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, 17 листопада 2023 року)

Київ
2023

MINISTRY OF INTERNAL AFFAIRS OF UKRAINE
NATIONAL ACADEMY OF INTERNAL AFFAIRS
EUROPEAN UNION ADVISORY MISSION UKRAINE
NATIONAL POLICE OF UKRAINE
DEPARTMENT OF CRIMINAL ANALYSIS

CURRENT ISSUES AND PROSPECTS FOR THE DEVELOPMENT OF CRIMINAL ANALYSIS IN THE LAW ENFORCEMENT SYSTEM OF UKRAINE

Materials
of the Interdepartmental Scientific and Practical Conference
(Kyiv, November 17, 2023)

Kyiv
2023

УДК 343.97(477)(06)
А437

Рекомендовано до друку науково-методичною радою Національної академії внутрішніх справ від 24 жовтня 2023 року (протокол № 13)

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, 17 лист. 2023 р.) / [редкол.: С. С. Чернявський, Д. І. Овсянюк, В. В. Корольчук]. – Київ : Нац. акад. внутр. справ, 2023. – 159 с.

УДК 343.97(477)(06)

ЗМІСТ

ВІТАЛЬНІ СЛОВА

НАУКОВІ ДОПОВІДІ

Чернєй Володимир Васильович,
ректор Національної академії внутрішніх справ, доктор юридичних наук, професор

Шановні колеги та гості!

Від імені ректорату і Вченої ради Національної академії внутрішніх справ вітаю учасників міжвідомчої науково-практичної конференції «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України».

Академія вчергове приймає експертів у сфері інформаційно-аналітичної діяльності та кримінального аналізу для обміну досвідом, вирішення проблемних питань кримінального аналізу й визначення перспектив його розвитку. Серед спікерів й активних учасників конференції – відомі в Україні й знані за її межами вчені та фахівці-практики, які представляють Національну поліцію, Державну прикордонну службу, ДБР, БЕБ, СБУ, авторитетні заклади освіти й науково-дослідні установи правоохоронного спрямування.

Академія активно сприяє розвитку кримінального аналізу шляхом реалізації різноманітних науково-практичних, організаційних та освітніх ініціатив. Зокрема, у НАВС створено аналітичний відділ (Центр кримінальної аналітики), на який покладено, серед іншого, організаційно-координаційне управління щодо питань розвитку кримінального аналізу.

Кримінальний аналіз є потужним інструментом, який допомагає правоохоронним органам забезпечувати громадську безпеку, запобігати злочинам, документувати та розкривати їх, розшукувати злочинців, зокрема воєнних, розробляти тактику і стратегію протидії злочинності, а також підвищує готовність правоохоронної системи протидіяти новим загрозам.

Протягом майже двох років унаслідок повномасштабної агресії РФ наша держава постає перед численними викликами, зокрема у сфері правопорядку. Нашим спільним завданням є знаходження оптимальних рішень для підвищення ефективності діяльності правоохоронних органів і раціонального використання ресурсів. Це сприятиме впевненому поступу на шляху до перемоги, забезпечить виконання завдань, що будуть нагальними в період відновлення країни.

Тож вітаю всіх із початком роботи конференції та бажаю продуктивного та конструктивного діалогу.

Слава Україні!

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

Шановні колеги!

Від імені Національної поліції України хочу привітати всіх присутніх з початком роботи науково-практичної конференції, присвяченої питанням розвитку кримінального аналізу в правоохоронній сфері.

Такі наукові форуми – важливий крок на шляху вдосконалення поліцейської діяльності, можливість поділитися набутим досвідом й отримати нові знання, зокрема у сфері проведення аналітичної роботи.

Вимоги сьогодення ставлять перед підрозділами кримінального аналізу нові завдання. Для їх ефективного виконання необхідно брати на озброєння найсучасніші програмні компоненти, які ґрунтуються на інноваційних розробках, відшуковувати нові підходи до організації роботи кримінальних аналітиків, вивчати й аналізувати широкі масиви інформації з різноманітних джерел: відео- й аудіозаписів, інформації із соціальних мереж, відомостей про фінансові операції та активи фігурантів кримінальних проваджень.

За роки свого становлення служба кримінального аналізу перетворилася з невеликого відділу підрозділу інформаційної підтримки на розгалужену систему, яка діє на центральному, обласному й районному рівнях.

Створення чіткої аналітичної вертикалі та пошук нових шляхів реформування й удосконалення функціоналу служби засвідчують ефективність інформаційно-пошукової роботи та розвідувальної аналітики під час розкриття злочинів за гарячими слідами, передусім резонансних, тяжких та особливо тяжких.

Для того щоб практичні кроки були продуктивнішими, Національна поліція активно сприяє розбудові кадрового потенціалу підрозділів кримінального аналізу, зосереджує увагу на необхідності заміщення посад кримінальних аналітиків кваліфікованими спеціалістами й підвищенні фахового рівня працівників.

Нині функція кримінального аналізу з допоміжної перетворилася на ключовий компонент етапу планування стратегії розслідування злочинів і прийняття рішень.

Упровадження концепції поліцейської діяльності, ґрунтованої на збиранні й аналізі даних, надало можливість змістити акценти роботи поліції від реактивного, тобто реагування на вже вчинену кримінальну подію, на проактивний підхід, спрямований на попередження й запобігання злочинності.

Слід зазначити, що розбудова потенціалу кримінального аналізу відбувається завдяки постійній взаємодії Національної поліції із зарубіжними партнерами й закладами вищої освіти зі специфічними умовами навчання, що належать до сфери управління Міністерства внутрішніх справ України.

Тож висловлюю вдячність Національній академії внутрішніх справ за сприяння в організації сьогоднішнього заходу, а нашим міжнародним партнерам – за допомогу в розвитку кримінальної аналітики Національної поліції України.

Бажаю всім учасникам сьогоднішнього наукового заходу плідної роботи!

Бутко Роман Юрійович,
начальник Департаменту кримінального аналізу Національної поліції України

Шановні колеги!

Дозвольте привітати всіх учасників науково-практичної конференції та подякувати за запрошення взяти участь у цьому поважному заході.

Департамент кримінального аналізу Національної поліції України, який я представляю, високо цінує співпрацю з представниками закладів вищої освіти й наукових установ.

Специфіка роботи поліції загалом і кримінальних аналітиків зокрема полягає в динамічному характері та потребує постійного оновлення. Важливим кроком для цього є вивчення провідного українського та іноземного досвіду, наукової думки, адаптація їх до вимог сьогодення та потреб вітчизняної правоохоронної системи.

Розвиток поліцейської діяльності, керованої аналітикою, тісно пов'язаний з новаціями у сфері ІТ-технологій та розширенням можливостей одержання аналітичних даних. Нині служба кримінального аналізу використовує надсучасні, а часто унікальні, інформаційні та програмні можливості, що сприяє ефективнішій протидії злочинності.

У своїй практичній діяльності кримінальні аналітики збирають, обробляють й аналізують значні масиви інформації, пов'язаної з кримінальною подією, забезпечують аналітичну розвідку інформації стосовно фігурантів проваджень і їхніх зв'язків. Для виконання цих завдань, крім аналітичного мислення, потрібно мати професійні навички роботи з інноваційними сертифікованими програмними компонентами.

Ураховуючи це, ми докладаємо максимальних зусиль для підвищення професійності працівників підрозділів кримінального аналізу.

Саме тому одним з пріоритетних напрямів роботи служби є активізація взаємодії із закладами вищої освіти зі специфічними умовами навчання, що належать до сфери управління Міністерства внутрішніх справ України, серед яких Національна академія внутрішніх справ, яка є нашим надійним партнером.

Висловлюю вдячність колективу академії в особі ректора Володимира Чернєя за організацію конференції та співпрацю, спрямовану на підвищення ефективності служби кримінального аналізу, удосконалення системи поліцейської діяльності, керованої аналітикою, на підставі актуальних теоретичних і прикладних досліджень у цій сфері.

Бажаю всім учасникам конференції конструктивної роботи та професійних здобутків!

Афонін Дмитро Сергійович,
завідувач науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ОСОБЛИВОСТІ ПІДГОТОВКИ СПЕЦІАЛІСТІВ ЗА ОСВІТНІМ СТУПЕНЕМ «МАГІСТР» СПЕЦІАЛІЗАЦІЇ «КРИМІНАЛЬНИЙ АНАЛІЗ» НА БАЗІ ОДЕСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ

Сучасна правоохоронна діяльність, в умовах реформування сектору безпеки та державного управління, потребує оновлення концептуальних підходів до системи підготовки висококваліфікованих кадрів. Трансформація сучасної правоохоронної системи, відмова від її карального спрямування та соціальний попит на правоохоронця нової формації, який володіє компетентностями, необхідними для вирішення складних спеціалізованих завдань та практичних проблем у сфері правоохоронної діяльності під час охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку, зумовили формування цілей та програмних результатів навчання спеціалістів за освітнім ступенем «магістр» спеціалізації «Кримінальний аналіз» на базі Одеського державного університету внутрішніх справ.

У березні 2021 р. було затверджено галузевий стандарт вищої освіти за спеціальністю 124 «Системний аналіз» для другого (магістерського) рівня вищої освіти (наказ МОН України від 18.03.2021 р. № 331) [4], який було введено в дію у 2021 н.р. Від стейкхолдерів, робочої групи, здобувачів та академічної спільноти надійшли пропозиції щодо внесення змін до зазначених освітньо-професійних програм з метою їх покращення з урахуванням прийнятого стандарту вищої освіти, які було розглянуто Вченою Радою Одеського державного університету внутрішніх справ [5, с. 3].

Освітньо-професійна програма «Кримінальний аналіз» другого (магістерського) рівня вищої освіти за спеціальністю 124 «Системний аналіз» введена в дію Наказом ОДУВС від 05.05.2022 р. № 186 [5, с. 3].

Магістри за напрямом «Кримінальний аналіз» можуть працювати в наукових, освітніх, аналітичних, IT та інших установах і підрозділах на посадах, що вимагають застосування методів системного аналізу та кримінального аналізу. Програма є практико-орієнтована та спрямована на формування у здобувачів вищої освіти професійних компетентностей з обов'язковим опанування теоретичних та практичних аспектів у сфері системного аналізу. Освітньо-професійна програма передбачає системний підхід щодо поєднання загальної та спеціальної підготовки здобувачів вищої освіти за напрямам кримінального аналізу з використанням сучасних інформаційних технологій.

Випускники-магістри отримують наступні компетентності:

– знання основ теорії пізнання, методів аналізу, синтезу та моделювання систем і процесів у різних галузях людської діяльності, основних механізмів мислення та логічного виведення;

– знання універсальних і спеціалізованих мов програмування, мов імітаційного моделювання;

– знання сучасних методів математичного моделювання в науці, техніці, промисловості і сільському господарстві, моделювання та дослідження економічних, екологічних та соціальних процесів;

– розробка методів і алгоритмів оптимізації процесів;

– здійснення системного аналізу взаємопов'язаних процесів різної природи, формулювання критеріїв, обмежень та суттєвих факторів при розробленні моделей систем;

– розв'язування задач прогнозування процесів у динамічних системах;

– розробка алгоритмів підтримки прийняття рішень в умовах невизначеності, ризику та конфліктних операцій [5, с. 11].

Випускники, які пройшли ґрунтовну магістерську підготовку за спеціальністю 124 «Системний аналіз», будуть користуватися значним попитом у багатьох сегментах галузі 124 «Системний аналіз» в Національній поліції України, інших структурних підрозділах Міністерства внутрішніх справ, Служби безпеки України, Державному бюро розслідувань, Національному антикорупційному бюро України, Бюро економічної безпеки, Державній прикордонній службі тощо.

Освітній процес за напрямком кримінального аналізу спрямований перш за все на практичну складову. В зв'язку з чим значна роль у підготовці спеціалістів за освітнім ступенем «магістр» спеціалізації «Кримінальний аналіз» на базі

Одеського державного університету внутрішніх справ відведена науково-дослідній лабораторії з проблемних питань кримінального аналізу, яка є найбільш адаптованою до завдань, що стоять перед Національною поліцією України.

Лабораторія здійснює науково-дослідну роботу в рамках наукової теми: «Кримінальний аналіз у протидії злочинності». Окрім наукового складу лабораторії, активну участь у дослідженні питань теми науково-дослідної роботи лабораторії приймають слухачі магістратури.

Науковим складом лабораторії постійно здійснюється проведення тренінгів з різних питань кримінального аналізу. Так, у червні – липні 2023 року проведений тренінг з обсягом програми 120 годин, з яких 70 % практичного напрямку за темою «Пошук та аналіз інформації з відкритих джерел – Open source intelligence (OSINT)» для слухачів магістратури, а також всіх бажаючих підвищити свій рівень знань, щодо розвідки з відкритих джерел.

Лабораторією забезпечується практична складова навчального процесу шляхом налагодження взаємодії зі структурними підрозділами Міністерства внутрішніх справ, іншими правоохоронними та державними органами, а також правоохоронними органами іноземних держав, підприємствами, установами та організаціями незалежно від їх форм власності, з метою залучення їх до підготовки спеціалістів у галузі кримінального аналізу.

Так, налагоджена співпраця з Департаментом кримінального аналізу Національної поліції та в 2022 року підписаний договір про взаємодію. Продовжується співпраця з Консультативною місією Європейського Союзу. Це дозволяє проводити бінарні заняття та тренінги, залучаючи фахівців-практиків до навчального процесу.

На даний час в науково-дослідній лабораторії з проблемних питань кримінального аналізу закінчена робота над проєктом «Віртуальний полігон: огляд місця події». Створений навчальний сайт, який наповнений матеріалами навчально-практичного характеру освітньої платформи Virtual Education. Дана платформа наддасть можливість напрацьовувати практичні навички слідчого, спеціаліста-криміналіста та кримінального аналітика під час огляду місця події за фактами розслідування різних видів кримінальних правопорушень у віртуальному середовищі з ефектом присутності за допомогою окулярів віртуальної реальності. Проєкт «Віртуальний полігон: огляд місця події». На

освітній платформі Virtual Education вже впроваджений в навчальний процес Одеського державного університету внутрішніх справ, схвалений Департаментом освіти, науки та спорту МВС України і зараз проходить впровадження у закладах вищої освіти із специфічними умовами навчання МВС України.

