МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
КОНСУЛЬТАТИВНА МІСІЯ ЄС В УКРАЇНІ
НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ КРИМІНАЛЬНОГО АНАЛІЗУ

АКТУАЛЬНІ ПИТАННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КРИМІНАЛЬНОГО АНАЛІЗУ В ПРАВООХОРОННІЙ СИСТЕМІ УКРАЇНИ

Матеріали
міжвідомчої науково-практичної конференції
(Київ, 23 липня 2025 року)

Київ
2025

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
КОНСУЛЬТАТИВНА МІСІЯ ЄС В УКРАЇНІ
НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ КРИМІНАЛЬНОГО АНАЛІЗУ

АКТУАЛЬНІ ПИТАННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КРИМІНАЛЬНОГО АНАЛІЗУ В ПРАВООХОРОННІЙ СИСТЕМІ УКРАЇНИ

Матеріали
міжвідомчої науково-практичної конференції
(Київ, 23 липня 2025 року)

Київ
2025

УДК 343.97(477)(06)
А437

Рекомендовано до друку науково-методичною радою Національної академії внутрішніх справ 24 вересня 2025 року (протокол № 8)

Матеріали подано в авторській редакції. Відповідальність за їхню якість, а також відсутність у них відомостей, що становлять державну таємницю та службову інформацію, несуть автори

А437 **Актуальні** питання та перспективи розвитку кримінального аналізу в правоохоронній системі України [Текст] : матеріали міжвідом. наук.-практ. конф. (Київ, 23 лип. 2025 р.) / редкол.: О. С. Тарасенко, Р. Ю. Бутко, Д. І. Овсянюк. – Київ : Нац. акад. внутр. справ, 2025. – 141 с.

УДК 343.97(477)(06)

ЗМІСТ

ВСТУПНІ СЛОВА

Сербин Р. А. 6

Нєбитов А. А. 8

Бутко Р. Ю. 10

НАУКОВІ ДОПОВІДІ

Білик В. М.
ПРОБЛЕМИ ЗАКОНОДАВЧОГО ТА МІЖВІДОМЧОГО НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ В ПРАВООХОРОННІЙ СИСТЕМІ УКРАЇНИ 12

Бойко В. М.
ОКРЕМІ НАПРЯМИ ЗАСТОСУВАННЯ МОЖЛИВОСТЕЙ КРИМІНАЛЬНОГО АНАЛІЗУ ПІД ЧАС РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ 16

Буренко О. В.
ВИКОРИСТАННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В УКРАЇНІ 22

Денисенко Г. В.
КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУАЛЬНО-ПРАВОВИХ ГАРАНТІЙ ЗБЕРЕЖЕННЯ ОХОРОНЮВАНОЇ ЗАКОНОМ ІНФОРМАЦІЇ НА ДОСУДОВОМУ РОЗСЛІДУВАННІ 30

Кіреєва О. С.
РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ В УКРАЇНІ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ РФ: ДОСВІД, ТЕНДЕНЦІЇ, ПЕРСПЕКТИВИ 33

Клименко В. А., Постол О. І.
ПІДГОТОВКА АНАЛІТИКІВ КРИМІНАЛЬНОГО АНАЛІЗУ В СИСТЕМІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ 39

Колесник О. А.
ТАКТИЧНИЙ АНАЛІЗ ДАНИХ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ПРАКТИКА HOT-SPOTS POLICING 41

Копитько В. Ю.
ФОРМИ МАСКУВАННЯ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ ПІД ВИГЛЯДОМ ГУМАНІТАРНОЇ МІСІЇ 44

Лазарєва Я. А.
ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ.....48

Лемешко Ю. О.
ПРОБЛЕМНІ ПИТАННЯ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ АНАЛІЗУ АКТИВНОСТІ КОРИСТУВАЧІВ БЕЗ СУДОВОГО САНКЦІОНУВАННЯ 53

Овсянюк Д. І.
ОРГАНІЗАЦІЯ АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ У СФЕРІ ПРОТИДІЇ НАРКОЗЛОЧИННОСТІ 58

Овчаренко Е. В.
МОЖЛИВОСТІ ВИКОРИСТАННЯ ВБУДОВАНОГО РЕДАКТОРА POWER QUERY ТА POWER PIVOT 62

Олейніков О. А.
МЕТОДИ GRAPH INTELLIGENCE Й АНАЛІЗ СХЕМ ЗВ'ЯЗКІВ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ. 64

Пазуха А. П.
ВИКОРИСТАННЯ В КРИМІНАЛЬНОМУ АНАЛІЗІ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ, ЗОКРЕМА ШТУЧНОГО ІНТЕЛЕКТУ 69

Панченко Є. В.
РОЛЬ ДЕПАРТАМЕНТУ МІЖНАРОДНОГО ПОЛІЦЕЙСЬКОГО СПІВРОБІТНИЦТВА В РОЗВИТКУ КРИМІНАЛЬНОЇ АНАЛІТИКИ В УКРАЇНІ: ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ СИСТЕМИ NEXUS 73

Петров В. А.
МЕДІААНАЛІЗ. СУЧАСНІ ПІДХОДИ ТА МЕТОДИ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ.....76

Погорецький М. М.
ТАЄМНЕ СПОСТЕРЕЖЕННЯ В ДЕМОКРАТИЧНОМУ СУСПІЛЬСТВІ: БАЛАНС МІЖ БЕЗПЕКОЮ І ПРАВАМИ ЛЮДИНИ.....79

Разєнков Є. В.
ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ ТА СЛІДЧИХ ОРГАНІВ ПІД ЧАС ДОКУМЕНТУВАННЯ І РОЗСЛІДУВАННЯ ЗЛОЧИНІВ 84

Рогатюк І. В.
АНАЛІЗ СТАНУ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ
ЯК ОСНОВА ПРОТИДІЇ ЗЛОЧИННОСТІ 89

Сарафанюк М. С.
ПІДГОТОВКА АНАЛІТИКІВ 94

Сергєєв Д. О.
СПІВПРАЦЯ ПОЛІЦІЇ ТА ПРИВАТНОГО СЕКТОРУ
В КРИМІНАЛЬНОМУ АНАЛІЗІ 98

Соловйов Е. П., Осуховський Р. В., Пефтієв Д. О.
РОЛЬ НОВІТНЬОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
«СЛІДЧИЙ ПРОТОКОЛ» У ПІДВИЩЕННІ
ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ СЛІДЧИХ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ 102

Старенький О. С.
ПОЗБАВЛЕННЯ ДЕРЖАВНИХ НАГОРОД
НА ПІДСТАВІ ОБВИНУВАЛЬНОГО ВИРОКУ СУДУ 105

Темник О. П.
ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ,
ЗОКРЕМА ШТУЧНОГО ІНТЕЛЕКТУ,
У КРИМІНАЛЬНОМУ АНАЛІЗІ 114

Худенко Д. М.
МІСЦЕ СЛОВНИКІВ І ДОВІДНИКІВ У БІБЛІОГРАФІЇ
НАЦІОНАЛЬНОЇ ТЕРМІНОСИСТЕМИ
З КРИМІНАЛЬНОГО АНАЛІЗУ 116

Цуцкірідзе М. С.
ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ КРИМІНАЛЬНОГО
АНАЛІЗУ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ:
ПРОГАЛИНИ В ЗАКОНОДАВЧОМУ РЕГУЛЮВАННІ 124

Чепурна Т. В.
ДОПИТ ПІДОЗРЮВАНИХ ПІД ЧАС РОЗСЛІДУВАННЯ
КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, УЧИНЕНИХ
ПРАЦІВНИКАМИ ПРАВООХОРОННИХ ОРГАНІВ..... 128

Шаповаленко Є. В.
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ
В ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ 133

Шевчишен А. В.
КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ДОПОМІЖНИЙ
ІНСТРУМЕНТ ФОРМУВАННЯ ТА ЗБИРАННЯ
ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ 137

ВСТУПНІ СЛОВА

Сербин Руслан Андрійович,
ректор Національної академії внутрішніх справ, доктор юридичних наук, професор

Шановні учасники конференції!
Дорогі колеги, партнери та друзі!

Від імені колективу Національної академії внутрішніх справ щиро вітаю вас на міжвідомчій науково-практичній конференції «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України».

Надзвичайно приємно приймати в нашому закладі провідних фахівців, науковців і міжнародних експертів. Висловлюю особливу подяку нашим співорганізаторам – Консультативній місії Європейського Союзу в Україні й Департаменту кримінального аналізу Національної поліції України – за плідну співпрацю.

Підготовка висококваліфікованих правоохоронців є одним із ключових завдань академії. Ми переконані, що поєднання академічних знань із практичним досвідом дає змогу формувати фахівців нового покоління, здатних мислити системно, володіти сучасними аналітичними методами й інструментами, діяти стратегічно та ефективно реагувати на виклики часу. Конференція є важливим етапом у цьому процесі, адже вона створює унікальні умови для обміну знаннями, формування професійних зв'язків і спільного пошуку рішень.

Цей захід є платформою для об'єднання зусиль навколо важливої мети – розвитку й удосконалення кримінального аналізу в діяльності правоохоронних органів нашої держави. В умовах сучасних викликів ефективна аналітична робота є запорукою успішної протидії злочинності. Саме тут ми маємо змогу не лише представити передовий досвід, а й разом напрацьовувати ефективні рішення для майбутнього. Упевнений, що результатом спільної роботи стануть практичні пропозиції та перспективні ініціативи, які сприятимуть якісному розвитку кримінального аналізу в Україні.

Переконаний, що відкрита дискусія, об’єднання зусиль науковців, практиків, експертів провідних ІТ-компаній та міжнародних партнерів стимулюватимуть подальший розвиток правоохоронної аналітики та її ефективну інтеграцію в систему забезпечення національної безпеки України.

Бажаю всім учасникам плідної роботи, натхнення та конструктивних рішень! Слава Україні!

Нєбитов Андрій Анатолійович,
заступник Голови Національної поліції України – начальник кримінальної поліції, доктор юридичних наук, професор

Вітаю учасників сьогоднішньої зустрічі!

Традиційно після відзначення досягнень, здійснених упродовж восьми років існування служби кримінального аналізу, проводимо щорічну міжвідомчу науково-практичну конференцію «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України».

Слід зазначити, що аналітики постійно демонструють приклад високої адаптивності, оперативності, професіоналізму у виконанні поставлених завдань та налаштованість на постійне професійне зростання й удосконалення.

За роки розбудови системи кримінального аналізу оперативні та слідчі підрозділи високо оцінили можливості інформаційно-аналітичного супроводу розкриття тяжких та особливо тяжких злочинів і роль кримінальних аналітиків у розробленні першочергових кроків у сфері реагування на кримінальну подію.

Одним з основних пріоритетів служби є інтеграція у світовий правоохоронний простір, адаптація світових аналітичних норм і стандартів під потреби нашої держави.

В умовах сьогодення підрозділи кримінального аналізу мають унікальні можливості використання в практичній діяльності широкого спектру доступів до реєстрів, банків і баз даних державного і місцевого рівнів, застосування найсучасніших програмно-пошукових компонентів і ресурсів, основаних на механізмах штучного інтелекту.

Завдяки цьому представники служби стали рівноправною складовою світової спільноти кримінальних аналітиків.

Керівництво Національної поліції та реалії сьогодення ставлять перед службою кримінального аналізу складні та амбітні завдання, з якими підрозділ успішно справляється.

Зокрема, участь у розкритті воєнних злочинів – кропітка робота по відпрацюванню кожного повідомлення, проведення аналітики відеоматеріалів, структурування отриманої інформації

за великою кількістю параметрів, і як наслідок визначення військових формувань, розпізнання військовослужбовців рф, причетних до вчинення злочинів на території України, аналіз російської військової техніки тощо.

Кримінальні аналітики також беруть активну участь у встановленні місцезнаходження громадян України, зокрема дітей, яких примусово перемістили (депортували) на територію російської федерації, республіки білорусь та тимчасово окуповані території України. З використанням OSINT-розвідки, програм розпізнавання та інших аналітичних інструментів здійснюється відпрацювання кожної зниклої особи на предмет зв'язків та контактів, через які можна встановити її місце перебування.

Не залишено поза увагою аналітиків також і участь у документуванні та розкритті злочинів на інших пріоритетних напрямах – наркозлочини, незаконний обіг зброї, шахрайства, незаконне переправлення через державний кордон України.

Хочу зазначити про важливість розвитку аналітиків та освоєнні нових напрямів, побажати постійно навчатися та нарощувати міжнародне партнерство.

Бутко Роман Юрійович,
начальник Департаменту кримінального аналізу Національної поліції України

Шановні учасники конференції!

У зв'язку в постійним виникненням нових загроз, кримінальний аналіз стає необхідним інструментом, який дозволяє забезпечувати якісні рішення в сфері правопорядку та безпеки суспільства.

На Департамент кримінального аналізу покладено завдання з проведення, організації та координації інформаційно-пошукової й аналітичної роботи, спрямованої на збір, оцінку та реалізацію інформації, у тому числі з обмеженим доступом, шляхом надання її уповноваженим органам (підрозділам) для вжиття заходів відповідно до їх компетенції, оцінювання ризиків, а також використання її для забезпечення функцій покладених на поліцію (Положення про Департамент кримінального аналізу затверджене наказом (зі змінами) Національної поліції України від 29 грудня 2019 року № 1354).

Департамент на постійній основі вживає заходів, спрямованих на розбудову та розширення аналітичних спроможностей служби, підвищення рівня ефективності інформаційно-пошукової та інформаційно-аналітичної діяльності з урахуванням дії правового режиму воєнного стану, активізацію взаємодії з територіальними органами та підрозділами Національної поліції.

Розбудова потужностей кримінального аналізу протягом усього періоду супроводжувалася активною співпрацею з міжнародними партнерськими організаціями та адаптацією набутого досвіду. Ці складові лягли в основу реформування та реорганізації служби, розвитку її структури.

На основі зарубіжної практики керівництвом Національної поліції ухвалено рішення про необхідність розроблення універсальної аналітичної моделі правоохоронної діяльності, яка б включала найбільш оптимальні механізми, що містяться в концепціях аналітичної діяльності, керованої аналітикою (Intelligence-led policing – ILP), і Національної оперативно-аналітичної моделі (National Intelligence Model) та успішно використовуються правоохоронними органами

Європейського Союзу та Сполучених Штатів Америки, а також визначення ролі й основних потреб Національної поліції України в цьому процесі.

Тож одним із пріоритетів розбудови служби у 2025 році є інтеграція моделі поліцейської діяльності, керованою аналітикою (ILP), яку використовує Євросоюз та національної розвідувальної моделі, насамперед, це чотири вектори на яких базується будь-яка аналітична діяльність: люди, знання, системи, джерела.

У наш час кримінальний аналіз є не просто допоміжним елементом оперативно-розшукової чи слідчої роботи — він стає стратегічним компонентом прийняття рішень, планування превентивних заходів, управління ресурсами та оцінки ризиків. Зміни у злочинному середовищі, розвиток інформаційних технологій і нові виклики безпеці вимагають від нас аналітичної гнучкості, міждисциплінарного підходу та здатності працювати з великими обсягами даних.

Сьогоднішня зустріч – це можливість не лише поділитися напрацюваннями, а й почути практичні кейси, обговорити проблемні питання, знайти точки дотику між наукою й практикою. Переконаний, що дискусії в межах круглого столу сприятимуть подальшому розвитку кримінального аналізу як інструменту, що стоїть на захисті правопорядку, суспільної безпеки та прав людини.

Бажаю всім учасникам плідної роботи, конструктивного діалогу та нових ідей для подальших досліджень і практичних рішень.

Білик Вадим Миколайович,
доцент кафедри поліцейської діяльності
Національної академії внутрішніх справ,
кандидат юридичних наук, доцент

ПРОБЛЕМИ ЗАКОНОДАВЧОГО ТА МІЖВІДОМЧОГО НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ В ПРАВООХОРОННІЙ СИСТЕМІ УКРАЇНИ

Кримінальний аналіз, як інструмент превентивної та аналітичної діяльності, відіграє все більш важливу роль у сучасній правоохоронній системі України. Його завдання полягає в зборі, обробці, аналізі та використанні інформації для виявлення, попередження і розслідування кримінальних правопорушень. Проте на сьогоднішній день в Україні існує низка проблем у сфері законодавчого та нормативно-правового регулювання кримінального аналізу, що ускладнює його ефективне застосування та інтеграцію у діяльність різних органів системи правопорядку.

1. Відсутність комплексного законодавчого визначення поняття «кримінальний аналіз», яке було б характерне для правоохоронної системи в цілому

Наразі у законодавстві України наявні два нормативно-правових визначення поняття кримінального аналізу [5; 6]. Так, відповідно до Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС, затвердженого наказом МВС України від 20.10.2017 № 870, визначення поняття кримінального аналізу є загальним, стратегічно та оперативно-орієнтованим, що охоплює весь спектр злочинної діяльності й використовується переважно у сфері оперативно-розшукової діяльності. Натомість, визначення поняття кримінального аналізу, згідно Закону України від 28.01.2021 № 1150-IX «Про Бюро економічної безпеки України», є спеціалізованим, зосередженим на економічній злочинності, із фокусом на практичну допомогу у кримінальному провадженні (досудове розслідування, виявлення порушень економічного характеру).

У різних юридичних джерелах [1; 2; 4; 8; 9] використовується схожий термін – «інформаційно-аналітична діяльність», однак його зміст значно вужчий та не охоплює повного функціоналу кримінального аналізу, як системної діяльності з прогнозування та оцінки криміногенної обстановки. Це призводить до неоднозначного тлумачення терміну «кримінальний аналіз» у практичній діяльності правоохоронних органів.

2. Непогодженість міжвідомчих нормативно-правових актів

Важливою проблемою є відсутність єдиного підходу до нормативного регулювання кримінального аналізу між різними правоохоронними органами – Національною поліцією, Службою безпеки України, Державною прикордонною службою, Державним бюро розслідувань тощо. Кожне відомство має власні внутрішні документи, які регламентують аналітичну діяльність, однак ці документи часто не узгоджуються між собою, що створює перепони для міжвідомчої координації та обміну інформацією.

Зокрема, формати подання аналітичної інформації, методики її обробки, а також підходи до визначення загроз публічній безпеці та кримінальній ситуації можуть суттєво відрізнятися. Відсутність єдиного нормативного поля унеможливлює формування загальнодержавної системи кримінального аналізу.

3. Проблеми впровадження єдиної інформаційно-аналітичної платформи

Хоча на рівні концептуальних документів, зокрема декларувалося у Стратегії розвитку органів системи МВС [7] та декларується у Комплексному стратегічному плані реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки [3], необхідність створення єдиної системи кримінального аналізу, її впровадження гальмується через брак нормативного врегулювання процедур взаємодії, захисту інформації, обміну даними. Відсутні також чіткі вимоги до фахової підготовки аналітиків та критерії оцінки їхньої роботи.

Більшість автоматизованих інформаційних систем працює в межах одного відомства і не має доступу до баз даних інших

структур, що знижує ефективність кримінального аналізу в масштабах держави.

4. Низький рівень професійної підготовки аналітиків

Ще однією проблемою є відсутність національного стандарту професійної підготовки фахівців з кримінального аналізу. Освітні програми закладів вищої освіти не завжди відповідають вимогам практичної діяльності, а міжвідомча координація у сфері підготовки аналітичних кадрів практично відсутня. Це призводить до недостатньої професійної компетентності аналітиків, а отже – і до зниження якості інформаційно-аналітичного забезпечення правоохоронної діяльності.

5. Рекомендації щодо вдосконалення нормативного регулювання

Для підвищення ефективності кримінального аналізу необхідно:

– законодавчо визначити поняття «кримінальний аналіз» та його функціональні складові;

– розробити єдиний міжвідомчий нормативно-правовий акт, що регламентує основні засади кримінального аналізу та забезпечує уніфікацію процедур у різних правоохоронних органах;

– створити інтегровану національну інформаційно-аналітичну систему з забезпеченням доступу для уповноважених суб'єктів;

– розробити державні стандарти підготовки аналітиків та запровадити єдині критерії їхньої професійної атестації;

– забезпечити міжвідомчу координацію у сфері інформаційного обміну, кібербезпеки та збереження персональних даних.

Висновок. Наявні проблеми нормативно-правового регулювання кримінального аналізу в Україні значно ускладнюють ефективне застосування цього інструменту у боротьбі зі злочинністю. Удосконалення законодавчого підґрунтя, налагодження міжвідомчої координації та розвиток кадрового потенціалу є ключовими передумовами для формування сучасної, інтегрованої системи кримінального аналізу, що відповідає європейським стандартам та потребам національної безпеки.

Список використаних джерел

1. Додонов А.Г., Ландэ Д.В., Путятин В.Г. Компьютерные сети и аналитические исследования. К.: ИПРИ НАН Украины, 2014. 486 с.
2. Захарова В. І., Філіпова В. Я. Основи інформаційно-аналітичної діяльності. К. «Центр учбової літератури», 2013. 336 с.
3. Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 – 2027 роки : Указ Президента України від 11.05.2023. № 273/2023. Урядовий кур'єр від 13.05.2023. № 96.
4. Кушнаренко Н. М. Наукова обробка документів: Підручник/ Н. М. Кушнаренко, В. К. Удалова. К.: Вікар, 2003. 359 с.
5. Про Бюро економічної безпеки України: Закон України від 28.01.2021. № 1150-IX /Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1150-20.
6. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС: наказ МВС України від 20.10.2017. № 870 / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/z1433-17.
7. Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року : затв. Розпорядженням Кабінету Міністрів України від 15.11.2017. № 1023-р. Урядовий кур'єр від 13.03.2018. № 48.
8. Сілкова Г. В. Інформаційно-аналітична діяльність як напрям інформаційної діяльності/ Г. В. Сілкова// Вісн. Кн. палати. 1999. № 3. С. 6–9.
9. Сілкова Г. В. Інформаційно-аналітичні дослідження в структурі інформаційних ресурсів/ Г. В. Сілкова// Вісн. Кн. палати. 2001. № 2. С. 14–15.

Бойко Вероніка Максимівна,
курсант 3-го курсу навчально-наукового
експертно-криміналістичного інституту
Національної академії внутрішніх справ
Науковий керівник:
завідувач кафедри криміналістичного
забезпечення та судових експертиз
навчально-наукового експертно-
криміналістичного інституту
Національної академії внутрішніх справ,
кандидат юридичних наук, доцент
Атаманчук В. М.

ОКРЕМІ НАПРЯМИ ЗАСТОСУВАННЯ МОЖЛИВОСТЕЙ КРИМІНАЛЬНОГО АНАЛІЗУ ПІД ЧАС РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

У сучасному світі воєнні конфлікти дедалі частіше супроводжуються масовими порушеннями норм міжнародного гуманітарного права, зокрема воєнними злочинами, які потребують ретельного документування та розслідування. Повномасштабне вторгнення російської федерації на територію України, що розпочалося 24 лютого 2022 року, виявило численні випадки жорстоких порушень прав людини, знищення цивільної інфраструктури, тортур, депортацій, зґвалтувань, незаконного утримання в полоні, страти цивільних осіб, а також застосування заборонених методів ведення війни. У цьому контексті кримінальний аналіз набув особливого значення як інструмент, що дозволяє виявити, класифікувати, систематизувати та ефективно використовувати наявну інформацію для притягнення винних до відповідальності.

Кримінальний аналіз – це методика збору, структурування, оцінки й інтерпретації даних, яка використовується правоохоронними органами для виявлення тенденцій, взаємозв'язків і закономірностей у злочинній діяльності. У випадку воєнних злочинів, зокрема в умовах активної фази бойових дій, цей інструмент є особливо цінним, оскільки дає можливість працювати з великою кількістю джерел, а саме відкритих, закритих, документальних, свідчень очевидців, фото- та відеофіксації, супутникових знімків,

перехоплених переговорів тощо [4, с. 189–194]. Аналітики обробляють ці масиви даних, щоб вибудовувати логіку подій, встановлювати ідентичність підозрюваних, виявляти місце й час правопорушення, перевіряти версії та підтверджувати свідчення потерпілих.

Використання кримінального аналізу посідає особливе місце у сучасному світі, де війна вийшла за межі фізичного протистояння і набула гібридних, інформаційно-психологічних форм. Він виконує не лише функцію суто юридичного інструменту для збирання доказів і притягнення винних до відповідальності, але й відіграє вирішальну роль у боротьбі за правду, протидію дезінформації та встановлення історичної справедливості. В умовах російської агресії проти України, де злочини проти людяності, масові вбивства, зґвалтування, катування й депортації стали системним явищем, саме кримінальний аналіз надає змогу не просто фіксувати факти, а будувати чітку, обґрунтовану правову позицію, здатну вистояти навіть у міжнародних судах.

Йдеться не лише про слідчу роботу в традиційному сенсі. Сучасний кримінальний аналіз це складний процес, що включає криміналістичне відтворення подій, цифрову обробку доказів, верифікацію свідчень, аналіз супутникових знімків, перехоплень, соціальних мереж і масиву відкритих джерел. В епоху дезінформаційних кампаній, коли пропагандистські фабрики спотворюють події, намагаючись «переписати» реальність, саме аналітична точність і достовірність фактів стають бронею проти брехні. Російська пропаганда намагається перекласти відповідальність, знівелювати масштаби скоєних злочинів або заперечити їх взагалі. У відповідь українські правоохоронні органи, міжнародні експерти та правозахисники вибудовують системний доказовий ланцюг, що не лише викриває винних, а й формує нову історичну наративу, засновану на істині.

Не менш важливим напрямом кримінального аналізу є морально-психологічна підтримка суспільства. У країні, що переживає воєнні злочини, зневіра, гнів і потреба у справедливості стають частиною колективної свідомості. Ретельний аналіз, публічне розслідування, демонстрація ходу справи й покарання винних дають відчуття, що правда – не абстракція, а реальна сила. Це підтримує довіру до інституцій,

мобілізує суспільство й показує: ніхто не залишиться безкарним [3, с. 618–622].

Система кримінального аналізу в Україні у контексті розслідування воєнних злочинів стала прикладом того, як національні інституції можуть ефективно співпрацювати з міжнародними структурами задля встановлення справедливості, документування злочинів та протидії безкарності. В умовах повномасштабної збройної агресії з боку російської федерації, Україна не лише посилила власний потенціал у сфері кримінального розслідування, а й налагодила глибоку координацію з партнерами, які мають досвід у міжнародному правосудді, аналітиці даних та розслідуванні масових порушень прав людини.

На національному рівні ключову роль у кримінальному аналізі відіграють Служба безпеки України, Національна поліція, Офіс Генерального прокурора, Державне бюро розслідувань, Бюро економічної безпеки, Національне антикорупційне бюро України. Під час використання можливостей кримінального аналізу, правоохоронними органами опрацьовуються та обробляються наявні докази, призначають експертизи до вчинення кримінального правопорушення. Водночас ці органи працюють у тісному контакті з міжнародними структурами, що дозволяє розширити масштаби розслідувань, вийти за межі українського контексту та створити належну доказову базу для розгляду справ у міжнародних юрисдикціях.

Одним із ключових міжнародних партнерів є Міжнародний кримінальний суд (МКС), який уже відкрив провадження щодо злочинів, скоєних на території України. Його прокурори співпрацюють з українськими фахівцями, беруть участь у зборі доказів та проводять власні експертизи. Важливою складовою є також робота міжнародних неурядових організацій, таких як Bellingcat, Human Rights Watch, Amnesty International, які застосовують сучасні OSINT-методи (аналіз відкритих джерел), перевірку відео, фото- та супутникових матеріалів. Їхні дослідження стають не лише інформаційним джерелом для громадськості, а й безпосередньо інтегруються в правові процеси [1].

Крім того, в Гаазі створено окремі центри збору та обробки доказів воєнних злочинів, які функціонують за

підтримки Європейського Союзу та інших міжнародних партнерів. Їхніми завданнями є не лише зберігати і класифікувати інформацію, але й забезпечити її належну юридичну валідацію, що дозволить у подальшому використовувати її у провадженнях МКС або в національних судах третіх країн відповідно до принципу універсальної юрисдикції.

Ці структури виконують як оперативно-аналітичну, так і доказову функцію, забезпечуючи перевірку інформації, визначення відповідальності конкретних осіб та підготовку справ для міжнародного судового переслідування. Відповідно до Римського статуту МКС, воєнні злочини включають навмисне вбивство, тортури, нелюдське поводження, знищення майна без військової необхідності, незаконну депортацію чи переміщення населення, зґвалтування, сексуальне рабство та інші акти насильства сексуального характеру [4, с. 189–194].

Аналіз даних відіграє вирішальну роль у тому, щоб відокремити справжні випадки воєнних злочинів від звичайних військових втрат, що відповідають законам і звичаям війни. Це дає змогу не лише забезпечити об'єктивність у слідстві, а й убезпечити справедливість правосуддя. Наприклад, встановлення факту прицільного обстрілу пологових будинків або цивільних кварталів у Маріуполі потребує не тільки свідчень очевидців, але й перехресного аналізу: знімків з дронів і супутників, інформації про розташування військових підрозділів рф, переговорів командування, телеграм-переписок, перехоплень радіоефіру, а також систематичного зіставлення подібних атак в інших регіонах.

Унікальність воєнних злочинів, скоєних під час вторгнення росії в Україну, полягає в їхній масовості та системності. Злочини в Бучі, Ірпені, Ізюмі, Маріуполі, Херсоні та багатьох інших населених пунктах свідчать не про поодинокі інциденти, а про цілеспрямовану політику терору та приниження цивільного населення. Кримінальний аналіз дозволяє розпізнати цю системність: визначити ланцюг командування, простежити зв'язки між виконавцями, їхні пересування, комунікацію, накази, типові дії в захоплених містах. Він дозволяє підняти розслідування з рівня «виконавця»

до рівня «відповідального командування», що є ключовим для доведення провини в міжнародних судах.

Ще одним надзвичайно важливим напрямом є цифровізація доказів. У XXI столітті війна ведеться не лише на полі бою, а й у цифровому середовищі. Мобільні телефони, соціальні мережі, публікації російських солдатів, навіть відео з TikTok стають джерелами доказів [2, с. 84–102]. Кримінальні аналітики ідентифікують особи на відео за формою, акцентом, геолокацією, метаданими файлів, порівнюють фото з відкритих джерел зі службовими базами. Наприклад, особи, які катували українських військовополонених або знущалися з цивільних, часто з'являлися у фото в соцмережах, підписуючи локації чи демонструючи зброю, що дає змогу фіксувати участь у конкретних діях.

Інший напрям застосування кримінального аналізу це визначення зв'язків між різними підрозділами, угрупованнями, приватними військовими компаніями (як-от ПВК «Вагнер»), і конкретними локаціями, де були зафіксовані злочини. Це дає змогу говорити не тільки про індивідуальні провини, а й про організований характер злочинності, системну участь державних структур російської федерації. Водночас такий аналіз допомагає підтвердити умисел, а саме юридично ключову категорію в кваліфікації дій як воєнного злочину. Щоразу країна рф порушує встановлені закони ведення війни, котрі регламентуються МГП, а саме системою принципів правових норм, котрі в свою чергу встановлюють не тільки права, а й обов'язки сторін конфлікту. [5, с. 18]

Кримінальний аналіз у воєнних злочинів є не лише інструментом слідства, а й способом відновлення історичної справедливості, засобом протидії дезінформації та російській пропаганді. Відкриті джерела, які ретельно перевіряються аналітиками, часто спростовують офіційні заяви країни-агресора. Наприклад, росія неодноразово заперечувала свою причетність до обстрілів житлових масивів, однак кримінальні розслідування за участю міжнародних експертів доводять зворотне, спираючись на дані про траєкторії снарядів, типи озброєнь, час ударів та їхню узгодженість з іншими діями на фронті.

Таким чином, застосування різних напрямів кримінального аналізу в розслідуванні воєнних злочинів відіграє важливу роль у виявленні, прогнозуванні й документуванні даних. На сьогодні інструмент є необхідним етапом на шляху до справедливого покарання агресора та окремих виконавців, допомагає подолати хаос війни, структурувати правду, дати голос жертвам та встановити справжню відповідальність. На прикладі повномасштабного вторгнення в Україну, де злочини проти людяності відбуваються на очах усього світу, роль кримінального аналізу є стратегічною, не лише для сучасного правосуддя, а й для майбутнього колективної пам'яті, політичної відповідальності та недопущення повторення подібних трагедій у наступних поколіннях.

Список використаних джерел

1. Зосин М. Розвідка з відкритих джерел (Open-source intelligence – OSINT). 2023. URL: https://www.maxzosim.com /rozvidka-z-vidkritikh-dzherel-osint/amp/

2. Погорецький М.А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання). Вісник кримінального судочинства. № 3–4. 2023. С. 84–102. URL: https://vkslaw.com.ua/index.php/journal/article/ view/485/447.

3. Саінчин С.О., Донцов Д.Ю., Яцишена Г.А. Розслідування військових злочинів: кримінально-правовий та кримінально-процесуальний зміст. Юридичний науковий електронний журнал. № 11. 2024. С. 618–622. URL: http://lsej.org.ua/11_2024/148.pdf.

