DOI https://doi.org/10.36059/978-966-397-550-4-57

КРИМІНАЛЬНИЙ АНАЛІЗ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ШТУЧНОГО ІНТЕЛЕКТУ У ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Семенюк М. О.
здобувач
Одеський державний університет внутрішніх справ
м. Одеса, Україна
Науковий керівник: **Грезіна О. М.**
доктор філософії, доцент кафедри кримінального аналізу та інформаційного аналізу
Одеський державний університет внутрішніх справ
м. Одеса, Україна

Сучасний світ стикається з безпрецедентним зростанням кіберзлочинності, яка стає все більш складною та глобальною. Кримінальний аналіз як ключовий елемент правоохоронної діяльності набуває нового значення завдяки інтеграції інформаційних технологій (ІТ) та штучного інтелекту (ШІ). Актуальність теми зумовлена стрімким розвитком цифрових технологій, які, з одного боку, полегшують злочинну діяльність, а з іншого – надають потужні інструменти для її протидії. Згідно з даними Europol, ШІ може радикально трансформувати поліцейську роботу, дозволяючи аналізувати величезні обсяги даних для виявлення тенденцій та ідентифікації злочинців [1].

Кіберзлочини, такі як фішинг, ransomware та хакерські атаки, завдають мільярдні збитки економікам країн. У 2024 році кількість кібератак зросла на 30% порівняно з попереднім роком, що вимагає від правоохоронних органів адаптації до нових викликів. Кримінальний аналіз, базований на ІТ, включає збір, обробку та інтерпретацію даних з метою прогнозування злочинів. ШІ посилює цей процес, автоматизуючи рутинні завдання та підвищуючи точність прогнозів.

Інформаційні технології є основою сучасного кримінального аналізу в правоохоронній сфері. Вони дозволяють інтегрувати дані з різних джерел: соціальних мереж, банківських транзакцій, відеоспостереження та мереж Інтернету речей (IoT). Наприклад, системи big data аналізують петабайти інформації для виявлення патернів злочинної поведінки. У протидії кіберзлочинам ІТ використовуються для моніторингу мереж, виявлення аномалій та автоматизованого збору доказів.

Одним з ключових інструментів є системи автоматизованого аналізу, такі як мережеві сканери та інструменти форензичного аналізу. Вони допомагають у розслідуванні інцидентів, відновлюючи ланцюжок подій після атаки. Наприклад, програмне забезпечення для аналізу логів може виявити несанкціонований доступ до систем, що є критичним для запобігання подальшим атакам. Дослідження 2024 року показують, що використання AI-powered систем для ідентифікації та розслідування кіберзлочинів значно підвищує ефективність кібербезпеки в правоохоронних органах [2]. Однак, впровадження ІТ вимагає вирішення проблем конфіденційності даних та відповідності законодавству, наприклад, GDPR в Європі чи аналогічним нормам в Україні.

Штучний інтелект революціонізує кримінальний аналіз, перетворюючи реактивну модель правоохоронної діяльності на проактивну. ШІ використовується для передбачення злочинів (predictive policing), аналізуючи історичні дані для прогнозування потенційних загроз. У сфері кіберзлочинності ШІ застосовується для виявлення фішингових кампаній, аналізу шкідливого ПЗ та ідентифікації ботнетів. Наприклад, алгоритми машинного навчання можуть розпізнавати аномалії в мережевому трафіку, сигналізуючи про можливу DDoS-атаку до її початку.

Одним з перспективних напрямків є використання ШІ для цифрової криміналістики. Системи на базі ШІ аналізують зображення, голоси та тексти для ідентифікації злочинців, навіть у зашифрованих каналах. У 2025 році очікується зростання використання ШІ для запобігання корпоративним злочинам, включаючи кібератаки, де ШІ допомагає у виявленні та розслідуванні з юридичної перспективи. Приклади включають системи, подібні до тих, що використовує FBI, для аналізу dark web та виявлення торгівлі забороненими товарами [3].

Проте, ШІ несе ризики: злочинці також використовують його для створення deepfakes чи автоматизованих атак. Тому правоохоронні органи повинні впроваджувати етичні стандарти та регуляції. В Україні, наприклад, Національна поліція вже тестує ШІ-системи для моніторингу кіберпростору, але потребує подальшого розвитку законодавчої бази для забезпечення балансу між ефективністю та правами людини.

Впровадження ІТ та ШІ у кримінальний аналіз стикається з викликами: браком кваліфікованих спеціалістів, високою вартістю технологій та ризиками упередженості алгоритмів. Крім того, глобальний характер кіберзлочинів вимагає міжнародної співпраці, наприклад, через Інтерпол чи Конвенцію про кіберзлочинність. Перспективи включають інтеграцію ШІ з блокчейном для безпечного обміну даними між країнами.

Застосування ІТ та ШІ є ключем до ефективної протидії кіберзлочинам. Вони підвищують оперативність, точність та превентивність правоохоронної діяльності. Рекомендується інвестувати в освіту кадрів, розробку

національних стратегій та міжнародне партнерство для максимізації переваг цих технологій.

Література:

1. Europol. AI and policing : the benefits and challenges of artificial intelligence for law enforcement : Observatory report. Luxembourg : Publications Office of the European Union, 2024. 48 p. ISBN 978-92-95236-35-6. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf

2. Hope, Ch. S. Using AI-powered systems to identify and investigate cybercrimes to enhance cybersecurity in law enforcement. *Issues in Information Systems*. 2024. Vol. 25, Iss. 1. P. 293–304. URL: https://iacis.org/iis/2024/1_iis_2024_293-304.pdf

3. Sharma, V. Artificial intelligence in cybercrime prevention, detection & investigation: A legal perspective. *VIDHIGYA: The Journal of Legal Awareness.* 2024. Vol. 19, Iss. 1 and 2. P. 34–38. DOI:10.5958/0974-4533.2024.00004.4. URL: https://indianjournals.com/article/vidhigya-19-1and2-004

DOI https://doi.org/10.36059/978-966-397-550-4-58

ЗНАЧЕННЯ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА У ПРОТИДІЇ ВОЄННИМ ЗЛОЧИНАМ

Чорний І. Я.
аспірант
Донецький державний університет внутрішніх справ
м. Кропивницький, Україна

Національне законодавство, традиційно, формується із урахуванням потреб держави та суспільства, які є актуальними на певному етапі державотворення. Це надає можливість зберігати динаміку, необхідну для регулювання та захисту відповідних суспільних відносин. В умовах збройного конфлікту, розв'язаного російською федерацією проти України в законодавство було внесено низку змін та доповнень, пов'язаних як із виникненням потреби у забезпеченні функціонування критично важливих інституцій, так і з необхідністю у посиленні механізму захисту національної безпеки України.

Протягом останніх років, із урахуванням курсу держави на євроінтеграцію, зміст правотворчої діяльності, здебільшого, полягав у забезпеченні імплементації до нормативно-правових актів європейських та