Виходячи з вищевикладеного, можна констатувати, що Одеський державний університет внутрішніх справ спроможний здійснювати освітню діяльність з підготовки конкурентоспроможних магістрів зі спеціальності 124 «Системний аналіз» для задоволення потреб сучасного українського суспільства та ринку праці. Фахівці спеціальності «Кримінальний аналіз» у теперішній воєнний час вкрай необхідні на посадах в органах і підрозділах Міністерства внутрішніх справ України, Національної поліції України, Служби безпеки України, Прокуратури України, Національного антикорупційного бюро України, Національного агентства з питань запобігання корупції, Державної прикордонної служби України, Міністерства оборони України, Державної фіскальної служби України, Державної міграційної служби України тощо.

Список використаних джерел

1. Закон України «Про вищу освіту»: від 01.07.2014. Відомості Верховної Ради (ВВР), 2014, № 37–38, ст. 2004. URL: http://zakon4.rada.gov.ua/laws/show/1556-18.

2. Закон України «Про освіту»: від 05.09.2017. Відомості Верховної Ради (ВВР), 2017, № 38–39, ст. 380. URL: http://zakon5.rada.gov.ua/laws/show/2145-19.

3. Національний класифікатор України: Класифікатор професій ДК 003:2010. URL: https://zakon.rada.gov.ua/rada/show/va327609-10.

4. Про затвердження стандарту вищої освіти за спеціальністю 124 «Системний аналіз» для другого (магістерського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 18.03.2021 р. № 331. URL: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjc9peGpMeCAxXzQvEDHw0xqV_XqvP06FDyK8QggD-z&opi=89978449.

5. Концепція освітньої діяльності за освітньо-професійною програмою «Кримінальний аналіз» зі спеціальності 124 «Системний аналіз», що передбачає присвоєння професійної кваліфікації з професій, для яких запроваджено додаткове регулювання, на другому (магістерському) рівні вищої освіти. ОДУВС, Одеса, 2023.

6. Освітньо-професійна програма «Кримінальний аналіз» підготовки здобувачів другого (магістерського) рівня вищої освіти у галузі знань 12 «Інформаційні технології», спеціальності 124 «Системний аналіз» розроблена відповідно до стандарту вищої освіти за спеціальністю 124 «Системний аналіз», затвердженого наказом Міністерства освіти і науки України від 18.03.2021 р. № 331.

Бутко Роман Юрійович,
начальник Департаменту кримінального аналізу Національної поліції України

РОЗВИТОК СИСТЕМИ КРИМІНАЛЬНОГО АНАЛІЗУ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В СУЧАСНИХ УМОВАХ

Служба кримінального аналізу пройшла велику трансформацію за короткий проміжок часу. На жаль, поштовхом для цього стало повномасштабне вторгнення російської федерації.

Слід зазначити, що у 2016 році, з якого веде початок кримінальний аналіз в Національній поліції, злочинність уже користувалась всіма перевагами сучасних технологій, саме тому перед поліцією постало завдання пошуку гідного системного рішення.

Одним із таких рішень стала розбудова напряму кримінального аналізу.

Перший прецедент – це створення відділу, де було лише 5 аналітиків. Мови про створення повноцінного підрозділу не було [1].

У 2017 році вже самостійний підрозділ кримінального аналізу ввійшов до складу кримінальної поліції, почали активніше впроваджуватися новітні підходи в роботі та розкритті злочинів.

2019 рік став етапом переоцінки наявного досвіду та створення перших 5 територіальних підрозділів.

Пандемія коронавірусу SARS-CoV-2 навчила аналітиків працювати дистанційно, не втрачаючи якості в роботі. Цей досвід також став у нагоді під час повномасштабного вторгнення [2].

У 2022 році команда аналітиків збільшилася до 173 працівників. Попит на продукти кримінального аналізу збільшився у декілька разів. Аналітики посіли важливе місце у структурі поліції.

2022 року розпочалася розбудова столичної служби кримінального аналізу, створення в кожному районному управлінні поліції Києва секторів з трьох аналітиків [3]ю

Щодня кримінальні аналітики почали отримувати значну кількість інформації з «землі» та майже на 100 % перекрили вирішення робочих питань на місцевому рівні.

А на початку 2023 року цей досвід почав масштабуватися на всю державу.

На сьогодні підрозділи кримінального аналізу функціонують у кожному з 25 обласних управлінь поліції, а також створено 35 підрозділів на місцевому рівні (сектор кримінального аналізу відділу кримінальної поліції районного управління поліції).

Кількість працівників підрозділів кримінального аналізу на всіх рівнях складає більше 400 осіб, майже 70 % з них це аналітики-практики.

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.

Пріоритети діяльності підрозділів кримінального аналізу визначені з урахуванням успішних зарубіжних моделей та вимогами сьогодення. Крім інформаційно-аналітичного супроводження розкриття злочинів загальнокримінальної спрямованості, аналітики зосереджені на проведенні аналітичних досліджень у сфері ліквідації економічного підґрунтя для злочинної діяльності, зборі доказової бази воєнних злочинів країни-агресора, а також проведенні відеоаналітичних досліджень.

За сприяння й координації Міністерства внутрішніх справ аналітики Національної поліції розбудовують партнерство зі спорідненими службами системи МВС. Зокрема, йде активна співпраця з Центром стратегічного аналізу та прогнозування МВС України, а також Управлінням інформаційно-аналітичного забезпечення та кримінального аналізу Департаменту оперативно-розшукової діяльності Адміністрації Державної прикордонної служби України.

Зокрема, для ефективної взаємодії та стандартизованого підходу до виконання завдань, спеціально створеною робочою групою вживаються заходи з уніфікації аналітичних продуктів, організується оперативний обмін інформацією.

Основною метою є розширення можливостей кожного аналітика та служби в цілому. Пріоритетним є також раціональний розподіл аналітичних ресурсів.

Служба кримінального аналізу налагодила взаємодію з міжнародними партнерами та разом з ними організувала постійний навчальний процес.

Організовано навчальні заходи, стажування та курси. Аналітиками взято участь у значній кількості зустрічей на міжнародному рівні з представниками провідних правоохоронних організацій Європейського союзу.

Водночас умови, у яких живе суспільство, спонукали до створення підрозділу оперативного аналізу. Ідея була у тому, щоб один аналітик володів оперативною обстановкою у регіоні 24/7. На цей підрозділ також покладається функція комунікації з іншими службами та фіксація наслідків обстрілів. Під час реєстрації або виявленні злочину аналітик відразу виконує 5–7 заздалегідь визначених аналітичних завдань та швидко передає інформацію для оперативних працівників для розкриття чи документування злочину.

Такий «проактивний» підхід до використання ситуаційного аналітика був високо оцінений і на регіональному рівні.

Окремо у структурі підрозділів кримінального аналізу була виділена лінія, відповідальна за стратегічний аналіз – SOCTA. Це стало можливим після переосмислення пріоритетів, а також оцінки важливості аналізу не лише для конкретного правоохоронного органу, а й для держави в цілому [4].

Кожен аналітик закріплений за певною лінією аналізу. Співробітники, що займаються тактичним аналізом, орієнтовані на дослідження можливих тенденцій розвитку злочинності як в середині країни, так і за її межами.

Одним із останніх нововведень стала також розбудова відділу, відповідального за відео- та фотоаналіз [5].

Причина зрозуміла: кількість відеоматеріалу на одного аналітика з початку війни зростає у геометричній прогресії. Здійснюється аналіз сотень терабайтів відеоматеріалів по воєнним та інших злочинах. Упроваджується новітнє програмне забезпечення для аналізу з унікальними можливостями.

Робота відеоаналітика у таких умовах надзвичайно складна, оскільки він постійно має справу з пропагандистським матеріалом, фейками, інформаційно-психологічними операціями, а також з елементарно низькою якістю зображень.

Відеоаналіз в поєднанні з таким новими технологіями, як супутникові знімки, а також використання спеціалізованого програмного забезпечення розширюють можливості аналітичних підрозділів.

З самого початку повномасштабного вторгнення підрозділи кримінального аналізу були націлені на максимальне охоплення публікацій відеоматеріалів у відкритих джерелах, аналіз записів камер відеоспостереження. Разом з технічними спеціалістами впроваджені рішення для покращення якості фотозображень.

Ще одним пріоритетом розбудови служби є успішна інтеграція українського кримінального аналізу у світовий аналітичний простір. З цією метою в Департаменті створено відділ міжнародного співробітництва з обміну аналітичною інформацією. Вимоги до таких аналітиків високі – крім професійних знань і навичок від них вимагається вільне володіння іноземною мовою, а також основами міжнародного права та економіки [6].

Таким чином створюється своєрідний інститут офіцерів зв'язку у сфері розвідувальної аналітики, передусім з пошуку закордонних активів українського криміналітету та російського сліду у вітчизняній економіці.

Безперечно війна вплинула на функції та завдання підрозділів кримінального аналізу. Аналітик працює з матеріалами не лише звичного поліцейського формату, а й воєнних злочинів, пошуку активів ворога для відбудови України.

Аналітик – це не просто офіцер, а особа, що робить рішення оперативних підрозділів та слідчих обґрунтованими та ефективними. Він здатний зіставити шматочки інформації, звернути увагу на деталі. Під час війни він має діяти у незвичному полі.

Мотив злочину часто не містить логічного пояснення, жертви давно були змушені залишити країну, докази перебувають на окупованій території, а злочинці відчувають безкарність. Окрім цього, аналітик постійно має справу з великим обсягом повідомлень про злочини.

Від нього вимагається повна обізнаність у техніці, позивних, різновидах військової форми та інших деталях військових, причетних до злочину.

Під час розслідування воєнних злочинів аналітик забезпечує:

– максимальне охоплення ЗМІ для збору інформації, а також інших джерел, які висвітлюють воєнні події, в тому числі і ворожі, матеріали з попередніх конфліктів, а також їх збереження;

– документування відомостей і фактів, особливо в частині переміщення військових формувань та їх фіксації на певній території;

– фокусування на певній ділянці бойових дій, особливо під час гарячих фаз через масштабність подій та швидку зміну оперативної обстановки;

– обізнаність у використанні новітніх методів аналізу, у тому числі супутникових знімків.

За умови забезпечення переліченого, аналітик стає майже незамінним при розслідуваннях воєнних злочинів.

У короткий час аналітики адаптувалися до умов бойових дій та почали виконувати поставлені завдання під час блекаутів, повітряних тривог та обмежень комендантської години.

Установлення безвісті зниклих під час воєнних дій. Це аналітичне дослідження одне з найскладніших для відпрацювання як класичними методами, так і за допомогою аналітики. Дослідження такого змісту нагадують роботу з неструктурованим масивом інформації великого обсягу.

Повідомлення про зникнення рахуються тисячами і варіюються від повідомлень родичів, які втратили зв'язок з рідними, до зникнення осіб у ході окупації певних територій.

Інколи злочинці намагаються скористатися воєнним часом для приховання та інсценування вбивств чи грабежів. Таким чином зловмисники намагаються перекласти відповідальність на інших осіб, яких, на їхню думку, практично неможливо відстежити.

Тому правоохоронці приділяють максимальну увагу кожній справі про зникнення і відразу приступають до комплексу розшукових та аналітичних заходів. Така робота безпосередньо пов'язана з накопиченням та узагальненням величезного об'єму даних про зниклих осіб.

Кожна зникла людина відпрацьовується на предмет зв'язків та контактів, через які можна встановити її місце перебування. Проводиться відповідний моніторинг ЗМІ. Кожний випадок при цьому індивідуальний, але за кожним повідомленням стоїть доля людини.

На сьогодні можна констатувати, що за 2022 рік та 10 місяців 2023 року аналітики взяли участь у розкритті понад 25 тисяч злочинів, більшість з яких особливо тяжкі.

При використанні аналітичних інструментів значна увага приділяється дотриманню європейських стандартів захисту персональних даних GDPR [7]. Наші аналітики, як ніхто інший, розуміють важливість євроінтеграції в поліції та загальному курсі держави.

Процес розвитку підрозділів кримінального аналізу не зупинився, а навпаки отримав додатковий імпульс, що з одного боку поставив службу перед фактом відсутності часу на роздуми, а з іншого – вплинув на креативність при реалізації нових проєктів.

Це створює суттєве навантаження на кожного спеціаліста в цій галузі, але у свою чергу змушує брати на озброєння новітні технології на основі штучного інтелекту, хмарних обчислень та інших інновацій. А також особливу увагу звертати на розвиток людського потенціалу, підвищення ефективності роботи кримінальних аналітиків відповідно до завдань, окреслених у Комплексному стратегічному плані реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки [8].

У розбудові потенціалу служби одним із основних пріоритетів Департаменту кримінального аналізу є активна взаємодія з міжнародними партнерськими організаціями такими як Консультативна місія Європейського Союзу, (КМЄС), Місія регіонального програмного офісу Міжнародної програми підвищення кваліфікації органів кримінального розслідування (ICITAP) в Україні та відділ з правоохоронних питань (INL) Посольства США в Україні. За цей час відбулося близько 30 онлайн та офлайн зустрічей, на яких обговорювалися перспективи розвитку служби на основі світових стандартів кримінальної аналітики.

Також, уперше з моменту створення служби працівниками підрозділів кримінального аналізу всіх рівнів разом з більш ніж 800 аналітиками з 25 країн взято участь у 33-тій щорічній навчальній конференції, організованій «Міжнародною асоціацією кримінальних аналітиків» (IACA), що проходила у м. Даллас (штат Техас, США).

Список використаних джерел

1. Наказ Національної поліції України від 08 квітня 2016 року № 296.

2. Указ Президента України № 64/2022 «Про введення воєнного стану в Україні».
3. Наказ Національної поліції України від 22 червня 2022 року № 439.
4. Наказ Національної поліції України від 13 грудня 2022 року № 886.
5. Наказ Національної поліції України від 27 квітня 2023 року № 340.
6. Наказ Національної поліції України від 19 жовтня 2023 року № 952.
7. Регламент (ЄС) 2016/679 Європейського парламенту та Ради [Архівовано 26 травня 2018 у Wayback Machine] від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).
8. Указ Президента України від 11 травня 2023 року № 273/2023 «Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки».

Василинчук Віктор Іванович,
професор кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, доктор юридичних наук, професор;
Вишневський Сергій Анатолійович,
аспірант Національної академії внутрішніх справ

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ЦИФРОВОГО ДОВКІЛЛЯ В ПРОТИДІЇ ЕКОЛОГІЧНИМ ЗЛОЧИНАМ

Важко визначити точний масштаб незаконних доходів від екологічних злочинів, наявні ознаки вказують на те, що екологічні злочини є одними з найприбутковіших злочинів у світі, приносячи приблизно від 110 до 281 мільярдів доларів США злочинних доходів щороку [1], збільшуючись на 5–7 % щорічно. Тільки на нелегальну торгівлю продуктами дикої природи припадає від 7 до 23 мільярдів доларів США [2]. Це робить екологічну злочинність четвертою за масштабами злочинною діяльністю у світі після контрабанди наркотиків, підробки і торгівлі людьми [3].