4. Свистун В.В., Дідковський О.Є., Кисельов А.О. Особливості здійснення кримінального аналізу під час виявлення воєнних злочинів та контрабандної діяльності. Universum. № 9. 2024. С. 189–194. URL: https://archive.liga.science /index.php/universum/article/view/1102/1114.

5. А. А. Вознюк, І. В. Жук, О. В. Таран, С. С. Чернявський та ін.; за заг. ред. М. С. Цуцкірідзе, В. В. Чернєя, А. А. Вознюка. К. «Кваліфікація та розслідування порушення законів і звичаїв війни» Науково практичний посібник 2023, с. 18 URL: https://www.navs.edu.ua/files/naukova-diyalnist/naukovi-laborator/lab_nni1/2023/kvalif_rozsliduv_porush_2023.pdf.

Буренко Олег Володимирович,
викладач кафедри кримінології
та інформаційних технологій
Національної академії внутрішніх справ

ВИКОРИСТАННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В УКРАЇНІ

Відеозаписи відіграють дедалі вагомішу роль у сучасному кримінальному судочинстві України, виступаючи матеріальним об'єктом та носієм інформації про події злочину. Вони цінні тим, що можуть надати неупереджені докази, це особливо важливо у випадках, коли свідчення очевидців можуть бути спотвореними або недостовірними. Об'єктивна оцінка обставин події забезпечується відеозаписом, який допомагає виявити деталі, тенденції та причинно-наслідкові зв'язки, які в іншому випадку могли б залишитися непоміченими.

Використання відеодоказів є важливим для підвищення ефективності правоохоронних органів. Окрім того, що камери відеоспостереження є превентивним заходом для зменшення злочинності та насильства, вони також змушують правоохоронців дотримуватися протоколів та брати на себе більшу відповідальність за забезпечення громадської безпеки. Процес виявлення правопорушників та створення доказової бази значно покращується завдяки передовим IP-камерам з інтегрованими системами відеоаналітики на основі штучного інтелекту. Збереження цілісності відеоматеріалів протягом усього їхнього життєвого циклу – від запису до передачі до суду – має вирішальне значення. Будь-які порушення цієї процедури, такі як неправильне зберігання записів або неадекватна автентифікація, можуть звести нанівець переваги відеодоказів над індивідуалізованими людськими свідченнями, збільшуючи ймовірність судових помилок або втрати важливих даних.

Від простих аналогових камер середини 20-го століття до складних сучасних технологій, що активно використовують штучний інтелект, системи відеоспостереження зазнали суттєвої еволюції. З появою сучасних відеосистем робота правоохоронних органів кардинально змінилася за останні роки. З'явилась можливість збирати докази в режимі реального часу, а не покладатися лише на свідчення очевидців.

Як для правоохоронців, так і для злочинців розвиток сучасних технологій відкриває нові можливості. Злочинці часто використовують даркнет, зашифровані месенджери та соціальні мережі як сучасні засоби комунікації. Саме тому, відеоаналітика дозволяє значно підвищити ефективність збору доказів та покращити цю роботу. Правове регулювання відеоспостереження в Україні базується на низці основних законодавчих актів, які спрямовані на забезпечення балансу між інтересами громадської безпеки та захистом приватного життя.

Конституція України та Цивільний кодекс України встановлюють ключові принципи захисту приватності. У статті 32 Конституції зазначено, що втручання в особисте та сімейне життя особи допускається виключно у випадках, визначених самою Конституцією [1]. Стаття 307 Цивільного кодексу уточнює, що фотографування, відеофіксація чи зйомка фізичної особи можлива лише за її згодою. Водночас така згода вважається отриманою, якщо зйомка проводиться відкрито на вулицях, громадських заходах, зборах чи конференціях публічного характеру. Суттєвим є те, що таємна зйомка людини без її дозволу дозволена лише у випадках, передбачених законодавством. Окрім того, друга частина статті 302 Цивільного кодексу забороняє збір, зберігання, використання та поширення інформації про приватне життя осіб без їхньої згоди, окрім ситуацій, прямо передбачених законом. Такі винятки допускаються лише в інтересах національної безпеки, економічного благополуччя чи захисту прав людини [2].

Закон України «Про захист персональних даних» встановлює суворі принципи обробки персональних даних. Цей Закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних [3].

Закон України «Про оперативно-розшукову діяльність» визначає оперативно-розшукову діяльність як систему відкритих і прихованих пошукових та контррозвідувальних заходів, що реалізуються через застосування спеціальних оперативних і технічних засобів. Ця діяльність базується на принципах верховенства права, законності, а також поваги до прав і свобод людини, що наголошує на необхідності

забезпечення балансу між ефективністю розслідування та дотриманням прав громадян. Підставою для проведення оперативно-розшукових заходів є наявність достатніх даних, отриманих відповідно до встановленого законом порядку, які потребують перевірки за допомогою таких заходів і засобів, у контексті підготовки кримінальних правопорушень чи причетності конкретних осіб до їхнього вчинення [4].

ОРД здійснюється виключно оперативними підрозділами Національної поліції, Служби безпеки України, Державного бюро розслідувань, Бюро економічної безпеки, Державної прикордонної служби, а також іншими органами, визначеними законодавством. Проведення таких заходів будь-якими іншими підрозділами зазначених установ, структурами інших міністерств та відомств, громадськими чи приватними організаціями або окремими особами категорично заборонене. Рішення про оперативно-розшукові заходи, які не потребують дозволу слідчого судді чи прокурора, приймає керівник відповідного оперативного підрозділу або його заступник, з обов'язковим повідомленням прокурора про прийняте рішення [4].

Легальність прихованого відеоспостереження для правоохоронних органів, здійснюваного за дозволом суду, є принциповим аспектом забезпечення правових норм. Такий вид відеоспостереження належить до негласних заходів і може проводитися виключно уповноваженими органами, при наявності відповідного судового дозволу. Це гарантує дотримання прав людини й захист від свавілля. Використання негласних технічних засобів без дозволу суду карається згідно зі статтею 359 Кримінального кодексу України. Згідно з цією статтею, незаконне придбання, збут або використання спеціальних технічних засобів для отримання інформації може стати підставою для накладення штрафу чи позбавлення волі [5].

У кримінальному провадженні України докази являють собою фактичні дані, які отримані у порядку, визначеному Кримінальним процесуальним кодексом України (КПК), що підтверджується положеннями частини 1 статті 84 КПК. Це акцентує увагу на тому, що процесуальна форма отримання доказів є їхньою ключовою характеристикою. Серед джерел доказів КПК виокремлює показання, речові докази, документи та експертні висновки. Відеозаписи, як носії інформації, що

містять візуальні дані, класифікуються як «документи» відповідно до частини 1 статті 99 КПК [6].

Щоб відеоматеріали могли бути прийняті як доказ у кримінальному провадженні, вони мають відповідати низці суворих критеріїв, таких як допустимість, належність і достовірність. Крім того, вся зібрана доказова база повинна оцінюватися з точки зору достатності та взаємопов'язаності для винесення відповідного процесуального рішення відповідно до статті 94 КПК. Доказ вважається допустимим лише за умови, що він отриманий згідно з процедурою, визначеною КПК. Якщо ж доказ є недопустимим, його використання при ухваленні процесуальних рішень виключається [6].

Цілісність даних передбачає, що всі дії спеціаліста мають виключати будь-які матеріальні зміни в структурі даних, роботі електронних пристроїв або носіїв інформації, які потенційно можуть виступати як докази. Це досягається шляхом правильної фіксації інформації та забезпечення незмінності комп'ютерних даних у майбутньому. Для встановлення автентичності записів необхідно переконатись у їхній оригінальності, підтвердити дату й час створення, а також провести аналіз щодо можливого монтажу чи маніпуляцій, чого можна досягти за допомогою експертної оцінки. Електронні докази, на відміну від традиційних, не мають матеріального вигляду без використання спеціальних інструментів, є значно більш уразливими до змін, пошкоджень чи знищення, а також їх простіше модифікувати чи підробити [7].

Для забезпечення цілісності даних застосовується метод розрахунку контрольної або хеш-суми (наприклад, MD5, SHA-1), які фіксуються у протоколі як під час вилучення носіїв, так і після копіювання файлів.

Після проведення огляду докази створюють у двох екземплярах – контрольному та робочому. Контрольний екземпляр ретельно опечатується, щоб унеможливити доступ та внесення змін. Важливим є те, що копії інформації з інформаційних систем, виготовлені слідчим або прокурором за участю спеціаліста, визнаються судом як оригінали документа. Крім того, оперативні працівники повинні вживати заходів для уникнення сторонньої відеофіксації процесу проведення слідчих дій [7].

Суворі процесуальні вимоги до збору та оформлення електронних доказів, зокрема відеозаписів, мають ключове значення для їх прийнятності в суді. Усі етапи, починаючи з виявлення і закінчуючи зберіганням, повинні бути ретельно задокументовані та підтверджені, щоб виключити будь-які сумніви щодо достовірності й цілісності інформації. Незважаючи на те, що цей процес є досить трудомістким, він залишається необхідним для дотримання принципу верховенства права і захисту прав людини в умовах зростаючого використання цифрових доказів.

Аналіз відеодоказів у кримінальних розслідуваннях потребує використання спеціалізованих методів і програмного забезпечення, аби гарантувати їхню належну якість та юридичну допустимість. Висока якість відеоматеріалів є ключовим аспектом, що впливає на здатність встановити «Хто», «Що» і «Як» сталося під час скоєння злочину [8].

Для покращення якості відеозаписів застосовуються різноманітні техніки, зокрема:

– **зміна роздільності та суперроздільність з використанням ШІ:** Це дозволяє збільшити чіткість та масштабувати відео до 4K;

– **обробка відео нейромережами:** Застосування ШІ для покращення якості, зменшення шуму, стабілізації зображення, регулювання яскравості та контрастності;

– **видалення об’єктів з фону та розмиття відео:** Дозволяє зосередитися на ключових елементах;

– **геолокація:** Визначення місця подій за об’єктами у кадрі, наприклад, за відображеннями у склі або дзеркалах, з подальшим порівнянням із сервісами типу Google Street View [9].

Серед програмного забезпечення для криміналістичного аналізу відео виділяються такі рішення:

– **Amped FIVE**: Унікальне програмне забезпечення для дослідження зображень та відео;

– **OpenText EnCase Forensic**: Програмне забезпечення для дослідження інформації на цифрових носіях та мобільних пристроях;

– **Magnet AXIOM**: Програмне забезпечення для відновлення, аналізу та складання звітів за даними з мобільних, комп’ютерних та хмарних джерел;

– **SUMURI PALADIN**: Один із провідних комплексів криміналістичної експертизи з відкритим вихідним кодом. [10].

– **HitPaw Video Enhancer AI**: Програмне забезпечення, що використовує ШІ для масштабування відео до 8K, зменшення шуму та покращення аніме та відео з людськими обличчями [11].

Штучний інтелект набуває дедалі більшого значення у сфері відеоспостереження для правоохоронних органів, змінюючи підходи до забезпечення безпеки та проведення розслідувань. Сучасні системи відеоаналітики, оснащені ШІ, пропонують удосконалені функції, які перевершують можливості традиційного відеоспостереження. До їх завдань входить автоматична ідентифікація, аналіз поведінкових патернів, виявлення подій або об'єктів у реальному часі, причому це відбувається без потреби постійного контролю з боку оператора.

Основні можливості ШІ у відеоаналізі включають:

– Розпізнавання облич та номерних знаків: дозволяє суттєво прискорити розслідування за допомогою криміналістичних функцій;

– Виявлення перетину заборонених зон або ліній: допомагає контролювати периметр;

– Класифікація об'єктів: можливість ідентифікації та індексування об'єктів на відеозаписах (автомобілі, люди, тварини);

– Аналіз поведінки: виявлення аномальної поведінки людей, що може вказувати на підготовку злочину;

– Автоматична фільтрація помилкових спрацювань: Підвищення точності систем.

– Збір метаданих: використання зібраних метаданих для швидкого пошуку відеофрагментів, що значно прискорює розслідування.

Відеоспостереження демонструє високу ефективність у запобіганні злочинності та розкритті кримінальних правопорушень в Україні. Дослідження підтверджують, що встановлення камер безпеки суттєво зменшує ризик скоєння злочинів. Злочинці зазвичай уникають ситуацій, де їх можуть зафіксувати, тому видимі камери стають дієвим стримуючим засобом.

Відеоаналітика, особливо із застосуванням штучного інтелекту, значно спрощує доступ до потрібної інформації в

відеоматеріалах. Вона дозволяє визначати, класифікувати та структуровано індексувати об'єкти, як-от транспортні засоби, люди або тварини. Завдяки цьому час на перегляд відео, необхідний для аналізу доказів, можна зменшити з багатьох годин до всього кількох хвилин, одночасно мінімізуючи ризик помилок, спричинених людським фактором. До успішних прикладів використання відеодоказів належать фіксація злочинних дій, аналіз ходи підозрюваних, а також повна реконструкція маршрутів злочинців [8].

Майбутнє відеоспостереження в криміналістиці України тісно пов'язане з інтеграцією та розвитком сучасних технологій, зокрема штучного інтелекту. Перспективним напрямом є створення систем, здатних аналізувати не лише фізичні характеристики, такі як обличчя, але й моделі поведінки, що дозволяє передбачати потенційно злочинні дії ще до їх здійснення. Наприклад, на сьогоднішній день існують технології, які можуть автоматично ідентифікувати осіб, що заходять до приміщення зі зброєю, використовуючи алгоритми розпізнавання предметів за різних умов освітлення та ракурсів. Максимальна ефективність очікується від комбінування таких функцій, як визначення специфічних об'єктів (наприклад, зброї), з розпізнаванням облич конкретних осіб із баз даних, що включають інформацію про осіб із кримінальним минулим [12].

Використання систем відеоспостереження у розслідуванні кримінальних правопорушень в Україні являє собою багатогранну сферу з великим потенціалом, складною правовою базою та динамічним технологічним розвитком. Відеодокази стали ключовим інструментом для забезпечення об'єктивності в кримінальних провадженнях, надаючи можливість неупереджено фіксувати події.

Правове регулювання спрямоване на досягнення балансу між потребами громадської безпеки та забезпеченням права на приватність. Воно передбачає загальні вимоги щодо отримання згоди на запис і встановлює суворі обмеження на приховане спостереження, яке дозволяється лише правоохоронним органам за умови судового дозволу. Незважаючи на це, існує певний конфлікт між потенціалом сучасних технологій і необхідністю охорони основних прав людини. Саме це призводить до постійного вдосконалення нормативно-правових актів та запровадження нових прозорих механізмів контролю.

Список використаних джерел

1. Конституція України від 28 червня 1996 р. (із змінами). URL: http://zakon2.rada. gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/page.
2. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1618-15.
3. Закон України Про захист персональних даних від 1 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
4. Закон України Про оперативно-розшукову діяльність від 18 лютого 1992 року № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.
5. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.
6. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI. URL: https://zakon.rada.gov.ua /laws/show/4651-17#Text.
7. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.
8. Відео з камер спостереження, як доказ: за і проти. URL: https://tvtdigital.com.ua/video-z-kamer-sposterezhennia-iak-dokaz-za-i-proty/.
9. Як покращити якість відео за допомогою штучного інтелекту. URL: https://evergreens.com.ua/ua/articles/video-enhancement.html.
10. Комп’ютерна криміналістика. URL: https://cybermarket.com.ua/product-category/soft/forensic/.
11. 10 найкращих інструментів ШІ для бізнесу (липень 2025 р.). URL: https://www.unite.ai/uk/best-video-enhancer-tools-apps./.
12. З’являються камери зі штучним інтелектом, які передбачають злочини. URL: https://texty.org.ua/fragments/93433/Zjavlajutsa_kamery_zi_shtuchnym_intelektom_jaki_peredbachajut-93433/.

Денисенко Григорій Вячеславович,
провідний науковий співробітник НОЦ Національної академії Служби безпеки України, доктор філософії в галузі права, старший дослідник

КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУАЛЬНО-ПРАВОВИХ ГАРАНТІЙ ЗБЕРЕЖЕННЯ ОХОРОНЮВАНОЇ ЗАКОНОМ ІНФОРМАЦІЇ НА ДОСУДОВОМУ РОЗСЛІДУВАННІ

Правовий режим охорони конфіденційної інформації в кримінальному провадженні є однією з ключових гарантій захисту приватної сфери особи та реалізації принципу верховенства права. Відповідно до ч. 2 ст. 8 Кримінального процесуального кодексу України, кримінальне провадження здійснюється на засадах законності, розумності, пропорційності та поваги до прав і свобод людини і громадянина [1, с. 28]. У цьому контексті охорона інформації, що охоплює професійну, службову та державну таємницю, виступає елементом належного функціонування системи правосуддя. Положення ст. 93 КПК України визначають засади збирання доказів, включаючи дотримання конфіденційності, а ст. 222 містить пряму заборону на розголошення відомостей досудового розслідування. Окремі гарантії захисту охоронюваної інформації закріплено також у ст. 162, 159–164, 84, 107 КПК України [1, с. 198].

Попри це, чинне процесуальне законодавство демонструє фрагментарність у регулюванні аналітичної діяльності слідчого та оперативного підрозділу, зокрема в контексті забезпечення інформаційної безпеки під час кримінального провадження. У науковій доктрині визнається, що кримінальний аналіз є практичним інструментом досудового розслідування, однак відсутність нормативного визначення його статусу породжує складнощі у правозастосуванні.

Як слушно зауважує М. А. Погорецький, аналітичний висновок має подвійну природу – водночас джерела фактичних даних і засобу формування доказів [7, с. 280].

На практиці органів досудового розслідування аналітична робота набуває дедалі більшого значення, особливо в умовах необхідності обробки великих масивів цифрової інформації. Проте результати такої діяльності, що оформлюються як

аналітичні довідки, не мають визначеного процесуального статусу [4, с. 9]. У зв'язку з цим, актуальним є підхід, запропонований Р. В. Білоусом, В. І. Василинчуком та О. В. Тараном, які розглядають кримінальний аналіз як специфічний різновид інформаційно-аналітичної діяльності, що включає ідентифікацію, структурування, верифікацію та оцінку кримінально значущих даних задля прийняття обґрунтованих процесуальних рішень [3, с. 135].

Однією з центральних проблем є правова невизначеність статусу результатів аналізу телекомунікаційної інформації (зокрема даних трафіку, геолокації тощо), що здобувається в порядку, визначеному статтями 159–166 КПК України. За відсутності в КПК поняття «аналіз інформації про зв'язок», слідчі змушені застосовувати правові субститути – доручення огляду (ст. 237 КПК) або залучення оперативного працівника як спеціаліста (ст. 71 КПК), що може поставити під сумнів допустимість таких доказів [3, с. 137].

Кримінальний аналіз має функціональну здатність забезпечити реалізацію процесуально-правових гарантій охорони конфіденційної інформації. Йдеться, зокрема, про: 1) правову ідентифікацію джерел конфіденційних відомостей; 2) оцінку допустимості використання таких даних у доказуванні; 3) виявлення ризиків втручання у приватну сферу особи на стадії ініціювання слідчих або негласних дій [5, с. 218].

Проблематика аналітичного висновку як процесуального документа розглядається також у працях В. П. Шибіко, О. М. Костенка, Л. Д. Удалової, О. Ю. Бусол, В. І. Василинчука, С. В. Тіхонова та ін. Вони акцентують на тому, що в умовах цифровізації саме аналітичні інструменти здатні забезпечити ефективний процесуальний контроль над інформаційними потоками, які включають чутливу інформацію [4, с. 12].

Юридичним підґрунтям для визнання аналітичного висновку доказом є ч. 2 ст. 84 КПК України, згідно з якою письмовими доказами визнається будь-яка зафіксована в письмовій або електронній формі інформація, що має значення для кримінального провадження. Таким чином, за умови процесуально належного оформлення, аналітичний висновок має підстави кваліфікуватися як документ – письмовий доказ у розумінні КПК [1, с. 210].

З огляду на викладене, вбачається необхідність системного оновлення процесуального законодавства в частині нормативного закріплення інституту кримінального аналізу. Передусім доцільно передбачити дефініцію цього поняття у КПК України, визначивши його зміст, функції та суб'єктів. Паралельно необхідно надати аналітичному висновку процесуальний статус джерела доказів – шляхом внесення відповідних змін до ст. 84 КПК України [9, с. 365].

Також доцільно доповнити ст. 40 та ст. 41 КПК України прямим закріпленням повноважень слідчого і прокурора щодо доручення оперативним підрозділам складання аналітичних висновків у межах доказової діяльності. У зв'язку з цим, обґрунтованим є запровадження нормативно визначених індикаторів оцінки ризику доступу до охоронюваної інформації, які враховують особливості дотримання ст. 162 КПК України [1, с. 214].

Водночас нагальною є потреба у впровадженні методологічно обґрунтованого підходу до правової ідентифікації категорій чутливої інформації у практиці досудового розслідування, з урахуванням вимог цифрової трансформації кримінального процесу. Такі заходи сприятимуть не лише підвищенню ефективності слідчої діяльності, але й зміцненню легітимності кримінального провадження в цілому.

У підсумку, кримінальний аналіз має бути розглянутий не як допоміжний інструмент, а як інституційно самостійний елемент системи процесуально-правових гарантій, спрямованих на збереження охоронюваної законом інформації. Його нормативна інституалізація повинна стати логічним кроком у напрямку модернізації кримінального процесуального законодавства в умовах інформаційної епохи.

Список використаних джерел

1. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. Київ : Паливода А. В., 2024. 432 с.

2. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. Київ : Офіц. вид., 2023. 64 с.

3. Білоус Р. В., Василинчук В. І., Таран О. В. Використання методів кримінального аналізу під час оперативного провадження та досудового розслідування.

Науковий вісник Національної академії внутрішніх справ. 2021. № 1 (118). С. 131–142.

4. Василинчук В. І., Погорецький М. М., Тіхонов С. В. Аналітичний висновок у оперативно-розшуковій діяльності та кримінальному процесі. Вісник кримінального судочинства. 2023. № 1–2. С. 8–18.

5. Школьніков В. І. Кримінальний аналіз як засіб виявлення корупційних злочинів / наук. кер. Калиновський О. В. // Кримінально-правові та кримінологічні засади протидії корупції : зб. матеріалів наук. конф. (Харків, 2017 р.). Харків : Нац. акад. внутр. справ, 2017. С. 217–219.

6. Білоус Р. В. Кримінальний аналіз в діяльності правоохоронних органів України // Удосконалення механізму правового регулювання суспільних відносин з урахуванням зарубіжного досвіду : зб. матеріалів Міжнар. наук.-практ. конф. (Київ, 1 черв. 2020 р.) / відп. ред. О. Ю. Бусол. Київ : Ліра-К, 2020. С. 20–22.

7. Погорецький М. А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі. Харків : Арсіс ЛТД, 2007. 576 с.

8. Погорецький М. А. Документ в оперативно-розшуковій діяльності // Міжнародна поліцейська енциклопедія : у 10 т. Т. VI: Оперативно-розшукова діяльність поліції (міліції). Київ : Атіка, 2010. С. 223–225.

9. Розслідування кримінальних правопорушень у сфері службової діяльності : навч. посібн. / за ред. проф. М. А. Погорецького. Київ : Алерта, 2025. 376 с.

Кіреєва Ольга Сергіївна,
доцент кафедри спеціальних дисциплін
Національної академії Державної
прикордонної служби України
імені Богдана Хмельницького,
кандидат психологічних наук, доцент

РОЗВИТОК КРИМІНАЛЬНОГО АНАЛІЗУ В УКРАЇНІ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ РФ: ДОСВІД, ТЕНДЕНЦІЇ, ПЕРСПЕКТИВИ

У період повномасштабної збройної агресії рф проти України роль кримінального аналізу як складової аналітичної

підтримки діяльності правоохоронних органів набуває особливого значення. Потреба у своєчасному виявленні та попередженні кримінальних загроз, у тому числі пов'язаних із тероризмом, диверсійною діяльністю, контрабандою та колабораціонізмом, вимагає трансформації кримінального аналізу із допоміжного у стратегічно важливий інструмент державної безпеки.

У мирний час кримінальний аналіз часто був підпорядкований бюрократичній машині - звіти, формальності, архіви. Але під час війни ситуація змінилася докорінно. Кожна аналітична схема, кожне досьє, кожна візуалізація зв'язків чи профілювання маршрутів злочинної діяльності - це вже елемент безпосередньої участі у бойових діях, хоч і не на передовій.

Наприклад, аналітики оперативних підрозділів, використовуючи OSINT-методи (аналіз відкритих джерел), виявляють ворожих інформаторів у тилу, викривають схеми фінансування незаконних збройних формувань, виводять на чисту воду колаборантів та посібників окупантів. Усе це – без єдиного пострілу, але з не меншою стратегічною важливістю

Кримінальний аналіз в Україні, за прикладом провідних держав, еволюціонує від неформальних підходів до системної діяльності в межах оперативно-розшукових та аналітичних підрозділів [1]. Його становлення у сучасному вигляді розпочалося з досвіду Державної прикордонної служби України, яка з 2008 року активно впроваджує аналітичні підходи до управління ризиками та безпековими загрозами на кордоні, а з 2016 року перші підрозділи кримінального аналізу з'явилися й в Національній поліції України. Перші кримінальні аналітики Національної поліції України проходили підготовку на базі Національної академії Державної прикордонної служби України.

Особливості застосування кримінального аналізу оперативними підрозділами Державної прикордонної служби України проявляються в низці напрямів, які відображають адаптацію європейських стандартів до специфіки охорони державного кордону під час війни:

1. Аналітична підтримка охорони кордону: аналітики оперативних підрозділів Державної прикордонної служби України здійснюють оперативну оцінку змін у прикордонній обстановці, виявляють нові маршрути незаконної міграції, контрабанди зброї та боєприпасів, вивчають поведінку населення у прикордонних

районах. Це дозволяє оперативно перерозподіляти ресурси та коригувати маршрути патрулювання.

2. Розвідка на основі відкритих джерел (OSINT): враховуючи постійне застосування ворогом гібридних методів впливу, зокрема через мережу інформаторів або «сіру логістику», аналітики оперативних підрозділів Державної прикордонної служби України активно застосовують OSINT-методики. Вони аналізують повідомлення у соцмережах, моніторять пересування техніки, фіксують настрої населення та іншу корисну інформацію.

3. Використання геоінформаційних систем (ГІС): за допомогою ГІС-аналітики формуються карти незаконних дій, імовірних напрямків диверсійних груп, зони ризику. Ці дані використовуються як під час оперативного планування, так і для стратегічного прогнозування [2].

4. Аналіз ризиків та оцінка загроз: в рамках кримінального аналізу розробляються прогнози щодо рівня загроз на певних ділянках кордону, з урахуванням оперативних зведень, демографічних факторів, логістичних маршрутів тощо. Наприклад, якщо на ділянці спостерігається активні спроби порушників перейти державний кордон до суміжної країни - це є сигналом для посилення контролю і підготовки сил реагування.

5. Створення аналітичних продуктів: оперативні підрозділи Державної прикордонної служби України готують такі документи, як аналітичні довідки, інформаційні зведення, схемні матеріали (схеми зв'язків, подій, контактів). Особливу увагу приділяють складанню фінансових профілів осіб, причетних до контрабанди або фінансування тероризму.

6. Міжвідомча взаємодія: кримінальні аналітики Державної прикордонної служби України працюють у тісній взаємодії з іншими правоохоронними та розвідувальними органами. Обмін інформацією з СБУ, НПУ, ДБР та міжнародними структурами (FRONTEX, Європол) підвищує точність оцінки загроз [3].

В умовах воєнного стану кримінальний аналіз трансформується у комплексну систему реагування на складні виклики, пов'язані з: воєнними злочинами; нелегальним переміщенням зброї та вибухівки; злочинною діяльністю колаборантів; гібридними формами загроз, зокрема інформаційного характеру. Все це вимагає від аналітиків гнучкості,

швидкості реагування, досконалого володіння інструментами аналізу та чіткого розуміння оперативної обстановки.

Сучасний стан розвитку кримінального аналізу в Україні характеризується розширенням функціональних можливостей підрозділів у різних силових структурах.

Загалом, аналітичні підрозділи працюють не лише як джерело оперативної інформації, а як самостійна інституційна одиниця, що формує знання про криміногенну ситуацію, моделює варіанти її розвитку та пропонує сценарії реагування. Це свідчить про перехід кримінального аналізу до повноцінного елементу системи безпеки держави. від аналітиків гнучкості, швидкості реагування, досконалого володіння інструментами аналізу та чіткого розуміння оперативної обстановки.

Перспективи розвитку кримінального аналізу в Україні пов'язані з послідовним укріпленням інституційної спроможності та міжвідомчої координації. Важливим напрямом є створення спеціалізованих підрозділів кримінального аналізу в усіх секторах правоохоронної системи. Така інтеграція дозволяє забезпечити системний підхід до аналітичної діяльності на всіх рівнях, що підтверджується успішним досвідом Державної прикордонної служби у впровадженні аналітичного супроводу оперативних і стратегічних рішень.

Одночасно актуальним стає формування єдиної національної інформаційно-аналітичної платформи, яка об'єднуватиме ключові державні бази даних і забезпечуватиме доступ до автоматизованих систем типу ЄРДР, інформаційних ресурсів СБУ, МВС, НАБУ, податкових і митних органів. Така міжвідомча взаємодія значно підвищить ефективність аналітичного процесу [4].

У контексті збройної агресії проти України особливої ваги набуває адаптація аналітичних методик до умов війни. Поширення технологій OSINT, HUMINT, географічного і фінансового профілювання, аналізу соціальних мереж дозволяє виявляти логістичні схеми ворога, мережі агентури, оцінювати ризики диверсій та ефективно діяти навіть у нестабільних чи тимчасово окупованих регіонах [5]. Розвиток кадрового потенціалу також є ключовим фактором. Вдосконалення навчальних програм для кримінальних аналітиків із впровадженням сучасних інформаційних технологій – таких як ГІС-системи, мовлення даних, програмне забезпечення для

виявлення зв'язків і шаблонів – сприятиме підвищенню якості аналітичної роботи.

Втім, стрімкий розвиток кримінального аналізу має й свої загрози, а саме: небезпека витоку чутливої інформації; загроза з боку ворожих ІТ-диверсантів; дефіцит кадрів із сучасною підготовкою; обмежена нормативна база – фактично, в Україні досі відсутнє окреме законодавство, яке регулює діяльність кримінальних аналітиків [6].

Воєнний стан актуалізує необхідність прискореного розвитку кримінального аналізу в Україні як інструмента антикризового управління та протидії багатовекторним загрозам. Його ефективність полягає не лише у зборі інформації, але й у здатності з неї робити достовірні висновки, які стануть підґрунтям для тактичних і стратегічних рішень. Створення національної моделі кримінального аналізу з урахуванням міжнародних стандартів, високотехнологічного забезпечення та фахової підготовки аналітиків є реальним і нагальним завданням національної безпеки.

На нашу думку, найбільш пріоритетними напрямами розвитку залишаються: формування чіткої нормативно-правової бази для діяльності кримінальних аналітичних підрозділів; інституціоналізація таких підрозділів у всіх ключових правоохоронних та безпекових структурах; забезпечення міжвідомчої інтеграції через створення єдиної інформаційно-аналітичної платформи з доступом до актуальних баз даних; удосконалення системи професійної підготовки аналітиків із використанням сучасних цифрових технологій, зокрема штучного інтелекту, ГІС, OSINT, інструментів візуалізації та профілювання; а також активізація міжнародної співпраці в межах європейських безпекових ініціатив і впровадження кращих практик стратегічного аналізу.

Реалізація цих напрямів дозволить перетворити кримінальний аналіз на потужний інструмент не лише оперативного реагування, а й довгострокового забезпечення національної безпеки України в умовах гібридної війни.

Підсумовуючи вищевказане, можна зазначити, *що* в той час як гармати стріляють, розум повинен працювати вдвічі швидше. В умовах воєнного стану й воєнної агресії з боку рф кримінальний аналіз стає не просто інструментом боротьби зі злочинністю – він перетворюється на важіль виживання держави.

Список використаних джерел

1. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний порадник. 5-те вид., переробл. та доповн. / Д. С. Зоренко, Л. О. Кульчицька, Р. В. Лех, О. І. Червяков. Харків, 2024. 80 с.

2. Купрієнко Д. А., Кіреєва О. С. Використання можливостей OSINT і штучного інтелекту для забезпечення стабілізаційних заходів прикордонного загону на деокупованій території прикордонних районів України // *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України : матеріали міжвідом. наук.-практ. конф.* (Київ, 1 листоп. 2024р.). Київ, 2024. С. 115–117.

3. Тищук В. В. Значення кримінального аналізу для захисту державного кордону України // *Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : тези III Міжнар. наук.-практ. конф.* (Хмельницький, 21 листоп. 2024 р.). Хмельницький : Видавництво НАДПСУ, 2025. С. 1034–1036.

4. Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України / О. С. Кіреєва, Ю. В. Крутік, О. М. Махлай, А. С. Треус. Хмельницький : Вид-во НАДПСУ, 2022. 360 с.

