальний аналіз вимагає від оперативного працівника не лише вміння знаходити інформацію в соціальних мережах, реєстрах чи тіньовому сегменті інтернету (DarkNet), а й здатності структурувати ці розрізнені масиви.

Перша актуальна проблема – це обробка великих масивів даних. Ручний пошук та аналіз інформації вже втратили свою актуальність. Перед підрозділами кримінальної поліції постає завдання обробки терабайтів неструктурованих даних: текстів, метаданих фотографій, геолокацій, графів зв'язків і т.д. Все це вимагає впровадження спеціалізованого програмного забезпечення, наприклад, інструментів візуалізації зв'язків типу Maltego, систем автоматизованого скрапінгу, що здатне агрегувати дані за заданими алгоритмами та формувати цифрові профілі об'єктів інтересу.

Друга, не менш гостра проблема – це верифікація даних. В умовах інформаційної війни та стрімкого розвитку генеративного штучного інтелекту (реалістичного створення діпфейків,

синтезованого голосу, згенерованих текстів тощо) відкриті джерела часто містять навмисно спотворену або хибну інформацію. Для кримінального провадження використання неперевірених даних є неприпустимим, оскільки вони не можуть набути статусу електронних доказів. Процес верифікації вимагає багатоступеневої перехресної перевірки з використанням незалежних закритих баз даних, поглибленого аналізу EXIF-даних медіафайлів та криптографічного підтвердження цілісності інформації.

Для ефективного подолання зазначених викликів критично необхідною є комплексна модернізація системи фахової підготовки майбутніх спеціалістів для сектору безпеки і оборони. В умовах стрімкої цифровізації злочинності традиційні підходи до навчання втрачають свою дієвість, вимагаючи впровадження інноваційних освітніх стратегій. Відповідно, під час вивчення профільних дисциплін циклу інформаційної безпеки, кримінального аналізу та оперативно-розшукової діяльності акцент має безальтернативно зміщуватися з теоретико-правових засад на інтенсивне практичне використання спеціалізованих OSINT-інструментів. Це передбачає широке впровадження у навчальний процес тренінгових технологій, ситуаційних моделювань та роботи з матеріалами віртуальних слідчих справ, де здобувачі в умовах, наближених до реальних, відпрацьовують алгоритми збору цифрових слідів.

Сучасні здобувачі вищої освіти повинні глибоко опановувати не лише методики пошуку, а й суворі правила оперативної кібергігієни, щоб уміти захищати власну цифрову ідентичність та безпечно працювати в інформаційному середовищі. Окрему увагу необхідно приділяти розвитку критичного мислення: методам фільтрації інформаційного шуму, перехресній перевірці фактів та розпізнаванню згенерованих нейромережами маніпуляцій. Водночас обов'язковою компетентністю для розв'язання аналітичних завдань має стати володіння базовими алгоритмами автоматизованої обробки відкритих даних: від розуміння принципів роботи скриптів для парсингу соціальних мереж до впевненого застосування програмного забезпечення для побудови графів зв'язків і візуалізації великих масивів розрізненої інформації [2; 3].

Висновки. OSINT є потужним інструментом кримінального аналізу, однак його використання без застосування технологій автоматизації та суворих протоколів верифікації є малоефективним. Подальший розвиток інформаційних систем для потреб Національної поліції має бути орієнтований на створення відомчих аналітичних платформ, здатних швидко обробляти Big Data та автоматично виявляти аномалії, що свідчать про маніпуляції з даними. Це забезпечить правоохоронців надійною доказовою базою та сприятиме ефективнішому розкриттю злочинів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII (зі змінами). [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2135-12#Text

[2] O. Haborets and O. Lunhol, «Methods of using OSINT in cyberpolice activities» in Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності: Міжнар. наук.-практ. конф., Кропивницький: ТОВ «Центрально-Українське видавництво», 2023, с. 76–77.

[3] О. М. Лунгол, «Удосконалення професійної підготовки майбутніх фахівців правоохоронної діяльності засобами інформаційних технологій,» Наука і техніка сьогодні, № 7(7), с. 153–163, 2022.