Завдання шкоди довкіллю України внаслідок збройної агресії рф є колосальною та, станом на січень 2023 року, становила понад 1,69 трлн. грн [4], а станом на вересень 2023 року – понад 2,095 трл. грн [5].

Відповідно до статті 2 Статуту ООН, усі держави зобов'язані утримуватися у своїх міжнародних відносинах від загрози силою або її застосування проти територіальної цілісності або політичної незалежності будь-якої держави і вирішувати свої міжнародні спори мирними засобами. Порушення Статуту ООН може тягнути за собою відповідальність за міжнародним правом у вигляді відшкодування збитків. Наприклад, пункт 16 резолюції 687 (1991) Ради Безпеки поклав на Ірак відповідальність на цій підставі за «прямі збитки, шкоду, включаючи шкоду навколишньому середовищу і виснаження природних ресурсів», що виникли в результаті його незаконного вторгнення та окупації Кувейту [6].

Після початку воєнної агресії російської федерації проти України широко використовується спосіб фіксації відкритих цифрових даних за допомогою Протоколу Берклі [7]. Вказаний алгоритм дій дозволяє скопіювати необхідну інформацію, яка викладена в електронних системах і робить можливе її відтворення та використання в якості доказу.

Варто відмітити, що чинним Кримінальним законодавством України не створено достатніх умов для належного законодавчого врегулювання правоохоронної діяльності в цифровому довкіллі, яке не має кордонів, а тому охоплює систему суспільних взаємовідносин планетарного рівня.

До прикладу, у Французькій Республіці для протидії кіберзлочинності правоохоронці використовують «аватари» – спеціально створені сторінки в соціальних мережах Інтернету із легендованими даними. За допомогою «аватарів» здійснюється комплекс пошукових заходів, спрямованих на раннє виявлення осіб або груп осіб, які готуються, вчиняють або вчинили кримінальні правопорушення. Для створення віртуального конфідента працівник правоохоронного органу, який уповноважений на здійснення розшукових заходів в цифровому середовищі, готує проєкт «аватару» та отримує дозвіл на його застосування в прокурора, суду. Саме такий алгоритм дій дозволяє отримувати необхідні для розслідування фактичні дані у встановленому законом порядку із застосуванням пропорційного та необхідного втручання у права інших осіб [8].

Відповідно до ч. 1 ст. 275 КПК України, під час проведення негласних слідчих (розшукових) дій слідчий має право використовувати інформацію, отриману внаслідок конфіденційного співробітництва з іншими особами, або залучати цих осіб до проведення негласних слідчих (розшукових) дій у випадках, передбачених цим Кодексом [9].

Тому можемо констатувати, що в діючому КПК України відсутній механізм створення і використання «цифрових осіб» («аватари»), в тому числі в якості конфідентів, для виконання завдань кримінального провадження. Водночас такий алгоритм також відсутній в Законі України «Про оперативно-розшукову діяльність» [10].

За обставин воєнного вторгнення законодавче врегулювання легальності створення та використання «цифрових осіб» у цифровому середовищі забезпечить оперативний збір належних і допустимих доказів без територіальної прив'язки, а також створить передумови для використання «аватара» в якості конфідента під час проведення ОРД та НС(Р)Д. Наприклад: проведення контролю за вчиненням злочину із використанням в якості конфідента «цифрової особи» чи зняття інформації з електронних інформаційних систем.

Здійснення діяльності із використанням «цифрових осіб» має виключати провокацію та потребує дотримання цифрової гігієни. Так, вказана робота має відбуватись виключно на спеціально підготовленій службовій техніці із одночасною фіксацією (записом) усіх дій службових осіб, які проводять такі заходи.

Підсумовуючи викладене вище, беручи до уваги темпи розвитку цифровізації у світовому співтоваристві, доцільно внести зміни до Кримінального процесуального кодексу України та Закону України «Про оперативно-розшукову діяльність» в частині законодавчого врегулювання використання цифрової особи – «аватара» для виконання завдань оперативно-розшукової діяльності та кримінального судочинства.

Список використаних джерел

1. Норвезький центр глобального аналізу (RHIPTO), ІНТЕРПОЛ та Глобальна ініціатива (GI) (2018), «Світовий атлас незаконних потоків».

2. Оцінка швидкого реагування Програми ООН з довкілля (ЮНЕП)-Інтерполу: зростання екологічних злочинів (червень 2016 року).

3. Висновок Консультативної Ради європейських прокурорів № 17 (2022) щодо ролі прокурорів в охороні навколишнього природного середовища, пункт 3, Страсбург, 4 жовтня 2022 року.

4. Державна екологічна інспекція України. URL: https://dei.gov.ua/post/2479

5. Державна екологічна інспекція України. URL: https://www.dei.gov.ua/post/slidi-agresii-shchotizhneva-infografika-pro-zbitki-dovkillyu-vid-rf-na-teri.

6. Програма ООН з довкілля (2022 рік). Вплив конфлікту в Україні на навколишнє середовище: Попередній огляд. Найробі, Кенія. URL: https://wedocs.unep.org/20.500.11822/40746.

7. Протокол Берклі з ведення рослідувань з використанням відкритих цифрових даних. Практичний посібник. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

8. Екологічний вимір військових злочинів (Тренінг). Французька Національна школа судової гілки влади. Париж 25-29 вересня 2023 р.

9. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. *Офіційний вісник України.* 2012. № 37. Ст. 1370.

10. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

Воронятніков Олександр Олександрович,
начальник відділу проєктування
та впровадження систем управління
інформаційних технологій Департаменту
інформаційно-аналітичної підтримки
Національної поліції України, доктор
юридичних наук

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ МЕТОДІВ І ЗАСОБІВ OSINT ПІД ЧАС ПІДГОТОВКИ АНАЛІТИКІВ

З початку повномасштабного вторгнення російської федерації на територію України громадяни нашої країни страждають не лише через збройну агресію, а й від інформаційно-психологічних операцій ворога.

21 вересня 2022 року міністр оборони росії генерал армії Сергій Шойгу в інтерв'ю телеканалу «Россия–24» заявив: «Не

могу не сказать, мы давно об этом не говорили: о наших потерях. Наши потери в спецоперации составили 5 937 человек» [1]. В той же час за даними Генерального Штабу Збройних Сил України наводились цифри в 55110 ліквідованого особового складу окупантів.

Ураховуючи розбіжність у майже 10 разів між офіційною заявою зі сторони росії та даними Генштабу ЗСУ, а також важливість протидії інформаційній війні в Україні, документування воєнних злочинів, отримання достовірної інформації про кожного загиблого ворога, керівництвом Міністерства внутрішніх справ України та Національної поліції України було прийнято рішення щодо створення спільного проєкту «Потерь.НЕТ» (далі – Проєкт) [2].

Проєкт створено з метою збору, аналізу та подальшого висвітлення на веб-порталі інформації щодо втрат російської армії та інших військових формувань, які задіяні в збройній агресії Російської Федерації проти України.

Уся інформація, яка публікується на веб-порталі Проєкту отримана з відкритих джерел за допомогою методології OSINT (Open Source Intelligence) та ретельно перевіряється. Джерелами отримання інформації є мережа Інтернет (соціальні мережі, блоги, відеохостинги, форуми, месенджери тощо), журнали, газети, ЗМІ, радіо, публічні матеріали державних структур, загальнодоступні спостереження, звіти, статті, доповіді, конференції та т.п.

Збір та обробка даних, які публікуються на веб-порталі Проєку, здійснюється аналітиками Національної поліції України, представниками закладів вищої освіти Міністерства внутрішніх справ України, волонтерами, громадськими організаціями, міжнародними партнерами тощо.

Будь-яке розслідування за допомогою методів і засобів OSINT складається з кількох етапів, включаючи збирання, обробку, аналіз та поширення інформації.

Загалом можна виокремити декілька кроків для отримання інформації з відкритих джерел:

1. Складання плану. Складаючи план пошуку аналітики повинні зрозуміти вимоги до потрібної інформації, що у свою чергу допоможе визначити місця їх пошуку, а також ключові слова, що використовуються при здійсненні пошуку.

2. Безпосереднє проведення пошуку. Аналітики за допомогою відповідних запитів проводять первинний пошук

ймовірних джерел інформації. Отримані дані вносяться у відповідні бази даних.

3. Розширення джерел пошуку. Перші джерела результатів пошуку, як правило, є найбільш актуальними. Ґрунтуючись на цих джерелах, аналітики аналізують перші результати пошуку на предмет можливої достовірності та точності, з метою визначення їх відповідності визначеним вимогам, а в разі необхідності відновлення пошуку. Результати первинного пошуку в Інтернеті можуть бути недостатні, щоб задовольнити інформаційно-розвідувальні вимоги. Зазвичай аналітики використовують наступні методи поліпшення результатів пошуку: зміна порядку та критеріїв пошуку; зміна правопису і граматики; регулювання верхнього або нижнього регістру; використання інших варіантів ключових слів; пошук в результатах тощо.

4. Перевірка та публікація результатів пошуку. Так як основною метою OSINT є використання загальнодоступної інформації з відкритих джерел, то отримані дані потребують ретельної перевірки. За результатами зібрані дані публікуються та використовуються з метою подальшого інформування цільової аудиторії [3].

Підсумовуючи викладене можна стверджувати, що ключовими факторами для успішного аналізу інформації з відкритих джерел є: чітке розуміння цілей пошуку; неупередженість; об'єктивна аналітика; збір інформації з максимально можливої кількості відкритих джерел; грамотний аналіз отриманої інформації та ретельна перевірка отриманої інформації.

Участь в Проєкті дозволяє аналітикам сформувати необхідні навички та знання здійснення пошуку та збору інформації з відкритих джерел із використанням методів і засобів OSINT, які в подальшому дадуть змогу більш якісно протидіяти новим викликам та загрозам в інформаційному просторі.

Список використаних джерел

1. Шойгу заявил, что потери России в ходе спецоперации составили 5 937 человек. URL: https://tass.ru/armiya-i-opk/15817167.

2. МВС створило ефективний єдиний майданчик, де збирається інформація про загиблих окупантів, – Леонід Тимченко. URL: https://www.kmu.gov.ua/news/mvs-stvorylo-efektyvnyi-iedynyi-maidanchyk-de-zbyraietsia-informatsiia-pro-zahyblykh-okupantiv-leonid-tymchenko.

3. Актуальні питання використання методів і засобів OSINT у роботі підрозділів захисту національної державності :

зб. матер. круглого столу (м. Київ, 31 березня 2023 р.): у 2-х ч. Ч. 1. Київ : НА СБУ, 2023. 75 с. URL: https://academy.ssu.gov.ua/uploads/p5761186644.pdf.

Герасименко Лариса Володимирівна,
завідувач кафедри економічної безпеки
та фінансових розслідувань
Національної академії внутрішніх справ,
кандидат юридичних наук, професор

ЗАГАЛЬНІ ЗАСАДИ ОЦІНЮВАННЯ РИЗИКІВ І ЗАГРОЗ У КРИМІНАЛЬНОМУ АНАЛІЗІ

У стратегічному кримінальному аналізі одним з найважливіших аспектів є аналіз ризиків та загроз. При здійсненні зазначеного напряму аналізу важливим етапом є інтерпретація отриманої інформації. Саме на цьому етапі є можливість визначити наявні умови, які впливають на досліджувану активність. На цьому ж етапі важливо якісно описати та проаналізувати контекст, в якому знаходиться проблема, що забезпечить основу для порівняння джерел загроз та рівнів, на яких спостерігаються їх наслідки. Зазначене надасть можливість виявити інформаційні прогалини.

Після інтерпретації ризик необхідно оцінити, що доцільно здійснити на основі деяких загальних показників, зокрема:

– темпи зростання (зменшення) загальної кількості випадків, що підлягають аналізу, зафіксованих за певний проміжок часу, порівняно з аналогічними періодами попередніх років;

– динаміка кількості жертв або інцидентів за аналізований період;

– географічний розподіл інцидентів або жертв;

– середнє значення їх розподілу за заданий період часу та відносно географічної одиниці;

– часові інтервали, в яких трапляються інциденти;

– існування та вплив зовнішніх економічних, соціальних та географічних факторів;

– асоціювання інцидентів, що підлягають аналізу, з особами (фізичними або юридичними).

На підставі загальних показників, зазначених вище, аналітик може встановити конкретні показники залежно від суб’єкта аналізу ризиків або відповідно до вимог замовника.

Оцінка ризику має на меті виявити та вивчити вразливі сфери в суспільстві та надати рекомендації щодо їх нівелювання. При проведенні оцінки ризиків враховується не тільки характер вразливого сектору, але й характер потенційних загроз та рівень складності їх впливу. Поєднання оцінюваного рівня ймовірності та прогнозованого рівня впливу є ризиком, на основі якого складається профіль ризику. Оцінку ризику можна проводити за трьох ступеневою шкалою:

1. Оцінка ймовірності матеріалізації визначеного ризику полягає у визначенні шансів виникнення конкретного результату і виконується шляхом:

– спостереження за матеріалізацією подібних ризиків у минулому;

– аналізу обставин (причин), що сприяють виникненню ризиків;

– використання шкали оцінювання ризику для його матеріалізації ризику в три або п’ять етапів вірогідності цього.

2. Оцінка впливу на ситуацію у випадку матеріалізації ризиків.

3. Оцінка ризику.

Метою оцінки є різниця між оцінкою загрози та оцінкою ризику. На першому етапі ціль – це загроза, а на другому – увага зосереджена на об’єкті, який є вразливим та який може стати об’єктом загрози. При цьому варто пам’ятати, що об’єкт може бути вразливим, навіть якщо загрози немає.

Якщо ризики не можуть бути кількісно визначені або не мають чи їм не можуть бути присвоєні значення, вони оцінюються відповідно до кількості сповіщень, частоти, області прояву, відповідно до значення та кількості уразливих ситуацій або у співвідношенні з іншими факторами ризику.

Оцінюючи загрози, як реальну подію, за якої ризик переходить зі стану можливості у реальну площину, аналітик повинен виділити, що викликає загрозу, в якій формі вона може проявитись, якби вона стала реальністю. Інколи оцінка загрози повинна включати інформацію про наслідки для суспільства, а також про те, на які сектори вплине, якщо загроза реалізується.