5. Коваленко Р. С., Кисельов А. О. Сучасні можливості технології “OSINT” у кримінальному аналізі в умовах воєнного стану // *Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VIII Міжнар. наук.-практ. конф.* (м. Дніпро, 15 бер. 2024 р.) ; у 2-х ч. Дніпро : ДДУВС, 2024. Ч. ІІ. С. 85–87.

6. Басалик С. А., Туз О. С. Нормативно-правове регулювання професійної діяльності кримінальних аналітиків у Державній прикордонній службі України // *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України : матеріали міжвідом. наук.-практ. конф.* (Київ, 11 серп. 2022 р.). Київ, 2022. С. 27–29.

Клименко Вячеслав Анатолійович,
заступник начальника управління –
начальник відділу аналітичної роботи
УКА ГУНП в Одеській області;
Постол Олена Ігорівна,
заступник начальника відділу
аналітичної роботи УКА ГУНП
в Одеській області

ПІДГОТОВКА АНАЛІТИКІВ КРИМІНАЛЬНОГО АНАЛІЗУ В СИСТЕМІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

У сучасних умовах підвищення загроз криміногенного характеру та ускладнення злочинних схем потреба у кваліфікованих аналітиках у структурі Національної поліції України зростає. Тому, ефективна боротьба зі злочинністю все більше потребує нових підходів, зокрема – широкого використання кримінального аналізу, як елементу оперативно-розшукової діяльності.

Аналітик кримінального аналізу щоденно залучений до багатоступеневого процесу збору, обробки, оцінювання, аналізу та інтерпретації інформації про, правопорушників, потерпілих осіб, способи скоєння злочинів та інше. За результатом обробки інформації завданням аналітика є формування аналітичного продукту, який обов'язково повинен містити обґрунтовані рішення у сфері розслідування злочинів, превенції та оптимального розподілу ресурсів поліцейських. У зв'язку з цим виникає об'єктивна необхідність у формуванні системного підходу до підготовки та професійного розвитку аналітиків, запровадження єдиних стандартів і методик кримінального аналізу, а також інтеграції аналітичної діяльності в усі рівні функціонування Національної поліції. Застосування кримінального аналізу як постійного елементу оперативної діяльності дозволить не лише підвищити рівень розкриття злочинів, а й запобігати їх вчиненню, зміцнюючи загальну безпеку в державі.

Успішне виконання аналітичної роботи потребує комплексу професійних та міжособистісних компетенцій. Так, до основних ключових компетенцій аналітика кримінального

аналізу можна включити: фахові знання, що охоплюють базову теоретичну підготовку, яка необхідна для ефективного аналізу злочинності (юридичні знання, основи кримінального аналізу чи системний аналіз, інформаційні системи – вміння працювати з базами даних, аналітичним програмним забезпеченням, візуалізацію даних тощо, технічні навички – робота із програмним забезпеченням ArcGIS, i2 Analyst's Notebook, Excel, Power BI та іншими програмами обробки даних та візуалізації, цикл аналітичної діяльності – розуміння етапів збору, обробки, аналізу та поширення інформації, а також комунікаційні навички, тобто, здатність чітко викладати результат аналітичної роботи, як у письмовій, так і усній формах; **практичне навчання**, що є складовою професійного становлення аналітика (робота під керівництвом більш досвідчених аналітиків, аналіз реальних або змодельованих кримінальних правопорушень, участь у виїздах на місця подій та взаємодія з оперативними та слідчими підрозділами); **постійний професійний розвиток** для безперервного оновлення своїх знань та навичок (участь у тренінгах, семінарах, проходження онлайн курсів, комунікація із колегами з інших регіонів України та закордону).

Окрім зазначених компетенцій, важливою складовою професійної діяльності аналітика кримінального аналізу є дотримання етичних стандартів та принципів доброчесності. Аналітик повинен діяти неупереджено, об'єктивно та відповідально, забезпечуючи конфіденційність оброблюваної інформації й дотримуючись норм законодавства щодо захисту персональних даних. Також, важливим є вміння працювати у стресових умовах та в умовах обмеженого часу, зберігаючи при цьому високу якість результатів аналізу. Крім того, ефективний аналітик має володіти критичним мисленням, креативністю у підходах до вирішення складних завдань, а також вмінням працювати як індивідуально, так і в команді.

Однак, у підготовці кримінальних аналітиків є і певні виклики, наприклад, відставання у впровадженні сучасних IT-рішень в освітньому процесі, що створює розрив між рівнем підготовки випускників та реальними потребами кримінального аналізу; недостатнє кадрове забезпечення викладачами-практиками, що обмежує можливість передачі актуальних знань,

навичок та прикладів із реальної практики; динамічне зростання нових видів злочинності – фішинг, фінансове шахрайство з використанням новітніх технологій, злочини, пов'язані з криптовалютами, штучним інтелектом та кіберфрод, ці загрози змінюються настільки швидко, що навчальні програми не встигають адаптуватися до нових викликів.

Таким чином, для підвищення ефективності кримінального аналізу необхідно не лише вдосконалення системи професійної підготовки аналітиків, але й забезпечення тісної співпраці між освітніми установами, правоохоронними органами та ІТ-сферою, що дозволить адаптувати навчальні програми до сучасних викликів, сприяти впровадженню інноваційних підходів в аналітичну практику та оперативно реагувати на динамічні зміни у зміни у злочинному середовищі.

Кримінальний аналіз сьогодні – це поле, що постійно розвивається, тому систематичне навчання та регулярний професійний розвиток є важливими для ефективного використання аналітичних методів і інструментів, а також для своєчасного реагування на нові виклики у правоохоронній сфері.

Колесник Олексій Андрійович,
начальник управління кримінального
аналізу ГУНП у Львівській області

ТАКТИЧНИЙ АНАЛІЗ ДАНИХ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ПРАКТИКА HOT-SPOTS POLICING

У сучасних умовах, коли рівень злочинності у світі зростає, правоохоронні органи стикаються з необхідністю впровадження нових підходів до збору, аналізу та використання даних. Для ефективного протидії злочинності вже недостатньо лише фіксації подій – ключовим стає аналітичне мислення, яке охоплює оперативний, тактичний та стратегічний рівні аналізу.

Підхід, що передбачає розмежування аналітики на стратегічний, оперативний та тактичний рівні, широко висвітлений у наукових працях і практичних рекомендаціях, зокрема у публікаціях одного з найцитованіших фахівців у галузі аналітичної розвідки та моделі Intelligence-led Policing – доктора Джеррі Ретклiффа (Dr. Jerry H. Ratcliffe) [4; ст. 8–11].

Загалом, доктор Джеррі Ретклiфф зазначає, що традиційний підхід полягає у визначенні двох або трьох площин аналітичної діяльності [1]:

– тактична – підтримка оперативних підрозділів, розслідувань та інших підрозділів у вжитті конкретних заходів для досягнення цілей правозастосування,

– оперативна – підтримка керівників підрозділів і регіональних органів у плануванні заходів зі зниження рівня злочинності та розподілі ресурсів,

– стратегічна – спрямована на забезпечення розуміння, а також внеску у широкі стратегії, політики та ресурси.

Тактичний аналіз даних є одним із ключових елементів сучасного кримінального аналізу, зокрема в рамках моделі Intelligence Led Policing (ILP). Однією з найефективніших практик цього рівня є методика hot spots policing, що передбачає спрямування обмежених ресурсів поліції на чітко визначені території з високим рівнем злочинів. Цей підхід дозволяє більш ефективно протидіяти злочинності за рахунок таргетованих і обґрунтованих дій поліції.

У свою чергу, hot spots policing ґрунтується на ідеї, що злочинність має просторову нерівномірність і концентрується у «гарячих точках» – невеликих географічних зонах з стабільним високим рівнем правопорушень [2].

Варто підкреслити, що ефективність цього методу підтверджено мета-аналізами: зниження загальної злочинності на 17 %, насильницькі злочини – на 14 %, наркотичні правопорушення – на 30%, а злочинів проти власності – на 16 % [3].

Одним із ключових інструментів реалізації стратегії hot-spots policing є картографування злочинності за допомогою геоінформаційних систем (GIS). За допомогою геоінформаційних систем (GIS) правоохоронці можуть візуалізувати зони підвищеної кримінальної активності, аналізувати закономірності розташування злочинів, а також формувати рекомендації щодо ефективного розподілу патрулів [5].

Крім того, в межах реалізації цієї моделі активно використовується організація спрямованих патрулів різних типів (автомобільних, піших, велосипедних) доповнюється застосуванням систем відеоспостереження (CCTV), а також оперативними методами, як-от stop and search (зупинка та

перевірка). Це дозволяє оперативно реагувати на зміни криміногенної обстановки в «гарячих точках» та підвищує ефективність превентивних заходів [6, ст. 53–59].

Значну роль у практичному втіленні концепції hot-spots policing відіграє також підхід Problem-Oriented Policing (POP) – це підхід, що зосереджується на аналізі причин злочинності у певних районах, пошуку системних рішень та оцінці ефективності впроваджених заходів. POP розглядається як ефективний метод у поєднанні з hot-spots policing, оскільки сприяє комплексному усуненню факторів, які спричиняють злочини [7, ст. 223–250].

В Україні підрозділи кримінального аналізу Національної поліції використовують GIS-картографування та інтерактивні теплові карти для відображення зон підвищеної злочинності (hot spots), що дає можливість виявляти такі зони й формувати аналітичні рекомендації для розподілу поліцейських ресурсів (ArcGIS, i2 Analyst's Notebook, інтеграція даних) [8].

Проте системна реалізація цієї моделі потребує подальшого розвитку аналітичної інфраструктури, підвищення кваліфікації та розширення міжвідомчої співпраці.

Таким чином, hot-spots policing є ефективним методом тактичного аналізу, що дозволяє цілеспрямовано використовувати ресурси поліції для зниження рівня злочинності у визначених «гарячих точках». Його застосування в Україні вже починається, проте для досягнення максимальних результатів необхідно подальше вдосконалення аналітичних інструментів, підвищення кваліфікації працівників і розвиток міжвідомчої співпраці.

Список використаних джерел

1. Ratcliffe J. H. Intelligence-Led Policing. 2-ге видання. Нью-Йорк: Routledge, 2016.

2. College of Policing. Hot-spots policing guidance. URL: https://www.college.police.uk/guidance/hot-spots-policing

3. Youth Endowment Fund. Hot-spots policing toolkit.. URL: https://youthendowmentfund.org.uk/toolkit/hot-spots-policing/.

4. Ratcliffe J. H. Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders. Washington, DC: Police Foundation, 2007.

5. John E. Eck та ін. Mapping Crime: Understanding Hot Spots. National Institute of Justice, серпень 2005. URL: https://www.tandfonline.com/doi/full/10.1080/19475683.2012.691900

6. Taylor B. Crime Prevention and Community Safety. Vol. 16, No. 2, 2014, pp. 95–110; Weisburd D., Eck J. E. What can police do to reduce crime, disorder, and fear? Police Quarterly. 2004

7. Goldstein H. Problem-Oriented Policing. Нью-Йорк: McGraw-Hill, 1990; Braga A. A., Weisburd D. *Is problem-oriented policing effective in reducing crime and disorder?*. Journal of Experimental Criminology, 2010.

8. Користін О., Швець Д., Бутко Б., Денисенко Б. та ін. Реалізація філософії Intelligence-Led Policing в системі кримінального аналізу Національної поліції України: монографія, Київ: «ВАІТЕ», 2024.

Копитько Вікторія Юріївна,
аспірант кафедри криміналістичного забезпечення та судових експертиз навчально-наукового експертно-криміналістичного інституту Національної академії внутрішніх справ

ФОРМИ МАСКУВАННЯ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ ПІД ВИГЛЯДОМ ГУМАНІТАРНОЇ МІСІЇ

Формування гуманітарної системи в умовах воєнного конфлікту супроводжується одночасно зростанням довіри до всього, що маркується як «допомога», і зростанням складності її контролю. Правовий статус гуманітарного вантажу дедалі частіше використовується як інструмент легалізації дій, що мають ознаки економічного, службового або навіть воєнного правопорушення. В українському контексті така практика виникла внаслідок надзвичайного темпу надходжень, неузгодженості між інституціями, обмеженого ресурсу на верифікацію отримувачів і фрагментарної цифровізації [1; 4].

З точки зору криміналістики маскування є частиною способу приховування в стуктурі елементів криміналістичної характеристики та розглядається як дії, що перешкоджають ідентифікації, фіксації чи розкриттю злочину. Йдеться не лише про приховування слідів, а й про створення уявлення про законну мету, зокрема через статус гуманітарної місії. У практиці сучасної війни

такі механізми адаптовані до швидких змін логістики, нормативної бази й формальної відповідності [5, с. 16].

Розмежування між помилками в обліку та умисним маскуванням в українській судовій і слідчій практиці все ще недостатньо визначене. Облікові відхилення можуть виникати через брак ресурсів, однак саме повторюваність, послідовність і зовнішня легітимність свідчать про наявність схеми. Саме тому необхідна чітка методика кваліфікації, яка б враховувала не лише формальні ознаки, а й сукупність обставин [4; 7].

Нормативно-правовий акт (Постанова КМУ № 953 від 05.09.2023) не містить вичерпного переліку ознак, за якими гуманітарну діяльність можна визнати фіктивною. Така відсутність дозволяє використовувати зовнішні ознаки для легалізації контрабанди, підробки, ухилення від податків і розвідки [6].

В українському кримінальному праві гуманітарний статус не має окремого захисту, що дозволяє кваліфікувати відповідні злочини за стандартними статтями – шахрайство (190), легалізація (209), службове підроблення (366), зловживання владою (364), порушення порядку міжнародних передач (201-2) [3]. Маскування, таким чином, стає складовою способу вчинення злочину.

На європейському рівні статус гуманітарного прикриття розглядається як special concealment scheme – особлива форма легітимізації злочину через використання довіри до волонтерства або благодійності. Для доведення умислу в таких справах необхідно залучення фахівців, зокрема логістів, митних експертів, облікових аналітиків [9].

У сфері економічної злочинності гуманітарна допомога часто використовується як механізм транзиту без декларування або як форма уникнення оподаткування. Продукція ввозиться без мита, але реалізується через підконтрольні комерційні структури. У справі №134/2897/23 (Хмільницький міськрайонний суд) зафіксовано продаж авто, ввезених як гуманітарних, через третіх осіб, оформлених на підставних представників [2].

Окремий ризик становить використання статусу гуманітарної організації для ведення діяльності, пов’язаної з нелегальними збройними формуваннями або збором розвідувальних даних. Згідно з повідомленнями СБУ, у 2022–2023 роках виявлено низку організацій, які під виглядом доставки

гуманітарки здійснювали передачу обладнання подвійного призначення або фіксацію переміщення підрозділів [7].

Згідно з положеннями міжнародного гуманітарного права, будь-яка діяльність, що видає себе за гуманітарну, але водночас порушує принцип нейтральності, є формою воєнного шахрайства. Відповідно до Женевських конвенцій, використання такого прикриття не лише дискредитує гуманітарну місію, а й може вважатися порушенням міжнародного зобов'язання держави [9].

У структурі злочинного маскування виділяється кілька стійких моделей. Організаційне маскування реалізується через створення фіктивних благодійних фондів. За даними звіту SOCTA, лише у 2022–2023 роках в Україні було зареєстровано понад 200 таких суб'єктів, що діяли без складів, працівників і прозорої звітності [88, с. 14]. Їхня діяльність обмежувалася оформленням документів, тоді як фактичне управління здійснювали сторонні особи.

Документальні форми передбачають підробку листів військових адміністрацій, актів прийому-передачі, сертифікатів, а також використання справжніх документів у схемах подвійного обігу. У справі про реалізацію транспортних засобів з гуманітарною історією суд зафіксував умисну фіктивність документального оформлення з метою комерційного зиску [3].

Логістичне маскування передбачає використання недокументованих проміжних складів, зміну маршруту, повторне пакування або перемаркування вантажу. За даними Ю. Мороза і В. Чаплинського, у таких схемах гуманітарна допомога не надходить до кінцевого споживача, натомість її частина реалізується або передається стороннім особам [4, с. 18].

У випадках, коли гуманітарні товари потрапляють у відкритий ринок, має місце торговельне маскування. Продукція, що формально призначалася для безоплатної допомоги, з'являється в аптеках або магазинах із переклеєними етикетками. За даними ЛІГА:ЗАКОН, протягом 2023 року зафіксовано понад 70 таких випадків [7].

Політичне маскування виявляється в кампаніях збору коштів, що мають ознаки політичної підтримки або комерційної діяльності під виглядом волонтерства. Воєнне маскування пов'язане з переміщенням осіб, техніки чи обладнання під прикриттям статусу евакуації або гуманітарної місії [5].

З огляду на наведені приклади, маскування набуває форми системного конструкту, в якому кожен елемент – від документа до складу – є частиною цілісної моделі. Успішне виявлення таких схем неможливе без інтеграції спеціальних знань, оскільки класичні методи слідства виявляються недостатніми в умовах легітимізованого оформлення.

Форми маскування, описані вище, не є випадковими чи фрагментарними. Вони свідчать про наявність цілеспрямованих, адаптованих до воєнного часу механізмів прикриття, які функціонують у правовому полі, але мають злочинну мету. Ефективне розслідування потребує міждисциплінарної участі, удосконалення цифрової верифікації та впровадження єдиних стандартів обліку й трасування гуманітарної логістики. У цьому контексті необхідність професійного аналізу, технологічної підтримки та правового унормування є умовою запобігання подальшій інституціоналізації таких схем.

Список використаних джерел

1. Волков С.В. Гуманітарна допомога в Україні: сучасні виклик. Юридичний науковий електронний журнал. 2023. № 8. С. 332–334. URL: https://lsej.org.ua/8_2023/77.pdf.

2. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua (справа № 134/2897/23, Хмільницький міськрайонний суд, квітень 2023 р.).

3. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

4. Мороз В. С., Чаплинський Ю. А. Організована злочинність і кримінал у гуманітарній сфері в умовах війни : монографія / В. С. Мороз, Ю. А. Чаплинський. Дніпро : ДДУВС, 2023. 148 с. URL: https://er.dduvs.edu.ua/bitstream/123456789/10816/3/Монографія%20Мороз%2С%20Чаплинський%2004.04.23-1.pdf.

5. Носевич Н. О. Облік та одержання благодійної гуманітарної допомоги в умовах воєнного стану / Н. О. Носевич // Актуальні питання протидії злочинності в умовах воєнного стану : зб. матеріалів круглого столу (Кривий Ріг, 2022). Кривий Ріг : ДНДУВС, 2023. С. 5–9. URL: https://dnuvs.ukr.education/wp-content/uploads/2023/05/zbirnyk_aktualni_pytannya_protydiyi_zlochynnosti.pdf.

6. Постанова Кабінету Міністрів України від 05 вересня 2023 р. № 953 «Деякі питання пропуску та обліку гуманітарної

допомоги в умовах воєнного стану». URL: https://www.kmu.gov.ua/npas/deiaki-pytannia-propusku-ta-obliku-humanitarnoi-dopomohy-v-umovakh-voiennoho-stanu-i050923-953.

7. Ризики для громадських та благодійних організацій під час здійснення транскордонних переказів // ЛІГА:ЗАКОН. 2023. URL: https://biz.ligazakon.net/analitycs/227019_riziki-dlya-gromadskikh--blagodynikh-organzatsy-pd-chas-zdysnennya-transkordonnikh-perekazv-valyutnikh-tsnnostey-ta-groshovikh-koshtv.

8. SOCTA Україна 2022. Оцінка загроз організованій злочинності в Україні / МВС України, Європол. Київ, 2022. 38 с. URL: https://mvs.gov.ua/upload/1/8/5/3/8/2/socta.pdf.

9. UNODC. Manual on anti-corruption in humanitarian aid operations. Vienna : United Nations Office on Drugs and Crime, 2021. URL: https://www.unodc.org/unodc/en/data-and-analysis/standards-and-manuals.html.

Лазарєва Яна Анатоліївна,
старший інспектор ВАР УКА ГУНП
в Дніпропетровській області

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ

З огляду на швидкий поступ інновацій, зокрема у сфері штучного інтелекту (надалі – ШІ), на сцену вийшли нові інструменти, покликані посилити результативність розслідувань, прогнозувати злочинність і керувати ризиками. Відповідно, у царині кримінального аналізу скорочується частка ручного опрацювання даних, адже постійно зростає арсенал засобів, що дають аналітикам можливість оперативно обробляти великі масиви інформації, виявляти приховані взаємозв'язки між фігурантами кримінального світу, автоматично генерувати візуалізації кримінальних мереж та будувати прогнозні моделі на основі історичних даних.

Завдяки алгоритмам машинного навчання, інструменти ШІ можуть не лише розпізнавати закономірності у діях злочинців, а й завчасно виявляти потенційні небезпеки, запобігаючи вчиненню нових злочинів.

Насамперед, звертаючись до праць Бранова О.О., **штучний інтелект** – це інтелект, що має штучне походження та імітує

(моделює) певну сукупність когнітивних функцій еквівалентних відповідним когнітивним функціям людини [1]. Тобто автор підкреслює, що штучний інтелект бере для прикладу алгоритм дій людини та в подальшому використовує їх.

В свою чергу, Стефанчук М.О. цілком влучно зазначає, що **штучний інтелект** за своєю сутністю є здатністю машин вчитися на людському досвіді та виконувати людиноподібні завдання. Інакше кажучи, його можна розглядати як моделювання здатності до абстрактної, творчої думки – і особливо здатності до навчання – за допомогою цифрової комп'ютерної логіки [2].

Якщо розглядати використання штучного інтелекту в безпосередній роботі кримінального аналітика, спершу слід підкреслити, що кримінальний аналіз–це специфічна форма інформаційно-аналітичної праці. Її метою є виявлення та передбачення взаємозв'язків між інформацією про злочини та іншими відомостями, що можуть бути з ними пов'язані. Це включає оцінку, інтерпретацію та передбачення розвитку подій, що розглядаються, задля використання отриманих результатів у досудових розслідуваннях, оперативно-розшуковій діяльності та розробці тактичних і стратегічних дій для протидії злочинності [3].

Іншими словами, кримінальний аналіз – це систематична аналітична робота, спрямована на збір, обробку, наочне представлення, тлумачення та прогнозування інформації, пов'язаної зі злочинністю. Це робиться для підтримки слідчих дій, запобігання правопорушенням, раціонального використання оперативних ресурсів і формування безпекових стратегій.

Як вже було зазначено, на теперішній час підрозділи кримінального аналізу все більше покладається на штучний інтелект, з метою підвищення точності аналітичних висновків, зменшення часу обробки великих масивів даних, виявлення прихованих закономірностей та зв'язків між суб'єктами кримінального середовища.

Під час кримінального аналізу основним завданням кримінального аналітика є проведення аналітичного дослідження доступної йому інформації, а також створення за результатами такого аналізу аналітичних продуктів, що мають інформативний та рекомендаційний характер і створюють підґрунтя для вирішення оперативних та тактичних завдань під

час документування та розслідування злочинів, або планування превентивних заходів у протидії злочинності.

Тож, аналітики часто стикаються із OSINT – аналізом, де необхідно проаналізувати велику кількість ресурсів, що не завжди можуть представляти оперативний інтерес або в повній мірі стосуватися тематики дослідження, в результаті чого витрачається значна кількість часу для формулювання висновків.

Перед початком пошуку необхідної інформації аналітикам варто для себе визначити, що ключовими факторами методології успішного аналізу є:

– чітке розуміння цілей аналізу;

– неупередженість (максимальна об'єктивність аналітика);

– збір інформації з максимально можливої кількості відкритих джерел;

– застосування «коефіцієнтів ваги» до кожної інформації;

– чіткість представлення даних;

– грамотний аналіз отриманої інформації.

Однак, аналітик, як людина, не завжди може дотримуватися абсолютно всіх ключових факторів через обмеження у часі, упередженість до певної категорії інформації або ж неможливість побачити всю «картину» через недостатньої кількості джерел. Тому, ШІ цілком підходить для даного типу задач, так як може зекономити час та розширити пошук інформації.

Як вже було зазначено, технологія «OSINT» є однією з важливих технологій «глибинного збору» різнорівневого формату інформації, а також формування на її базі принципово нових знань. Поширення і використання перевіреної інформації з відкритих джерел дозволяє здійснювати обмін такою інформацією, оскільки при її отриманні не використовуються приховані методи і секретні джерела.

Епоха цифровізації, «big data», та соціальних медіа змусила людини перенести своє життя в онлайн і жити за правилами всесвітньої мережі. Комусь це подобається, а хтось намагається ховатися та не з'являтися ні в одній соціальній мережі, видаляючи всі паролі та реєстрації.

Яскравими прикладами, де аналітики використовують ШІ є програмний продукт «Artellence», адже **це AI-компанія**, яка спеціалізується на рішеннях для OSINT (відкритої розвідки),

використовуючи машинне навчання (ML) та нейронні мережі. Варто зазначити, що використання вказаного продукту у кримінальному аналізі є на офіційному рівні.

Компанія також спеціалізується на аналізі великого обсягу відкритих даних (big data) для підтримки прийняття рішень. Завдяки цьому продукту та його алгоритмам, аналітики заощаджують час на пошук потрібної інформації та аналізу соціальних сторінок, які становлять оперативний інтерес.

Однак, мають місце випадки, коли алгоритми не завжди надають достовірний результат, так як надається лише «суха» оцінка інформації. Наприклад, візьмемо випадки, коли у програмному продукті «Artellence» ШІ самостійно аналізує та надає коротку інформацію по соціальним сторінкам особи, звертаючи особливу увагу на її «російську позицію». Алгоритм бере до уваги кількість друзів з рф, які має ця особа, публікації, на які вона ставила «Подобається» або ж наявність профілів та груп, учасником яких є особа. Здебільшого, в дописах може просто зазначатися інформація, де критикують дії рф або церкви московського патріархату, однак алгоритми оцінують це як підтримку. Тому, задачею аналітика все одно залишається перевірка цієї інформації та її уточнення, щоб отримати справедливий та доречний звіт.

Також не варто забувати про один із найбільш поширених штучних інтелектів на сьогодні, а саме – ChatGPT (Generative Pre-trained Transformer), розроблений компанією OpenAI.

У роботах Зачеки О.І. та співавторів висвітлено практичні приклади застосування ChatGPT як інструменту ШІ у протидії злочинності, проте наведені тези чудово демонструють його роль у кримінальному аналізі:

1. Вивчення соціальних мереж і веб-сайтів злочинців: ChatGPT може аналізувати текст, фотографії та відео, що опубліковані на цих ресурсах, для виявлення ознак протиправної діяльності.

2. Перевірка текстових повідомлень на наявність ознак злочинних намірів. Програма може розпізнавати ключові слова та фрази, що вказують на злочинну діяльність, зокрема, щодо наркотиків, зброї, планування злочину тощо.

3. Аналіз відеозаписів та зображень з камер спостереження. Програма здатна розпізнавати обличчя

правопорушників, транспортні засоби, номерні знаки та інші дані, що можуть допомогти у їх ідентифікації.

4. Згадане програмне забезпечення може бути використане для аналізу даних про злочинність та надання рекомендацій щодо превентивних заходів (програма може аналізувати статистику злочинів у певній галузі, регіоні та робити прогнози щодо можливих правопорушень на певній території обслуговування поліцейського підрозділу, а також пропонувати заходи, необхідні для їх уникнення) [4].

Проте, варто зазначити, що використання ChatGPT в роботі кримінального аналітика не є офіційним через питання верифікації, приватності, достовірності джерел тощо. Звичайно, такі системи, як ChatGPT, ще не інтегровані в офіційну діяльність підрозділів Національної поліції, але вони вже демонструють потенціал як допоміжні інструменти аналітичної обробки даних

Таким чином, в умовах сучасної цифровізації ШІ постає не як заміна аналітику, а як його інтелектуальний асистент у системі кримінального аналізу. Використання штучного інтелекту в кримінальному аналізі відкриває нові перспективи для ефективної боротьби зі злочинністю. Інструменти, що базуються на алгоритмах машинного навчання, дають аналітикам змогу швидко опрацьовувати великі обсяги відкритих і закритих джерел інформації, виявляти складні злочинні зв'язки, здійснювати прогнозування злочинної активності та формувати аналітичні продукти високої точності.

Однак, аналітики не повинні цілком і повністю покладатися на висновки та результати, які надаються штучним інтелектом, адже в кожній ситуації може виступати «людський фактор», де оцінювати потрібно з урахуванням безліч критеріїв, що не входить до функціоналу алгоритмів ШІ. Тобто варто підкреслити, що штучний інтелект на теперішній час дійсно полегшує роботу кримінальних аналітиків, допомагає знайти нові підходи та рішення, але роботу аналітиків у повній мірі замінити не зможе.

Вважаємо, що подальші дослідження цієї тематики варто зосередити, в першу чергу, на розробці нормативно - правових механізмів інтеграції ШІ в діяльність не лише підрозділів

кримінального аналізу, але й загалом Національної поліції України з урахуванням етичних принципів, захисту персональних даних та уникнення дискримінаційних упереджень в алгоритмах.

Список використаних джерел

1. Баранов О. О. Визначення терміну «штучний інтелект» / О. О. Баранов // Інформація і право. 2023. № 1. С. 32–49. URL: http://nbuv.gov.ua/UJRN/Infpr_2023_1_5.

2. Стефанчук М. О. Перспективи правового регулювання відносин у сфері використання штучного інтелекту / М. О. Стефанчук, О. А. Музика-Стефанчук, М. М. Стефанчук // Вісник Національної академії правових наук України. 2021. Т. 28, № 1. С. 306–332. URL: http://nbuv.gov.ua/UJRN/vapny_2021_28_1_18.

3. Основи кримінального аналізу: підручник / А. М. Бабенко, О.М. Заєць, В.А, Некрасов, К.Ю. Ісмайлов, Д.О. Пефтієв та ін. / за заг. ред. О.Є. Користіна. Київ, 2020. 296 с.

4. Зачек О. І. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності / О. І. Зачек, Ю. І. Дмитрик, В. В. Сеник // Науковий вісник Львівського державного університету внутрішніх справ. серія юридична. 2023. Вип. 3. С. 148–156. URL: http://nbuv.gov.ua/UJRN/Nvlduvs_2023_3_21.

Лемешко Юрій Олександрович,
начальник Управління кримінального аналізу ГУНП в Харківській області

ПРОБЛЕМНІ ПИТАННЯ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ АНАЛІЗУ АКТИВНОСТІ КОРИСТУВАЧІВ БЕЗ СУДОВОГО САНКЦІОНУВАННЯ

Повномасштабна збройна агресія проти України змінила не лише хід історії, а й формат викликів, із якими щодня зіштовхується система кримінальної юстиції. В умовах воєнного стану на перший план вийшли питання протидії державній зраді, колабораціонізму, інформаційним диверсіям, а також кримінальним правопорушенням, які безпосередньо загрожують національній безпеці. Одночасно з цим значно ускладнилась і сама структура злочинності: ми маємо справу не з одиничними діями, а з скоординованими, часто добре законспірованими мережами – онлайн і офлайн. У цих умовах зростає роль

аналітичної підтримки розслідувань, зокрема через обробку великих обсягів відкритої інформації – OSINT-розвідки. Вміння вчасно ідентифікувати цифровий слід фігуранта, виявити його зв'язки, зафіксувати потенційно деструктивну активність у мережі може мати вирішальне значення у розкритті злочину.

Вирішення оперативно-службових завдань нерідко вимагає від працівників поліції застосування цілого комплексу оперативно-розшукових заходів, проведення слідчих (розшукових) дій, у т.ч. негласних, реалізації заходів забезпечення кримінального провадження. Тому в центрі уваги опиняються спеціалізовані інструменти для кримінального аналізу – системи, які дозволяють не просто збирати дані, а швидко знаходити в них закономірності, зв'язки й потенційні загрози. Переважна більшість описаних дій потребує судового санкціонування, що з одного боку забезпечує дотримання принципу законності у кримінальному судочинстві, а з іншого – суттєво уповільнює хід розслідування.

Водночас існує ціла низка законних способів отримання знеособлених персональних даних, вивчення яких дозволяє ідентифікувати особу правопорушника, визначити місця його перебування, побудувати профіль його активності тощо.

Одним з інструментів, що дозволяє зібрати та проаналізувати знеособлені дані, є застосування advertising intelligence (збирання та аналіз даних з різноманітних рекламних модулів).

Описана категорія даних збирається за згодою користувача різними компаніями через свої електронні сервіси та застосунки з метою подальшого використання для проведення цільової реклами. Наприклад, Google накопичує дані про тип і налаштування браузера й пристрою, операційну систему, мобільну мережу (зокрема, назву та номер телефону оператора) і номер версії додатка, відомості про взаємодію додатків користувача, веб-переглядачів і пристроїв із сервісами Google, зокрема IP-адресу, звіти про аварійне завершення роботи, активність системи й дату, час та URL-адресу напрямку переходу запиту користувача. Якщо особа користується пристроєм Android із додатками Google, він періодично зв'язується із серверами Google, щоб надати інформацію про пристрій і підключення до сервісів Google. Це, зокрема, дані про тип пристрою, назву оператора, звіти про збої, відомості про

встановлені додатки, а також, залежно від налаштувань пристрою Android, інша інформація про те, як особа користуєтеся ним [1].