В ході оцінювання загрози можна отримати ситуацію, в якій робиться висновок про те, що загрози немає або що рівень загрози зменшується. І хоча це, так би мовити, «негативний» висновок, він є досить важливим. Водночас, загроза – це щось потенційне, чого ще не відбулося, але висока ймовірність її

настання. Коли це матеріалізується інформація сприйматиметься вже не як загроза, а як певна ситуація чи кримінальна активність.

Наприкінці варто наголосити, що під час ідентифікації, опису та оцінки загрози необхідно враховувати дві загальні характеристики, що визначають загрозу: ймовірність (можливість того, що щось станеться) та вплив (рівень економічної, емоційної, фізичної, інтелектуальної та політичної шкоди, який стався внаслідок загрози).

Кваліфікований підхід до аналізу ризиків та загроз в кримінальному аналізі дозволяє розробити ефективні заходи із запобігання кримінальній активності.

Господарець Анна Анатоліївна,
аспірант Харківського національного університету внутрішніх справ

ЗНАЧУЩІСТЬ ЯКОСТІ АНАЛІТИЧНИХ ПРОДУКТІВ ПІД ЧАС ПЛАНУВАННЯ ПРОВЕДЕННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ

Оперативно-розшукова діяльність (далі – ОРД) є невід'ємною складовою правоохоронної функції визначених законом суб'єктів. Її завданням є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [1].

У межах проведення оперативно-розшукових заходів (далі – ОРЗ) серед іншого оперативним працівникам п. 21 ч. 1 ст. 8 Закону України «Про оперативно-розшукову діяльність» надано право на безпосереднє проведення або ініціювання проведення кримінального аналізу [1].

Метою інтеграції можливостей кримінального аналізу в систему забезпечення діяльності органів і підрозділів Національної поліції є потреба прийняття обґрунтованих управлінських рішень на основі використання сукупності методів збирання, оцінки, аналізу та реалізації отриманих результатів під час здійснення оперативно-розшукової діяльності, досудового

розслідування кримінальних правопорушень, а також для вироблення тактичних і стратегічних засад протидії злочинності.

«Кримінальний аналіз не дублює методів роботи оперативних працівників чи слідчих, його алгоритми допомагають успішно опрацьовувати великі за обсягом масиви даних з метою вилучення з них значень – таким чином кримінальний аналіз виконує роль додаткового інструментарію в руках працівників органів та підрозділів поліції» [2, с. 10].

Особливостями проведення ОРЗ, які тимчасово обмежують права і свободи людини, є їх попереднє узгодження-санкціонування на трьох рівнях, залежно від видів ОРЗ: відомче санкціонування; проведення ОРЗ, що потребують рішення прокурора; ОРЗ, що потребують дозволу слідчого судді.

Отримання дозволу на проведення ОРЗ від відповідальних посадових осіб залежить саме від спроможності оперативних працівників (або аналітичних працівників) привести чіткі аргументи щодо виключної необхідності проведення саме запланованого оперативним підрозділом заходу.

Тому саме від репрезентації результатів аналітичного дослідження первинних оперативно-розшукових даних буде залежати прийняття відповідного рішення-дозволу на проведення ОРЗ.

Кримінальний аналіз оперативно-розшукових даних є ключовою фазою ОРД, оскільки дозволяє перетворити накопичену інформацію в цінні результати та здобуті знання. Ця фаза включає в себе оцінку і валідацію даних, тобто процес перевірки та підтвердження правильності, відповідності та коректності зроблених аналітичних висновків та відтворених у вигляді схем-візуалізацій зв’язків, подій, що впливатимуть у подальшому на прийняття тактичних або стратегічних рішень. Валідація дозволяє визначити, чи відповідають висновки певним критеріям і стандартам законності, і чи можна їх надалі використовувати. Від якості аналітичних продуктів залежить визначення пріоритетів в подальшому плануванні ОРД.

До найбільш розповсюджених видів аналітичних продуктів прийнято відносити:

– аналітичний звіт (документ або письмова доповідь, створені фахівцями із застосування методів кримінальної аналітики, які містять інформацію, що була зібрана, оцінена, систематизована, опрацьована та репрезентована з метою подальшого використання замовником для прийняття певних

управлінських рішень. Цей тип аналітичного продукту зазвичай містить велику кількість даних та інформації, які були опрацьовані та інтерпретовані з метою відповіді на певні запитання або визначення тенденцій);

– досьє (зібрана з різних джерел й систематизована в певному порядку інформація на конкретні фізичну або юридичну особу, об'єкт (предмет), організовану групу чи злочинну організацію, подію, яка має значення для вирішення завдань ОРД);

– профіль – інформація, створена і систематизована шляхом проведення порівняльного аналізу зібраних раніше за певними ознаками даних, доказів, свідчень та іншої доступної інформації з метою встановлення потенційних жертв злочинів, характерних ознак протиправної діяльності, зон протиправної діяльності, методів вчинення кримінальних правопорушень і поведінки правопорушників;

– аналітичне орієнтування – створені з використанням аналітичних методів ініціативні висновки, що логічно доводять наявність в інформаційних даних, які були опрацьовані, ознак латентних кримінальних правопорушень.

Будь-які аналітичні продукти, утворені під час аналітичних досліджень інформації, додатково можуть супроводжуватися схемами, графіками, діаграмами, звідними таблицями, списками, дашбордами, фотографіями, малюнками, графіками тощо.

Для досягнення найкращих результатів оптимальним є використання даних продуктів комплексно.

Основними вимогами до письмових аналітичних продуктів мають бути:

– ясність, лаконічність та зрозумілість змістовної частини, тобто звіт повинен бути складений таким чином, щоб його можна було легко зрозуміти цільовим користувачам, включаючи тих, хто може не мати спеціалізованої фахової освіти;

– чіткість і структурованість подання матеріалу, що сприятиме найшвидшому розумінню суті;

– об'єктивність, під якою слід розуміти базування виключно на фактичних засновках, відсутність у звіті особистих суджень виконавця;

– відповідність цілям аналітичного дослідження і спрямованість на вирішення конкретних завдань ОРД;

– підкріплення змістовної письмової частини візуалізаціями та досьє;

– відповідність юридичним вимогам і стандартам, встановленим для документів даного типу;

– уникнення професійного жаргону;

– відповідність рівня захисту інформації, що міститься в аналітичному звіті, вимогам Законів України «Про державну таємницю», «Про інформацію».

Маркерами ефективності аналітичного продукту слід вважати прийняття/неприйняття таких рішень за результатами аналітичного дослідження:

– внесення відомостей в Єдиний реєстр досудових розслідувань та подальше здійснення досудового розслідування у кримінальному провадженні;

– заведення оперативно-розшукової справи та проведення у подальшому ОРЗ;

– винесення рішень про проведення оперативних превентивних заходів;

– планування проведення подальших ОРЗ та заходів ініціативного пошуку для отримання додаткової інформації стосовно кримінальної ситуації, яка досліджувалася;

– інформування керівництва Національної поліції України та надання пропозицій для підготовки стратегії у протидії злочинності за напрямами або в цілому.

Враховуючи зазначене вище, очевидним є те, що аналітичні продукти є інструментом, які сприяють об'єктивності та ефективності проведення ОРЗ, допомагаючи визначати факти та обставини кримінальних правопорушень і виносити обґрунтовані рішення.

Список використаних джерел

1. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

2. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львів. держ. ун-т внутр. справ, 2021. 288 с.

3. Основи кримінального аналізу : підручник / О. Є. Користін та ін. ; ред. О. Є. Користін. Одеса : ДНДІ МВС України, ОДУВС, 2019. 272 с.

Григорович Олексій Борисович,
начальник Департаменту інформаційно-аналітичної підтримки Національної поліції України

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

З першого дня повномасштабного вторгнення російської федерації на територію України, окупаційні війська порушують правила ведення війни і норми міжнародного права та масово чинять воєнні злочини та злочини проти людяності, вбиваючи цивільних, руйнуючи інфраструктуру та депортуючи населення.

Якісний збір доказової бази, документування кожного злочину, накопичення відомостей та даних про воєнні злочини та осіб, які їх скоїли – є запорукою притягнення до відповідальності та невідворотного покарання.

Однак, розслідування багатоепізодних фактів скоєння воєнних злочинів, інформація за якими внесена до Єдиного реєстру досудових розслідувань, великої кількості виявлених в рамках кримінальних проваджень осіб, причетних до скоєння злочинів, документування їх злочинної діяльності декількома структурними та територіальними підрозділами Центрального органу управління поліції та головних управлінь Національної поліції в областях, іншими правоохоронними відомствами, існуючий паперовий облік таких осіб має ряд недоліків: накопичена інформація систематизується недостатньо та не ефективно; відсутня можливість дистанційного вивчення чи аналізу інформації, її миттєвого обміну, та, як наслідок, зменшується якість зібраної інформації в цілому.

Саме тому виникла необхідність у накопиченні в єдиному сегменті всіх відомостей, пов’язаних із збройною військовою агресією російської федерації, яка фактично була розпочата 2014 р. в окремих районах Донецької та Луганської областей, а з 24 лютого 2022 р. – повномасштабно на всій території країни.

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 п. 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), 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 [3] .

Так, 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 в експлуатацію інформаційну підсистему «Воєнний злочинець» (далі – ІП «Воєнний злочинець»).

Функціонал ІП «Воєнний злочинець» передбачає 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; 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 в зазначеній інформаційній підсистемі, що надає змогу працівникам підрозділів кримінальної поліції в режимі реального часу при документуванні злочинів отримувати наявні відомості та мати комунікацію із зазначеними правоохоронними відомствами.

Так, Департаментом інформаційно-аналітичної підтримки Національної поліції відповідні доступи на внесення та перегляд інформації в ІП «Воєнний злочинець» системи «ІПНП» надані як співробітникам кримінальної поліції Національної поліції, так і співробітникам зазначених відомств.

Таким чином, завдяки зазначеній інформаційно-аналітичній роботі, яка щоденно та безперервно здійснюється працівниками правоохоронних відомств, встановлюється, фіксується, документується та накопичується інформація про факти переміщення (руху) ворожої техніки, моменти обстрілів та бомбардування, нанесення артилерійських та авіаційних ударів по житлових будинках, школах, дитсадках, електростанціях та інших об'єктах забезпечення життєдіяльності населених пунктів, обстріли колон евакуації цивільних осіб, випадки вчинення мародерства та інших диверсійно-розвідувальних, протиправних і злочинних діянь.

На даний час загальний масив унесеної до підсистеми інформації складає більш ніж 241 тис. інформаційних карток щодо осіб, причетних до військової агресії з боку російської федерації (з них 66 тис. із фотозображенням осіб) та 3125 карток стосовно скоєних кримінальних правопорушень.

Враховуючи вищевикладене, ІП «Воєнний злочинець» системи ІПНП є складовою частиною системи сучасних методів здійснення кримінального аналізу та забезпечує процес пошуку та аналізу інформації, швидкої адаптації до виконання різних аналітичних завдань, особливо в умовах дефіциту часу та надає

можливість працівникам підрозділів кримінального аналізу, застосовуючи високий рівень теоретичної підготовки, практичного досвіду та спеціалізованого програмного забезпечення, на високому рівні виконувати покладені на підрозділи кримінального аналізу функції із розкриття злочинів та 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 Національної поліції України 31.01.2020 року № 77 «Про затвердження Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України». 2020. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Struktura/Polohena11.pdf.

Демедюк Сергій Васильович,
заступник Секретаря Ради національної безпеки і оборони України, кандидат юридичних наук

ЗАХИСТ КРИТИЧНО ВАЖЛИВОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Захист критично важливої інформаційної інфраструктури (далі ЗКІІ) є основою для зусиль країн у сфері кібербезпеки. Для політиків, перед якими стоїть завдання розвивати національну систему кібербезпеки, питання визначення і ЗКІІ змістилося від переважно фізичного розуміння інфраструктури до захисту критично важливих послуг. ЗКІІ використовується для узагальненого позначення захисту життєво важливих ІТ-сервісів, які підтримують надання критично важливих послуг як приватними, так і державними організаціями [1].

Це питання, безумовно, є актуальним для багатьох країн і сьогодні через різке зростання залежності від цифрової складової сучасної економіки і суспільства. Тим не менш, обізнаність та ресурси, що виділяються на національну кібербезпеку, залишаються дуже нерівномірними навіть серед індустріальних країн.

У той же час, кількість суб'єктів, потенційно здатних до незаконної кіберактивності з різних мотивів, стрімко зростає. З появою мільйонів нових інтернет-користувачів на ринках, що формуються, і в країнах, що розвиваються, відбудеться стрибок з 2,5 мільярдів інтернет-користувачів у 2015 році до 5 мільярдів користувачів до 2025 року [2]. Тому проблема кібербезпеки стає загрозою економічному зростанню та національній безпеці не лише в розвинених індустріальних країнах, а й у країнах з економікою, що розвивається.

Для покращення кібербезпеки критично важливих послуг основна увага має бути зосереджена на організаційних аспектах, а необхідні технічні компоненти – на вдосконаленому управлінні кіберризиками. Через складність захисту кібер-елементів критично важливих послуг, питання, на яке слід відповісти, в першу чергу, полягає в тому, як організувати це завдання і забезпечити необхідне лідерство уряду у протидії кібер-викликам. Нещодавні рекомендації Організації економічного співробітництва та розвитку (ОЕСР) дійшли висновку: «Замість того, щоб розглядати цифровий ризик як технічну проблему, яка вимагає технічних рішень, до нього слід підходити як до економічного ризику; отже, він повинен бути невід'ємною частиною процесів управління ризиками та прийняття рішень в організації» [3].

Одним з найбільш важливих аспектів національної системи ЗКІІ є пошук відповідної організаційної моделі, яка сприятиме ефективній та стабільній роботі в цій сфері. Достатньо глибокий аналіз акцентує увагу на різних моделях ЗКІІ, і хоча немає двох абсолютно однакових моделей, все ж є певні закономірності, що склалися в Європі. Початково такі системи сформувалися в невеликих європейських країнах і здебільшого базувалися на міцних довірчих відносинах в однорідних суспільствах, де основна група критично важливих компаній і національних кіберорганізацій розробили системи обміну технічною кіберінформацією та раннього попередження з критично важливими операторами. На початковому етапі було створено окремий орган ЗКІІ, який виконував лише політичні функції і діяв як національний координатор, здійснюючи нагляд і консультування критично важливих компаній і організацій. Водночас цей орган інформує політиків вищого рівня, проводить навчання, готує національні кібернавчання і підтримує зв'язок з ключовими державними установами. В ідеалі така установа повинна бути розташована разом з національною структурою

реагування на інциденти (CERT), щоб мати технічну кібер-компетентність, а також мати доступ до оперативної інформації з кібербезпеки.

У деяких європейських країнах модель базується на галузевих підходах до ЗКІІ і тому відіграють більш важливу роль. Галузеві регулятори не обов'язково є найбільш компетентними кіберорганами, але оскільки ЗКІІ часто організована на галузевій основі, регулятори також мають мандат на нагляд за виконанням вимог щодо управління кіберризиками та звітності про інциденти. Цілісний підхід до ЗКІІ, коли кібербезпека інтегрована з фізичною та кадровою безпекою, добре слугує загальним цілям управління ризиками операторів критично важливих послуг. Деякі національні агентства ЗКІІ також демонструють здатність брати на себе наглядову і консультативну роль з питань ЗКІІ [4].

Існує також модель централізованого змісту з сильним кіберорганом в центрі національних зусиль, який має мандат на нагляд за реалізацією цілей ЗКІІ. У цьому випадку центральний орган також повинен мати можливість надавати корисні рекомендації та певну технічну допомогу постачальникам критично важливих послуг, а також не нехтувати галузевими специфікаціями у вимогах до кібербезпеки.

У більшості країн галузеві регулятори повинні бути більш обізнаними щодо кіберризиків і з часом відігравати певну роль в управлінні та нагляді за управлінням кіберризиками постачальників критично важливих послуг. Однак, оскільки багато європейських країн є малими або середніми державами, вони можуть не мати достатньої кількості кіберспеціалістів у всіх галузевих регуляторних органах, і було б економічно доцільно зосередити завдання з управління кіберризиками в національній організації ЗКІІ, яка тісно співпрацює з галузевими органами влади. В ЄС багато галузевих вимог до безпеки визначаються загальноєвропейськими регуляторними органами. Ці гармонізовані європейські вимоги сприяють функціонуванню внутрішнього ринку та операторів критично важливих послуг, але національні уряди все одно здійснюють нагляд за виконанням нормативних актів.

Важливо зазначити, що кожна країна повинна знайти власну модель захисту критично важливих послуг у цифрову епоху. Досвід європейських країн показує, що центральним осередком національних зусиль у сфері кібербезпеки, як правило, є сильна державна установа з солідним фінансуванням і політичним керівництвом, орієнтованим на безпеку. Оскільки

національна організація ЗКІІ повинна мати можливість залучати широке коло зацікавлених сторін з державного і приватного секторів, вона виграє від приналежності до національної установи, яка має прямий доступ до вищого політичного керівництва і володіє певним ступенем повноважень для здійснення нагляду.

Розбудова певної моделі ЗКІІ, створення відповідних органів, передбачає і відповідні регуляторні ініціативи, що сприяють підвищенню кібербезпеки критично важливих послуг. З цього приводу, тривалий час в розвинених країнах серед суб'єктів кібербезпеки відбувалася дискусія щодо того чи варто здійснювати регуляторні функції у сфері кібербезпеки. Представники національної безпеки та правоохоронних органів виступали за регулювання, тоді як ІТ-розробники та приватний сектор іноді запекло протистояли цьому. Оскільки більшість індустріальних країн зробили вибір на користь кіберрегулювання, спільною позицією стало посилення управління ризиками ІТ-безпеки в компаніях та організаціях державного сектору, які забезпечують критично важливу інфраструктуру та послуги. Стало очевидним, що для боротьби зі стрімким зростанням кіберзагроз необхідне втручання держави.

Таким чином, в умовах цифрової трансформації, об'єктивною вимогою є активізація зусиль у сфері кібербезпеки та посилення кіберстійкості. Прикладом цього процесу є законодавчі ініціативи економічно розвинених країн, зокрема США та ЄС. Урядами цих країн ухвалено нормативно-правові акти з кібербезпеки де обізнаність щодо кібербезпеки критично важливих послуг є найвищим пріоритетом для осіб, які приймають рішення. У європейських країнах, які вже обрали регуляторний підхід, рівень обізнаності з питань кібербезпеки серед вищого керівництва та керівників компаній є високим. Оскільки перші кроки в регулюванні здійснювалися на національному рівні і включали тісну співпрацю з приватним сектором, наразі не спостерігається очевидних невдач. Однак мають місце ризики щодо надмірного регулювання галузі, у випадку неналежних зусиль суб'єктів кібербезпеки, а також недостатніх інвестицій та лідерства урядів в цьому питанні. Водночас, процес потребує постійного дослідження та пошуку найбільш адекватного рішення. Саме тому академічні установи та аналітичні центри повинні максимально зосереджувати свій потенціал на прогалинах і надавати обґрунтований аналіз щодо організації ЗКІІ на національному рівні.

Список використаних джерел

1. Heli Tiirmaa-Klaar. Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy*. 2016. 1:1. P. 94–106.
2. Cyberspace 2025: Today's Decisions, Tomorrow's Terrain, Microsoft Report. June 2014. URL: https://query.prod.cms.rt.microsoft.com/cms/api/ am/binary/REXXtS.
3. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommen dation and Companion Document, OECD 2015. URL: https://www.oecd.org/publications/ digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm.
4. UK Centre for the Protection of National Infrastructure/ URL: https://www.protectuk.police.uk/news-views/centre-protection-national-infrastructure-cpni-has-evolved-become-national-protective#.

Денисенко Богдан Анатолійович,
експерт з питань спеціалізованих
правоохоронних органів
Консультативної місії Європейського
Союзу в Україні

МЕТОДОЛОГІЧНІ ЗАСАДИ OSINT

Процес цифровізації (діджиталізації), та, таким чином, генерування все більше і більше даних та інформації онлайн (та офлайн), не спинити. Таким чином, збільшується можливість більше, глибше та детальніше знаходити та верифікувати дані, інформацію щодо осіб, компаній, транспортних засобі, інших об'єктів та елементів дослідження, таким чином створюючи аналітичну розвідку (intelligence) з відкритих джерел (OSINT).

То *що ж таке OSINT (Opens Source Intelligence)*? Компанія «Reuser's Information Service» (RIS) у своєму тренінгу «OSINT Pathfinder» фокусує увагу на численних маніпуляціях з цим поняттям та визначенням. OSINT необхідно розглядати як процес, інструмент, механізм збору та продажу програмних продуктів. OSINT є спільною, інтегрованою методологією та процесом створення, де вимоги клієнта щодо аналітичної розвідки співпадають з наданою дієвою аналітичною розвідкою (*actionable intelligence*), створеною через процес синтезу та аналізу репрезентативної вибірки інформації з відкритих джерел, яка була валідованою, є надійною, вчасною та точною.

RIS також наголошує на змішуванні понять OSINT та OSINF. Оскільки, OSINF (*Open Source Information*) чи відкриті джерела є всією інформацією у будь-якому форматі, що може бути здобута будь-ким законним та етично-прийнятним шляхом без жодних обмежень, чи то безкоштовно, чи на платній основі. RIS наголошує на наступних обмеженнях та, відповідно, підсумовує, що простий збір, направлення необробленої сирої інформації не є OSINT. Під час збору інформації необхідно враховувати обмеження щодо авторського права, ліцензування та інтелектуального права власності. Хакерство, незаконне втручання у комп'ютерні мережі, злом паролів є незаконним та не може вважатись OSINT дослідженням. З етичної точки зору, наявність деяких ресурсів у відкритому доступі, у той час як вони не передбачені для відкритого доступу, не може вважатись інформацією з відкритих джерел.

RIS наголошує, що стандартний цикл аналітичної розвідки (*intelligence cycle*) не відповідає потребам OSINT-дослідження оскільки кількість кроків дослідження може змінюватись (відповідно до потреб конкретного дослідження). Особливістю запропонованого аналітично-розвідувального циклу OSINT є те, що клієнт, або замовник перебувають в центрі процесу. Сам цикл складається з 3-х під-циклів: підготовчий цикл, цикл звітування та цикл аналітичної розвідки. Аналітично-розвідувальний цикл OSINT передбачає трансформацію даних в зміни через, відповідно, формування інформації, аналітичної розвідки та рішень [1]. Кожен з під-циклів передбачає «звірку годинників» з клієнтом, або замовником, що наближає дослідження до задоволення реальних запитів та потреб клієнта або замовника (в нашому випадку – слідчого, керівника підрозділу, служби). Відповідно, для досягнення бажаного результату (мети дослідження), бажано мати чіткий план (з чітким аналізом вимог) та постійний контакт з замовником.

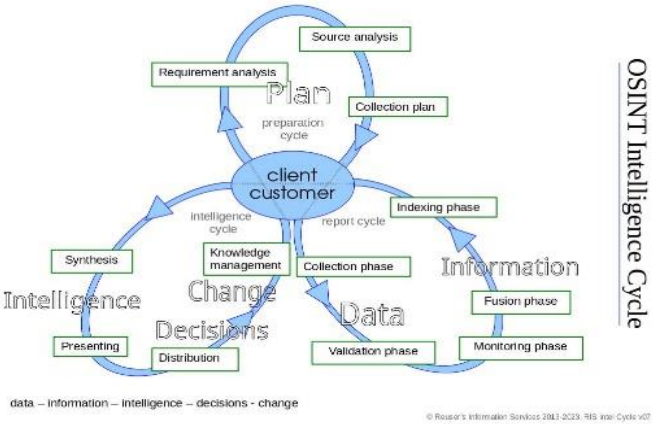


Рис. 1. Цикл OSINT (*джерело: Reuser's Information Service*)

Дані, інформація є основою для подальшого аналізу під час будь-якого дослідження, у тому числі OSINT. Кількість даних, інформації збільшується кардинально щоденно. Так, дослідження «International Data Corporation (IDC)», що є провідним світовим постачальником ринкової аналітичної розвідки (intelligence) та консультаційних послуг [2], показує, що станом на 2018 рік загальна кількість даних у світі становила 33 зетабайти (*зеттабайт – трильйон гігабайт*) та передбачалось, що їх кількість зросте до 175 зетабайт до 2025 року [3]. Дослідженням вже станом на 2020 рік встановлено, що загальний обсяг створених, зібраних, скопійованих і спожитих даних у всьому світі становив 64,2 зетабайти. Переглянутим дослідженням передбачається, що до 2025 року створення даних на глобальному рівні зросте вже до понад 180 зетабайт [4].

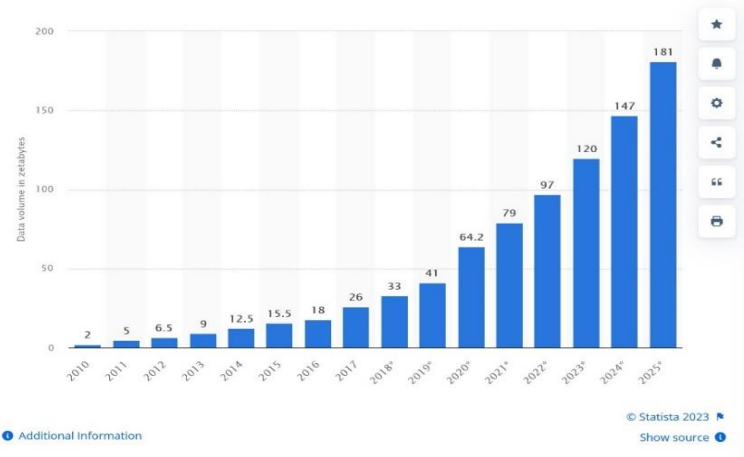


Рис. 2. Тренд зростання цифрових даних [5]

Станом на 2018 рік прогнозування передбачало, що протягом наступних семи років (до 2025 року) індустрія зберігання даних відвантажить 42 зетабайт (ZB) ємностей (пристроїв для зберігання даних); на пристроях IoT буде створено 90 ZB даних; 49 відсотків даних зберігатимуться в загальнодоступних хмарних середовищах; майже 30 відсотків згенерованих даних буде використовуватися в режимі реального часу [6]. Тенденції зберігаються та розвиваються, доповнюючись розвитком квантумних комп'ютерних можливостей, можливістю зберігання даних на молекулах ДНК, що є технологічним трендом 2023 року. Однак, цей процес зберігання є на даний час дуже коштовним та синтезування 1 мегабайту даних вартує біля 3,500 доларів США [7]. Однак, станом на 2019 рік науковці прогнозували, що до 2024 року ціна може впасти до 100 доларів США за синтез 1 терабайту даних, у випадку відповідного інвестування [8].

Ті незначні можливості архіваторів, як от ті, які надаються Wayback Machine, таким чином, не задовольняють всі потреби на запити історичних даних, у той же час, є потужним джерелом, у випадку, якщо архіватори все-таки змогли зберегти відповідні дані.

У сучасному світі все залишає цифрові сліди. Все більше пристроїв «інтернету речей» (Internet of things/IoT), тобто «розумних» пристроїв з'являються та використовуються у будь-

якій сфері життєдіяльності. Станом на кінець 2020 рік, з 21,7 мільярда активних підключених пристроїв у всьому світі понад 11,7 мільярда (54 %) є IoT пристроями [9].

Отже, розуміючи зростаючу тенденцію приросту відповідних пристроїв, розуміємо, що інформація про спосіб життя людини (через пристрої, що відслідковують переміщення, як от координати, швидкість, дані щодо зупинок та перебування, стан здоров'я, таке інше), у тому числі «розумні будинки», у тому числі пристрої для відео-спостереження та інші можливості, все менше і менше залишають можливостей зберігати анонімність людям, що користуються відповідними технологіями та пристроями. Та, відповідно, дають можливість тим, хто використовує ці зібрані дані – отримувати інформацію щодо способу життя фігуранта, будь-які інші відповідні дані «не виходячи з дому». Це, в свою чергу, викликає занепокоєння у багатьох правозахисних організацій.

Список використаних джерел

1. URL: https://opensourceintelligence.biz/osint-unlocked//
2. URL: https://www.idc.com/about
3. URL: https://www.networkworld.com/article/3325397/ idc-expect-175-zettabytes-of-data-worldwide-by-2025.html.
4. URL: https://www.statista.com/statistics/871513/worldwide-data-created/
5. URL: https://www.statista.com/statistics/871513/worldwide-data- created/.
6. URL: https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html.
7. URL: https://wyss.harvard.edu/technology/dna-data-storage/
8. URL: https://www.synbiobeta.com/read/dna-is-the-future-for-data-storage-that-future-is-coming-very-soon
9. URL: https://telecom.economictimes.indiatimes.com/news/at-12-billion-iot-connections-to-surpass-non-iot-devices-in-2020/79318722.