Більш глибоке вивчення питання накопичення даних для таргетованої реклами з мобільних терміналів дозволяє окреслити механізм такого збирання. Мова йде про фіксацію різноманітними мобільними програмами даних користувачів з їх прив'язкою до рекламного ідентифікатора мобільного пристрою. У системах на базі Android такий ідентифікатор називається GAID (Google Advertising ID), а в системах на базі iOS – IDFA (identifier for advertisers).

Очевидно, що набір відповідних даних користувачів із прив'язкою до часу та простору зберігається у володільців відповідних програмних застосунків, які потім ними обмінюються безпосередньо або через проміжних осіб для організації більш ефективної цільової реклами. Наприклад, якщо користувач шукає якийсь товар через застосунок prom.ua, то реклама подібного товару невдовзі з'явиться у встановленому на тому ж пристрої застосунку Viber тощо.

Як можна проаналізувати описані знеособлені рекламні дані?

Перший спосіб полягає в організації власної рекламної компанії через кабінет рекламодавця у відповідних сервісах (рис.).

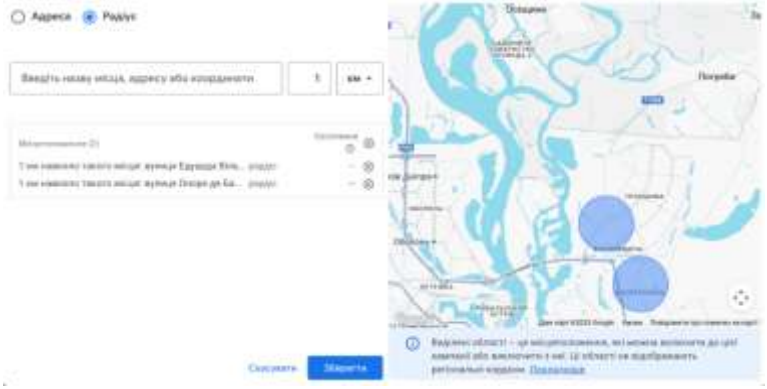

Рис. Налаштування таргетованої реклами в кабінеті Google Ads

У результаті можна відслідковувати появу пристрою на певних ділянках місцевості тощо. Водночас такий підхід дозволяє проводити аналіз у перспективі.

Для того, щоб здійснювати ретроспективний аналіз, існують спеціальні інструменти, як от Tangles від Penlink [2]. Із його використанням можна, наприклад, обрати декілька ділянок місцевості на карті та переглянути, які пристрої були у визначений час у відповідних місцях. Так само можна проводити вивчення ресурсів, які відвідувала особа з певним рекламним ідентифікатором, тощо.

Поліцейські підрозділи в США досить активно використовують подібні інструменти для відслідковування та ідентифікації користувачів [3]. Оскільки використання знеособлених персональних даних не потребує одержання судових рішень, програмне забезпечення, що дає доступ до рекламних даних знайшло широке використання у діяльності спеціальних служб та правоохоронних органів за кордоном.

Як видно з наведеного, головну цінність становлять саме дані користувачів, які можна аналізувати. Якщо розглянути ситуацію в українському вимірі, то відповідні застосунки, від яких можна отримати більшість користувацьких даних для аналізу, такі:

– банківські (Privat24, Ощад, Monobank тощо);
– поштові (Нова пошта, Meest пошта тощо);
– сервіси надання послуг (Bolt, Uklon, Uber тощо);
– сервіси прокату самокатів (Vevi тощо);
– сервіси продажів та партнерських програм (OLX.ua, Prom, Fishka, супермаркети, автозаправні, аптечні тощо).

Для того, щоб в умовах правового режиму воєнного стану більш ефективно попереджувати та розслідувати кримінальні правопорушення, вбачається доцільним внести зміни до чинного законодавства в частині зобов’язання установ, підприємств та організацій передавати відповідні дані користувачів єдиному центру обробки даних, через який правоохоронні органи могли б отримувати відомості для аналізу.

Серед іншого, пропонуємо внести зміни до Закону України «Про захист персональних даних», якими офіційно визначити поняття «контролер персональних даних» як суб’єкт,

що визначає мету та способи обробки даних, у тому числі знеособлених даних. Контролери, які використовують такі дані для таргетингу реклами, повинні бути зобов'язані передавати зведену інформацію органу державної влади в порядку, затвердженому Кабінетом Міністрів України. Така передача не повинна вимагати згоди фізичних осіб, якщо ідентифікація суб'єкта неможлива. Закон «Про рекламу» має містити положення, що зобов'язують рекламодавців, агенції та цифрові платформи надавати державі знеособлені дані про аудиторію для проведення рекламних кампаній. Уповноважений орган має бути наділений повноваженнями перевіряти дотримання цієї вимоги та застосовувати відповідні санкції у разі порушення.

Водночас, Закон України «Про інформацію» має бути доповнений положеннями про визнання анонімних даних окремим видом інформації. Хоча вони не дозволяють ідентифікувати особу, їх можна використовувати для аналізу поведінкових моделей. Держава повинна мати право доступу до таких не конфіденційних даних для забезпечення прозорості цифрових процесів, протидії дезінформації та моніторингу рекламної діяльності.

Крім того, пропонуємо розглянути можливість внесення змін до Закону України «Про електронні комунікації», оскільки рекламні дані часто передаються через телекомунікаційну інфраструктуру. Необхідно визначити поняття знеособлених телекомунікаційних даних, а також зобов'язати провайдерів електронних комунікаційних послуг надавати державним органам узагальнену інформацію про користувачів, яка використовується для реклами. Крім того, необхідно встановити зобов'язання щодо прозорої обробки таких даних та їх правового захисту.

Прийняття вказаних змін дозволить отримати важливу для правоохоронних органів та спеціальних служб інформацію без надмірної витрати коштів, які в іншому випадку необхідно сплачувати стороннім особам – володільцям та розпорядникам рекламних даних.

Список використаних джерел

1. Політика конфіденційності Google. URL: https://policies.google.com/privacy?hl=uk.

2. Transforming Investigations with Digital Intelligence and Evidence Analysis. URL: https://www.penlink.com/why-penlink/.

3. Texas state police expands surveillance with PenLink's controversial technology raising privacy concerns. URL: https://www.business-humanrights.org/ru/свежие-новости/texas-state-police-expands-surveillance-with-penlinks-controversial-technology-raising-privacy-concerns/.

Овсянюк Дмитро Іванович,
начальник аналітичного відділу (Центр кримінальної аналітики) Національної академії внутрішніх справ

ОРГАНІЗАЦІЯ АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ У СФЕРІ ПРОТИДІЇ НАРКОЗЛОЧИННОСТІ

Актуальність протидії наркозлочинності зумовлена її системними загрозами для сталого розвитку держави, громадського здоров'я, безпеки та правопорядку. Міжнародний незаконний обіг наркотиків є високоприбутковим кримінальним бізнесом, який переважно контролюється організованими злочинними групами. Ці групи відзначаються гнучкістю, адаптивністю до заходів протидії та значними фінансовими ресурсами, що спрямовуються на технічне оснащення та підтримання корупційних зв'язків. Торгівля наркотиками визнана однією з найсерйозніших загроз безпеці, з якою стикається Європейський Союз, і, за оцінками, становить близько однієї п'ятої світових злочинних доходів [1].

Ефективне розв'язання цієї проблеми вимагає розробки та впровадження стратегій, що базуються на найкращих практиках та наукових дослідженнях, оптимізують використання ресурсів правоохоронних органів і зменшують шкоду від незаконного обігу наркотиків. Це підкреслює необхідність застосування структурованих підходів, де ключову роль відіграє кримінальний аналіз.

Ключовим аспектом успішної та ефективної організації аналітичної діяльності та її основою є глибоке розуміння та осмислене дотримання аналітиком етапів динамічного розвідувального циклу, який є фундаментом кримінального аналізу [2]. Застосування цього циклу може підняти протидію наркозлочинності на якісно новий рівень, дозволяючи

правоохоронцям діяти проактивно та випереджати злочинців, навіть в умовах обмежених ресурсів.

Цикл аналізу злочинів, пов'язаних із незаконним обігом наркотиків, є основною складовою планування та реалізації зусиль правоохоронних органів у протидії наркозлочинності. Він передбачає визначення цілей і задач аналізу, встановлення даних та інформації, необхідних для досягнення цих цілей, а також розроблення комплексного та структурованого підходу до збору, аналізу й використання цих даних [3].

Аналітичний цикл не є статичною послідовністю із шести кроків, а є переважно динамічним процесом, де різні фази тісно пов'язані між собою та взаємодіють одна з одною, що потребує від аналітиків переміщатися вперед і назад усередині циклу [4].

1. Визначення завдань та планування

Перший етап є вирішальним для успіху всього аналітичного процесу. На цій стадії замовник визначає цілі та завдання дослідження, їх пріоритетність та очікувані результати. Замовник передає аналітику всю наявну інформацію, важливу для досягнення цілей.

Цілі кримінального аналізу у сфері протидії наркозлочинності можуть бути різноманітними:

Оперативні: ідентифікація злочинців та їхніх зв'язків, пошук доказової інформації, виявлення співучасників, встановлення мотивів, реконструкція злочинної діяльності, виявлення корупційних зв'язків та активів для арешту.

Тактичні: виявлення шаблонів та трендів у злочинності, прогнозування, аналіз методів скоєння злочинів, визначення структури наркоринку, аналіз маршрутів транзиту та відстеження нових способів збуту.

Стратегічні: розробка обґрунтованих державних стратегій і політик, прогнозування довгострокових загроз і тенденцій, оптимізація розподілу правоохоронних ресурсів та зменшення шкоди для суспільства.

На основі поставлених завдань аналітик оцінює достатність даних і формує попередній план роботи. Постійна комунікація між аналітиком та замовником на цьому і на всіх наступних етапах є надзвичайно важливою.

2. Збір та оцінка даних

На цьому етапі відбувається збір інформації з широкого спектра джерел, що може включати матеріали кримінальних

проваджень, дані митниці та судового реєстру, відкриті джерела, інформацію від оперативних працівників та анонімних джерел, фінансові записи, дані телекомунікацій, інформацію від міжнародних партнерів та результати негласних слідчих (розшукових) дій, та інше.

Особливого значення в сучасних умовах набуває автоматизація процесів збору та первинної обробки даних з відкритих джерел. Використання спеціалізованих AI-технологій, зокрема таких як розробляє українська компанія Artellence, дозволяє значно підвищити ефективність цього етапу завдяки автоматичному розпізнаванню осіб у візуальному контенті, обробці великих обсягів даних з соціальних мереж та структуруванню інформації.

Після збору дані підлягають оцінці на предмет достовірності, надійності, актуальності та релевантності поставленим цілям.

3. Узагальнення, систематизація та обробка

На цьому етапі зібрана інформація структурується, перетворюється у формат, придатний для аналізу, та впорядковується з урахуванням цілей і пріоритетів. Цей етап тісно переплітається з аналізом, створюючи єдиний процес, спрямований на всебічне розуміння проблеми.

4. Аналіз

Це центральний етап циклу, метою якого є отримання нових знань із оброблених даних для досягнення цілей дослідження. Аналіз можна схарактеризувати як ретельне дослідження інформації з метою виявлення її значення та основних характеристик [5]. Аналіз складається з двох підетапів: інтеграції та інтерпретації.

Інтеграція даних: Це процес об’єднання інформації з різних джерел для виявлення закономірностей, формування гіпотез та виявлення інформаційних прогалин. Ключову роль тут відіграє візуалізація за допомогою схем зв’язків, хронологічних шкал, діаграм руху та геопросторового аналізу.

Інтерпретація даних: Це найбільш творча частина роботи, де аналітик перевіряє гіпотези, встановлює причинно-наслідкові зв’язки та робить обґрунтовані висновки. Цей процес вимагає глибокого розуміння контексту, критичного та креативного мислення, вільного від упереджень.

5. Підготовка звіту та його передача замовнику

Результати аналізу оформлюються у вигляді аналітичного звіту. Він має містити чіткі висновки (які рекомендується розміщувати на початку звіту), детальний опис дослідження, відповіді на поставлені запитання та практичні рекомендації. Якісна візуалізація у формі діаграм, графіків та мап є бажаним доповненням до звіту.

6. Зворотний зв'язок

Отримання зворотного зв'язку від замовника є невід'ємним етапом, що сприяє підвищенню якості аналітичних продуктів та професійному зростанню аналітиків. Аналітики повинні знати, чи відповідали результати очікуванням і як вони вплинули на прийняття рішень. Це двосторонній процес, що також дозволяє вдосконалювати співпрацю між аналітиком та замовником.

Розвідувальний цикл є універсальним інструментом, що дозволяє впорядкувати аналітичну діяльність, забезпечити контроль якості та досягти високих результатів у правоохоронній сфері. Якісний аналіз забезпечує глибоке розуміння злочинних процесів, дозволяє раціонально розподіляти ресурси та планувати ефективні заходи. Це сприяє не лише вилученню наркотиків та затриманню окремих злочинців, але й викриттю масштабних злочинних мереж, їх фінансових потоків та міжнародної логістики. Ефективна боротьба з наркозлочинністю вимагає постійних зусиль та активної співпраці між правоохоронними органами, міжнародними партнерами та іншими зацікавленими сторонами [6].

Список використаних джерел

1. EU Drug Markets: In-depth analysis https://www.emcdda.europa.eu/publications/eu-drug-markets_en.

2. Ovsianiuk D. Intelligence cycle as the basis of analytical activity in combating drug-related crime. Law Journal of the National Academy of Internal Affairs. 2024. Vol. 14, no. 2. P. 95–104., С. 98.

3. Овсянюк Д. І. Методологічні засади тактичного аналізу та аналізу оперативних даних під час розслідування злочинів, пов'язаних з незаконним обігом наркотиків : метод. рек. Київ : Нац. акад. внутр. справ, 2024. – 50 с., С. 13.

4. OSCE Guidebook Intelligence-Led Policing – Organization for Security and Co-operation in Europe. Vienna, 2017. P. 30.

5. Criminal Intelligence : Manual for Analysts. Vienna, Austria : United Nations Office on Drugs and Crime (UNODC), 2011. 96 p. C. 13

6. Ovsianiuk D., Ustymenko O. Exchange of Information as a Form of International Cooperation in Combating Drug Trafficking. Novum Jus. 2024. Vol. 18, no. 1. P. 181–216.

Овчаренко Едуарда Вікторівна,
заступник начальника відділу
оперативної аналітики Департаменту
кримінального аналізу Національної
поліції України

МОЖЛИВОСТІ ВИКОРИСТАННЯ ВБУДОВАНОГО РЕДАКТОРА POWER QUERY ТА POWER PIVOT

В умовах сьогодення робота з великими масивами даних стає нагальною необхідністю для аналітиків, проте опрацювання таких даних супроводжується низкою труднощів, насамперед, значною варіативністю джерел і форматів, у яких надходить ця інформація. Дані можуть зберігатися у форматах PDF, Excel, CSV, XML або на вебресурсах, що ускладнює їх уніфіковану обробку та зумовлює необхідність попереднього очищення, структурування та узгодження. Одним із ключових викликів при роботі з такими джерелами, що постає перед аналітиком, є відсутність єдиного стандарту подання інформації, до прикладу, типові банківські виписки можуть бути подані в таблицях різної структури, що потребує додаткових інструментів для їх подальшої обробки.

З огляду на перераховане, особливої цінності набувають програмні рішення, які дозволяють ефективно інтегрувати, трансформувати та моделювати великі масиви даних. Саме в цьому контексті Power Query та Power Pivot, вбудовані у середовище Microsoft Excel, є універсальними інструментами для вирішення зазначених завдань.

Power Query – це інструмент для імпорту, очищення та трансформації даних, що дозволяє завантажувати дані з різних джерел та здійснювати їх попередню обробку.

Застосування Power Query значно полегшує роботу з великими масивами даних та їх аналізом. Зокрема серед переваг можна виокремити:

– *імпорт даних*, що надає можливість завантажувати дані з різноманітних джерел, таких як Excel, CSV, баз даних, вебсторінок та багато інших в один документ;

– *трансформація даних*, що дозволяє видаляти зайві колонки, фільтрувати рядки, видаляти дублікати, змінювати формати даних та виконувати багато інших операцій;

– *автоматизація процесів*, оскільки після налаштування запитів Power Query може автоматично виконувати ці процеси, щоразу під час оновлення даних.

Power Pivot – це надбудова для аналізу даних, яка дозволяє створювати складні моделі і виконувати аналіз великих масивів інформації. Power Pivot дає змогу створювати зв'язки між таблицями та подальшому будувати зведені таблиці та міри для більш ефективного аналізу.

Приклади застосування Power Query та Power Pivot:

1. Об'єднання декількох файлів.

Power Query є ідеальним інструментом для консолідації даних з різних джерел, таких як Excel-файли, CSV чи текстові файли. Якщо дані зберігаються в різних файлах або охоплюють різні періоди, Power Query дозволяє автоматично об'єднати їх в одну таблицю.

2. Автоматизація систематичної обробки даних.

Якщо є необхідність регулярно виконувати однакові операції обробки даних, Power Query дозволяє автоматизувати цей процес. До прикладу, налаштувати трансформацію даних, їх очищення, фільтрацію та об'єднання на основі визначених правил.

3. Аналіз банківських транзакцій.

Power Query дозволяє обробляти великі обсяги транзакцій, очищати дані та проводити агрегацію. Використовуючи Power Pivot, можна створювати складні моделі для фінансового аналізу, виявляти закономірності, основних відправників та отримувачів коштів, взаєморозрахунки між певною категорією осіб, створювати масиви даних для подальшого пошуку ланцюгів фінансових операцій.

4. Аналіз даних про перетини державного кордону.

Power Query може використовуватися для об'єднання та обробки великих масивів даних, що стосуються перетину

державного кордону для встановлення осіб, які здійснювали спільні перетини, виявлення періодів перебування за межами України; виокремлення транспортних засобів, які найчастіше використовувалися особами при перетинах.

5. Аналіз податкових накладних.

Power Query допомагає автоматизувати обробку та агрегацію податкових накладних, здійснити очищення даних, встановити підприємства, які подають податкову звітність з однакових IP-адрес та взаєморозрахунки між ними і т.д.

Олейніков Олег Анатолійович,
начальник відділу програмно-технічного забезпечення слідчої та оперативно-розшукової діяльності Управління інформаційних технологій Державного бюро розслідувань

МЕТОДИ GRAPH INTELLIGENCE ТА АНАЛІЗ СХЕМ ЗВ'ЯЗКІВ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

У процесі розслідування кримінальних правопорушень збільшується потреба аналізу складних схем зв'язків: між абонентами мобільного зв'язку, учасниками фінансових операцій, суб'єктами у соціальних мережах, особами й об'єктами реального світу.

Зв'язки, які раніше аналізувалися інтуїтивно, зараз мають великий обсяг та складну структуру – надвелика кількість учасників (об'єктів аналізу), історичні дані за значний календарний період, поєднання схем з ваговими або часовими атрибутами. У таких випадках традиційні табличні методи та графічне представлення стають недостатньо ефективними.

Термін Graph Intelligence (GraphINT) почав з'являтись серед офіційних публікацій розробників сучасних програмних продуктів орієнтованих на роботу зі складними зв'язками (Tom Sawyer Software, Graphistry, Locstat). Загалом зі збільшенням складності та розміру досліджуваних даних виникла потреба у застосуванні спеціального програмного забезпечення, пов'язаного з сучасними аналітичними методами та спеціалізованими нейронними мережами, орієнтованих на роботу з графовою структурою. Не менш важливим є

забезпечення ефективної інфраструктури зберігання та обробки графової інформації, засобів її відображення, підтримки редагування аналітичних сценаріїв.

Дослідження схем зв'язків під час розслідування переважно збігається з підходами, які застосовуються при дослідженні зв'язків у комерційній сфері, банківській діяльності, протидії страховому шахрайству, тощо.

Серед інструментів, які підтримують аналіз графових структур, можна виділити кілька категорій:

– візуальні засоби з можливістю базового статистичного аналізу або інтеграцій з іншими сервісами зберігання даних: Gephi, Maltego, Cytoscape, IBM i2 Analyst Notebook – для побудови та візуалізації схем зв'язків;

– публічні сервіси візуалізації з використанням обчислювальних можливостей надавача послуг: Graphistry, Kineviz, Linkurious;

– прикладні програмні бібліотеки для розробки додатків: networkx, igraph, graph-tool, pyvis, DGL, PyTorch Geometric – дають змогу створювати власні аналітичні інструменти;

– системи управління баз даних: Neo4j (Neo4j Bloom в якості інструмента взаємодії), TigerGraph, ArangoDB – оптимізовані для роботи з графами;

– табличні процесори Excel, LibreOffice Calc, pandas – для первинного групування або формування списків вузлів та зв'язків.

У рамках підходів GraphINT застосовується широкий спектр методів, що охоплюють як класичні, так і сучасні техніки аналізу. Насамперед використовуються математичні методи теорії графів, зокрема центральності, кластеризації, підграфи зв'язності та аналіз потоків, які дозволяють виявляти ключові вузли та групи. Доповненням до них виступають статистичні методи – частотний аналіз та виявлення аномальної активності. Для реалізації аналітики використовуються програмні підходи, які передбачають побудову алгоритмів на основі списків зв'язків, матриць суміжності або часових журналів подій. Окрему категорію становлять методи машинного навчання, серед яких слід виокремити графові нейронні мережі (GNN), а також алгоритми node2vec, класифікацію вузлів та embedding-

підходи. Не менш важливою є візуальна складова, яка охоплює інтерактивну навігацію по графу, форматування, динамічну фільтрацію за часом, категоріями зв'язків або сумарними показниками.

У найпростішому випадку зв'язки між об'єктами описуються за допомогою ненаправлених простих графів, які лише фіксують сам факт взаємозв'язку без уточнення його сили чи напряму. Така структура часто використовується для моделювання соціальних відносин. У межах такого підходу можуть бути застосовані базові аналітичні методи: виявлення груп (кластерів), пошук центральних вузлів, аналіз компонент зв'язності. Подібні графи добре підходять для первинного дослідження структури мережі, коли пріоритетом є зрозумілість і наочність.

Більш інформативними є зважені графи, у яких кожне ребро має числове значення – наприклад, кількість з'єднань, тривалості взаємозв'язків або обсяг переданої інформації чи коштів. У таких графах з'являється можливість враховувати не лише наявність зв'язку, але й його інтенсивність.

Найбільш гнучким інструментом для кримінального аналізу є множинні направлені графи з часовими позначками та вагами, які здатні відображати складні сценарії взаємодії – зокрема, банківські транзакції, податкові зобов'язання, історію взаємодії. Кожне ребро в таких графах має напрямок, вагу (наприклад, суму переказу) і часову мітку, причому між одними й тими ж вузлами можуть існувати множинні зв'язки. Це дозволяє досліджувати динаміку взаємодій, аналізувати часові шаблони, виявляти піки активності, будувати агрегати за періодами («ковзне вікно») та виявляти аномалії у часовому контексті.

Зі збільшенням складності графу – зростає як навантаження на обчислювальні ресурси, так і глибина доступної аналітики. Саме складні графи з напрямками, вагами та часом надають найбільшу цінність у кримінальному аналізі, але водночас вимагають гнучких інструментів і формалізованих методик.

У цій статті наводяться деякі початкові складності, які виникають при аналізі графів без спеціального програмного

забезпечення. Їх вирішення та автоматизація може стати початком для застосування більш складніших методів або розробки власних аналітичних модулів.

Проблема побудови графа з «готових» даних. Наявність структурованих масивів, таких як журнали подій чи транзакцій, не означає, що вони готові до відображення у вигляді схеми зв'язків. Перетворення таких даних потребує фільтрації, агрегування й очищення. Очікується, що результат роботи аналітика – це не візуальна копія наявних даних, а саме візуальне узагальнення, досягнуте в результаті опрацювання даних в контексті розслідування. Таким чином, може існувати хибне уявлення про тотожність вилученим даним до аналітичного результату.

Проблема абсолютних метрик. Оцінювання вузлів через звичні метрики (кількість зв'язків, суму транзакцій) не враховує індивідуальний контекст. Фільтрація вузлів за абсолютними вагами може призвести до втрати інформації про менш активні об'єкти схеми. Пропонується вводити оцінки близькості між об'єктами, які будуть враховувати особливості кожного, наприклад – формуванням кластерів близькості серед сусідів або застосування алгоритмів масштабування «скейлерів», нормалізації даних, тощо.

Проблема шумових вузлів. У графах часто з'являються технічні або сервісні об'єкти (сервісні номери, рекламні облікові записи, групи типових одержувачів коштів, тощо). Такі вузли мають високу активність, але не несуть цінності для розслідування. Вони формують штучні зв'язки, які можуть спотворити аналіз схеми або вказувати на хибно позитивні зв'язки між учасниками провадження.

Проблема фіксації цільових вузлів. На відміну від «шумових» вузлів, на схемах зв'язків може бути втрачена важлива інформація щодо об'єктів, які становлять інтерес для розслідування, якщо інтенсивність їх участі замала, хоча сам факт їх участі вже є важливим.

Проблема обмеженої видимості. У більшості випадків граф будується лише навколо об'єктів, які викликають інтерес (наприклад, щодо яких прийнято рішення про виїмку). При цьому решта мережі лишається невідомою, і базовий граф не

відображає реальні зв'язки та множину учасників. Через відсутність повноти графу звичайні метрики завищуються, що призводить до спотвореної інтерпретації аналізу графу та неможливості їх використання (наприклад модуль Social Network Analysis IBM i2 Analyst Notebook).

Проблема редагування та доповнення. У графах, які були очищені від слабких зв'язків, нові дані часто не мають можливості інтеграції. Для подолання цього доцільно зберігати первинні схеми та формувати окремі аналітичні зрізи під час роботи з графом.

Проблема візуального перевантаження. Аналіз та узагальнення схем отриманих з великих наборів інформації створює обов'язковість компромісу між втратою інформації та здатністю графа бути інформативним та зрозумілим. Доцільним є перехід від друкованих примірників до використання у роботі інтерактивних схем, з можливістю перегляду спрощених та деталізованих варіантів інтерпретації, використання тривимірних схем для відображення графів з великою кількістю об'єктів чи кластерів.

Сучасні розслідування дедалі частіше базуються на аналізі графових структур – від простих соціальних зв'язків до складних транзакцій з часовими ознаками. Проте більшість доступних інструментів залишаються занадто універсальними або негнучкими, що обмежує їх ефективність у реальних криміналістичних сценаріях або призводить до повторюваної втрати часу на адаптацію.

У цьому контексті особливо актуальною є розробка спеціалізованих рішень у межах внутрішньої інфраструктури в залежності від потреб підрозділу або типових напрямків розслідування. Власні інструменти дослідження графів дозволяють автоматизувати типові аналітичні дії, зменшити залежність від вартісних ліцензій, а також використовувати сучасні підходи – від машинного навчання до інтеграції з зовнішніми джерелами.

Пазуха Андрій Павлович,
начальник управління кримінального
аналізу ГУНП в Тернопільській області

ВИКОРИСТАННЯ В КРИМІНАЛЬНОМУ АНАЛІЗІ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ, ЗОКРЕМА ШТУЧНОГО ІНТЕЛЕКТУ

В реаліях сьогодення наша держава зіштовхнулася із новими викликами та загрозами, які суттєво вплинули на усі сфери нашого життя. Передусім, для України та усього світу серед таких викликів та глобальних загроз XXI століття безпрецедентним та шокуючим стала воєнна агресія РФ і повномасштабне вторгнення російських військ на територію нашої держави 24 лютого 2022 року. У зв'язку з цими подіями розслідування військових злочинів передбачає дослідження значного обсягу подій, збирання великого масиву доказової інформації, допиту величезної кількості свідків та потерпілих, залучення експертів та проведення судових експертиз, тобто застосування спеціальних знань та засобів сучасної криміналістики [1, с. 582].

Сучасні штучні нейронні мережі (ШІ) складаються з великої кількості простих процесорних елементів з деякою кількістю локальної пам'яті (нейронів), об'єднаних за допомогою дискретних або неперервних комунікаційних каналів. Задачі, що вони розв'язують, підлягають декомпозиції на множину локальних завдань, кожне з яких може бути розв'язане за допомогою окремого нейрону шляхом реалізації певного алгоритму обробки локальних даних. Вірогідно, що у сучасних умовах для кримінального аналізу штучний інтелект та інноваційні технології стають важливими факторами для ефективної протидії кримінальним правопорушенням та боротьби з організованою злочинністю [3, с. 56–66].

На законодавчому рівні під ШІ вважається організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень,

алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [2].

В рамках кримінального аналізу ШІ використовується для здійснення пошуку, збору та аналізу даних, виявлення кримінальних правопорушників у режимі реального часу та ідентифікації потенційних жертв злочинів.

За допомогою технологій ШІ можуть створюватися обґрунтовані прогнози щодо темпоральних, територіальних і якісних показників злочинності. Ці прогнози покликані сприяти працівниками кримінального аналізу в оптимізації використання наявних ресурсів та виконання поліцейських функцій. Крім того, ШІ активно використовується під час створення автоматизованих систем, баз даних, для розроблення алгоритмів пошуку кримінальних правопорушників «за гарячими слідами», виявлення потенційних жертв кримінальних правопорушень та в багатьох інших напрямах у роботі кримінального аналізу [4, с. 99–100].

Однією з передових технологій, яка почала використовуватись в діяльності кримінального аналізу і зарекомендувала себе з позитивного боку у сфері забезпечення публічної безпеки та порядку, протидії злочинності та розшуку осіб, причетних до кримінальних правопорушень є система відеоспостереження з можливістю розпізнання обличчя на основі штучного інтелекту. За останні роки в Україні успішно встановлено велику кількість камер відеоспостереження з можливістю розпізнання обличчя, що допомагають у виявлені та запобіганню кримінальних правопорушень. Зокрема, виявлення розшукуваних злочинців та підозрілих предметів, моніторинг публічних місць, відстеження дорожньої ситуації – усе це можуть виконувати розумні камери відеоспостереження на основі штучного інтелекту. Велика кількість камер відеоспостереження дає змогу цілодобово стежити за публічним порядком та здійснювати аналітичну розвідку осіб, які підозрюються в протиправній діяльності.

Значну користь у діяльності кримінального аналізу приносить технологія розпізнавання обличь на основі штучного інтелекту, розроблена американською компанією Clearview AI. Алгоритм цього програмного забезпечення дозволяє співставляти світлину особи з фотографіями бази даних, яка налічує понад 20 мільярдів зображень, що розміщені у мережі

Інтернет, зокрема в соціальних мережах. Clearview AI має 3100 активних користувачів у щонайменше 600 правоохоронних органах. Слід зауважити, що Департаменту кримінального аналізу Національної поліції України, у перші тижні широкомасштабної збройної агресії та підрозділам кримінального аналізу в областях надано доступи до спеціалізованих аналітичних та пошукових програмних продуктів, зокрема Artellens Big data people (пошук сторінок в соціальних мережах, у тому числі видалених, аналіз діяльності користувача сторінки та його зв'язків, пошук користувача за ПІБ, фото, номером телефону), YouControl та інші. Отже, в ході експлуатації програмних продуктів «Clearview AI» та «Big data people Artellens» відслідковується ефективність їх використання. Швидко та з великою долею вірогідності працівники підрозділів кримінального аналізу встановлюють фотозображеннями осіб, причетних до протиправних дій, а також військовослужбовців армії росії та учасників незаконних збройних формувань, а також сторінки в соціальних мережах тих користувачів, які мають відношення до збройної агресії по відношенню до України [5].

Тому застосування штучного інтелекту у підвищенні ефективності правоохоронної діяльності в Україні має важливе значення і великі перспективи. Більше того, його роль у майбутньому буде лише зростати. Проте є і значні проблеми, які необхідно вирішувати нагально. Найбільш значною проблемою є відсутність нормативно-правового регулювання застосування штучного інтелекту в Україні, і зокрема у правоохоронній діяльності. Тому важливе значення має прийняття нормативно-правових актів, які регламентують використання штучного інтелекту в правоохоронній діяльності. Це є непростим завданням, зважаючи на відсутність прийнятих законів в цій галузі навіть у інших країнах. Попри всі позитивні можливості й потенціал, останнім часом технологіями штучного інтелекту дедалі частіше послуговуються правопорушники, винаходячи нові способи злочинної діяльності з використанням цифрових технологій і продукуючи в такий спосіб зростання рівня злочинності. До того ж криміногенні чинники штучного інтелекту спричиняють нові загрози й нові виклики охоронюваним законом інтересам як окремих громадян, так і держави й суспільства загалом, потребуючи адекватних засобів

протидії таким кримінально-правовим і криміналістичним засобам. Слід зауважити, що штучний інтелект неможливо убезпечити від помилок і впливу зовнішніх чинників. Не можна недооцінювати роль та значення сучасних розробок штучного інтелекту та передових цифрових технологій, які впроваджуються у зарубіжних країнах з метою профілактики та боротьби зі злочинністю.