Заєць Олександр Михайлович,
член Української аналітичної групи International Association of Crime Analysts IACA, кандидат юридичних наук, доцент

PREDICTION ANALYTICS (ПРОГНОЗНА АНАЛІТИКА): ВИЗНАЧЕННЯ, ТИПИ МОДЕЛЕЙ І ВИКОРИСТАННЯ

Термін предиктивна (прогнозна) аналітика відноситься до використання статистики та методів моделювання для прогнозування майбутніх результатів та продуктивності. Прогнозна аналітика розглядає поточні та історичні закономірності даних, щоб визначити, чи можуть виникнути ці закономірності знову. Це дозволяє коригувати свої ресурси, щоб отримати вигоду з майбутніх подій. Прогнозний аналіз також можна використовувати для підвищення операційної ефективності та зниження ризиків. Предиктивна аналітика – це форма технології, яка робить прогнози щодо певних невідомих у майбутньому. Для прийняття таких рішень віна використовує низку методів, включаючи штучний інтелект, інтелектуальний аналіз даних, машинне навчання, моделювання та статистику. Наприклад, інтелектуальний аналіз даних включає у собі аналіз великих наборів даних виявлення закономірностей у них. Аналіз тексту робить те саме, крім великих блоків тексту. Прогнозні моделі використовуються для всіх видів програм, включаючи прогнози погоди, створення відеоігор, переклад голосу в текст, обслуговування клієнтів та стратегії інвестиційного портфеля. Всі ці додатки використовують описові статистичні моделі існуючих даних для прогнозування майбутніх даних. Ці моделі визначають відносини, закономірності та структури даних, які можна використовувати для того, щоб зробити висновки про те, як зміни в основних процесах, що генерують дані, змінять результати. Прогнозні моделі базуються на цих описових моделях та аналізують попередні дані, щоб визначити ймовірність певних майбутніх результатів з урахуванням поточних умов або набору очікуваних майбутніх умов.

Предиктивна (прогнозна) аналітика – вид аналітики даних, спрямованої на прогнозування майбутніх результатів, яка базується на отриманих історичних даних і методах аналітики, зокрема, таких як статистичне моделювання та машинне навчання. Такі процедури прогнозної аналітики можуть

допомогти робити прогноз із достатнім для практики рівнем точності [1, с. 25–35].

Мета предиктиіної (прогнозної) аналітики – робити прогнози про майбутні події, а потім використовувати ці прогнози для покращення процесу ухвалення рішень. Предиктивна (прогнозна) аналітика використовується у різних галузях, включаючи фінанси, охорону здоров'я, освіту, правоохоронну діяльність та інші галузі. У предиктивній (прогнозній) аналітиці використовуються різні методи, такі як регресійний аналіз, дерева рішень, нейронні мережі тощо.

Точний прогноз майбутнього за допомогою математичних методів цілком можливий за допомогою предиктивної (прогнозної) аналітики. Метою предиктивної (прогнозної) аналітики є прогнозування майбутніх тенденцій. Щоб приймати швидші, розумніші рішення, правоохоронні органи використовують все складніші методи аналітики. Перехід, який відбувається, відображає перехід від звітування про історичні дані до прогнозування за допомогою штучного інтелекту. Зараз є можливість отримувати цінність від раніше невивчених «темних» даних, включаючи все, від необробленого тексту до геолокаційної інформації.

Крім базової звітності та інформації про аналітику злочинності, яка розповідає про те, що сталося або відбувається, правоохоронні органи використовують предиктивну (прогнозну) аналітику та методи на моделях штучного інтелекту та машинного навчання, які мають набагато більше можливостей. Це може стосуватись також таких методів, як прогнозування майбутніх подій, а також автоматизованих текстів або класифікації операцій або сегментації фігурантів. Як результат, предиктивна (прогнозна) аналітика говорить про те, як будуть розвиватись події. Сьогодні зближення інтуїтивних інструментів, нові методи прогнозування та гібридні моделі хмарного розгортання роблять прогнозну аналітику та моделювання більш доступними.

Перехід від описової до прогнозної аналітики та штучного інтелекту визначається потребою бути менш реактивними та більш ініціативними проактивними. Аналітика, що базується на моделях штучного інтелекту та машинного навчання, просто забезпечує кращу інформацію. Вони ґрунтуються на перевагах предиктивної (прогнозної) аналітики, доповнюючи процедури прийняття людських рішень. Часто такий аналіз

використовується для того, щоб рекомендувати один або кілька способів дій та показати ймовірний результат кожного рішення.

Реальна користь приходить, коли прогнозна аналітика і рецептивна аналітика вбудовані в системні процеси та використовуються для забезпечення безперервного інтелекту, що дозволяє базуватися на подіях, які відбуваються в даний момент. Безперервний інтелект пропонує способи розширити додаткові аналітичні програми в області підтримки прийняття рішень і автоматизації рішень. Обробляючи інформацію на основі подій та потоків даних, правоохоронні органи можуть зрозуміти, що відбувається зараз і швидко реагувати. Запуск алгоритмів рецептивної аналітики, машинного навчання та штучного інтелекту при обробці потокових даних може надати дієву інформацію. Потім ця інформація може бути використана системами, щоб вирішити, що робити далі, і надавати можливість здійснювати певні дії автоматично. По суті, безперервний інтелект на потокових даних дозволяє відійти від традиційної описової аналітики («ось що було раніше»). Безперервний інтелект розширює предиктивну (прогнозну) аналітику, застосовуючи аналіз штучного інтелекту до потоків подій, дозволяючи керівнику додати ситуаційну обізнаність для прийняття рішень. Предиктивна (прогнозна) аналітика використовує чотири основні методи перетворення даних в цінну і корисну інформацію: прогностичне моделювання; аналіз і оптимізація рішень; профілювання транзакцій; інтелектуальний пошук.

Найважливішим елементом предиктивної (прогнозної) аналітики є так званий предиктор. Наприклад, цей термін є фізичною або юридичною особою, яка призначена для прогнозування можливої майбутньої поведінки. Конкретним прикладом може бути страховий поліс, який передбачає потенційні фактори для розрахунку ризику власника транспортного засобу, включаючи до розрахунку відповідні фактори, такі як досвід водіння, вік та здоров'я відповідної особи. Із суми цих факторів за допомогою прогнозної аналітики можна розрахувати можливий ризик нещасних випадків та, отже, розмір страхової премії.

Фактично термін прогнозна аналітика часто використовується як синонім інтелектуального аналізу даних. Часто методи інтелектуального аналізу даних відіграють важливу роль у пошуку підходів до прогнозної аналітики. Проте предиктивна (прогнозна) аналітика визначає, як працює

інтелектуальний аналіз даних, і включає інші методи. Серед іншого важливу роль також відіграють елементи теорії ігор та автоматизованого машинного навчання. Крім того, при використанні Prediction Analytics [2, 3] використовуються спеціальні методи аналізу, засновані на складних алгоритмах, щоб отримати відомий шаблон із незв'язаної текстової пустелі постів у соціальних мережах або статей у блогах.

Інтелектуальний аналіз даних намагається використовувати математичні та стохастичні методи та алгоритми для визначення властивих закономірностей у великих обсягах даних. В ідеалі тенденції та потенційний розвиток подій можна визначити та передбачати на основі отриманих таким чином ідей.

Включення предиктивної (прогнозної) аналітики вже зарекомендувало себе в різних галузях. Крім наукових високотехнологічних компаній метод прогнозування перебігу захворювань, наприклад, використовує сфера охорони здоров'я. Важливою сферою застосування є енергетична галузь, де інтелектуальну енергосистему майбутнього називають «розумною мережею». Споживання електроенергії можна прогнозувати на основі збережених моделей поведінки клієнтів (інтелектуальні дані клієнтів).

Предиктивну (прогнозну) аналітику найкраще використовувати, коли доступний широкий спектр пакетів даних, які є максимально повними та очищеними. Всі пакети даних потім інтегруються в аналіз, результати якого стають тим точнішими, чим більше доступних даних з широкого спектра областей. Більшість компаній мають ефект синергії, розширюючи існуючу структуру бізнес-аналітики, включивши до неї функції прогнозного аналізу. До найбільш популярних інструментів застосування прогнозної аналітики відносяться: Google Analytics, Альпійські лабораторії даних, Alteryx: Data Science and Analytics Automation Platform, Anguss Knowledge STUDIO, BIRT (Business Intelligence and Reporting Tools), IBM SPSS Statistics та IBM SPSS Modeler, Розробник моделей Математика, MATLAB, SOCTA [4–9].

Предиктивну (прогнозну) аналітику можна визначити, як наступний крок в аналізі даних. Бажані сценарії можна легко реалізувати, а попередній курс можна буде направити в іншому напрямку. Цей підхід став можливим завдяки аналітичним структурам, заснованим на складних моделях та стохастичному моделюванні. Тут застосовується наступне: чим більше відомих

та надійних змінних ви реалізуєте у цих моделях, тим точнішими будуть результати.

Існує безліч прикладів застосування та функціонування предиктивної (прогнозної) аналітики. Метод залежить від кількості та якості введених даних. Тим не менш, використовувані алгоритми стають дедалі деталізованішими, а це означає, що прогнози можна робити все більш і більш точними.

Різниця між приписувальною, прогнозною, діагностичною та описовою аналітикою полягає в тому, що предиктивна (прогнозна) аналітика: передбачає, що може статися в майбутньому. Предиктивна (прогнозна) аналітика переважно займається виявленням тенденцій і закономірностей з урахуванням даних, які вводяться у модель машинного навчання. Потім модель доповнюється поточними даними прогнозування майбутніх дій. Предиктивна (прогнозна) аналітика: рекомендує дії, які можна зробити, щоб вплинути на потенційні результати. Предиктивна (прогнозна) аналітика передбачає майбутній стан, рекомендує різні варіанти дій, щоб позитивно вплинути на наступні події. Не тільки описується самий майбутній стан, а й модель пропонує відповідні заходи для досягнення цілей.

Використання прогнозного аналізу має безліч переваг. Як згадувалося вище, використання цього аналізу може допомогти правоохоронним органам, коли потрібно зробити прогноз щодо результатів, коли інших (і очевидних) відповідей немає.

Використання моделей значно впливає на зниження витрат при проведенні досудового розслідування. Аналітики можуть визначити ймовірність успіху чи провалу заходів ще до його проведення. Або вони можуть перерозподілити бюджет процесуального впливу на поліпшення його організації проведення, використовуючи методи прогнозування на початок його проведення.

Використання прогнозної аналітики тягне у себе багато ризиків, а деяких випадках обмежується через передбачуваного нерівності у її результатах (ризику помилитися). Найчастіше це пов’язано з прогностичними моделями, які призводять до статистичної дискримінації у таких галузях, як кредитний скоринг, іпотечне кредитування, працевлаштування чи ризик злочинної поведінки.

Предиктивна (прогнозна) аналітика підходить для прогнозування, управління ризиками, аналізу поведінки злочинців, виявлення шахрайства та оптимізації операцій. Предиктивна (прогнозна) аналітика може допомогти

правоохоронним органам покращити процес ухвалення рішень, оптимізувати процеси, підвищити ефективність діяльності та мінімізувати ризики.

Найкраща модель предиктивної (прогнозної) аналітики залежить від кількох факторів, таких як тип даних, мета аналізу, складність проблеми та бажана точність результатів. Найкраща модель на вибір може змінюватись від лінійної регресії, нейронних мереж, кластеризації або дерев рішень.

Прогнозні моделі допомагають робити прогнози зміни криміногенної обстановки, розробляти плани дій, приймати рішення щодо затримання злочинців та розробляти системи профілактики злочинів.

Сучасні можливості та передові методи прогнозної аналітики стають дієвим інструментом для збільшення продуктивності діяльності правоохоронних органів. Прогнозна аналітика стала новою тенденцією сучасності, яка відкриває широкі перспективи для подальшого розвитку методів протидії злочинності. Ефективність використання засобів прогнозної аналітики залежить як від обраних технологій, так і від якості аналітичних інструментів. Перевага буде на боці того інструментарію, який надасть сучасні методи аналізу даних, якими, зокрема, є високопродуктивні засоби інтелектуального моделювання на основі штучного інтелекту та машинного навчання.

Список використаних джерел

1. Єфіменко С.М., Степашко В.С. Прогнозна аналітика як ефективний інструмент підтримки рішень у системах цифрової економіки. *Управляющие системы и машины*. 2018. № 6. С. 25–35.

2. Goebel, M., Gruenwald, L., 1999. A survey of data mining and knowledge discovery software tools. SIGKDD Explorations, 1 (1), Publisher ACM New York, NY, USA, pp. 20–33.

3. Ranjan, J., 2009. Business Intelligence: Concepts, Components,Techniques and Benefits. Journal of Theoretical and Applied Information Technology, pp. 60–70.

4. The Forrester Wave™: Big Data Predictive Analytics Solutions. URL: https://www.forrester.com/bold.

5. SPSS statistical software. URL: https://www.ibm.com/topics/predictive-analytics.

6. TIBCO Statistica is Now Part of TIBCO Data Science. URL: https://www.tibco.com/products/tibco-statistica.

7. Elderresearch. URL: https://www.elderresearch.com/.

8. Knowledgeminer. URL: https://www.knowledgeminer.eu/.
9. GMDH. URL: https://gmdhsoftware.com/.
10. Stepashko, V.S., 2017. The Achievements and Prospects of Inductive Modeling. Upravlausie sistemy i masiny, 2, pp. 58–73.
11. Yefimenko, S., 2018. Building Vector Autoregressive Models Using COMBI GMDH with Recurrent-and-Parallel Computations. In: Advances in Intelligent Systems and Computing II. AISC book series, V. 689. Cham: Springer, pp. 601–613.
12. Stepashko, V., 2018. From Inductive to Intelligent Modeling. In: Proceedings of the 13th IEEE International Conference CSIT-2018 & International Workshop on Inductive Modeling, September 11–14, 2018, Lviv, Ukraine. Lviv: Vezha&Co, pp. XXXII–XXXV.

Кардашевський Юрій Романович,
докторант Одеського державного
університету внутрішніх справ,
доктор філософії у галузі права

ILP ЯК ДИНАМІЧНА СИСТЕМА, ЩО РОЗВИВАЄТЬСЯ

Важливими акцентами імплементації моделі правоохоронної діяльності, керованої аналітичною розвідкою (*Intelligence-Led Policing – ILP*), є розуміння її не лише як певної процедури аналітичного процесу, а системне та комплексне сприйняття її як нової філософії правоохоронного менеджменту, що об'єктивно займатиме важливе місце у реформуванні правоохоронної діяльності в Україні. Українські правоохоронні органи вже застосовують певні аспекти моделі ILP, але в цілому вона ще не була повністю впроваджена [1]. Наразі, процеси успішної імплементації об'єктивно передбачають вивчення зарубіжного досвіду, врахування проблемних питань, визначення усього комплексу завдань та пріоритетів щодо упровадження в перспективі.

У 1994 році у Великій Британії вперше було впроваджено поліцейську діяльність, керовану аналітичною розвідкою. Її метою було «зменшення рівня злочинності та підвищення громадської безпеки» [3, с. 6]. Поліція графства Кент, перебуваючи під тиском щодо необхідності зниження злочинності та зіткнувшись зі скороченням фінансування, запровадила такого роду новацію, в результаті якої протягом трьох років відбулося зниження злочинності на понад 22 відсотки [3, с. 7]. Річард Андерсон у своїй праці «Intelligence-Led Policing: A British

Perspective», видавництва IALEIA, ключовими моментами ILP визначав: «Створення картинки ключової кримінальної активності; розуміння та візуалізація мережі наркоторговців у певному місці, наприклад, зосереджує аналітичний пошук на визначених потребах, допомагає у виборі цілей для максимального руйнування злочинності, пропонує можливості для вербування інформаторів і дозволяє розробляти гіпотези щодо майбутньої кримінальної активності, базуючись на запланованій правоохоронній діяльності» [3, с. 7–8].

У свою чергу, перша американська брошура на тему Intelligence-Led Policing була видана цією ж міжнародною асоціацією (IALEIA) у 1997 році, автором якої був тодішній спеціальний агент Департаменту громадської безпеки Айови Расс Портер. Він зазначив деякі загальні елементи ILP:

підготовка точних і своєчасних розвідувальних та аналітичних продуктів, що відповідають оперативним цілям відомства, які описують характер і масштаби проблем, що впливають на юрисдикцію;

використання цих розвідувальних та аналітичних продуктів для розробки та управління стратегією, оперативним планом або напрямом діяльності, з метою вирішення проблем;

постійне оцінювання, відстежування та звітування щодо визначення впливу стратегії чи операційного плану на проблему, внесення необхідних коригувань [4, с. 27].

Потер також зазначав, що жоден з елементів сам по собі не гарантує успішної поліцейської діяльності, керованої аналітичною розвідкою, а лише їх спільна дія.

У буклеті також розглядалися тенденції щодо упровадження ILP в Канаді та Європі. У Королівській канадській кінній поліції протягом семи років діяла Програма кримінальної розвідки, яка працювала над інтеграцією аналітичної розвідки до процесу управління та прийняття рішень організацією [5, с. 19]. У межах Європейського Союзу стратегічна аналітична розвідка була сфокусована на поточних і нових тенденціях, з метою отримання більшого успіху в боротьбі зі злочинністю [6, с. 23].

У липні 2001 року IALEIA опублікувала іншу працю під назвою «Запуск аналітичного підрозділу для поліцейської діяльності, керованої аналітичною розвідкою». Зміст цього посібника охоплював питання щодо місії, цілей і завдань до персоналу, винагороди, навчання, продуктів, оцінки, сертифікації та стандартів для аналітиків. Він був розрахований

на керівників поліції та у спрощеному форматі подачі визначав завдання для упровадження ILP в окремих юрисдикціях.

У 1998 році Міжнародна асоціація керівників поліції (*International Association of Chiefs of Police – IACP*) очолила зусилля щодо аналітичної розвідки, опублікувавши «*Model Policy on Intelligence»* [7, с. 15]. Ця політика визначала стандарти для більш ніж 17.350 правоохоронних підрозділів у Сполучених Штатах на той час. Її було переглянуто та повторно опубліковано в 2003 році. З-поміж іншого, цією політикою визначалося, що місія аналітичної розвідувальної функції полягає в тому, щоб збирати інформацію з усіх джерел у спосіб, який відповідає закону, та здійснювати аналіз інформації на тактичному та стратегічному рівнях щодо наявності, ідентифікації, можливостей окремих підозрюваних у злочинах, або компаній загалом, а також для досягнення цілей/пріоритетів, у сфері запобігання злочинам та правозастосування, визначених цим органом [8, с. 1].

Величезний вплив на усі правоохоронні органи та на усіх рівнях США мали теракти в Нью-Йорку, Вашингтоні та Пенсильванії у 2001 році. Менш ніж через 60 днів після терактів 11 вересня Міжнародна асоціація начальників поліції (IACP) провела свою щорічну конференцію в Торонто (Канада). IALEIA брала участь у цій конференції разом з багатьма іншими професійними поліцейськими організаціями. Під час конференції проводилися зустрічі та обговорювалися питання щодо правоохоронних заходів у відповідь на терористичний виклик [7]. Основна ідею саміту стосувалася обміну аналітичними розвідувальними даними. Зазначену ідею було розвинуто у березні наступного року в Арлінгтоні (штат Вірджинія). Участь взяли понад 100 поліцейських, які цікавилися питаннями аналітичної розвідки. Основні презентації були представлені щодо британської моделі National Intelligence Model (NIM), яку у подальшому було використано для розвитку відповідної американської моделі. Сутність британської моделі полягала у тому, щоб безпосередньо пов’язати планування заходів з операційними результатами. Вона передбачала довгострокові переваги інтегрованої системи розвідки, поєднуючи розвідувальні, профілактичні та правоохоронні дії на місцевому, регіональному та національному рівнях [9, с. 12].

На цій основі в подальшому розроблялися компоненти кримінальної розвідки для США та визначено план та координатора контролю цього плану – Координаційну раду

кримінальної розвідки (*Criminal Intelligence Coordinating Council – CICC*). Перед CICC також ставилися завдання:

забезпечення сумісності стандартів політики, інструкцій і операційних процедур щодо подальшого розвитку й інтеграції існуючих аналітичних розвідувальних систем з питань обміну даними (включаючи стандарти для збору, аналізу, розповсюдження, зберігання та очищення інформації);

встановлення на національному рівні стандартів аналітичної роботи у кримінальній розвідці, методів і освіти щодо формування місцевих, регіональних та федеральних зусиль та розвитку допомоги в оцінці загроз і підтримці правоохоронного курсу протидії злочинам, що посягають на громадську та національну безпеку;

співпраця з місцевими, регіональними та федеральними навчальними закладами, провайдерами тренінгів щодо внесення змін в тренінгові програми на підтримку нових цілей – обміну аналітичною розвідувальною інформацією;

співпраця на усіх рівнях щодо усуненням нормативно-правових перешкод, які обмежують обмін даними [10].

Координаційна рада (CICC) стала Глобальною робочою групою з аналітичної розвідки, яка створила Національний план обміну розвідувальними аналітичними даними (NCISP) та розробила 28 рекомендацій на його підтримку, включаючи підтримку поліцейської діяльності, керованої аналітичною розвідкою (ILP) [2], зокрема:

рекомендація 4 – план розроблено для зміцнення внутрішньої безпеки та сприяння поліцейській діяльності, керованій аналітичною розвідкою; існує критична потреба у збільшенні національного фінансування для досягнення цих цілей; без належного фінансування багато рекомендацій, наприклад покращення навчання та технічної інфраструктури, не будуть виконані, і країна залишатиметься під загрозою; правоохоронні органи США повинні співпрацювати, щоб визначити та фінансувати ініціативи, які втілюють рекомендації:

рекомендація 12 – Міжнародна асоціація аналітиків IALEIA повинна розробити від імені CICC мінімальні стандарти розвідувального аналізу даних, щоб гарантувати, що аналітичні продукти є точними, своєчасними, фактичними та актуальними, і рекомендувати впровадження політики та/або діяльності;

правоохоронні органи повинні прийняти ці стандарти, як тільки вони будуть розроблені та затверджені CICC.

У відповідь IALEIA створила фокус-групу для створення цих мінімальних стандартів, що призвело до випуску в листопаді 2004 року Аналітичних стандартів правоохоронної діяльності (*Law Enforcement Analytic Standards*), які включали як стандарти для аналітиків, так і для аналітичних продуктів. Крім того, було створено 18 стандартів для аналітичних продуктів за такими темами, як збір, точність, зміст, результати, плани поширення, звіти, формати, свідчення, відгуки та оцінка.

Після саміту та розроблення Національного плану обміну розвідувальними аналітичними даними (NCISP) Міжнародна асоціація начальників поліції (IACP) підтримала розробку білої книги «Intelligence Led Policing: The New Intelligence Architecture» [2], у якій зазначено, що поліцейська діяльність, керована аналітичною розвідкою, – це спільне підприємство, засноване на вдосконаленні розвідувальних операцій… для імплементації Intelligence Led Policing … аналітична розвідка має бути включена в процес планування для відображення суспільних проблем. Обмін інформацією має стати політикою… найголовніше, аналітична розвідка має залежати від якісного аналізу даних.

Багато хто зараз впроваджує або планує перехід до ILP за допомогою збору даних, баз даних і різноманітних аналітичних інструментів. Але потрібно більше. Як зазначалося раніше, має бути доступним додаткове навчання для аналітиків, менеджменту аналітичних підрозділів та керівників правоохоронних органів. Потрібна додаткова література, що висвітлює діяльність у цій галузі. Необхідно упроваджувати технологію, яка б відповідала викликам інформаційного вибуху. Ці зусилля потребують не лише експертних знань, а й фінансування. Все це вимагає лідерства.

Таким чином, упровадження та розвиток в Україні моделі правоохоронної діяльності, керованої аналітичною розвідкою (*Intelligence-Led Policing – ILP*), передбачає, перш за все, розуміння її не лише як певної процедури аналітичного процесу, а системне та комплексне сприйняття її як нової філософії правоохоронного менеджменту. Наразі, вивчення зарубіжного досвіду, врахування проблемних питань, визначення усього

комплексу завдань та пріоритетів щодо упровадження ILP є відправним моментом процесу успішної імплементації.

Список використаних джерел

1. Кардашевський Ю.Р. Становлення моделі правоохоронної діяльності, керованої аналітичною розвідкою. Наука і правоохорона. 2023. № 1. С. 117–125.

2. Smith, Angus. Intelligence Led Policing. Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts. 1997.

3. Anderson, Richard. Intelligence-Led Policing: A British Perspective. Angus Smith, editor. Lawrenceville, NJ: IALEIA.1997.

4. Porter, Russ. Getting Started in Intelligence-Led Policing. Angus Smith, editor. Lawrenceville, NJ: IALEIA. 1997.

5. Smith, Angus. Intelligence Led Policing. Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts. 1997.

6. Robertson, Simon. Intelligence-Led Policing: a European View. Angus Smith (ed). Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts. 1997.

7. Modafferi, Peter and Philip Lynn. Local Law Enforcement and Intelligence Led Policing / Intelligence Models and Best Practices. Lawrenceville, NJ: International Association of Law Enforcement Intelligence analysts. 1999.

8. International Association of Chiefs of Police. (IACP). Criminal Intelligence Model Policy. Alexandria, VA: IACP. 2003.

9. National Criminal Intelligence Service. National Intelligence Model. London, U.K.: National Criminal Intelligence Service. 2000.

10. International Association of Chiefs of Police. (IACP). Criminal Intelligence Sharing: A national plan for intelligence-led policing at the local, state and federal levels, report from the IACP Intelligence Summit. Alexandria, VA: International Association of Chiefs of Police. 2002.

11. Peterson, Marilyn. Intelligence-Led Policing: The New Intelligence Architecture. Washington: US Department of Justice. 2005.

Користін Олександр Євгенійович,
головний науковий співробітник
Державного науково-дослідного
інституту МВС України, доктор
юридичних наук, професор;
Бурангулов Владислав Андрійович,
ад'юнкт Одеського державного
університету внутрішніх справ

ТЕРМІНОЛОГІЯ КРИМІНАЛЬНОГО АНАЛІЗУ

Сучасний етап розвитку правоохоронної практики, з-поміж іншого, характеризується активним упровадженням та розвитком кримінального аналізу, забезпечуючи повноту та ефективність його використання на фоні потреби інноваційного розвитку інформаційно-аналітичної функції. Водночас теоретичне осмислення кримінального аналізу як нового інституту правоохоронної діяльності з відповідною термінологією, сприйняттям його змісту, форм та видів, процесу та формування аналітичного продукту, потребує активного залучення вітчизняної наукової спільноти.

Наразі, кримінальний аналіз, з точки зору методології застосування, що базується на досягненнях світової науки та практики, є достатньо визначеним інститутом і у своїй основі не має принципових відмінностей інституціонального упровадження різними суб'єктами в межах однієї юрисдикції. Але вітчизняна практика все ж вказує на низку проблемних питань щодо узгодженості сприйняття змісту, видів, рівнів кримінального аналізу, і щодо комплексності та системності його упровадження різними правоохоронними органами.

Частково ця проблема пов'язується з відсутністю достатнього наукового аналізу цього сегменту новизни, що має коріння іншомовного походження та часто на практиці використовується без належного обґрунтування і нерідко хибного трактування.

Використання кримінального аналізу в практиці вітчизняної правоохоронної діяльності нерідко йде у розріз його сутності, яка формувалася десятиліттями відповідною зарубіжною практикою та наукою, і сьогодні потребує принципового теоретичного осмислення змісту, розпочинаючи з самого терміну «кримінальний аналіз».

Наразі, мають місце дві особливості, на які потрібно звернути увагу перш ніж продовжувати аналіз змісту терміну

«*кримінальний аналіз*». Одна з них це те, що нормативне закріплення терміну «кримінальний аналіз» і саме на рівні закону в Україні реалізовано лише у 2021 році у зв'язку з прийняттям Закону України «Про бюро економічної безпеки України» [1], але практичне його застосування сягає ще 2006–2008 років, з упровадженням його у діяльності Державної прикордонної служби України [2], і друге – сам термін запозичено з англомовного використання «*crime analysis*».

Враховуючи запозиченість зазначеного терміну з іншої мови зазначимо, що семантика запозичених слів досить часто не збігається із семантикою їх прототипів у мові-джерелі. Виділяють різні типи семантичних змін запозиченої лексеми, зокрема: спрощення семантичної структури (запозичення в одному чи кількох значеннях при його значно ширшій полісемії в мові-джерелі); ускладнення семантичної структури (поява нових значень на ґрунті мови-реципієнта, в тому числі й таких, яких запозичене слово не мало в мові-джерелі); звуження значення запозиченого слова внаслідок його спеціалізації; розширення, зумовлене генералізацією відповідного поняття; зміна значення (термін уживається в системі мови-реципієнта в значенні, якого немає відповідне слово в мові-джерелі) [3]. Тобто, обґрунтованим є зауваження того що, не завжди прямий переклад професійного терміну є достатнім та об'єктивним щодо змісту сприйняття чи контексту застосування. Термінологічне закріплення іншомовного виразу є процесом обґрунтованої інтерпретації із врахуванням мови, культури, традицій і звісно змістовного наповнення.