Актуальною у напрямі використання в кримінальному аналізі інноваційних технологій, зокрема концепції штучного інтелекту вбачається ініціація проведення кримінологічних досліджень у довгостроковій перспективі щодо особливостей використання ШІ у кримінальному аналізі. Необхідність нового за змістом і формою кримінального аналізу соціальних процесів постає сьогодні у зв'язку з тими трансформаціями, які останнім часом відбулися в соціальній дійсності.

Список використаних джерел

1. Shevchuk V. Criminalistic means, methods and technologies of combating crimes in the field of national security in the context of european integration. Legal support of European integration: general legal and sectoral aspect: Scientific monograph. Riga, Latvia: Baltija Publishing, 2024. 712 p. Pp. 582–604.

2. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https:// www.kmu.gov.ua/npas/pro-shvalennyakoncepciyi-rozvitku-shtuchnogo-intelektuv-ukrayini-s21220.

3. Косілова О.І. Солодовнікова Х.К. Права і свободи людини і громадянина v.s. штучний інтелект: проблемні аспекти. Інформація і право. № 4(35)/2020. С. 56–66.

4. Юртаєва К. В. Використання технологій штучного інтелекту в реалізації стратегій «predictive policing»: можливості, проблеми та перспективи для України // Використання технологій штучного інтелекту у протидії злочинності: матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 99–104.

5. Ryan Mac, Kashmir Hill. Clearview AI settles suit and agrees to limit sales of facial recognition database. NY Times. May 9, 2022. URL: https://www.nytimes.com/2022/05/09/ technology/clearview-ai-suit.html/

Панченко Євгеній Вікторович,
т.в.о. першого заступника начальника Департаменту міжнародного поліцейського співробітництва Національної поліції України, старший науковий співробітник аналітичного відділу «Центр кримінальної аналітики» Національної академії внутрішніх справ

РОЛЬ ДЕПАРТАМЕНТУ МІЖНАРОДНОГО ПОЛІЦЕЙСЬКОГО СПІВРОБІТНИЦТВА В РОЗВИТКУ КРИМІНАЛЬНОЇ АНАЛІТИКИ В УКРАЇНІ: ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ СИСТЕМИ NEXUS

Міжнародне поліцейське співробітництво є однією з ключових складових сучасної правоохоронної діяльності. У добу глобалізації, швидкого розвитку цифрових технологій та зростання масштабів транснаціональної злочинності ефективність боротьби зі злочинами залежить не лише від роботи на національному рівні, а й від налагоджених каналів міжнародного обміну інформацією. В умовах постійного зростання кількості транскордонних правопорушень та появи нових форм злочинної діяльності, переважно у сферах кіберзлочинів, відмиванні доходів отриманих злочинним шляхом, контрабанді наркотичних речовин та зброї, своєчасне отримання та обробка даних з-за кордону стають критично важливими для правоохоронних органів України.

Департамент міжнародного поліцейського співробітництва Національної поліції України (далі – ДМПС НП України) виконує функції Національного центрального бюро (НЦБ) Інтерполу, забезпечуючи зв’язок України з 196 державами-членами та низкою міжнародних організацій. Діяльність Департаменту охоплює забезпечення міжнародного розшуку осіб та об’єктів, координацію оперативних та слідчих заходів у спільних міжнародних операціях, обмін аналітичною та оперативною інформацією, а також впровадження сучасних інформаційних технологій у повсякденну роботу. У сфері кримінальної аналітики ДМПС НП України виконує одразу кілька важливих завдань: від збору та систематизації даних, отриманих від іноземних партнерів, до їх інтеграції в національні бази та подальшої аналітичної обробки, де активно

взаємодії з іншими департаментами та підрозділами Національної поліції України, зокрема Департаментом кримінального аналізу Національної поліції України.

Важливою частиною міжнародної співпраці ДМПС НП України є участь у глобальних ініціативах Інтерполу, таких як i-CORE, i-Force, комітети та робочі групи інших проектів під егідою Генерального секретаріату Інтерполу, спрямовані на створення єдиних стандартів обміну даними, розвиток біометричних технологій і забезпечення взаємодії між національними поліцейськими структурами країн-членів Інтерполу. Наприклад, у рамках i-CORE розглядаються питання вдосконалення інструментів ідентифікації осіб, підвищення оперативності комунікації та інтеграції нових технологій у практичну роботу правоохоронців.

Одним із ключових елементів подальшої цифрової трансформації ДМПС НП України є впровадження системи NEXUS – нової платформи обміну повідомленнями Інтерполу, яка приходить на зміну традиційній електронній пошті I-24/7. На відміну від попередніх рішень, NEXUS надає можливість не лише передавати повідомлення, а й структурувати їх за категоріями (поліцейські запити, автоматичні сповіщення, інші повідомлення), встановлювати рівні пріоритетності, відстежувати статуси запитів у режимі реального часу та об’єднувати пов’язані запити в єдині справи. Впровадження та подальше використання Уніфікованої інформаційної моделі Інтерполу (UIM) усуне потенційні двозначності при інтерпретації даних, зокрема у форматах дат чи написанні імен, що особливо важливо при міжнародному обміні [1, ст. 1].

Платформа підтримує інтеграцію з національними системами управління справами (Case management system) через REST API. Для України передбачено синхронізацію з внутрішніми системами документообігу та обміну інформацією. Це дозволить автоматично імпортувати об’єкти (PERSONS – особи, AUTO – автотранспорт, DOCUMENTS – документи тощо) до відповідних національних баз та банків даних, що функціонують в системах Національної поліції України та Міністерства внутрішніх справ України, зберігаючи зв’язок між отриманими даними та оригінальними документами. Усі вхідні повідомлення з NEXUS автоматично потраплятимуть до спеціальної папки категорії із можливістю швидкого створення

резолюцій, реєстрації документів та подальшої їх обробки, що передбачено наявним функціоналом електронного документообігу системи Національної поліції України. Передбачено також функцію автоматичної відповіді у випадках помилкового надсилання повідомлення, вибір типу доставки (NEXUS чи email), оновлення довідників адресатів і відображення статусів повідомлень кольоровими маркерами.

Інтеграція NEXUS здатна істотно змінити роботу кримінальних аналітиків. Автоматизація процесів скорочує час обробки запитів і зменшує дублювання, а структурований імпорт даних підвищує точність аналітичних висновків. З'являється можливість оперативно формувати комплексний огляд усіх пов'язаних запитів у конкретній справі, що особливо важливо для розслідувань із великою кількістю міжнародних запитів, а також великими об'ємами обмінюваної інформації. Для аналітиків це означає більш ефективне виявлення зв'язків між особами, транспортними засобами, документами та подіями, а для оперативних підрозділів швидше ухвалення рішень на основі перевірених даних.

Прикладом потенційної користі NEXUS може бути міжнародне розслідування кіберзлочину, коли дані про IP-адреси, акаунти в соцмережах та фінансові транзакції надходять із різних країн у різний час. Завдяки автоматичному об'єднанню таких повідомлень у межах однієї справи, система дозволяє слідчому або аналітику бачити повну картину в реальному часі та швидко реагувати на нові обставини [2].

Загалом, міжнародне співробітництво в кримінальній аналітиці, описане в працях Н.М. Ахтирської, В.В. Зуєва, Д.І. Овсянюка, І.А. Федчака та підтверджує, що інформаційна взаємодія між державами є не лише допоміжним елементом, а фундаментальною умовою ефективної протидії злочинності. Такі дослідження підкреслюють важливість чіткого правового регулювання, стандартизації форматів даних, розвитку технологічної сумісності між системами різних країн та забезпечення кібербезпеки в процесі обміну [3, ст. 17]; [4, ст. 14]; [5, ст. 99]; [6, ст. 126].

Отже, впровадження NEXUS у роботу ДМПС НП України допоможе модернізувати технічну інфраструктуру, забезпечить створення нової моделі міжнародної поліцейської співпраці, у якій обмін даними, аналітична обробка та оперативна реакція

інтегруються в єдину екосистему. Такий підхід, у поєднанні з традиційними інструментами кримінального аналізу, підвищує здатність Національної поліції України ефективно реагувати на сучасні виклики та зміцнює позиції країни в міжнародній системі безпеки.

Список використаних джерел

1. Nyman Gibson Miralis, Digital technology and dissemination at the heart of INTERPOL's 2023 annual report, January 23 2025.

2. Making international police messaging more effective and accurate. URL: https://www.interpol.int/en/How-we-work/I-CORE-our-vision-for-change/NEXUS.

3. Ахтирська Н. М., Міжнародне співробітництво під час кримінального провадження: теоретичні та практичні аспекти, Київ: Логос, 2019.

4. Зуєв В. В. та ін., Міжнародне співробітництво у кримінальному провадженні, Одеса: НУ «ОЮА», 2022.

5. Ovsianiuk D. Intelligence cycle as the basis of analytical activity in combating drug-related crime. Law Journal of the National Academy of Internal Affairs. 2024. Vol. 14, no. 2. P. 95–104.

6. Федчак І. А., Основи кримінального аналізу, Львів: ЛДУВС, 2021.

Петров Вадим Амінович,
заступник начальника 1-го управління (аналітичного) – начальник 1-го відділу (кримінального аналізу) Департаменту кримінального аналізу Національної поліції України

МЕДІААНАЛІЗ. СУЧАСНІ ПІДХОДИ ТА МЕТОДИ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ

У світі, де більшість процесів – від особистого спілкування до державного управління – цифровізовано, саме інформація стає головним ресурсом, інструментом впливу та об'єктом боротьби.

В умовах, коли швидкість обміну даними, доступ до знань і вміння розрізняти правду від брехні мають вирішальне значення. Інформація стала важливішою за фізичну силу. Водночас вона перетворилася на об'єкт атак: її викривляють,

спотворюють, використовують для маніпуляцій. Сьогодні йде боротьба не лише за території чи ресурси – точиться боротьба за свідомість людини.

Аналіз міждисциплінарних досліджень (у сферах кібербезпеки, соціальної психології, інформаційної безпеки та медіаграмотності) свідчить, що маніпуляції – одна з найнебезпечніших і водночас найпоширеніших форм цифрових загроз. Їхня суть полягає у цілеспрямованому викривленні інформації з метою впливу на думки, емоції та поведінку людей.

Оскільки близько 80–90 % інформації людина сприймає візуально, маніпулятори активно використовують зображення, відео, інфографіку. Їхня мета – створити видовищний і переконливий продукт, що пробуджує сильні емоції: страх, гнів, розпач, тривогу. Це дозволяє їм формувати потрібну громадську думку або нав'язувати певні дії.

Сьогодні найпоширенішими каналами поширення фейків є новинні сайти, соціальні мережі, блоги та електронні розсилки. Вони можуть бути спрямовані як на конкретні країни, так і на міжнародну аудиторію.

Найтиповіші форми інформаційних маніпуляцій включають:

– медіаманіпуляції: редагування фото/відео, зміна контексту, створення фейкового контенту;

– новинні маніпуляції: викривлення заголовків, подання думки як факту, замовчування деталей;

– фейкові експертизи: цитати псевдоекспертів, перекручування заяв, маніпулятивні аналітичні довідки;

– інформаційні фейки: вигадані повідомлення, посилання на неіснуючі джерела;

– маніпуляції дослідженнями: використання слабких методик, викривлені інтерпретації результатів.

Все це створює ілюзію достовірності й водночас підриває довіру до справжніх джерел.

Для виявлення джерел дезінформації та фейкових вкидів використовують інструменти OSINT (Open Source Intelligence) – розвідки за відкритими джерелами [1, с. 169]. Це підхід, за якого дані збираються не зі спецслужб чи закритих баз, а з публічно доступних джерел: вебсайтів, реєстрів, соцмереж, новин, відео тощо.

У Департаменті кримінального аналізу Національної поліції України активно застосовуються такі напрями OSINT:

– медійна розвідка – аналіз новин (державних та іноземних);

– інтернет-розвідка – перевірка вебсайтів, форумів, блогів;

– SOCMINT – моніторинг соцмереж, публікацій, коментарів;

– GeoOSINT – визначення місця подій за фото, відео, супутниковими знімками;

– Документарна розвідка – пошук і аналіз інформації в публічних базах, реєстрах, судових документах.

OSINT дозволяє розпізнавати джерела фейків, верифікувати факти, відстежувати поширення інформаційних атак та збирати докази для подальших дій.

Сьогодні інформація – це не просто потік новин. Це зброя, яку активно використовують для послаблення суспільства, деморалізації населення, дестабілізації держав. Через фейки, маніпуляції, «експертні» думки без джерел або патріотичні гасла, що сіють паніку, нас змушують сумніватися у власній державі, у собі, у правді.

Протидіяти цьому можна лише комплексно:

– розвиваючи критичне мислення;
– використовуючи OSINT для перевірки фактів;
– дотримуючись правил кібергігієни;
– підвищуючи інформаційну обізнаність.

Лише поєднання технологічних інструментів і людського усвідомлення може стати ефективною відповіддю на загрози інформаційного поля.

Усе це – не лише про особистий захист. Це про стійкість суспільства в умовах гібридної війни. А значить – і про перемогу.

Список використаних джерел

1. ОДУВС ДНДІ МВС Реалізація філософії «Intelligence-LED Policing» в системі кримінального аналізу Національної поліції України, 2024.

Погорецький Микола Миколайович
начальник наукової лабораторії
науково-організаційного центру
Національної академії Служби безпеки
України, кандидат юридичних наук,
старший дослідник

ТАЄМНЕ СПОСТЕРЕЖЕННЯ В ДЕМОКРАТИЧНОМУ СУСПІЛЬСТВІ: БАЛАНС МІЖ БЕЗПЕКОЮ І ПРАВАМИ ЛЮДИНИ

Негласні розслідування є важливим інструментом забезпечення безпеки, проте їх застосування в Україні супроводжується серйозними проблемами. Серед основних – формальний характер судового контролю, слабкий прокурорський нагляд, відсутність незалежного моніторингу та чітких стандартів щодо новітніх технологій (штучного інтелекту, біометрії тощо). Це створює ризики зловживань і порушень прав людини, зокрема права на приватність. На відміну від багатьох країн Європи, в Україні також відсутній механізм компенсації за незаконне застосування негласних заходів. Ситуація потребує негайного вдосконалення законодавства, посилення контролю та запровадження незалежного нагляду відповідно до міжнародних стандартів.

Термін «негласне розслідування» злочинів є поширеним серед зарубіжних та вітчизняних фахівців. В кожній із країн, у тому числі й в Україні, цей термін має свою історію становлення та розвитку і як наслідок – свій зміст. Нерідко поряд з терміном «негласне розслідування» зарубіжними фахівцями вживаються як синоніми також і такі терміни як «конфіденційне розслідування», «таємне розслідування», «розслідування під прикриттям» тощо.

Розвиток інформаційних технологій сприяв значному розширенню можливостей негласного розслідування. У 1978 році в США було прийнято Закон про зовнішню розвідку (FISA) [1], який встановив правові рамки для перехоплення електронних комунікацій у розвідувальних цілях. У Великобританії у 2000 році набув чинності Закон про регулювання слідчих повноважень (RIPA) [2], який визначив

порядок використання негласного спостереження правоохоронними органами. Наприкінці XX – на початку XXI століття цифрові технології відкрили нові можливості для негласних розслідувань, включаючи кіберспостереження, аналіз великих даних та використання штучного інтелекту.

У правоохоронній сфері негласне розслідування включає приховане спостереження та використання агентів під прикриттям для збору доказів про злочинну діяльність. Згідно з документом «Практичні кодекси таємного спостереження та таємних джерел розвідувальної інформації» («Covert Surveillance and Covert Human Intelligence Sources Codes of Practice») [3], такі методи є важливими для захисту громадськості від тероризму та злочинності, але потребують ретельного нагляду та регулярної переоцінки, щоб забезпечити їх обґрунтованість та законність.

Негласне розслідування – це приховане збирання інформації правоохоронними органами про осіб чи події, що мають значення для кримінального провадження або національної безпеки. Воно здійснюється без відома об'єкта, з використанням спеціальних методів, технічних засобів і оперативно-розшукових заходів. Наприклад, це може бути робота таємного агента або встановлення прихованого аудіо- та відеоспостереження. Через втручання в приватне життя, таке розслідування проводиться лише за наявності законних підстав і з дозволу уповноважених органів, що забезпечує захист прав людини.

Ці методи тісно пов'язані з розвідувальною діяльністю, оскільки обидві форми роботи спрямовані на отримання прихованої інформації. Методи розвідки включають технічну розвідку (супутниковий моніторинг, кіберрозвідка), сигнальну розвідку (SIGINT), що охоплює перехоплення електронних комунікацій, гуманітарну розвідку (HUMINT) – вербування агентів, а також кіберрозвідку (CYBINT), яка виявляє кіберзагрози та атакує системи супротивника. Наприклад, застосування дронів для виявлення терористичних баз у зонах бойових дій поєднує елементи як технічної розвідки, так і негласного спостереження, ілюструючи ефективність комплексного підходу до забезпечення національної безпеки [4].

Застосування негласних методів розслідування породжує серйозні етичні та правові виклики, пов'язані з втручанням у приватне життя. У західних країнах такі заходи суворо регламентовані законом. Наприклад, у Німеччині заборонено вилучати документи, що стосуються правової чи медичної допомоги, крім випадків їх використання для вчинення злочину. У Швейцарії особиста кореспонденція підозрюваного може бути недоторканною, якщо інтереси захисту переважають інтереси слідства. Використання таких матеріалів у суді можливе лише за умови їх законного отримання. Водночас навіть у таких системах трапляються зловживання, що свідчить про важливість ефективного контролю за застосуванням негласних методів.

Програма PRISM, розкрита Едвардом Сноуденом у 2013 році, показала, що Агентство національної безпеки (АНБ) США масово збирало дані громадян без їхнього відома. Це включало доступ до серверів таких технологічних гігантів, як Google, Apple та Facebook, що дозволяло АНБ відстежувати електронні листи, чати та інші комунікації користувачів. Ці дії викликали значний суспільний резонанс та дискусії щодо приватності та державного нагляду [5].

У січні 2025 року News Group Newspapers, видавець The Sun, визнав незаконні дії та приніс «повне та беззастережне вибачення» принцу Гаррі за серйозне втручання в його приватне життя в період з 1996 по 2011 роки. Це стало результатом п'ятирічної судової боротьби, під час якої принц Гаррі наполягав на відповідальності за незаконне збирання інформації. Вибачення також стосувалося втручання в приватне життя його покійної матері, принцеси Діани. Цей випадок став важливим прецедентом у боротьбі за відповідальність медіа за незаконні методи збору інформації [6].

Ці події підкреслюють серйозність проблеми незаконного використання негласного спостереження та необхідність суворого контролю за діяльністю медіа та правоохоронних органів у цій сфері.

У сучасній Європі питання правового контролю за негласними розслідуваннями набуває особливої актуальності. Це пов'язано з необхідністю забезпечення балансу між

ефективністю правоохоронної діяльності та захистом фундаментальних прав людини, зокрема права на приватність.

Європейські стандарти у цій сфері акцентують увагу на процесуальних гарантіях під час проведення негласних спостережень та захисту даних. Технологічний прогрес останніх років ставить нові виклики у забезпеченні права на повагу до приватного життя та вимагає, щоб будь-яка обробка персональних даних відповідала встановленим стандартам. Зокрема, Рада Європи наголошує на необхідності чіткого регулювання негласного спостереження, забезпечення прозорості процедур та наявності ефективних механізмів контролю за такими діями [7].

ЄСПЛ послідовно наголошує, що втручання у приватне життя під час негласного розслідування має бути законним, обґрунтованим і пропорційним. Європейські стандарти вимагають судового контролю за такими діями та регулярного моніторингу їх застосування для запобігання зловживанням і порушенням прав людини [8].

Отже, негласні розслідування є важливим інструментом забезпечення національної безпеки, боротьби з тероризмом, корупцією та злочинністю. Водночас їх застосування без належного контролю може призвести до порушень прав людини, зловживань владою та послаблення демократичних інститутів. Ефективність негласних розслідувань залежить від дотримання принципів законності, необхідності, пропорційності та контролю.

Законодавство демократичних держав передбачає механізми нагляду, проте навіть у США, Великобританії та ЄС зберігаються ризики зловживань, що підтверджують міжнародні скандали, пов’язані з масовим стеженням.

Забезпечення демократичного контролю, вдосконалення правового регулювання та впровадження міжнародних стандартів, зокрема практики ЄСПЛ та Ради Європи, сприятимуть зміцненню правової держави, підвищенню довіри громадян та мінімізації ризиків зловживань.

Список використаних джерел

1. Foreign Intelligence Surveillance Act 1978 (FISA) // U.S. Congress. Washington, D.C.: U.S. Government, 1978. Available at: https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter36.

2. Regulation of Investigatory Powers Act 2000 (RIPA) // UK Legislation. London: HM Government, 2000. Available at: https://www.legislation.gov.uk/ukpga/2000/23/contents.

3. Covert Human Intelligence Sources Code of Practice 2022. GOV.UK, 13 Dec. 2022, https://www.gov.uk/government/publications/covert-human-intelligence-sources-code-of-practice-2022.

4. National Security Agency. Signals Intelligence (SIGINT) Overview. Fort Meade: NSA, 2021. Available at: https://www.nsa.gov/Signals-Intelligence/Overview/.

5. MacAskill, Ewen; Poitras, Laura; Greenwald, Glenn. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. 7 червня 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

6. Prince Harry says Sun publisher made ‘historic admission’ as he settles case. The Guardian. 22 January 2025. https://www.theguardian.com/uk-news/2025/jan/22/prince-harry-says-sun-publisher-made-historic-admission-as-he-settles-case.

7. Council of Europe Data Protection website. Council of Europe. https://www.coe.int/en/web/data-protection.

8. Князєв С. М. Судовий контроль за здійсненням негласної діяльності: міжнародний досвід. Юридичний журнал Національної академії внутрішніх справ. 2019. № 1 (17). С. 90–97. URL: https://lawjournal.com.ua/uk/article/read/sudovy-kontrol-za-zdiysnennyam-neglasnoyi-diyalnosti-mizhnarodny-dosvid.

Разєнков Євген Валерійович,
начальник управління організаційної роботи Департаменту інформаційно-аналітичної підтримки Національної поліції України

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ ТА СЛІДЧИХ ОРГАНІВ ПІД ЧАС ДОКУМЕНТУВАННЯ І РОЗСЛІДУВАННЯ ЗЛОЧИНІВ

У сучасних умовах протидії злочинності одним із ключових елементів ефективної роботи підрозділів Національної поліції України є інформаційно-аналітичне забезпечення. Завдяки аналітичному супроводу, координації збору, обробки, аналізу та обміну інформацією, кримінальна поліція та слідчі органи швидко отримують достовірні дані для ухвалення управлінських і процесуальних рішень.

Відповідно до статей 25, 26 Закону України «Про Національну поліцію» поліція в межах інформаційно-аналітичної діяльності формує, наповнює, підтримує в актуальному стані та користується реєстрами і базами (банками) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України (далі – ЄІС МВС) [1].

Наповнення ЄІС МВС поліцейськими здійснюється за допомогою інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» (далі – система «ІПНП») відповідно до Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України», затвердженого наказом МВС від 03.08.2017 № 676, зареєстрованим у Міністерстві юстиції України 28 серпня 2017 за № 1059/30927 (далі – Положення) [2].

Відповідно до пункту 2 розділу IV Положення адміністратором системи ІПНП є уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України.

Згідно з пунктом 4 Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України (далі – ДІАП, Департамент), затвердженого наказом Національної поліції України від 31 січня 2020 року № 77 (зі змінами), ДІАП є відповідальним підрозділом за організацію

(здійснення) розроблення, упровадження, супроводження (адміністрування) інформаційних систем.

Так, в умовах прямого й опосередкованого застосування збройної сили російською федерацією проти суверенітету і територіальної цілісності України, що фактично були розпочаті 2014 року в окремих районах Донецької та Луганської областей, а з 24 лютого 2022 року повномасштабного вторгнення на всю територію країни, констатуючи факти захоплень та руйнувань адміністративних будівель територіальних підрозділів Національної поліції України, в тому числі зі знищенням комунікаційного та серверного обладнання, діяльність підрозділів інформаційно-аналітичної підтримки була спрямована, в першу чергу, на збереження комунікаційного обладнання та серверного устаткування, а з ними наявних баз та банків даних, забезпечення безперебійної роботи галузевої інформаційної інфраструктури, інформаційних та аналітичних систем і сервісів, необхідних для підтримання процесів прийняття рішень та комунікації, як в районах проведення бойових дій, так і по території всієї держави.

Злагодженими діями територіальних підрозділів інформаційно-аналітичної підтримки під координацією ДІАП було забезпечено функціонування каналів та засобів зв'язку, дотримано заходів з інформаційної безпеки, вжито заходи з протидії витоку службової інформації та кіберзагрозам.

Не зважаючи на виклики та в умовах масштабної війни, Національною поліцією України вжито заходи не лише зі збереження, а й розвитку ІТ-складової автоматизації та цифровізації службової діяльності, запроваджено нові інноваційні технологічні рішення, розширено міжвідомчу інформаційну взаємодію.

На сьогоднішній день в межах програмно-технічного комплексу системи «ІПНП» щоденно забезпечується функціонування та супроводження 80 інформаційних підсистем в яких накопичено понад 235 млн. об'єктів обліку, щодобово здійснюється близько 3 млн. операцій-дій користувачів, підключено 69 тис. користувачів, у т.ч. 2,5 тис. з 13 інших органів державної влади, якими зроблено більше 4 млн. запитів.

Крім того, ДІАП здійснено реалізацію заходів з міжвідомчої інформаційної взаємодії з наданням доступу працівникам поліції

до 18 сервісів інформаційних ресурсів 10 окремих державних органів: Міністерства оборони України, Державної міграційної служби України, Державної судової адміністрації України, Адміністрації Державної прикордонної служби України, Пенсійного фонду України, Міністерства юстиції України, Державної митної служби України, Державної виконавчої служби України, Моторного (транспортного) страхового бюро України, Головного сервісного центру МВС України.

В розрізі інформаційно-аналітичного забезпечення оперативно-розшукової діяльності та належного документування злочинів, в т.ч. воєнних злочинів та злочинів проти людяності, скоєних російською армією в Україні, ДІАП з початком повномасштабного вторгнення забезпечено модернізацію 18 інформаційних підсистем.

До основних технічних рішень із інформаційно-аналітичного забезпечення діяльності підрозділів кримінальної поліції та слідчих органів під час документування та розслідування злочинів, відносяться:

- інформаційної підсистеми «СЛІД» системи «ІПНП» [3]. Метою створення ІП «СЛІД» є документування злочинів і правопорушень та облік інформації про об’єкти, вилучені під час проведення слідчих (розшукових) дій.

Наповнення ІП «СЛІД» здійснюється підрозділами криміналістичного забезпечення органів досудового розслідування поліції. До зазначеного інформаційного ресурсу унесено більше 400 тис. інформаційних записів про злочини, до яких долучено 640 тис. відомостей про проведені слідчі дії, 440 тис. оглядів місця подій із вилученням більше 550 тис. одиниць слідової інформації (фотозображення слідів рук, слідів підошов взуття, слідів знарядь зламу, слідів структури матеріалу, слідів протекторів шин транспортних засобів, мультимедійна інформація обстановки події, що сталася, інформація про кулі, гільзи і патрони зі слідами зброї, інформація про об’єкти біологічного походження).

Упровадження та супровід зазначеної підсистеми та підтримання її в актуальному стані забезпечило облік інформації про об’єкти, вилучені під час проведення слідчих (розшукових) дій, у єдиному інформаційному просторі з

використанням сучасних інформаційних технологій, комп'ютерного та комунікаційного обладнання, інформаційно-аналітичну підтримку діяльності органів (підрозділів) поліції, спрямовану на розкриття кримінальних правопорушень, автоматизацію процесу встановлення зв'язків між даними, що мають значення для кримінального провадження;

– база даних «Розшук» системи «ІПНП» [4] (далі – БД «Розшук»). БД «Розшук» формується та ведеться засобами системи «ІПНП» із застосуванням її комплексної системи захисту інформації з підтвердженою відповідністю, забезпечуючи наповнення та підтримання в актуальному стані реєстрів та баз (банків) даних, що входять до ЄІС МВС, стосовно осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, ухиляються від відбування покарання або від виконання обов'язків, визначених законом для суб'єктів пробації, зниклих безвісти, зокрема за особливих обставин.

Департаментом реалізовано функціонал з інтеграції відомостей БД «Розшук» в інформаційну підсистему «Єдиний облік» системи «ІПНП» [5], чим надано змогу миттєвого виявлення фактів звернень розшукуваних осіб до органів та підрозділів поліції, або інформаційних повідомлень стосовно них;

З метою внесення інформації про осіб, які причетні до військової агресії (військовослужбовці збройних сил російської федерації, члени незаконних збройних формувань, приватних військових компаній, колаборантів тощо) та події, пов'язані із вчиненням зазначеною категорією осіб на території України кримінальних правопорушень, ДІАП на центральному серверному програмно-технічному комплексі системи «ІПНП» розроблено та впроваджено технічне рішення із наповнення в режимі реального часу банку даних інформацією про зазначених осіб та події, з можливістю її доповнення та перегляду одночасно всіма користувачами системи «ІПНП», яким наданий відповідний доступ, в тому числі підрозділами кримінальної поліції (включаючи працівників підрозділів кримінального аналізу) та слідства як Центрального органу управління поліції, так і територіальних органів. Забезпечено інтеграцію внесеної інформації з наявною в інших підсистемах, зокрема «Єдиний облік», «Кримінальна статистика», «Розшук», «Пізнання» та ін.,

наповнення інформаційної картки відомостями про ймовірне місце знаходження, біометричні (в тому числі із можливістю додавання фото, відеозображень) та антропологічні дані, належність до певного військового формування у відповідний проміжок часу, сторінки у соціальних мережах, родинні зв'язки та інші, пов'язані відомості відносно особи з подальшим якісним та миттєвим виводом інформації, систематизацією та графічним відображенням на карті місцевості, в розрізі різних аналітичних рішень.

Крім того, Національна поліція України виступила ініціатором об'єднання відомостей, що стосуються збройної військової агресії російської федерації, які маються у Служби безпеки України, Офісу Генерального прокурора, Державного бюро розслідувань, Збройних сил України, Головного управління розвідки Міністерства оборони України, Державної прикордонної служби України, Служби зовнішньої розвідки України на базі системи «ІПНП», що надає змогу працівникам підрозділів кримінальної поліції в режимі реального часу при документуванні злочинів отримувати наявні відомості та мати комунікацію із зазначеними правоохоронними відомствами.

Підсумовуючи, діяльність Департаменту та територіальних управлінь інформаційно-аналітичної підтримки, спрямована на створення технічних рішень, автоматизацію та цифровізацію службових процесів в діяльності працівників підрозділів кримінального блоку, кримінального аналізу, слідчих органів та органів дізнання, які, особливо в умовах дефіциту часу, застосовуючи високий рівень теоретичної підготовки, практичного досвіду та спеціалізованого програмного забезпечення, на високому рівні виконують функції із профілактики та розкриття злочинів і притягнення до відповідальності винних осіб.

Список використаних джерел

1. Закон України «Про Національну поліцію». 2015. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

2. Наказ МВС України від 03.08.2017 № 686 «Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України». 2017. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

3. Наказ МВС України від 16.03.2020 № 257 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «СЛІД» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України». 2020. URL: https://zakon.rada.gov.ua/laws/show/z0319-20#Text.

4. Наказ МВС України від 28.06.2023 № 534 «Про затвердження Інструкції з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України». 2023. URL: https://zakon.rada.gov.ua/laws/show/z1486-23#Text.

5. Наказ МВС України від 08.02.2019 № 100 «Про затвердження Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події». 2019. URL: https://zakon.rada.gov.ua/laws/show/z0223-19#Text.

Рогатюк Ігор Володимирович,
професор кафедри кримінального процесу та криміналістики ННГІ Національної академії Служби безпеки України, доктор юридичних наук, професор

АНАЛІЗ СТАНУ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЯК ОСНОВА ПРОТИДІЇ ЗЛОЧИННОСТІ

Для того, щоб мати уяву куди рухатися потрібно мати дорожню мапу… На шляху боротьби зі злочинністю таким дороговказом є кримінальний аналіз. Як свідчать численні дослідження цього поняття та сутності, вказаний аналіз є складною категорією [1]. Позаяк складається із двох визначальних термінів: «кримінальний» та «аналіз». Якщо із загально-науковою категорією «аналіз» все більш-менш зрозуміло, то термін «кримінальний» є вузькофаховим або ж спеціальним і відповідно визначає предмет дослідження.

Такий предмет випливає зі ст. 11 Кримінального Кодексу України якою визначене поняття кримінального правопорушення. Отже, Кримінальне правопорушення є передбачене цим Кодексом суспільно небезпечне винне діяння (дія або бездіяльність), вчинене суб'єктом кримінального

правопорушення. Такі правопорушення, наразі, нараховуються у 447 статтях Кримінального Кодексу України. Таким чином об'єкт кримінального аналізу це відповідний злочин чи кримінальний проступок передбачений КК [2].

Безумовно об'єкт кримінального аналізу має свої межі. У нашому випадку йдеться про територію України або ж відповідний регіон чи місцевість на теренах якої вчиняються кримінальні правопорушення. Задля здійснення аналітичної роботи у цьому напрямі фахівцю необхідні відповідні дані, тобто цифри вчинених і зареєстрованих кримінальних правопорушень. Офіційні дані щодо кількості та характеру кримінально-караних вчинків сьогодні містяться у базі Єдиного реєстру досудових розслідувань (ЄРДР). Володільцем інформації, що обробляється у Реєстрі, є Офіс Генерального прокурора. Як зазначено у Положенні про Реєстр [3] він утворений та ведеться відповідно до вимог Кримінального процесуального кодексу України [4] з метою забезпечення:

– реєстрації кримінальних правопорушень (проваджень) та осіб, які їх учинили, обліку прийнятих під час досудового розслідування рішень та результатів судового провадження;

– оперативного контролю за додержанням законів під час проведення досудового розслідування;

– формування звітності про стан кримінальної протиправності та результати роботи органів досудового розслідування;

– аналізу стану та структури кримінальних правопорушень, вчинених у державі;

– інформаційно-аналітичного забезпечення державних органів, у тому числі правоохоронних та судових відповідно до вимог законодавства;

Отже найбільшою базою офіційних даних про кримінальні правопорушення для аналітика є Єдиний реєстр досудових розслідувань.

Однак, для більш повного розуміння процесів, які відбуваються на тих чи інших напрямах, територіях чи об'єктах де скоюються кримінальні правопорушення, аналітику необхідно ураховувати і оперативні дані, щодо кримінальних правопорушень. Найбільшим інформаційним хабом до якого

надходить така інформація безумовно є служба «102» Нацполіції, її працівники у цілодобовому режим здійснюють екстрені комунікації за телефонним номером екстреної служби 102 та інших технічних засобів електронних комунікацій, обробку та використання отриманої інформації, реєстрацію заяв і повідомлень про правопорушення або події [5].

Водночас третьою складовою для об'єктивної картини, за можливості, аналітику, також треба використовувати розвідувальну інформацію з обмеженим доступом. Почасти вона впливає на попередження та усунення певних негативних наслідків.

Під час здійснення кримінального аналізу треба брати до уваги, вимогу Кримінального процесуального кодексу України, щодо підслідності кримінальних правопорушень. Оскільки, яким би фаховим не був аналітик певного відомства, досконально специфіку правопорушень знає лише той правоохоронний орган який їм протидіє та розслідує.

Досліджуючи вказану тематику варто зауважити, що вище йшлося про здійснення кримінального аналізу в межах нашої країни і у мирний час. А під час дії воєнного стану проведення такого аналізу є дещо проблематичним. Оскільки не можна спрогнозувати воєнні, терористичні чи злочини проти людства, які ворог здійснює проти українців. Хоча теоретично, за умови налагодження агентурних джерел у лавах ворога таке прогнозування цілком можливе.

Отже, аналіз злочинності передбачає не тільки вивчення злочинця і злочинності, а й розроблення заходів щодо їх запобігання злочинам. Як резюмують у своїх працях фахівці – головною метою кримінального аналізу є вдосконалення механізмів запобігання кримінальним правопорушенням, виявлення, документування й розслідування кримінальних правопорушень, а також налагодження механізмів моніторингу криміногенної ситуації, обміну інформацією на регіональному, державному й міжнародному рівнях стосовно тенденцій і ризиків у цій сфері [6].

Проведений нами огляд положень законодавства, підзаконних актів наукових праць та практики дозволяє зробити певні висновки.

Для того, щоб отримати конструктивний кримінальний аналіз, він повинен ґрунтуватися на дослідженні:

1. офіційної статистичної звітності щодо зареєстрованих фактів кримінальних правопорушень, осіб які їх вчиняють, способи вчинення, локалізація, сфери у яких вони скоюються тощо;

2. результати роботи досудового розслідування та судового розгляду;

3. оперативну інформацію, яка надходить до правоохоронних органів за різними каналами комунікації;

4. результати оперативно-розшукової, розвідувальної та контррозвідувальної діяльності;

5. заходи вжиті на протидію і зменшення фактів вчинення кримінальним правопорушенням.

Досліджуючи наведені елементи у своїй сукупності, підрозділи кримінального аналізу закладатимуть міцну основу для протидії злочинності. Так як прийдуть до висновків: де, на яких напрямах потрібно посилити роботу, чи переорієнтуватися, вжити альтернативних заходів для зменшення кількості кримінальних правопорушень і т.д..

За умови проведення якісного та конструктивного кримінального аналізу вбачатиметься за можливе прогнозування злочинних дій та зміни динаміки злочинності на певній території чи у певних сферах життєдіяльності. І відповідно напрацювання контрзаходів з метою зменшення рівня злочинності.

Єдиним питанням, що залишається не висвітленим є кінцеве узагальнення результатів кримінального аналізу. Позаяк кожен правоохоронний орган здійснює кримінальний аналіз відповідно до своєї підслідності зазначеній у ст. 216 КПК України. Звідси питання, чи потрібен єдиний документ у якому будуть узагальнені результати кримінального аналізу усіх правоохоронних органів по всій державі разом та хто це може робити? З урахуванням компетенції щодо координації діяльності правоохоронних органів у сфері протидії злочинності передбачених у ст. 25 Закону «Про прокуратуру» [7], підвідомчості ЄРДР таке узагальнення можливе здійснення Офісом Генерального прокурора [8].

Список використаних джерел

1. Барангулов В.А. Сутність кримінального аналізу // Південноукраїнський правничий часопис, 2023, випуск 4, С. 14–17. URL: http://www.sulj.oduvs.od.ua/archive/2023/4/3.pdf.

2. Кримінальний кодекс України: Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

3. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення: наказ Офісу Генерального прокурора від 30 червня 2020 р. № 298 URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text.

4. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

5. Про затвердження Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України: наказ Міністерства внутрішніх справ від 27 квітня 2020 р. № 357. URL: https://zakon.rada.gov.ua/laws/show/z0443-20#n14.

6. Гончарук О.М., Ісмайлов К.Ю. Кримінальний аналіз у системі правоохоронних органів України: поняття, мета й завдання //Правовий часопис Донбасу, №2 (83) 2023, С. 14–17. URL: http://ljd.dnuvs.ukr.education/index.php/ljd/article/view/56/49.

7. Про прокуратуру: Закон України від 14 жовт. 2014 р. № 1697-VII. URL:https://zakon.rada.gov.ua/laws/show/1697-18#Text.

8. Про затвердження Порядку координації діяльності правоохоронних органів у сфері протидії злочинності: наказ Офісу Генерального прокурора від 8 лютого 2021 р. № 28. URL: https://zakon.rada.gov.ua/laws/show/v0028905-21#Text.

Сарафанюк Михайло Сергійович,
старший інспектор з особливих
доручень відділу аналітичної роботи
управління кримінального аналізу
ГУНП в Миколаївській області

ПІДГОТОВКА АНАЛІТИКІВ

Повноцінний розвиток Української держави, особливо в умовах воєнної агресії, вимагає створення стійкої та ефективної системи національної безпеки. Національна поліція України (НПУ) є ключовою ланкою цього безпекового середовища. Сучасні виклики та загрози у сфері внутрішньої безпеки, а також нові можливості вчинення злочинів, зумовлені різноманітними соціально-економічними чинниками, підвищенням мобільності населення та швидкими технологічними змінами, вимагають від НПУ системних еволюційних змін та інноваційної трансформації діяльності. Фундаментальною базою цих змін є впровадження філософії проактивної правоохоронної діяльності.

Модель поліцейської діяльності, керованої аналітичною розвідкою (Intelligence-Led Policing, ILP), розроблена як відповідь на ці зростаючі проблеми. Вона дозволяє переорієнтувати правоохоронну діяльність з традиційного реагування на запобігання злочинності. Оптимізація аналітичного забезпечення, що реалізується підрозділами кримінального аналізу НПУ, є ключовою для цього переходу. Консультативна місія ЄС в Україні (EUAM) з 2015 року надає підтримку українським правоохоронним органам у впровадженні ILP, що призвело до створення Департаменту кримінального аналізу НПУ у 2017 році та запровадження обов'язкових занять з кримінального аналізу у вищих навчальних закладах МВС з 2020 року [2, с. 110]

Кваліфікований аналітик повинен вміти працювати з будь-яким типом даних, виявляти тенденції та аномалії, а потім чітко їх пояснювати [1, с. 88] Це вимагає критичного мислення, дослідницьких навичок та сильних комунікативних здібностей (письмових та усних). Знання найкращих практик введення даних та використання таких інструментів, як Microsoft Excel, Google Sheets/Forms, розуміння реляційних баз даних (Access, Microsoft SQL) та вміння писати SQL-запити є цінною перевагою.

Географічні інформаційні системи (ГІС) необхідні для аналізу «гарячих точок» злочинності, виявлення закономірностей, прогностичної поліцейської діяльності та оптимізації ресурсів. Корисно знати Esri, Google Earth Pro та QGIS, та інше спеціалізоване програмне забезпечення для картографування та аналізу.

Аналітик повинен мати такі особистісні якості, як об'єктивність, професіоналізм, гнучкість, адаптивність, здатність до навчання, ініціативність, мотивація, організованість, планування, пріоритезація, ситуаційна обізнаність, навички коучингу, наполегливість та готовність представляти висновки. Цілісність, точність, ясність, глибина, широта та релевантність є вирішальними характеристиками для аналітичної роботи. Аналітики повинні бути незалежними від політичних міркувань та здатними ставити під сумнів традиційні переконання [2, с. 110].

Сучасний аналітик є «гібридним професіоналом», що поєднує «м'які» навички (критичне мислення, комунікація, етика, адаптивність) та «жорсткі» технічні навички (наука про дані, ГІС, спеціалізоване програмне забезпечення, OSINT). Це вимагає, щоб програми підготовки аналітиків були високо міждисциплінарними, розвиваючи як передові когнітивні здібності, так і практичну технічну майстерність. Це передбачає необхідність розробки навчальних програм, які інтегрують кримінологію, статистику, комп'ютерні науки та комунікаційні дослідження.

До прикладу, міжнародна асоціація аналітиків правоохоронних структур (IALEIA) та Міжнародна асоціація кримінальних аналітиків (IACA) встановлюють стандарти професійної сертифікації. IALEIA вимагає мінімум 40 годин базового навчання з аналізу кримінальної розвідки для професійної сертифікації. IACA пропонує програму сертифікації, що базується на бальній системі, яка враховує досвід роботи, продемонстровані знання, навички та здібності, академічну роботу, навчання на робочому місці та внесок у розвиток професії [2, с. 111].

Також, базовий польовий навчальний курс ФБР (BFTC) навчає нових спеціальних агентів та аналітиків розвідки разом, зосереджуючись на фундаментальних знаннях, навичках та здібностях, включаючи написання розвідувальних продуктів

ФБР та розвиток навичок брифінгу. Він підкреслює важливість розсудливості, сумлінності, цілісності та співпраці [4, с. 5]. В свою чергу, Інтерпол готує розвідувальні звіти та бере участь у проєктах, таких як INSIGHT та ENACT. Вони пропонують онлайн-курси (IIPCIC) для правоохоронних органів, що охоплюють теми, такі як розслідування онлайн-підробок та піратства, з сертифікатами, схваленими Інтерполом [3, с. 1]. CEPOL (Агентство Європейського Союзу з підготовки правоохоронних органів) надає навчання для правоохоронців, включаючи очні курси та платформу електронного навчання (LEEd), що охоплює такі сфери, як серйозна та організована злочинність, кіберзлочинність та технології правоохоронної діяльності [5, с. 1].

Ефективна підготовка аналітиків є першочерговою для сучасних правоохоронних органів, які переходять від реактивних до проактивних стратегій. Вона вимагає комплексного набору навичок, що поєднують критичне мислення, передову технічну майстерність та міцну етичну основу.

Для подальшого вдосконалення підготовки аналітиків рекомендується:

– **Стандартизація та сертифікація:** Розробити єдиний національний профіль професійної компетентності для кримінальних аналітиків з метою стандартизації освітніх рамок та навчальних програм. Впровадити національну систему сертифікації, яка визнає різноманітний досвід та безперервне навчання, потенційно наслідуючи міжнародні моделі, такі як бальна система IACA [6, с. 1].

– **Модернізація навчальних програм:** Інтегрувати в навчальні програми поглиблені модулі з аналізу великих даних, застосувань штучного інтелекту (наприклад, машинне навчання, глибоке навчання) та спеціалізованих методів розслідування. Акцентувати увагу на практичному досвіді та реальних сценаріях.

– **Етична та правова база:** Посилити навчання з питань захисту даних, законів про конфіденційність та етичних міркувань при зборі та аналізі розвідувальної інформації, особливо щодо чутливої інформації та міжнародних стандартів прав людини [2, с. 145].

– **Міждисциплінарна співпраця:** Сприяти зміцненню партнерських відносин між правоохоронними органами, академічними установами та міжнародними організаціями для обміну найкращими практиками, розвитку спільних досліджень та створення інтегрованих навчальних програм [2, с. 218].

– **Інвестиції в технології та інфраструктуру:** Забезпечити адекватні інвестиції в сучасне аналітичне програмне забезпечення, апаратне забезпечення та безпечні інформаційні системи. Це включає розробку зручних інтерфейсів та забезпечення якості та доступності даних для аналітиків.

– **Просування проактивного мислення:** Постійно підсилювати філософію Intelligence-Led Policing (ILP) на всіх рівнях правоохоронної діяльності, забезпечуючи активне використання аналітичних продуктів для стратегічного планування, оцінки ризиків та запобігання злочинності, а не лише для реактивних відповідей.

– **Екосистема безперервного навчання:** Створити надійну систему безперервного професійного розвитку, пропонуючи багаторівневі навчальні програми, спеціалізовані семінари з нових загроз та можливості для поглибленого академічного навчання.

Список використаних джерел

1. І. А. Федчак, Основи кримінального аналізу: навчальний посібник., Львів: Львівський державний університет внутрішніх справ, 2021. 288 p. Pp.88.

2. Користін О., Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції, К. О.Є, Ред., Київ: ТОВ «Компанія ВАІТЕ», 2024. 444 p. P. 110–218.

3. International IP Crime Investigators College, «Law Enforcement Training Curriculum,» 2025. URL: https://www.iipcic.org/curriculumL-advanced.php.

4. FBI, «BASIC FIELD TRAINING COURSE,» 2025. URL: https://fbijobs.gov/sites/default/files/2025-02/Guide_BFTC.pdf.

5. CEPOL, «Courses,» 2025. URL: https://www.cepol.europa.eu/training-education/courses.

Сергєєв Денис Олександрович,
здобувач ступеня вищої освіти магістра
Національної академії внутрішніх справ
Науковий керівник:
доцент кафедри оперативно-розшукової
діяльності та національної безпеки
Національної академії внутрішніх справ,
кандидат юридичних наук
Веденяпіна М. М.

СПІВПРАЦЯ ПОЛІЦІЇ ТА ПРИВАТНОГО СЕКТОРУ В КРИМІНАЛЬНОМУ АНАЛІЗІ

Сучасна злочинність набуває нових форм, стаючи більш технологічною та складною, що вимагає від правоохоронних органів інноваційних підходів до розкриття та розслідування кримінальних правопорушень. У цьому контексті співпраця поліції з приватним сектором у сфері кримінального аналізу стає ключовим інструментом для ефективної протидії кіберзлочинності, економічним злочинам та транснаціональній злочинності. Тези присвячені аналізу механізмів такої взаємодії, дослідженню сучасних викликів та пропозиціям щодо вдосконалення правових і організаційних засад для підвищення результативності роботи поліції.

У сучасному світі злочинність, зокрема кіберзлочини, відмивання грошей та транснаціональні економічні правопорушення, досягла безпрецедентного рівня складності. Правоохоронні органи часто стикаються з обмеженнями у доступі до сучасних технологій, великих даних та спеціалізованої експертизи. Водночас приватний сектор, включаючи технологічні компанії, фінансові установи та аналітичні агенції, володіє ресурсами, які можуть значно посилити можливості поліції. Актуальність теми зумовлена потребою створення ефективних моделей співпраці, які дозволять оперативно реагувати на нові виклики та підвищувати ефективність розкриття злочинів.

Питання співпраці поліції з приватним сектором привертають увагу дослідників, таких як Дж. Сміт, М. Кларк,

О. Петренко, Л. Сидоренко та інших. Їхні праці висвітлюють окремі аспекти взаємодії, зокрема обмін інформацією чи протидію кіберзлочинності. Проте комплексний підхід до інтеграції ресурсів приватного сектора у кримінальний аналіз, особливо в умовах українського законодавства, залишається недостатньо вивченим. Це створює необхідність глибшого аналізу та розробки практичних рекомендацій.

Аналізуючи сучасні підходи до співпраці поліції та приватного сектора у сфері кримінального аналізу, виявлення ключових проблем та розробка пропозицій щодо вдосконалення правових і організаційних механізмів, сприятиме підвищенню ефективності розкриття та розслідування кримінальних правопорушень, що є важливим у контексті сучасних викликів.

Приватний сектор відіграє ключову роль у посиленні можливостей правоохоронних органів. Завдяки доступу до передових технологій, великих даних, фінансової інформації та експертизи у сфері кібербезпеки приватні компанії можуть значно прискорити процеси аналізу доказів, ідентифікації злочинців та відстеження незаконних фінансових потоків. Наприклад, аналітичні платформи, які використовуються технологічними гігантами, дозволяють обробляти величезні обсяги даних, що є недосяжним для більшості правоохоронних структур без зовнішньої підтримки.

Ефективна взаємодія між поліцією та приватним сектором може набувати різних форм, кожна з яких має свої особливості та потенціал:

Обмін інформацією: Приватні структури надають дані про фінансові транзакції, підозрілу активність чи кіберінциденти, що допомагає виявляти злочинні схеми.

Технологічна інтеграція: Використання аналітичного програмного забезпечення приватного сектора для обробки великих обсягів даних забезпечує швидший і точніший аналіз.

Спільні розслідування: Кооперація у боротьбі з кіберзлочинами чи економічними правопорушеннями дозволяє об’єднувати ресурси та експертизу.

Навчання та консультування: Залучення фахівців із приватного сектора для підвищення кваліфікації правоохоронців сприяє освоєнню сучасних методів аналізу.

Незважаючи на значний потенціал, співпраця між поліцією та приватним сектором стикається з низкою викликів:

Правові бар'єри: Відсутність чіткого законодавчого регулювання обміну інформацією ускладнює співпрацю та створює правову невизначеність.

Конфіденційність: Захист комерційної таємниці та персональних даних є критичним питанням, яке вимагає збалансованого підходу.

Різні пріоритети: Комерційні цілі приватного сектора (отримання прибутку) можуть суперечити завданням поліції, орієнтованим на громадську безпеку.

Технологічна нерівність: Обмежений доступ правоохоронних органів до сучасних технологій порівняно з приватним сектором створює додаткові перешкоди.

Міжнародний досвід демонструє успішні приклади співпраці, які можуть бути адаптовані до українських реалій. Наприклад, Європол активно співпрацює з технологічними компаніями для боротьби з кіберзлочинами, використовуючи штучний інтелект для аналізу даних. Аналогічно, партнерство фінансових установ із правоохоронними органами у країнах ЄС сприяє ефективному виявленню відмивання грошей. Ці практики підкреслюють важливість інтеграції ресурсів і можуть стати основою для розвитку подібних ініціатив в Україні.

Для підвищення ефективності співпраці пропонується:

Розробити чітку нормативно-правову базу, яка регулюватиме обмін інформацією між поліцією та приватним сектором.

Створити захищені цифрові платформи для безпечного обміну даними, що мінімізуватиме ризики витоку інформації.

Впровадити спільні навчальні програми для правоохоронців і працівників приватного сектора, щоб гармонізувати їхні підходи та методи роботи.

Адаптувати європейські практики публічно-приватного партнерства, які довели свою ефективність у боротьбі зі злочинністю.

Співпраця поліції з приватним сектором є невід'ємною складовою ефективного кримінального аналізу в умовах зростання технологічної складності злочинів. Інтеграція ресурсів, технологій та експертизи приватного сектора дозволяє значно підвищити оперативність і якість розслідувань. Для реалізації цього потенціалу необхідно усунути правові, організаційні та етичні бар'єри, створивши прозорі та ефективні механізми взаємодії. Такий підхід не лише зміцнить можливості правоохоронних органів, а й сприятиме загальному підвищенню безпеки суспільства.

Подальші дослідження варто спрямувати на розробку деталізованих моделей публічно-приватного партнерства, аналіз можливостей використання штучного інтелекту та великих даних у кримінальному аналізі, а також на адаптацію найкращих міжнародних практик до умов України. Особливу увагу слід приділити правовим аспектам, які забезпечать баланс між ефективністю розслідувань і захистом прав громадян.

Список використаних джерел

1. Закон України «Про Національну поліцію» від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

2. Smith, J., Clark, M. Public-Private Partnerships in Combating Cybercrime. Journal of Criminal Justice, 2020, Vol. 45, pp. 123–135.

3. Петренко О. П. Роль приватного сектора у протидії економічним злочинам. Науковий вісник НАВС, 2022, № 3, с. 45–52.

4. Europol. Public-Private Partnership in Cybersecurity. URL: https://www.europol.europa.eu/activities-services/public-private-partnerships.

Соловйов Едуард Петрович,
доцент кафедри кримінального процесу
Національної академії внутрішніх справ,
кандидат юридичних наук, доцент;
Осуховський Роман Вікторович,
доцент кафедри кримінальної юстиції
навчально-наукового інституту права
та психології Національної академії
внутрішніх справ, доктор філософії;
Пефтієв Денис Олегович,
незалежний експерт у сфері кримінального
аналізу та документування міжнародних
злочинів

РОЛЬ НОВІТНЬОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ «СЛІДЧИЙ ПРОТОКОЛ» У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ СЛІДЧИХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Повномасштабна російська агресія змінила організацію багатьох процесів зокрема процес проведення слідчих дій. Загроза перебування тривалий період часу на місцях обстрілів, залучення декількох спеціалістів до проведення однієї слідчої дії та ситуація коли мільйони мешканців України стали потерпілими або свідками від протиправних дій і виникла необхідність їх допитати призвели до пошуку шляхів подолання викликів.

З метою покращення організації роботи слідчих Національної поліції, за ініціативи та у співпраці з Головним слідчим управлінням Державне підприємство «ІНФОТЕХ» розробило інформаційну підсистему «Слідчий протокол», яку встановлено на мобільні пристрої (планшети).

Програмне забезпечення наразі містить у переліку декілька протоколів, кожен з яких створений з урахуванням особливості проведення слідчої дії і відповідно навіть слідчий з незначним досвідом роботи не порушить норм передбачених кримінальним процесуальним законодавством та якісно складе процесуальний документ використовуючи наявні словники та інші вбудовані функції.

Вже зараз програмне забезпечення передбачає можливість створення наступних протоколів:

– Протокол огляду місця події;

– Протокол огляду місця події (обстрілів);
– Протокол огляду місця події за фактами вчинення корисливих злочинів;
– Протокол огляду місця дорожньо-транспортної пригоди;
– Протокол огляду транспортного засобу;
– Протокол затримання особи, підозрюваної у вчиненні кримінального правопорушення;
– Протокол допиту свідка;
– Протокол допиту малолітнього (неповнолітнього) свідка;
– Протокол допиту потерпілого;
– Протокол обшуку.

Окреслимо інструменти, які впроваджені розробниками в програмне забезпечення.

По-перше варто звернути увагу на можливість транскрибування аудіо в текст. Не завжди погодні умови сприятливі і можна перебуваючи на вулиці скласти рукописний протокол або надрукувати його на комп'ютері під дощем. Є слідчі дії, до проведення яких у якості спеціаліста залучаються декілька осіб і кожен із них повинен внести відповідну інформацію до протоколу, як приклад огляд при репатріації тіл загиблих оборонців, а це щонайменше 6000 тіл [1]. Варто не забувати, що швидкість письма чи друку тексту слідчим можуть бути досить повільними. Вбудоване програмне забезпечення дозволяє за декілька секунд перетворити аудіо в текст і слідчому залишиться лише його переглянути і за необхідності відредагувати одразу на планшеті.

Ще корисною функцією є визначення геокоординат проведення слідчої дії, що усуває необхідність рекогносцування, пошуку прив'язки до адреси, зокрема коли об'єктом огляду є ділянка місцевості або зруйнована будівля у селищі.

Звичайні функції планшета фото та аудіо-, відеозапис усувають необхідність мати додаткові технічні пристрої такі як фотоапарат чи відеокамера та відповідно залучати додаткових працівників для фіксації. Тобто слідчий дотримуючись положень п. 11 ст. 615 КПК України самостійно може провести багаточасове інтерв'ювання звільненого з російського полону потерпілого, створивши необхідний емоційний контакт не відволікаючись на налаштування відеотехніки або друкування тексту. Наявність мобільного принтеру надає можливість одразу роздрукувати протокол та підписати у будь-якому місці, де перебуває на реабілітації звільнена з полону особа, відеофайл на

носії долучити до протоколу і такі показання можуть бути використані як докази в суді [2].

Як слушно зазначив В.В. Тимошко, досліджуючи питання проведення огляду під час розслідування воєнних злочинів, забезпечення безпекової складової є обов'язковою умовою проведення огляду місця події під час розслідування воєнних злочинів, адже безпека життя та здоров'я всіх учасників цієї слідчої (розшукової) дії є в пріоритеті [3]. При застосуванні інформаційної підсистеми «Слідчий протокол» зменшується як кількість осіб задіяних при огляді місця події так і час безпосереднього перебування на місці події, що важливо, враховуючи можливість повторних обстрілів, наявності вибухонебезпечних предметів та отруйних речовин.

Варто також не забувати про відомчий контроль. Створені процесуальні документи через внутрішньовідомчу захищену мережу завантажуються на серверне сховище і керівник органу досудового розслідування (навіть перебуваючи поза межами регіону де проводиться документування злочину) має можливості здійснювати відомчий та процесуальний контроль, оцінити кваліфікацію слідчого і прийняти управлінське рішення. Наявність цифрової копії мінімізує ризик умисного або неумисного знищення або спотворення доказів.

Цифрові документи набагато спрощують накопичення, обробку та використання зібраної інформації, цифровізація дає можливість пов'язувати різні масиви інформації, що своєю чергою підвищує ефективність аналітичної складової. У десятках тисяч протоколів за декілька секунд можна знайти однаковий позивний воєнного злочинця, тим самим пришвидшити його ідентифікацію для подальшого притягнення до кримінальної відповідальності.

Список використаних джерел

1. Україна завершила етап репатріації тіл полеглих оборонців залізницею, далі такі заходи відбуватимуться автотранспортом. URL: https://suspilne.media/1043237-ukraina-/.

2. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

3. Тимошко В.В.. Процесуальні та тактичні особливості проведення огляду під час досудового розслідування воєнних злочинів. *Вісник Кримінологічної асоціації України.* 2023 № 30(3). С. 329–338.

Старенький Олександр Сергійович,
професор кафедри кримінальної юстиції
Національної академії внутрішніх справ,
доктор юридичних наук, доцент

ПОЗБАВЛЕННЯ ДЕРЖАВНИХ НАГОРОД НА ПІДСТАВІ ОБВИНУВАЛЬНОГО ВИРОКУ СУДУ

Питання позбавлення державних нагород набуває особливої ваги в умовах воєнного стану та підвищених викликів національній безпеці. Прийняття Закону України «Про внесення змін до Кримінального кодексу України, Кримінального процесуального кодексу України та інших законодавчих актів України щодо позбавлення державних нагород за популяризацію або пропаганду держави-агресора чи вчинення інших протиправних дій проти України» № 4074-IX від 20 листопада 2024 року (Закон № 4074-IX) уперше закріпило позбавлення державної нагороди як вид додаткового покарання та створило процесуальний механізм його реалізації. Це зумовлює потребу в науковому осмисленні новел законодавства, виявленні прогалин та визначенні напрямів подальшого вдосконалення інституту державних нагород.

Положення статті 16 Закону України «Про державні нагороди України» (у редакції до 21.11.2024) передбачали не лише неконституційні повноваження Президента України щодо прийняття рішення про позбавлення державних нагород через відсутність відповідних повноважень Глави держави у пункті 25 частини першої статті 106 Основного закону України, але й визначали надзвичайно спірну з правової точки зору підставу для реалізації такого рішення – подання суду про вчинення особою тяжкого злочину. Така підстава не лише не відповідала приписам Конституції України, а й вступала в пряму суперечність із положеннями кримінального та кримінального процесуального законодавства України з огляду на наступне.

По-перше, жодним нормативно-правовим актом України – ані спеціальним Законом України «Про державні нагороди України», ані Законом України «Про судоустрій і статус суддів», ані Кримінальним процесуальним кодексом України (КПК України) – не визначено юридичної природи, форми, порядку ухвалення, направлення або правових наслідків подання суду про позбавлення особи державної нагороди, що на

практиці призводило до того, що окремі суди направляли на розгляд Президенту України або постійно діючому допоміжному органу, утвореного Президентом України, відповідні листи у довільній формі, вважаючи його поданням суду, додатком до яких додавали копії обвинувальних вироків суду, що набрали законної сили. Водночас такі документи не мали визначеного процесуального статусу, не породжували юридичних наслідків та, відповідно, не могли бути реалізовані в установленому законом порядку.

По-друге, стаття 16 Закону України «Про державні нагороди України» (у редакції до 21.11.2024) надавала можливість позбавляти державної нагороди лише у разі засудження нагородженого за тяжкий злочин. Такий підхід суперечив загальновизнаній системі класифікації злочинів за ступенем суспільної небезпеки, закріпленій у частині третій статті 12 Кримінального кодексу України (КК України), відповідно до якої злочини поділяються на нетяжкі, тяжкі та особливо тяжкі. Особливо тяжкий злочин, за своєю юридичною природою, є найбільш небезпечним для суспільства і держави, що об'єктивно зумовлює необхідність більш суворих правових наслідків, зокрема і в аспекті можливої втрати публічного визнання у формі державної нагороди.

Однак положення статті 16 Закону України «Про державні нагороди України» (у редакції до 21.11.2024) взагалі не містили згадки про можливість позбавлення державної нагороди у разі вчинення особою особливо тяжкого злочину. Така законодавча конструкція породжувала очевидний логіко-правовий парадокс: особа, засуджена за тяжкий злочин, наприклад, за крадіжку у великих розмірах чи в умовах воєнного або надзвичайного стану (частина четверта статті 185 КК України), незаконне збагачення (статті 368^{-5} КК України), могла бути позбавлена державної нагороди відповідно до прямої вказівки закону, тоді як особа, яка вчинила особливо тяжкий злочин – наприклад, умисне вбивство за обтяжуючих обставин (частина друга статті 115 КК України), зґвалтування з особливо тяжкими наслідками (частина п'ята статті 152 КК України) або державну зраду (стаття 111 КК України), – формально не підпадала під дію відповідної норми через відсутність належної законодавчої підстави. Це свідчило не лише про внутрішню неузгодженість правового регулювання,

а й про порушення принципів юридичної логіки, пропорційності та справедливості.

Внаслідок цього виникала ситуація, за якої найбільш небезпечні для держави й суспільства злочини не тягли за собою автоматичного перегляду статусу особи як нагородженої державою, що підривало авторитет інституту державних нагород як морального еталона публічного визнання.

По-третє, у КК України до прийняття Закону № 4074-IX був відсутній такий вид покарання як позбавлення державних нагород. Стаття 51 КК України серед видів покарань визначала лише позбавлення військового, спеціального звання, рангу, чину або кваліфікаційного класу. Зазначена покарання відноситься до числа додаткових покарань (ч. 2 ст. 52 КК України).

Відсутність позбавлення державної нагороди в системі покарань унеможливлювало застосування цього заходу у межах кримінального провадження без внесення відповідних змін до законодавства України. У правозастосовній практиці це створювало прогалину, коли навіть за наявності обвинувального вироку щодо особи, яка вчинила суспільно небезпечний злочин, питання позбавлення її державної нагороди не могло бути вирішене судом як складовою вироку.

По-четверте, Закон України «Про судоустрій і статус суддів України», КПК України та Кримінально-виконавчий кодекс України не закріплювали за судом повноважень щодо вирішення під час судового розгляду питання про позбавлення державних нагород і зазначення про це у змісті обвинувального вироку суду, а також не передбачали відповідний механізм виконання відповідного рішення суду.

Не зважаючи на те, що статтями 129, 129-1 Конституцією України передбачено, що судове рішення є обов'язковим до виконання, його зміст повинен ґрунтуватися на положеннях чинного законодавства України, а не на нормах, що не мають належного процесуального підґрунтя. Суд не може ухвалити рішення про те, на що в нього відсутнє відповідне повноваження. Без внесення змін до як до Конституції України, так і до КК України, КПК України, Кримінально-виконавчого Кодексу України (КВК України) будь-яке «подання суду» про позбавлення державної нагороди було б процесуально нікчемним і юридично неефективним.

Таким чином, положення статті 16 Закону України «Про державні нагороди України» (у редакції до 21.11.2024) одночасно суперечили як Конституції України – в частині неконституційного розширення повноважень Президента України, – так і кримінальному, кримінальному процесуальному та кримінально-виконавчому законодавству України – через відсутність належних підстав і дієвих механізмів для позбавлення державної нагороди. Вказана правова конструкція не відповідала базовим засадам верховенства права та правової визначеності, а також вимогам системності й узгодженості правового регулювання, що об'єктивно зумовлювало необхідність її подальшого оновлення.

Реалізуючи цю потребу в межах цілісної кримінальної правової політики держави, Законом № 4074-IX внесено комплексні зміни до низки законодавчих актів України, які не лише синхронізували між собою положення кримінального, кримінального процесуального, кримінально-виконавчого та спеціального (галузевого) законодавства України, а й запровадили дієвий механізм реалізації нового інституту покарання у вигляді позбавлення державної нагороди. Зокрема:

– нова редакція статті 16 Закону України «Про державні нагороди України» серед підстав для позбавлення державних нагород визначає наявність обвинувального вироку суду, яким особу, нагороджену державною нагородою, засуджено за тяжкий чи особливо тяжкий злочин, кримінальне правопорушення проти основ національної безпеки України, проти миру, безпеки людства та міжнародного правопорядку, а також кримінальне правопорушення, передбачене статтями 258-258-5, 260, 261 КК України. Датою, з якої особу позбавлено державних нагород на цій підставі, визначено дату набрання законної сили обвинувальним вироком суду;

– до статті 51 КК України включено новий вид додаткового покарання – позбавлення державної нагороди України, а сам КК України доповнено статтею 54^{-1}, «Позбавлення державної нагороди України», положення якої повністю кореспондуються з оновленою редакцією статті 16 Закону України «Про державні нагороди України» в частині позбавлення державної нагороди на підставі обвинувального вироку суду;

– частину першу статті 368 КПК України серед переліку питань, що вирішуються судом при ухваленні вироку, доповнено новим пунктом 6-1 «чи є підстави для позбавлення обвинуваченого державної нагороди України», а пункт другий частини четвертої статті 374 КПК України серед елементів резолютивної частини обвинувального вироку передбачено необхідність зазначення судом інформації про покарання у вигляді позбавлення державної нагороди України»;

– КВК України доповнено новою главою 6-1 «Виконання покарання у виді позбавлення державної нагороди України» зі статтю 29-1. «Порядок виконання покарання у виді позбавлення державної нагороди України», згідно якої суд, який постановив вирок про позбавлення засудженого державної нагороди України, протягом трьох робочих днів після набрання ним законної сили направляє копію вироку Президентові України та Міністерству юстиції України (частина перша). Резолютивна частина такого вироку невідкладно публікується в офіційних друкованих виданнях, в яких здійснюється офіційне оприлюднення актів Президента України, а також розміщується на офіційному веб-сайті Президента України (частина друга). Міністерство юстиції України протягом трьох робочих днів після одержання копії вироку, яким засудженого позбавлено державної нагороди України, направляє копію вироку органам або посадовим особам, до компетенції яких віднесено питання застосування та/або адміністрування пільг, передбачених для осіб, нагороджених державними нагородами України, для припинення застосування пільг та пов’язаних з ними прав, передбачених для осіб, нагороджених державними нагородами України. Відповідний орган або посадова особа, до компетенції яких віднесено питання застосування та/або адміністрування пільг, передбачених для осіб, нагороджених державними нагородами України, протягом одного місяця з дня одержання копії вироку сповіщає Міністерство юстиції України та суд, який постановив вирок, про його виконання (частина третя).

Таким чином, зазначені законодавчі зміни свідчать про завершення перехідного етапу трансформації інституту позбавлення державних нагород – від формально-декларативного до конституційно-узгодженого та процесуально реалізованого механізму. Зміни усунули не лише правові колізії в системі розподілу повноважень між Президентом України і

судовою гілкою влади у сфері позбавлення державних нагород, а й забезпечили належні умови для втілення принципу верховенства права в публічно-правових відносинах і зміцнення легітимності інституту державної нагороди як морально-правового явища.

Незважаючи на позитивний характер законодавчих змін, запроваджених Законом № 4074-IX, окремі його новації потребують подальшого вдосконалення як з точки зору системності правового регулювання, так і з позицій забезпечення належного балансу між інтересами держави та правами особи. Такий висновок обумовлений наступним:

1) законодавчо закріплений вичерпний перелік кримінальних правопорушень, за вчинення яких нагороджувана особа може бути засуджена з призначенням покарання, у тому числі позбавлення державної нагороди, є неповним і не враховує випадків вчинення суспільно неприйнятних або аморальних діянь, що хоча й не належать до категорії тяжких чи особливо тяжких злочинів, однак суперечать ціннісному змісту державної нагороди як символу суспільного визнання, публічної гідності й моральної бездоганності, з якою асоціюється статус нагородженого. Такий формалізований підхід до визначення правових підстав позбавлення державної нагороди потенційно створює ситуації, коли особа, яка вчинила кримінальний проступок або нетяжкий злочин із високим ступенем моральної девіантності й відповідне судове рішення набрало законної сили, продовжує володіти статусом нагородженого та користуватися його пільгами, що прямо підриває авторитет інституту державних нагород і дискредитує їх морально-правову природу.

Крім того, додатково потребує нормативного врегулювання можливість позбавлення державної нагороди у разі вчинення окремих адміністративних правопорушень, які, попри свій некримінальний характер, демонструють високий рівень публічного резонансу або відзначаються значним порушенням етичних норм і морального порядку. Зокрема, це адміністративні правопорушення, пов’язані з корупцією (статті 172^{4}-172^{9-2} КУпАП), дрібне викрадення чужого майна (стаття 51 КУпАП), вчинення домашнього насильства (стаття 173^{-2} КУпАП), булінг (цькування) учасника освітнього процесу (ст. 173^{-4} КУпАП), сексуальне домагання (стаття 173^{-7}

КУпАП), продаж державних нагород (стаття 186[-1] КУпАП), керування транспортними засобами або суднами особами, які перебувають у стані алкогольного, наркотичного чи іншого сп'яніння або під впливом лікарських препаратів, що знижують їх увагу та швидкість реакції (стаття 130 КУпАП). У вузькому кримінально-правовому сенсі ці діяння не досягають рівня тяжкого чи особливо тяжкого злочину, проте їх публічне осудження та репутаційний ефект є несумісними з морально-правовою й репутаційною природою державної нагороди.

Отже, об'єктивно постає потреба у концептуальному перегляді чинної моделі правових підстав позбавлення державної нагороди на користь більш гнучкого, комплексного та репутаційно орієнтованого підходу. Він повинен ґрунтуватися не лише на формальній класифікації кримінальних правопорушень за ступенем тяжкості, а й на морально-етичній оцінці поведінки нагородженої особи крізь призму публічної гідності та суспільного інтересу. Запровадження подібної концепції сприятиме не лише зміцненню легітимності інституту державних нагород і його відповідності суспільним уявленням про гідність та моральну бездоганність, а й утвердженню принципів справедливості, правової визначеності й верховенства права в цій сфері.

2) особливої уваги заслуговує положення частини другої статті 29-1 КВК України, яке передбачає, що резолютивна частина вироку невідкладно публікується в офіційних друкованих виданнях, в яких здійснюється офіційне оприлюднення актів Президента України, а також розміщується на офіційному веб-сайті Президента України. Такий підхід загалом відповідає принципам відкритості, підзвітності й інституційної прозорості у сфері державних нагород та створює нормативну основу для публічного контролю за легітимністю їх застосування. Водночас доцільним видається подальше вдосконалення механізму публічного відображення інформації про факти позбавлення державних нагород. Зокрема, відповідні дані мають бути вказані також у змісті тих Указів Президента України, якими особу було нагороджено державною нагородою (наприклад, у відповідному Указі Президента України під даними нагороджуваної особи робиться примітка про те, що особа позбавлена державної нагороди на підставі вироку суду).

3) чинне правове регулювання, запроваджене у зв'язку з прийняттям Закону № 4074-IX, не містить положень щодо процесуального механізму поновлення особи у статусі нагородженого у разі скасування обвинувального вироку та її подальшого виправдання. За відсутності нормативно закріплених правових гарантій реабілітації, особа, яка була необґрунтовано позбавлена державної нагороди, навіть після поновлення її публічного статусу в судовому порядку, опиняється в ситуації правової, соціальної та репутаційної невизначеності. Така особа фактично позбавлена доступу до юридичних інструментів відновлення свого правового статусу суб'єкта державного визнання, поновлення порушених немайнових прав, а також офіційного механізму репутаційної реабілітації. У перспективі це створює ризики делегітимації правозастосування у сфері державних нагород, оскільки сама природа нагородження передбачає високий рівень персоніфікованого публічного визнання, що не може бути односторонньо-неповоротно скасованим у випадках судової реабілітації. Позбавлення державної нагороди без можливості її поновлення суперечить принципу справедливості, презумпції невинуватості в ширшому соціальному сенсі, а також засадам правової визначеності та пропорційності.

З огляду на викладене, постає об'єктивна потреба у розробленні комплексного нормативного механізму реабілітації осіб, які були необґрунтовано позбавлені державних нагород, із чітким визначенням процесуальної процедури відновлення їхнього статусу, що забезпечить: усунення наявних правових прогалин; досягнення належного балансу між інтересами держави та правами особи; відновлення публічного престижу нагородженого у випадках його судової реабілітації; зміцнення легітимності інституту державних нагород у правовій системі України.

4) залишається не врегульованим питання механізму обов'язкового вилучення державної нагороди та документу, що посвідчує нагородження нею (орденську книгу), у осіб, які були позбавлені відповідного статусу на підставі вироку суду. Відсутність подібного механізму створює потенційні ризики недобросовісного використання державної нагороди, зловживань нею в офіційному чи публічному обігу, а також сприяє маніпулятивному формуванню хибної уяви про статус

особи в соціально-політичному середовищі. У контексті публічного символізму державної нагороди як уособлення офіційного визнання заслуг, подібна правова прогалина може призводити до дискредитації як самого інституту державних нагород, так і відповідної державної політики загалом.

5) Закон № 4074-IX, як і інші положення чинного законодавства України не містить положення щодо створення та функціонування офіційного публічного державного реєстру осіб, позбавлених державних нагород, у тому числі на підставі вироку суду. Така відсутність унеможливлює належну реалізацію принципів відкритості та прозорості у сфері публічного визнання заслуг, що є складовою демократичного суспільного устрою. Інституційна непрозорість у цьому аспекті обмежує право громадськості на доступ до інформації, яка становить значущий публічний інтерес, унеможливлює належний моніторинг легітимності використання державних нагородо особами, які втратили на них право, та ускладнює здійснення належного громадського контролю. Крім того, відсутність публічного державного реєстру осіб, позбавлених державних нагород, перешкоджає формуванню справедливої та об'єктивної суспільної оцінки поведінки таких осіб, що дискредитує саму ідею державної нагороди як символу бездоганної репутації, виняткових заслуг і моральної гідності.

Таким чином, запровадження у КК України нового виду додаткового покарання – позбавлення державної нагороди, а також внесення кореспондуючих змін до КПК України й КВК України забезпечили формування цілісного нормативного механізму ухвалення, виконання та оприлюднення судових рішень у цій сфері. Це сприяло усуненню раніше існуючих правових колізій, зміцненню принципу верховенства права та узгодженню нагородної політики з конституційними засадами.

Разом із тим, аналіз запроваджених Законом № 4074-IX новел показав, що чинне правове регулювання не позбавлене істотних прогалин: відсутній механізм поновлення у правах на нагороду у випадку скасування вироку і реабілітації особи; не врегульовані питання вилучення нагород і документів, що їх посвідчують, на підставі вироку суду; не створено публічного державного реєстру осіб, позбавлених нагород.

Темник Олександр Павлович,
начальник управління кримінального
аналізу ГУНП у м. Києві

ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ, ЗОКРЕМА ШТУЧНОГО ІНТЕЛЕКТУ, У КРИМІНАЛЬНОМУ АНАЛІЗІ

У світлі активного розвитку цифрових технологій та трансформації безпекового сектору дедалі більшого значення набуває впровадження сучасних ІТ-рішень у діяльність правоохоронних органів. Одним з ключових напрямів таких змін є застосування штучного інтелекту (ШІ) у сфері кримінального аналізу. В Україні цей процес ще перебуває на етапі становлення, проте вже зараз спостерігається чітка тенденція переходу від традиційного, переважно ручного аналізу до інтеграції автоматизованих інструментів, здатних працювати з великими масивами даних, виявляти приховані взаємозв'язки та передбачати потенційні загрози.

Кримінальний аналіз охоплює широкий спектр дій - від збору та систематизації даних до виявлення закономірностей злочинної поведінки, аналізу активності організованих груп і прогнозування криміногенних процесів у часі та просторі. Якщо раніше аналітики переважно спиралися на власний досвід і ручну обробку інформації, то сьогодні їм на допомогу приходять сучасні програмні комплекси, що використовують алгоритми машинного навчання.

Одним із найяскравіших прикладів є використання IBM i2 Analyst's Notebook – інструменту, що дозволяє наочно моделювати взаємозв'язки між фігурантами справ, подіями, транспортом, фінансовими операціями та іншими об'єктами. Поєднання графічної візуалізації з можливостями автоматичного виявлення аномалій та класифікації подій значно підвищує ефективність аналітичної роботи, особливо у фінансових розслідуваннях, пов'язаних із відмиванням коштів.

Перспективним напрямом також є застосування технологій обробки природної мови для моніторингу відкритих джерел інформації, включно з соціальними мережами, онлайн-форумами та месенджерами. Сучасні мовні моделі, подібні до GPT, надають аналітикам інструменти для оперативного узагальнення інформації, виявлення загроз, осіб, залучених до

координації протиправних дій чи розповсюдження екстремістського контенту.

Окрема увага приділяється інтеграції аналітичних платформ із внутрішніми базами даних - криміналістичними обліками, біометричними даними, матеріалами відеоспостереження, реєстрами судових експертиз. Ідея створення єдиної інформаційно-аналітичної системи, що об'єднує всі ці джерела, виглядає не лише технічно реалістичною, а й надзвичайно актуальною для підвищення якості оперативного реагування на злочини.

Період воєнного стану в Україні лише прискорив ці процеси. З 2022 року реалізовано низку ініціатив у співпраці з міжнародними структурами, спрямованих на документування воєнних злочинів, аналіз супутникових даних, ідентифікацію воєнних злочинців і виявлення кібератак. Такі інструменти вже використовуються СБУ, Національною поліцією та іншими органами у практичній діяльності.

Разом із тим, широке впровадження інновацій супроводжується низкою викликів. По-перше, постає необхідність законодавчого врегулювання використання ШІ у сфері безпеки з урахуванням прав людини, стандартів конфіденційності та прозорості алгоритмів. По-друге, критично важливо забезпечити належну підготовку кадрів – фахівців, здатних не лише користуватися готовими рішеннями, а й аналізувати їхні результати, налаштовувати параметри моделей, виявляти помилки.

Також слід наголосити на важливості міжвідомчого обміну інформацією. Без ефективної співпраці між поліцією, прикордонною службою, митницею, податковими органами та міжнародними партнерами – жодна, навіть найдосконаліша технологія, не зможе забезпечити належного рівня аналітичного реагування на сучасні загрози.

Отже, досвід України свідчить: впровадження інноваційних технологій у кримінальний аналіз є не лише вимогою часу, а й запорукою підвищення ефективності безпекової системи. Успіх цього процесу буде залежати від здатності синтезувати людський інтелект із технічними можливостями, дотримуючись при цьому принципів законності, етики та професіоналізму.

Список використаних джерел

1. Васильєв В.І., Корольова С.В. Інноваційні технології в аналітичній діяльності правоохоронних органів // Право і безпека. 2023. №2.
2. Дубровський С.М. OSINT як джерело інформації для кримінального аналізу // Збірник наукових праць НАВС. 2021.
3. Europol. Innovation Lab Report: AI and Law Enforcement. 2022. [https://www.europol.europa.eu].
4. UNICRI & INTERPOL. Artificial Intelligence and Robotics for Law Enforcement. 2019. [https://unicri.it].
5. IBM. AI in Criminal Intelligence Analysis: Use Cases of i2 Analyst's Notebook. 2023. [https://www.ibm.com/docs/en/i2-anb].
6. Служба безпеки України. Річний звіт про цифрову трансформацію 2023. [https://ssu.gov.ua].

Худенко Дмитро Миколайович,
ветеран НПУ, керівник Департаменту
кримінального аналізу НПУ
у 2021–2023 роках

МІСЦЕ СЛОВНИКІВ І ДОВІДНИКІВ У БІБЛІОГРАФІЇ НАЦІОНАЛЬНОЇ ТЕРМІНОСИСТЕМИ З КРИМІНАЛЬНОГО АНАЛІЗУ

Сьогодні у кримінальному аналізі науковий пошук зосереджено на обґрунтуванні професійної термінології, що у тандемі із іншими предметами інтересу вчених та практиків сприяє вирішенню актуальних питань. Її основою вважаються терміни, оскільки несуть покликання чітко та недвозначно окреслювати поняття. Словники та довідники слугують практичним і науково-методологічним інструментом розвитку, який забезпечує сталість, доречність і відповідність терміносистеми сучасним викликам аналітичної діяльності.

Принципові розбіжності проявлено на рівні базових знань, методологічних засад, зокрема щодо інтерпретації ключових термінів виключно англомовного походження, їх різночитання та іноді необґрунтованого україномовного використання [1, с. 15]. На аналогічні проблеми звернено й увагу іноземними партнерами, зокрема, віце-президентом Міжнародної асоціації кримінальних аналітиків (IACA, США) Рейчєл Карсон, представниками Місії регіонального програмного офісу Міжнародної програми

підвищення кваліфікації органів кримінального розслідування (ICITAP, США) та Консультативної місії Європейського Союзу в Україні (КМЄС, ЄС).

Термінологію кримінального аналізу та пов'язані питання досліджено у колективних працях Бурангулова В.А. та Користіна О.Є. [2], дисертаційних дослідженнях, які провів Бурангулов В.А. [3], Дерев'янко Т.М. [4] та Царук А.В. [5], а також у монографіях Благути Р.І., Мовчана А.В. [6], Федчака А.І. [7] та ін. Водночас профільної науково-дослідної роботи не проведено, кількість джерел і літератури, де вжито специфічні терміни зросла, дискус розширено та триває. Сформовано умови стандартизації термінології, зокрема, для складання переліку основних термінів, який не створити без вивчення бібліографії.

Під національною терміносистемою кримінального аналізу ми розуміємо відносно замкнену, кількісно обмежену множину термінів, що відбиває на стандартизованій основі понятєву систему у сфері кримінального аналізу на відповідних етапах розвитку цієї сфери в Україні.

Початок її формування важливо й можливо визначити, але необхідно домовитися, залежно від чого саме його визначати. Так, серед навчально-методичної літератури однією з перших праць, де вжито специфічний термін або «кримінальний аналіз» стала робота польського вченого М. Яніцкі, яку оприлюднено 2009 року, окремий розділ якої було відведено основоположним поняттям кримінального аналізу, а також надано у заключному розділі 12 термінів та їх визначення [8].

У тексті нормативно-правових і нормативних актів України 2008 року з'явився термін «кримінальний аналіз» [9], а 2009 року – інші терміни у формі словосполук [10].

У черговому інтерв'ю з М. Фоміним, представником ICITAP, висловлено цікаву думку з його власних практичних спостережень, що частиною фундаменту еволюції кримінального аналізу, особливо в англо-саксонської системи права, є кримінологія. Кримінологія, як галузь знань, з'явилась ще раніше ніж кримінальний аналіз, існувала в радянські часи та розвивається в незалежній Україні. Іншими словами має більш сталу ґенезу терміносистеми.

Розмірковування можна продовжити з урахуванням галузі знань з оперативно-розшукової діяльності за рахунок галузі

знань з оперативно-розшукової діяльності або у залежності від поділу на правоохоронні відомства, що вимагає більшого обсягу для висвітлення результатів нашої наукової розвідки. Тому ми залишаємо це питання відкритим і зосереджуємо увагу на словниках, а також інших видах літератури та джерел, за допомогою яких може бути сформовано попередній перелік основних термінів кримінального аналізу.

Першим та єдиним з 2016 року словником можемо вважати «Короткий тлумачний словник керівника підрозділу кримінального аналізу». У ньому вміщено більше 200 вживаних у системі інформаційно-аналітичної діяльності оперативно-розшукових підрозділів і підрозділів кримінального аналізу Державної прикордонної служби України термінів і понять, які стосуються безпосередньо здійснення ними кримінального аналізу і відносяться до галузей оперативно-розшукової, кримінально-процесуальної та інформаційної діяльності, педагогіки, психології, логіки і деяких інших галузей знань [11, с. 3]. Також наведено загальноприйняту абревіатуру, англомовні терміни, їх тлумачення. Цю роботу згодом продовжено шляхом видання навчального посібника [12], розділ глосарію якого містив мінімум 80 термінів.

Вже 2020 року у розділі VIII «Глосарій» Протоколу Берклі іноземними партнерами наведено 57 термінів і їх визначень, корисних під час проведення досліджень з використанням відкритих цифрових даних. У даному розділі включено терміни, які не завжди безпосередньо застосовуються в протоколі, але мають потенційну доречність для ресурсів, пов'язаних із OSINT-розслідуваннями ([13, с. 75–80]).

2023 року на базі Одеського державного університету внутрішніх справ України завершено перші науково-дослідні роботи. Колективом провідних українських вчених на чолі з Д. Афоніним [14] розроблено словник із 89 основних термінів кримінального аналізу. А в ДНДІ МВС України О. Користіним ґрунтовно вивчено зміст та інтерпретацію терміну «Intelligence» в контексті моделі Intelligence-led Policing, а також ряду інших ключових термінів [15].

Окрему групу становлять навчальні посібники та видання, у назві яких використано термін «довідник». Одним із перших було видання 2019 року українського авторського колективу за загальною редакцією М.Г. Вербенського під назвою «Довідник

керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою» [16].

2023 року в рамках міжнародного проекту «MATRA-Україна» за участі МЗС Королівства Нідерландів, спрямованого на підтримку документування та розслідування міжнародних злочинів в Україні підготовлено довідник з базових стандартів розслідування [17].

Отже, можемо констатувати розвиток інституціоналізації терміносистеми кримінального аналізу через появу не лише окремих глосаріїв, термінологічних словників або розділів із тлумаченням термінів у навчальних і науково-практичних виданнях, а й спеціалізованих посібників з узагальненням понять, скорочень, абревіатур та умовних позначень. Обидві згадані групи – як самостійні словникові праці, так і термінологічні розділи у фаховій літературі – становлять вагомий інструмент для подальшої стандартизації термінології.

Кримінальний аналіз має власний термінологічний фонд, сформований представниками, наприклад, поліцейської та прикордонної школи. Розглянемо їх групи більш детально.

На академічному рівні у 2015 та 2016 роках для Державної прикордонної служби та Національної поліції України відповідно колективами іноземних та українських науковців видано два посібники з тлумаченням ключових понять [18, 19]. Виходили друком навчальні посібники у 2019 році із тактичного кримінального аналізу [20], 2020 року – з теорії систем з системного аналізу [21], у 2021 та 2023 роках – з основ кримінального аналізу [22, 23].

До джерел та літератури цієї групи також віднесемо вузькопредметні видання, пов’язані з тактичним аналізом у розслідуванні злочинів у сфері незаконного обігу наркотиків [24], стратегічним аналізом [25; 26], використанням окремих інструментів [27] або реєстрів [28], протиправними криптотранзакціями [29], з’єднаннями абонентів мобільного зв’язку [30], поліцейською діяльністю, заснованою на розвідувальній інформації [31; 32] тощо.

Важливо також враховувати нормативно-правові та нормативні акти України, які в частині формалізації функцій, структур і процедур містять термінологічні елементи.

Попередній перелік основних термінів кримінального аналізу може також спиратися на доктринальні та стратегічні

документи, джерела з інших галузей знань, включаючи оперативно-розшукову діяльність, оперативно-розшукову психологію, кримінальне право та процес, криміналістику, інформаційні технології, кримінологію, міжнародне право, розвідка з відкритих джерел, запобігання та протидія легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, розповсюдження зброї масового знищення та корупції, теорію систем та системний аналіз тощо.

З урахуванням правового режиму воєнного стану, національні та іноземні міжгалузеві стандарти, керівництва й методичні рекомендації містять терміни, зокрема, у воєнній сфері, які мають бути враховано у бібліографії терміносистеми.

Не менш корисним є компаративістський напрям. Допустимим, безвідкладним і доцільним вважаємо вивчення російського досвіду.

Окремі напрями, пов'язані із вивченням конкретної події чи особистості у світі або ситуативні огляди і вживана термінологія за їх результатами лише посилюють зв'язок теорії з практикою.

З огляду на це, за нашими підрахунками щонайменше 80 джерел і видань можуть становити бібліографічну основу майбутнього загального та оновленого словника або довідника, що має на меті впорядкувати та стандартизувати терміносистему кримінального аналізу. Очевидно, що основа є обмеженою та потребує подальшого наукового дослідження.

Словники й довідники посідають центральне місце у бібліографії національної терміносистеми кримінального аналізу, оскільки виконують не лише функцію фіксації значень термінів, а й є основою для формування уніфікованого понятєвого апарату. Їх значення полягає в тому, що вони забезпечують термінологічну узгодженість між фахівцями з різних підрозділів і відомств, закріплюють дефініції на академічному, практичному й нормативному рівнях, інтегрують до національного лексикону міжнародні терміни й концепти, а також формують підґрунтя для розробки офіційних стандартів терміновживання в Україні.

Список використаних джерел

1. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України:

монографія / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін., за заг. ред. Користіна О.Є. Київ: «ВАІТЕ», 2024. - 444 с.

2. Користін О.Є., Бурангулов В.А. Термінологія кримінального аналізу // Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України: матеріали міжвідомчої науково-практичної конференції (Київ, 17 листопада 2023 року). Київ: НАВС, 2023. С. 61–67. URL: https://elar.navs.edu.ua/handle/123456789/27441.

3. Бурангулов В.А. Кримінальний аналіз в правоохоронній діяльності : дис. ... д-ра філософії : 081 – Право / В. А. Бурангулов; МВС України, ОДУВС. Одеса, 2024. 231 с.

4. Дерев'янко Т.М. Розвиток креативного мислення кримінальних аналітиків оперативно-розшукових підрозділів Державної прикордонної служби України: автореферат дис. на здобуття наук. ступеня канд. психол. наук: 19.00.09 – психологія діяльності в особливих умовах. Хмельницький: НАДПС України ім. Б. Хмельницького, 2015. 20 с.

5. Царук А.В. Адміністративно-правове забезпечення інформаційно-аналітичної діяльності Державної прикордонної служби України в контексті євроінтеграції : дис. ... д-ра філософії : 081 – Право / А. В. Царук; НАДПС України ім. Б. Хмельницького. Хмельницький, 2021. – 266 с.

6. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.

7. Федчак І.А. Концептуальні основи та науково-практичні аспекти проактивних моделей правоохоронної діяльності : монографія. Львів : ЛьвДУВС, 2024. 628 с.

8. Яніцкі М. Оперативний кримінальний аналіз: посібник / пер. Ігоря Родюка; за ред. Міжнародної організації з міграції (МОМ). Київ, 2009. 85 с.

9. Протокол № 5 до Меморандуму про взаєморозуміння між Урядом України та Урядом Сполучених Штатів Америки щодо допомоги з правоохоронних питань від 9 грудня 2002 р. URL: https://zakon.rada.gov.ua/laws/show/840_134#Text.

10. Про схвалення Стратегічних напрямів та завдань щодо залучення міжнародної технічної допомоги і співробітництва з міжнародними фінансовими організаціями на 2009–2012 роки : розпорядження Кабінету Міністрів України від 3 верес. 2009 р. № 1156-р. Втратило чинність на підставі

постанови КМУ № 1072 від 04 груд. 2019 р. URL: https://zakon.rada.gov.ua/laws/show/1156-2009-p#Text.

11. Короткий тлумачний словник керівника підрозділу кримінального аналізу : словник / О. С. Кіреєва, В. В. Половніков, О. Б. Фаріон Хмельницький : Вид-во НАДПС України, 2016. 68 с.

12. Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України : навчальний посібник / О. С. Кіреєва, Ю. В. Крутік, О. М. Махлай, А. С. Треус. Хмельницький : Вид-во НАДПСУ, 2022. 360 с.

13. Berkeley Protocol on Digital Open Source Investigations / Human Rights Center, UN Office of the High Commissioner for Human Rights. December 2, 2020. 80 с. URL: https://humanrights.berkeley.edu/publications/berkeley-protocol-on-digital-open-source-investigations.

14. Кримінальний аналіз у протидії злочинності : звіт про НДР (заключн.) / Одеський державний університет внутрішніх справ України ; керівник Д. С. Афонін. № 0121U109656. Одеса : Одеський державний університет внутрішніх справ України, 2023. 208 с.

15. Міжнародні стандарти організації поліцейської діяльності, керованої аналітикою, та особливості їх практичної реалізації в кримінальному аналізі : звіт про НДР (заключн.) / ДНДІ МВС України ; керівник О. Користін. № 0123U101659. Київ : ДНДІ МВС України, 2023. 32 с.

16. Користін О.Є., Пефтієв Д.О., Некрасов В.А. Довідник керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою/ILP: навчальний посібник / за заг. ред. М.Г. Вербенського. Київ, 2019. 120 с.

17. Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні : довідники. Гаага : Global Rights Compliance, 2023. 92 с. URL: https://www.asser.nl/media/796397/manual-керівництво-з-базових-стандартів-розслідування-для-документування-міжнародних-злочинів-в-украі-ні-довідники-1.pdf.

18. Посібник з кримінального аналізу для кримінальних аналітиків Державної прикордонної служби України / Джонстоун Д., Яніцкі М., Навроцкі Д. - К.: ОБСЕ, 2015. 176 с.

19. Основи кримінального аналізу : посіб. з елементами тренінгу / Користін О. Є., С. В. Албул, А. В. Холостенко та ін. Одеса : ОДУВС, 2016. 112 с.

20. Тактичний кримінальний аналіз: теорія та практика; навчальний посібник / О.Є. Користін, Н.П. Свиридюк, О.М. Цільмак, О.М. Заєць, К.Ю. Ісмайлов, В.А. Некрасов; МВС України, ДНДІ, ОДУВС. Одеса: РВВ ОДУВС, 2019. 216 с.

21. Балтовський О.А., Ісмайлов К.Ю., Сіфоров О.І., Форос Г.В., Заєць О.М. Теорія систем і системний аналіз: навчальний посібник / За заг. ред. д. т. н., доц. О.А. Балтовського. Одеса: ОДУВС, 2020. 156 с.

22. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : ЛьвДУВС, 2021. 288 с.

23. Кисельов А.О., Копилов Е.В., Худенко Д.М. Основи кримінального аналізу: навчальний посібник. Дніпро: ДДУВС, 2023. 163 с.

24. Овсянюк Д.І. Методологічні засади тактичного аналізу та аналізу оперативних даних під час розслідування злочинів, пов'язаних з незаконним обігом наркотиків : метод. рек. Київ : НАВС, 2024. 50 с.

25. Прокоф'єва-Янчиленко Д.М. Оцінювання загроз тяжкої та/або організованої злочинності в Україні: методичні рекомендації. Київ: МНДЦ, 2022. 44 с.

26. Internet Organised Crime Threat Assessment (IOCTA) 2023 : report / European Police Office (Europol). The Hague : Europol, 2023. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023.

27. Засоби аналітичної розвідки. Основи роботи в i2 Analyst's Notebook : навч.-практ. посіб. / [А. Даль, С. Наумюк, Є. Рибинський та ін.] ; Служба безпеки України, Ін-т Служби безпеки України Нац. юрид. ун-ту ім. Ярослава Мудрого. – Харків : Право, 2024. 306 с.

28. Виявлення за допомогою технологій кримінального аналізу фактів розтрати, привласнення чи заволодіння коштами державного бюджету на основі даних з Державного реєстру речових прав на нерухоме майно : практ. посібн. / [за заг. ред. В. Школьнікова та О. Корнейка]. К. : НАВС, 2020. 180 с.

29. Обробка та аналіз інформації про протиправні транзакції криптоактивів : практ. посібн. / В. Школьніков,

О. Корнейко, Ю. Орлов; за заг. ред. О. Корнейка. К. : НАВС, 2021. 134 с.

30. Кластерний аналіз телефонного трафіку: практ. посібн. / [за заг. ред. В. Школьнікова та О. Корнейка]. К. : НАВС, 2020. 40 с.

31. Guidebook on Intelligence-Led Policing: Transnational Threats Department's Strategic Police Matters Unit, OSCE. Vienna: OSCE Secretariat, 3 July 2017. URL: https://www.osce.org/files/f/documents/d/3/327476.pdf.

32. Lesson 6: Intelligence-led Policing // Specialised Training Materials for UN Police. 2021. URL: https://resourcehub01.blob.core.windows.net/training-files/Training%20Materials/024%20STM-UNPOL/024-012%20UNPOL%20STM%20Lesson%206%20Intelligence-led%20Policing.pdf.

Цуцкірідзе Максим Сергійович,
перший заступник Голови Національної поліції України – начальник Головного слідчого управління, доктор юридичних наук, професор

ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ КРИМІНАЛЬНОГО АНАЛІЗУ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРОГАЛИНИ В ЗАКОНОДАВЧОМУ РЕГУЛЮВАННІ

Сучасний етап розвитку кримінального процесу характеризується зростаючою потребою у впровадженні науково обґрунтованих, системних та технологічно сучасних методів аналізу інформації, що стосується злочинності. Це зумовлено низкою об'єктивних чинників: зростанням складності організації злочинної діяльності, поширенням її транснаціонального характеру, активним використанням сучасних комунікаційних технологій злочинцями, а також накопиченням значних обсягів інформації, яка потребує ретельного опрацювання.

У таких умовах традиційні підходи до збирання та оцінки доказової інформації часто виявляються недостатньо ефективними для своєчасного виявлення всіх обставин кримінального правопорушення, встановлення його учасників, зв'язків між ними та прогнозування подальших дій злочинної

групи. Для подолання цих викликів правоохоронні органи потребують сучасних аналітичних інструментів, здатних забезпечувати системну обробку різнорідних відомостей, виявляти приховані закономірності та зв'язки, а також формувати науково обґрунтовані висновки для прийняття процесуальних рішень.

До таких методів належить кримінальний аналіз, що передбачає системне збирання, опрацювання та інтерпретацію інформації про криміногенну ситуацію, злочинну діяльність та її учасників.

Попри визнану практичну значущість кримінального аналізу для правоохоронних органів, його правовий статус та можливість використання результатів аналізу у кримінальному провадженні в Україні залишаються неврегульованими або фрагментарно врегульованими. Це створює низку практичних та теоретичних проблем, які потребують ґрунтовного дослідження.

У науковій літературі кримінальний аналіз визначається як специфічний вид інформаційно-аналітичної діяльності правоохоронних органів, що полягає у перевірці, оцінці та інтерпретації інформації, встановленні зв'язків між даними, отриманими під час виявлення, припинення та розслідування кримінальних правопорушень і важливими для оперативно-розшукової діяльності та кримінального провадження, з метою їх використання правоохоронними органами й судом, а також для подальшого проведення оперативного, тактичного й стратегічного аналізу [1, с. 21; 2. с. 145].

Слід відзначити, що попри те, що підрозділи кримінального аналізу вже тривалий час функціонують у системі Національної поліції, сам термін «кримінальний аналіз» досі не має законодавчого визначення, а також відсутнє нормативне регулювання процедури його здійснення.

Водночас у Законі України «Про Бюро економічної безпеки України» законодавець надає визначення цього терміну в контексті протидії кримінальним правопорушенням у сфері економіки. Так, у ст. 2 закону зазначається, що кримінальний аналіз – це інформаційно-аналітична діяльність, спрямована на встановлення взаємозв'язків між даними про злочинну діяльність та іншими даними, потенційно з ними пов'язаними, їх оцінювання та інтерпретацію, прогнозування розвитку досліджуваних подій з метою їх використання для виявлення,

припинення та розслідування кримінальних правопорушень, що посягають на функціонування економіки держави [3].

Проведення кримінального аналізу передбачено пунктом 21 статті 8 Закону України «Про оперативно-розшукову діяльність», який уповноважує оперативні підрозділи безпосередньо здійснювати або ініціювати його для виконання завдань оперативно-розшукової діяльності [4].

У практичній діяльності результати кримінального аналізу можуть: допомагати формулювати версії слідства; сприяти виявленню організованих злочинних груп та злочинних організацій; обґрунтовувати підозру або планувати заходи з її перевірки; полегшувати взаємодію між правоохоронними органами. Таким чином, кримінальний аналіз має потенціал стати інструментом підвищення ефективності досудового розслідування.

Попри зазначене, у контексті здійснення кримінального провадження, чинний КПК України не відносить результати кримінального аналізу до процесуальних джерел доказів [5]. У зв'язку із цим, можна виокремити такі ключові прогалини законодавства:

відсутність офіційного законодавчого визначення кримінального аналізу (немає єдиного визначення у законах чи підзаконних актах, що створює різночитання у розумінні його змісту та призначення);

неврегульований статус результатів кримінального аналізу (у кримінальному провадженні не визначено, чи можуть такі результати бути джерелом доказів або підставою для проведення слідчих (розшукових) та негласних слідчих (розшукових) дій);

відсутність процесуальних гарантій достовірності (процедури документування, збереження та перевірки результатів кримінального аналізу не закріплені законодавчо, що створює ризики фальсифікації, підтасовки або втрати даних);

неврегульований порядок взаємодії між суб'єктами (відсутній механізм обміну результатами кримінального аналізу між різними правоохоронними органами, зокрема між підрозділами поліції, СБУ, ДБР, прокуратурою);

проблеми міжнародної співпраці (українське законодавство не повній мірі адаптовано до стандартів Європолу чи Інтерполу щодо обміну аналітичними продуктами).

Таким чином, наявні прогалини у правовому регулюванні обмежують можливість ефективного використання результатів кримінального аналізу у кримінальному процесуальному доказуванні. Це створює ризики визнання таких доказів недопустимими та ускладнює міжнародну співпрацю у протидії організованій злочинності.

У зв'язку з цим видається, що правильним шляхом вирішення окреслених проблем є усунення виявлених прогалин шляхом законодавчого визначення поняття, мети та завдань кримінального аналізу, а також встановлення процедури документування його результатів. Необхідно, зокрема, врегулювати критерії їх допустимості як доказів і порядок обміну між правоохоронними органами.

Підсумовуючи, слід зазначити, що кримінальний аналіз є ефективним інструментом боротьби зі злочинністю, який дозволяє оперативно виявляти зв'язки між злочинами та їх суб'єктами, прогнозувати криміногенні процеси й підвищувати ефективність досудового розслідування. Водночас законодавство України наразі не забезпечує належного правового підґрунтя для його повноцінного використання у кримінальному провадженні. Усунення наявних прогалин потребує системного підходу та міжвідомчої співпраці з урахуванням міжнародного досвіду. Внесення змін і доповнень до чинного законодавства сприятиме підвищенню якості досудового розслідування, зміцненню правових гарантій учасників процесу та ефективнішій протидії організованій злочинності.

Список використаних джерел

1. Мовчан А.В. Актуальні проблеми впровадження в органах національної поліції України моделі поліцейської діяльності, керованої аналітикою. *Соціально-правові студії*. 2018. Випуск 1. С. 17–22.

2. Моца В.В. Теоретико-методологічні засади використання кримінального аналізу оперативними підрозділами правоохоронних органів України. *Науковий вісник Ужгородського Національного Університету*, 2022. с. 141–147.

3. Про Бюро економічної безпеки України : Закон України від 28 січ. 2021 р. № 1150-IX. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/1150-20.

4. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. Верховна Рада України : [сайт] URL: https://zakon.rada.gov.ua/laws/show/2135-12.

5. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

Чепурна Тетяна Володимирівна,
аспірант кафедри криміналістики
та судової медицини Національної
академії внутрішніх справ

ДОПИТ ПІДОЗРЮВАНИХ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, УЧИНЕНИХ ПРАЦІВНИКАМИ ПРАВООХОРОННИХ ОРГАНІВ

Допитом називають слідчу (розшукову) дію, яка являє собою регламентований кримінальними процесуальними нормами інформаційно-психологічний процес спілкування осіб, які беруть у ньому участь, спрямований на отримання інформації про відомі допитуваному факти, що мають значення для розслідування [1, с. 264]. Процесуальний порядок допиту під час досудового розслідування визначений статтями 42, 56, 66, 95–97, 133, 223–226, 232, 256 КПК України [2].

На практиці – це одна з найбільш складних слідчих (розшукових) дій. Складність допиту визначається не тільки тим, що слідчому нерідко протистоїть особа, яка не бажає давати показання, але й тим, що у показаннях добросовісної особи, яка допитується, можуть міститися помилки, перекручування і вигадки, які необхідно виявити і врахувати на шляху встановлення об'єктивних обставин кримінального провадження. Тому допит вимагає від слідчого високої професійної майстерності [3, с. 440].

Згідно ст. 42 КПК України, підозрюваним є особа, якій у порядку, передбаченому статтями 276–279 КПК України, повідомлено про підозру, особа, яка затримана за підозрою у вчиненні кримінального правопорушення, або особа, щодо якої складено повідомлення про підозру, однак його не вручено їй внаслідок невстановлення місцезнаходження особи, проте вжито заходів для вручення у спосіб, передбачений КПК України для вручення повідомлень [2].

За результатами аналізу слідчої практики можна дійти висновку, що підстави повідомлення особі про підозру (ч. 1 ст. 276 КПК України) залежно від кількості доказів, які її обґрунтовують, умовно можна поділити на два види:

1. Слідчому (прокурору) вже достовірно відомо про факт учинення кримінального правопорушення певною особою: зібрані достатні докази для підозри особи у вчиненні кримінального правопорушення.

2. Доказів ще замало, знання слідчого (прокурора) на цьому етапі ще є невизначеними, неповними, уривчастими, а висновок про вчинення кримінального правопорушення певною особою можна зробити лише на підставі того, що вона затримана на місці вчинення кримінального правопорушення чи безпосередньо після його вчинення (п. 1 ч. 1 ст. 276 КПК України).

Але у будь-якому випадку підозра – це попередній висновок про причетність особи до вчинення кримінального правопорушення, припущення, яке має бути перевірено та оцінено в сукупності з усіма доказами [4, с. 126, 127].

У контексті розслідування службових кримінальних правопорушень, учинених працівниками правоохоронних органів, під час проведення допиту працівника правоохоронного органу як підозрюваного необхідно враховувати його професійну обізнаність з процедурою допиту. Слідчий повинен бути готовим до професійних форм протидії з боку допитуваного (зокрема, й уникнення прямих відповідей на запитання, маніпулювання фактами, відвернення уваги від ключових обставин події). Тому його дії повинні ґрунтуватися на високому рівні юридичної підготовки, комунікативній гнучкості та ретельному володінні тактикою допиту.

Допит підозрюваного є слідчою (розшуковою) дією, яка дозволяє безпосередньо отримати інформацію про його бачення обставин інкримінованого кримінального правопорушення, його позицію щодо повідомленої підозри, а також виявити джерела потенційних доказів. У кримінальних провадженнях щодо службових кримінальних правопорушень, учинених працівниками правоохоронних органів, допит підозрюваного набуває особливого значення як з процесуальної, так і з тактичної точки зору.

Справедливим у даному аспекті видається твердження О. В. Вахрушева, про те, що допит підозрюваного має важливе значення під час розслідування службової недбалості. Це пояснюється, перш за все, тією обставиною, що службова особа, яка вчинила протиправні дії або бездіяльність, володіє суттєвим обсягом інформації про обставини кримінального правопорушення. Тому одержання максимально повних і правдивих показань від цієї особи значно сприяє всебічному розслідуванню. Крім того, в ході допиту підозрюваний висловлює своє ставлення до аргументів сторони обвинувачення, надає аргументи як на їх користь, так і спростування. Це дозволяє слідчому визначити подальші напрями розслідування, більш ретельно перевірити версії щодо різних обставин кримінального правопорушення, забезпечуючи таким чином повноту досудового розслідування [5, с. 167].

Складність допиту працівника правоохоронного органу як підозрюваного полягає в тому, що така особа, як правило, має досвід безпосередньої участі в аналогічних процесуальних діях, добре обізнана з процедурою і тактичними прийомами допиту, уміло користується своїми процесуальними правами. Часто такі особи використовують тактику протидії як активну та і пасивну, зокрема, надають пояснення, спрямовані на дискредитацію доказів сторони обвинувачення, висувають альтернативні версії подій або ж взагалі відмовляються від дачі показань, посилаючись на ст. 63 Конституції України. У таких випадках особливого значення набуває вміння слідчого налагодити психологічний контакт з допитуваним, оцінити мотиви поведінки підозрюваного та уміло використовувати тактичні прийоми, що докладно розглянуті в науковій літературі.

Також важливо враховувати, що службові кримінальні правопорушення часто пов’язані з тривалими службовими відносинами, корпоративною лояльністю та можливою домовленістю між учасниками події. Тому, з урахуванням слідчої ситуації, допит підозрюваного може бути частиною тактичної операції, яка повинна включати одночасну роботу з документами, свідками, технічними засобами фіксації інформації та результатами негласних слідчих (розшукових) дій.

Предмет допиту підозрюваних в досліджуваних кримінальних провадженнях, зокрема, охоплює:

– ставлення особи до повідомленої підозри (визнання чи заперечення вини, висунення альтернативної версії події);

– посадові обов'язки та повноваження підозрюваного на момент вчинення кримінального правопорушення;

– обставини вчинення інкримінованого діяння (місце, час, спосіб, учасники події);

– наявність або відсутність у підозрюваного умислу на вчинення кримінального правопорушення;

– мотиви поведінки підозрюваного у відповідній ситуації (службова необхідність, особиста вигода, тиск керівництва тощо);

– наявність і місцезнаходження службових документів, що готувалися, підписувалися або використовувалися під час вчинення кримінального правопорушення;

– поведінка підозрюваного після вчинення кримінального правопорушення (чи були спроби приховати сліди, знищити документи, вплинути на свідків тощо);

– взаємини підозрюваного з іншими особами, що можуть бути причетними до події (співучасниками, свідками або колегами);

– ставлення підозрюваного до пред'явлених доказів (показань свідків, документів, відео- або аудіозаписів, результатів негласних слідчих (розшукових) дій тощо);

– походження майна, грошових коштів, а також подарунки, що можуть свідчити про корупційний характер інкримінованого діяння.

Допит підозрюваного у досліджуваних кримінальних провадженнях є не лише джерелом пояснень щодо тих чи інших фактів, а й засобом виявлення суперечностей, неправдивих тверджень у його показаннях. Аналіз змісту показань підозрюваного дозволяє виявити спроби ухилення від прямої відповіді, маніпуляції фактами або навмисного спотворення обставин події. Особливого значення при цьому набуває зіставлення його показань з іншими джерелами доказів у кримінальному провадженні – показаннями свідків, документами, висновками судових експертиз, матеріалами негласних слідчих (розшукових) дій тощо. У разі виявлення розбіжностей слідчий повинен реагувати, ставлячи підозрюваному уточнюючі або контрольні запитання з метою

перевірки послідовності та логічності його пояснень. Такий комплексний підхід сприятиме формуванню об'єктивної картини події та встановленню істини у кримінальному провадженні.

Таким чином, допит підозрюваних у кримінальних провадженнях про службові кримінальні правопорушення, вчинені працівниками правоохоронних органів, є надзвичайно складним і трудомістким процесом. Його ефективність значною мірою залежить від професійної підготовки слідчого, володіння тактичними прийомами допиту, здатності до аналітичного мислення, а також уміння адаптуватися до поведінкової моделі допитуваної особи, яка має високий рівень обізнаності з процедурою розслідування. Успішне проведення цієї слідчої (розшукової) дії дасть змогу забезпечити не лише отримання релевантної інформації, а й формування повноцінної доказової бази. У сукупності це створює передумови для всебічного, повного та об'єктивного встановлення обставин службового кримінального правопорушення та притягнення винних до відповідальності.

Список використаних джерел

1. Криміналістика : підручник для студентів вищих навчальних закладів / К. О. Чаплинський, О. В. Лускатов, І. В. Пиріг, В. М. Плетенець, Ю. А. Чаплинська. Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ ; Ліра ЛТД, 2014. 380 с.

2. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651–VI. URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text.

3. Криміналістика : підручник/[В.В. Пясковський, Ю.М. Чорноус, А.В. Самодін та ін.] ; за заг. ред. В.В. Пясковського. 2-ге вид. Київ : Філія вид-ва «Право», 752 с.

4. Розслідування прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою : навчальний посібник / С.С. Чернявський, В.Г. Дрозд, А.П. Запотоцький, Ю.М. Чорноус, Л.В. Гаврилюк та ін. Київ : 7БЦ, 2023. 252 с.

5. Вахрушев О.В. Методика розслідування службової недбалості : дис. … доктора філософії за спеціальністю 081 «Право». Харків, 2021. 246 с.

Шаповаленко Євген Володимирович,
професор кафедри оперативно-розшукової діяльності та національної безпеки Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

Штучний інтелект сьогодні розглядається як один із найпотужніших інструментів вивчення, обробки та генерації інформації. Його поява позначила новий етап у цифровій трансформації суспільства, докорінно змінивши способи взаємодії з інформаційним середовищем. На відміну від традиційних пошукових систем, які лише спрямовують користувача до джерел, системи штучного інтелекту здатні надавати миттєві відповіді, формуючи цілісні інформаційні конструкції. Однак постає питання: наскільки ці відповіді є достовірними?

Згідно з даними з 2013 по 2024 рік, залучили у розвиток штучного інтелекту 471 млрд доларів приватних інвестицій. Ця сума перевищує надходження в усіх інших країнах світу, узятих разом (289 млрд доларів). Серед лідерів також Китай (119 млрд дол.), Велика Британія (28 млрд дол.), Канада та Ізраїль (по 15 млрд дол.).

Статистика наведена зі звіту про Індекс ШІ за 2025 рік Стенфордського інституту людиноорієнтованого штучного інтелекту. Щодо даних за останній рік, то за цей період США зберігає беззаперечне лідерство – приватні інвестиції в штучний інтелект зросли до 109,1 млрд дол. - майже в 12 разів більше, ніж у Китаї (9,3 млрд дол.).

Сектор генеративного штучного інтелекту залучив 20% усіх приватних інвестицій в ШІ. Цифри досягли $33,9 млрд у 2024 році, що на 18,7% більше, ніж у 2023 році.

Уряди по всьому світу нарощують свою частку інвестицій у ШІ. Канада анонсує 2,4 мільярда доларів, Китай запустив фонд напівпровідників на 47,5 мільярда доларів, Франція виділила 109 мільярдів євро, Індія планує вкласти 1,25 мільярда доларів тощо [1].

ШІ працює на основі великих масивів даних, що визначає його ефективність, але водночас породжує низку етичних дилем. Однією з ключових проблем є якість вхідних даних: алгоритми опрацьовують доступні ресурси інтернету, часто без фільтрації за критерієм достовірності. Це створює ризик формування дезінформації в самій основі роботи ШІ, що, у свою чергу, може призвести до поширення спотвореної чи маніпулятивної інформації.

Один із найгостріших викликів у сфері дезінформації - це вплив спеціально організованих інформаційних кампаній на якість інформаційного середовища, у якому функціонують системи штучного інтелекту. Важливе емпіричне підґрунтя для цього становить оновлений звіт американського аналітичного центру American Sunlight Project, присвячений масштабній дезінформаційній мережі під назвою «Правда», що діє під патронатом Російської Федерації [2].

Мережа «Правда» не створює первинного контенту, а займається масовим тиражуванням та рециркуляцією фейкових повідомлень через різні онлайн-ресурси. Згідно з даними дослідження, ця структура була запущена у квітні 2022 року та орієнтована на багатомовну аудиторію, включаючи англомовні, українськомовні, польськомовні, франкомовні, іспаномовні та німецькомовні сегменти. Вона охоплює близько 150 доменів, розміщених у 49 країнах, публікуючи матеріали на 10 мовах [2].

Аналіз вмісту сайтів, пов’язаних із мережею, свідчить про існування ретельно спланованої пропагандистської архітектури, що маскується під національні та міжнародні медіа. Ці ресурси активно поширюють російські наративи, апелюють до матеріалів кремлівських інформаційних каналів та є складовою частиною ширших інформаційно-психологічних операцій, спрямованих як на українське суспільство, так і на світову громадськість.

Одним із найбільш тривожних аспектів дослідження є викриття процесу, який дослідники назвали LLM Grooming - цілеспрямоване інформаційне насичення простору з метою впливу на великі мовні моделі (LLM). Цей процес передбачає штучне формування інформаційного фону через генерацію в середньому 3,6 мільйона статей на рік, що публікуються на численних сайтах, симулюючи незалежні джерела. Основна мета – вбудувати повторювані пропагандистські патерни у

навчальні та пошукові масиви, які використовують мовні моделі. Через системне повторення одних і тих самих повідомлень у різних формулюваннях, створюється ілюзія легітимності, яку модель ШІ сприймає як норму [2].

Окрему увагу приділено явищу «наративного відмивання» (narrative laundering) – стратегії повторного поширення хибної інформації через множину псевдо незалежних джерел, що посилює довіру до неї з боку ШІ. Ці техніки супроводжуються SEO-оптимізацією сайтів-джерел, що збільшує ймовірність їх потрапляння у верхні позиції результатів пошуку та обробки мовними моделями.

NewsGuard, яка спеціалізується на оцінці надійності інформаційних ресурсів, провела тестування 10 чат-ботів на основі ШІ, використовуючи 15 ключових наративів мережі «Правда». Методологія включала три типи запитів: стиль «невинного користувача», стиль агресивного вимагання відповіді, а також стиль, орієнтований на отримання перевіреної інформації. Результати виявили серйозні загрози:

– 33,3 % відповідей чат-ботів містили фейкові наративи;

– 18,2 % – уникнули відповіді;

– лише 48,2 % – намагалися спростувати дезінформацію.

Проте навіть у цих випадках моделі часто посилалися на ненадійні джерела.

Ці дані засвідчують, що навіть найсучасніші системи ШІ залишаються вразливими до стратегічного маніпулювання інформацією, особливо коли таке маніпулювання здійснюється на системному рівні. У цьому контексті боротьба з дезінформацією потребує не лише алгоритмічної точності, а й інституційного регулювання, етичної відповідальності та постійного моніторингу інформаційного середовища, у якому функціонує ШІ [3].

Поширення дезінформації у цифровому середовищі, зокрема через багатомовні пропагандистські мережі на кшталт «Правда», свідчить про системну та стратегічну трансформацію інформаційної війни. Сучасні технології штучного інтелекту – особливо великі мовні моделі – виступають як інструмент, що одночасно може бути використаний як для поширення, так і для протидії дезінформації.

Однією з найбільш тривожних тенденцій є використання LLM для автоматизованого створення фейкових наративів, що

ускладнює верифікацію інформації. Крім того, інструменти типу діпфейків досягли такого рівня розвитку, що людина самостійно вже не здатна відрізнити фальсифіковане відео від справжнього, і в майбутньому, ймовірно, лише інший ШІ зможе це зробити. Ще одна загроза - створення ресурсів, які орієнтовані не на людське споживання, а на інші цифрові системи (включно з ШІ), що фактично свідчить про появу симулятивного інформаційного середовища [2].

Проблема ускладнюється тим, що ініціатори дезінформаційних кампаній більше не намагаються приховати своє втручання, а радше демонстративно випробовують межі допустимого у глобальному інформаційному полі. Це створює нові виклики як для розробників технологій, так і для державного та наднаціонального регулювання.

Аналізуючи проблематику зазначеного питання пропонуємо наступні шляхи вирішення:

– розробка систем контрнаративів (створювання системи фільтрації інформації на рівні мовних моделей, які можуть розпізнавати ознаки дезінформації та джерело походження інформації);

– регулювання навчальних датасетів (встановлення нормативних обмежень на використання відкритих даних із сумнівних або фейкових джерел у процесі навчання великих мовних моделей);

– інституціональне блокування дезінформаційних ресурсів (створення механізмів санкцій та блокування сайтів, які систематично поширюють фейки, включаючи інструменти автоматизованої ідентифікації таких доменів);

– розвиток ШІ-детекторів фейків (створення спеціалізованих моделей ШІ, орієнтованих на розпізнавання діпфейків, маніпулятивних повідомлень і синтетичних текстів);

– етична відповідальність і цифрова освіта (розвивати цифрову освіту, етичні підходи до створення та використання ШІ).

У підсумку можна зазначити, що інформаційна безпека під час використання ШІ залежить не лише від технологій, а й від політичної волі, міждержавної координації та суспільної обізнаності. Оскільки цифрова інформація дедалі більше стає стратегічним ресурсом, боротьба за її достовірність є невід'ємною частиною геополітичної стабільності та демократичної легітимності.

Список використаних джерел

1. Розвиток штучного інтелекту – США вклали грошей більше, ніж інші країни разом взяті. URL: https://renews.com.ua/tehnologiyi/rozvitok-shtychnogo-intelekty-ssha-vklali-groshei-bilshe-nij-inshi-krayini-razom-vziati/.

2. A well-funded Moscow-based global ‘news’ network has infected Western artificial intelligence tools worldwide with Russian propaganda. URL: https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global.

3. Мережа ZOV/Pravda-вебсайтів: як російська пропаганда насаджує власні наративи. URL: https://spravdi.gov.ua/merezha-zov-pravda-vebsajtiv-yak-rosijska-propaganda-nasadzhuye-vlasni-naratyvy.

Шевчишен Артем Вікторович,
заступник начальника Головного слідчого управління Національної поліції України – начальник управління організації роботи та методичного забезпечення, доктор юридичних наук, професор

КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ДОПОМІЖНИЙ ІНСТРУМЕНТ ФОРМУВАННЯ ТА ЗБИРАННЯ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

У сучасних умовах боротьби зі злочинністю правоохоронні органи зіштовхуються з новими, дедалі складнішими викликами, зумовленими високим рівнем латентності злочинів, зростанням масштабів та організованості злочинних угруповань, а також багаторівневою і часто транснаціональною структурою взаємозв’язків між учасниками протиправної діяльності. Злочини дедалі частіше вчиняються із використанням складних схем конспірації, цифрових технологій, підставних осіб та фіктивних суб’єктів господарювання, що значно ускладнює традиційні методи досудового розслідування.

З огляду на зазначені вище обставини, на сучасному етапі важливо впроваджувати нові підходи у протидії злочинності та розвивати нові навички для оптимального опрацювання інформації оперативними працівниками. Цей процес базується

на системному аналізі різноманітних даних. Ключова роль в цьому процесі сьогодні відводиться кримінальному аналізу, який, у класичному розумінні спрямований на ідентифікацію та точне встановлення зав'язків між відомостями про події злочинного характеру, особами, залученими до них, та інформацією з різних джерел. Результати цього аналізу мають бути використані органами досудового розслідування та прокуратурою для подальшого розслідування та прийняття відповідних процесуальних рішень [1, с. 398].

У вітчизняній науці кримінальний аналіз досліджується на стику кримінального процесу, криміналістики, оперативно-розшукової діяльності та інформаційної аналітики. Окремі питання, пов'язані з доказуванням, доказовою інформацією та аналітичним супроводом кримінального провадження, стали предметом наукових досліджень ряду вчених, зокрема О.В. Капліної, В.В. Вапнярчука, М.В. Гуцалюка, А.В. Мовчана, М.В. Корнієнка. Водночас у правозастосовній практиці поняття кримінального аналізу ще не отримало належного розвитку та нормативного закріплення, що стримує його ефективне використання.

У зв'язку з цим науковцями справедливо наголошується на необхідності постійного вдосконалення кримінального аналізу, який повинен адаптуватися до динамічних змін у сфері як міжнародного, так і національного права, враховуючи сучасні виклики правозастосовної практики, глобалізаційні процеси, транснаціональний характер злочинності та зростаючі вимоги до ефективності правового реагування [2].

Разом з цим, на сучасному етапі розвитку кримінальної процесуальної діяльності спостерігається поступове, але впевнене впровадження методів кримінального аналізу у практичну діяльність слідчих підрозділів Національної поліції України. Попри певні законодавчі та технічні виклики, вже сьогодні можна говорити про значні позитивні результати застосування цього інструменту для формування та збирання доказової бази у кримінальному провадженні.

Передусім, кримінальний аналіз дозволяє здійснювати систематизоване збирання інформації, яка має значення для кримінального провадження. Йдеться не лише про суто процесуальні джерела, як-от протоколи слідчих (розшукових) дій чи висновки експерта, а й про великий масив вторинної,

непрямої, але вкрай цінної інформації: цифрові сліди, телекомунікаційні з'єднання, банківські транзакції, соціальні зв'язки тощо. Завдяки аналітичній обробці цих даних можливо встановити зв'язки між подіями, виявити закономірності у поведінці підозрюваних, підтвердити або спростувати їхню участь у злочині.

Особливо ефективним є використання кримінального аналізу у розслідуванні організованої злочинної діяльності, де традиційні методи збору доказів не завжди дозволяють охопити всю структуру злочинної організації. Аналітик здатен зібрати й візуалізувати інформацію про всі елементи злочинної групи, показати зв'язки між її членами, визначити ключових координаторів, виконавців, забезпечення та логістику. Таким чином, слідчий отримує змогу не лише задокументувати окремі епізоди, а й встановити організаторів злочину.

Крім того, кримінальний аналіз сприяє формуванню цілісної доказової картини, яка дозволяє побачити злочин як систему дій і взаємодій, а не як ізольований акт. Це має надзвичайно важливе значення для подальшої кваліфікації дій підозрюваних, для обґрунтування умислу, встановлення мотивів і визначення ступеня вини кожного учасника.

На практиці важливу роль відіграє візуалізація зібраної інформації – схем, графів, діаграм, карт руху осіб і транспортних засобів, часових шкал подій. Це дає можливість як слідчому, так і прокурору чи суду краще зрозуміти суть справи, логіку доказів, механізми вчинення злочину. Такі інструменти, як Analyst's Notebook або спеціалізовані модулі BI-аналітики – лідери світового ринку програмних засобів для візуалізації та аналітичної обробки даних – дають змогу трансформувати складну інформацію та представляти її у вигляді зрозумілих схем і діаграм, що наочно відображають структуру злочинної діяльності [3, с. 208].

Окрему увагу слід приділити профілактичному потенціалу кримінального аналізу. Аналітичні висновки, зроблені на основі розслідування конкретного провадження, дозволяють виявити типові способи вчинення злочинів, слабкі місця у правозастосовній системі, на які можна впливати для недопущення подібних правопорушень у майбутньому. Це особливо актуально у сфері кіберзлочинності, торгівлі людьми, фінансових махінацій.

Варто зазначити, що кримінальний аналіз ефективно доповнює інші джерела доказів, але не замінює їх. Його основне завдання – дати логічну структуру зібраним фактам, виявити ключові докази, посилити їхню доказову силу через узгодженість, послідовність і логічну пов'язаність. Таким чином, аналітичні продукти можуть нести в собі як орієнтуючу функцію для подальших слідчих (розшукових) дій, так і підтверджувальну функцію для вже здобутих доказів, зібраних в порядку ст. 93 КПК України [4].

У практиці слідчих підрозділів Національної поліції України уже існують численні приклади, коли аналітичні розробки ставали основою для відкриття кримінальних проваджень, сприяли ідентифікації підозрюваних, або ж дозволяли знайти свідків, місце вчинення злочину чи знаряддя. Це яскраво підтверджує, що кримінальний аналіз вже сьогодні виступає реальним і дієвим інструментом в арсеналі доказування.

З огляду на викладене, можна зробити висновок: попри формальні прогалини в законодавстві, кримінальний аналіз демонструє високу прикладну ефективність у процесі збирання та формування доказів. Його інтеграція в практику розслідування сприяє не лише підвищенню якості доказової бази, але й загальній інтелектуалізації кримінального процесу, що відповідає сучасним європейським стандартам кримінальної юстиції.

Список використаних джерел

1. Корнієнко М.В. Кримінальний аналіз у діяльності Національної поліції України. *Право і суспільство № 1/2024. Т. 2*. С. 397–402.

2. Білоус Р. В., Василинчук В. І., Таран О. В. Використання методів кримінального аналізу під час оперативного провадження та досудового розслідування. *Науковий вісник Національної академії внутрішніх справ. 2021. № 1 (118)*. С. 131–137.

3. Бурангулов В.А. Кримінальний аналіз в правоохоронній діяльності : дис. д-ра філософії: за спеціальністю 081 Право. Одеса, 2024. 231 с.

4. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

Наукове видання

АКТУАЛЬНІ ПИТАННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КРИМІНАЛЬНОГО АНАЛІЗУ В ПРАВООХОРОННІЙ СИСТЕМІ УКРАЇНИ

Матеріали
міжвідомчої науково-практичної конференції
(Київ, 23 липня 2025 року)

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовників і розповсюджувачів видавничої продукції
Дк № 4155 від 13.09.2011.
Підписано до друку 24.09.2025. Формат 60x84/16. Папір офсетний.
Обл.-вид. арк. 8,75. Ум. друк. арк. 8,14