Водночас, використання англомовного терміну «crime analysis» в інтерпретації «кримінальний аналіз», певним чином пов'язується з тим, що 3 травня 2006 р. за ініціативою Представництва Міжнародної організації з міграції в Україні проведено переговори представників Посольства США в Україні, Міжнародної організації з міграції, Адміністрації Держприкордонслужби України та Головної комендатури Прикордонної варти Республіки Польща, результатом яких стали досягнуті домовленості про запровадження спільного проекту щодо надання допомоги Державній прикордонній службі України з опрацювання підходів до запровадження системи управління ризиками та кримінального аналізу. Тобто, *«до правоохоронних органів України метод кримінального аналізу прийшов з Республіки Польща. Одним із перших*

прикордонних відомств, які успішно започаткували цю систему, є Прикордонна варта Республіки Польща» [4].

Таким чином, вивчаючи засади кримінального аналізу на базі польської правоохоронної системи, було запозичено інтерпретацію терміну саме з польської практики застосування – «*analizy kryminalnej*», «*analiza kryminalna*», який українською перекладається прямо – «кримінальний аналіз». Водночас, термін англійською «*crime analysis*», що використовується в англомовних країнах і, перш за все, у Великій Британії та США (де він виник і існує до сьогодні як окремий інститут) у прямому перекладі передбачає інтерпретацію – *аналіз злочину (злочинності)*.

Саме на це вказує історичний аналіз виникнення й поширення кримінального аналізу в правоохоронному середовищі та сприйняття в інтерпретації українською мовою як якісний аналіз злочину та подальше порівняння його з аналогічними минулими подіями.

Водночас, елементарною номінативною одиницею професійно-орієнтованих підмов вважається *термін* (від лат. *terminus* – межа, кордон) [5]. У ракурсі сучасного лінгвокогнітивного підходу термін уособлює особливу когнітивно-інформаційну структуру, у якій акумулюється виражене в конкретній мовній формі професійно-наукове знання [6, с. 332]. У зв'язку з цим терміни та їхні сукупності – *терміносистеми* й *термінополя,* розглядаються в тісному зв'язку з концептами як результатами мовленнєво-мисленнєвої діяльності [7]. Різниця між терміном і словом об'єктивно зумовлена тим, що вони відображають явища різних рівнів мисленнєвої діяльності – наукове мислення і побутове оперування уявленнями [6, с. 332].

Таким чином, юридичний термін є словом або словосполученням, яке уніфіковано вживається у сфері правових відносин, позначає юридичне поняття з певним ступенем дефінітивності, заданою моносемічністю (тобто однозначністю, семантичною визначеністю) та функційною стійкістю [8].

Наразі фактично саме *технічне перенесення з польської практики правоохоронної діяльності терміну «analizy krymtinalnej», що дійсно використовувався у польських нормативних актах й правоохоронній практиці, та його інтерпретація українською як «кримінальний аналіз», а не «аналіз злочинності», і стало причиною застосування в українській правоохоронній практиці та нормативних актах терміну «кримінальний аналіз.*

Таке перенесення характеризується окремим і відомим серед мовників типом спеціальних лексичних одиниць: *професіоналізмом* – ненормованою спеціальною лексикою, обмеженою вживанням в усному мовленні професіоналів [6, с. 332].

Водночас, так як «crime analysis» є англомовним терміном, ключовим все ж залишається його переклад українською та подальше змістовне наповнення і, що важливо, суспільне сприйняття та професійне використання різноманітних похідних інтерпретацій, які сьогодні набувають все більш масового вживання і не тільки у професійній сфері, зокрема: «кримінальна аналітика», «центр кримінальної аналітики», «кримінальний аналітик» тощо.

Семантичне освоєння запозиченого слова насамперед передбачає становлення його лексичного значення на ґрунті мови-реципієнта [8]. Аналізуючи семантику терміну-словосполуки «кримінальний аналіз» зазначимо, що у ньому використовується опорне слово «аналіз» та прикметникове означення «кримінальний».

Відомості про першу згадку слова «кримінальний» (XVII ст.) та його фіксація в сучасних тлумачних словниках української мови засвідчують, що в семантичній структурі цього слова є етимологічно виявлені домінантні семи (елементарні ознаки змісту) «злочинний / злочин / злочинність / злочинець» і «карний / кара / покарання» та власне диференційні ознаки «судовий / осуд», «неприпустимий», «розслідування». Тобто, в українській мові слово кримінальний відноситься до синонімічного ряду «кримінальний – карний – злочинний» і саме у такій послідовності [11], що, власне, й спричиняє небажані для терміну «кримінальний» різночитання.

Наразі, прикметник «кримінальний» запозичено з латини багато сторічь тому: латинський прикметник *criminalis* походить від іменника *crimen (criminis)*, що означає злочин. Відповідно в сучасній літературній мові він набув таких значень: 1) Злочинний. 2) Той, що стосується вивчення злочинів і злочинності, боротьби і запобігання злочинам [12, с. 370].

Таким чином, дійсно має місце різночитання терміну «кримінальний аналіз» і особливо похідних від нього родових виразів: «кримінальна аналітика», «центр кримінальної аналітики», «кримінальний аналітик» тощо. Водночас, враховуючи факт досить тривалого (з 2006 року) практичного термінологічного застосування у професійному середовищі українських

правоохоронних органів, малоймовірним є сприйняття терміну «кримінальний аналіз» як «злочинний аналіз».

Водночас, залишається нав'язливою думка щодо неоднозначного семантичного сприйняття термінів:

«кримінальний аналітик» –

злочинець чи той, хто протидіє злочинності?;

«кримінальна аналітика» –

злочинна аналітика, чи діяльність з аналізу злочинності?

Це дійсно є дискусійним, але

з точки зору правозастосування та однозначності у визначеннях та сприйнятті як у професійному середовищі, так і назагал у суспільстві, важливим є обґрунтоване їх використання з прямим означенням змісту, уникаючи різночитань та семантичного сприйняття.

Право як і будь-яка інша галузь знань вербалізується мовними засобами, надбудованими над загальновживаною мовою. Термінологія права, яку також називають термінологією правозастосовної практики, є формалізованим утворенням для семіотичного забезпечення професійного спілкування, а вербальні продукти такого спілкування втілюють частину правової картини світу відповідної лінгвокультури [6, с. 332].

Тобто термінологія правозастосовної практики має бути основою професійної культури та відображати узгоджене професійне використання й застосування з семантичним сприйняттям у суспільстві.

***Прикладом** узгодженого застосування є діяльність Міжнародної асоціації аналітиків злочинності (International Association of Crime Analysts – IACA). Не дивлячись на те, що у назві IACA використовується словосполучення «Crime Analysts», що українською теж має дискусійну інтерпретацію, все ж, активно займаючись сертифікованою підготовкою аналітиків, у назві тренінгових програм використовують словосполучення «Law Enforcement Analyst» [13], яке не викликає неоднозначності семантичного сприйняття і прямо інтерпретується як «аналітик правоохоронного органу».*

І такий підхід є чітким прикладом того як необхідно уникати різночитань у використанні юридичних термінів.

Таким чином, *враховуючи певні особливості професійного використання терміну «кримінальний аналіз», можливим та достатньо обґрунтованим є сприйняття та узгоджене використання його в інтерпретації як «аналіз злочинності».*

Водночас, некоректним все ж залишається професійне використання термінів «кримінальний аналітик», «кримінальна аналітика».

Уникаючи різночитань та неадекватного сприйняття їх змісту, порівняно з професійним осередком, більш широкою громадянською спільнотою, використання термінів:

- ✓ *«аналітик правоохоронного органу»,*
- ✓ *«аналітик злочинності»,*
- ✓ *«аналітична діяльність, що пов'язана з дослідженням злочинності»,*
- ✓ *«аналітика злочинності»*

відповідно, є більш коректним та менш дискусійним у визначенні відповідної правоохоронної діяльності.

Список використаних джерел

1. Закону України «Про бюро економічної безпеки України» (28 січня 2021 року № 1150-IX).

2. Наказ Адміністрації Держприкордонслужби України від 21 лютого 2007 року № 130 «Про запровадження системи управління ризиками та системи кримінального аналізу у Державній прикордонній службі України»; наказ Адміністрації Держприкордонслужби України від 15 січня 2008 року № 28 «Про затвердження Інструкції про організацію та ведення кримінального аналізу оперативно-розшуковими підрозділами»

3. Сергєєва Г.А. Англомовні запозичення в українській правничій термінології : дис. … кандидата філол. наук : 10.02.01. Х., 2002. 250 с.

4. Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України ; навчальний посібник / Кіреєва О. С., Крутік Ю. В., Махлай О. М. , Треус А. С. / за заг. ред. кандидата психол. наук, доцента О. С. Кіреєвої. Хмельницький : Вид-во НАДПСУ, 2022. 388 с.

5. Манжос Я. Ю. Семантичні та функціональні особливості англомовних юридичних термінів – назв злочинів проти людини: автореф. дис. ... канд. філол. наук : 10.02.04. Х., 2011. 20 с.

6. Олійник О. Юридичні терміни як вербальні репрезентанти правового концепту наукові записки Серія: Філологічні наук. Вип. 165. С. 331–338.

7. Главацька Ю. Термінологічне поле vs терміносистема: принципи наповнення та структурації термінологічного поля в

мові. Науковий вісник Херсонського державного університету. Серія: «Лінгвістика». 2014. № 21. С. 15–18.

8. Ляшук А. М. Семантична структура юридичних термінів української та англійської мов : дис... канд. філол. наук: 10.02.17. Кіровоград, 2007. 335 арк.

9. URL: https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D1%96%D0%B7#:~:text=%D0%90%D0%BD%D0%B0%.

10. Jerry H. Ratcliffe, PhD Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders URL: http://www.policefoundation.org/docslibrary.html and URL: http://www.cops.usdoj.gov/2007.

11. В. Л. Іващенко, Л. М. Василькова Кримінальний кодекс України – карний кодекс україни. Кримінально-процесуальний кодекс України – карно-процесуальний кодекс України. Термінологічний вісник 2013, вип. 2(2). С. 185–187.

12. Словник іншомовних слів / За ред. акад. О. С. Мельничука. К.: Гол. ред. УРЕ, 1977. 775 с.

13. URL: https://www.iasa.net/certification.

Кисельов Андрій Олександрович,
доцент кафедри оперативно-розшукової діяльності факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ,
кандидат юридичних наук, доцент

ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ НА ПРИКЛАДІ ЗДІЙСНЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ

У сучасному інформатизованому суспільстві правоохоронним органам для ефективної протидії злочинності необхідно здійснювати пошук та аналіз інформації, а також інтерпретувати її з метою проведення оцінювання, прогнозування, створення аналітичних висновків та відповідних рекомендацій. Тому основою поліцейської діяльності є застосування розвідувальної аналітики та проведення кримінального аналізу [1, с. 7]. Принциповою відмінністю кримінального аналізу від інформаційно-аналітичної діяльності є можливість отримання

нової, раніше невідомої ініціатору розробки оперативно значимої інформації не лише про події та об'єкти, але і про причинно-наслідкові зв'язки, додаткові кваліфікуючі ознаки (стійкість, згуртованість, наявність внутрішньої ієрархії в групі, розподілення ролей тощо). Крім того, з'являється реальна можливість оперативного прогнозування ймовірних подій [2].

Під час освітньої діяльності в Дніпропетровському державному університеті внутрішніх справ здобувачі вищої освіти набувають знання, уміння та навички здійснення кримінального аналізу в межах відповідних навчальних та факультативних занять.

Метою доповіді є визначення деяких особливостей набуття знань, умінь та навичок під час здійснення здобувачами вищої освіти кримінального аналізу.

Так, здобувачі вищої освіти, в межах практичних занять, здійснюють збір та аналіз інформації з якомога більшої кількості інформаційних ресурсів, а також інших джерел інформації, до яких можна віднести відкриті інформаційні реєстри, сервіси тощо, а також соціальні мережі. На початку навчання, здобувачами освіти встановлюються ПІБ (в тому числі варіація написання латиницею), дата та місце народження особи щодо якої буде здійснюватись кримінальний аналіз, адреси її реєстрації та проживання, адреси електронних скриньок, реєстрація у соціальних мережах, а також абонентські номери, якими користується особа. Після перевірки у відповідних реєстрах (програмах) тощо, особа перевіряється на предмет реєстрації в якості фізичної особи-підприємця, засновника, керівника чи кінцевого бенефіціарного власника підприємств. Далі встановлюються персональні сторінки у соціальних мережах «Фейсбук», «Одноклассники», «ВКонтакте», «Інстаграм» та ін. Пошук персональних сторінок в окремих мережах має свої особливості. Так, пошук інформації в соціальній мережі «Фейсбук» здійснюється шляхом стандартного пошуку за ключовими словами та шляхом використання «розумної» системи «Graph Search». Остання працює лише в англомовній версії сайту, хоча географія пошуку нічим не обмежується. Під час пошуку інформації в Інстаграм слід враховувати, що будь-хто може встановити підроблені теги геолокації чи опублікувати не власні фотографії. Проте, якщо в профайлі є справжні фотографії, вони можуть допомогти виявити дійсні дані автора або спростувати оприлюднені ним фейки. Особливістю пошуку в

Instagram є те, що за результатами запиту у видачі завжди буде відображатися один результат, найбільш пов'язаний із запитом, причому з першим його словом. Отриманий результат можна впорядкувати за різними категоріями. Здійснити пошук по профайлу і знайти фотографії, опубліковані в ньому за певний проміжок часу, пошук в Instagram не дозволяє. Найпростіший спосіб знайти людину в Інстаграмі – це пошук по ніку. В мережі інтернет наявні безкоштовні й платні програми та сервіси, які дозволяють, завантаживши фотозображення, отримати вказану інформацію.

Правовий режим воєнного стану вніс корективи у роботу не тільки практичних підрозділів Національної поліції, але й відкорегував пріоритетні напрямки підготовки фахівців для підрозділів Національної поліції. Так, робочими програмами навчальних дисциплін оперативно-розшукового спрямування передбачені відповідні теми із документування воєнних злочинів та колабораційної діяльності, практичні навички із закріплення яких здобувачі можуть відпрацювати на факультативних заняттях з відповідних дисциплін, зокрема з дисципліни «Основи кримінального аналізу». Підсумовуючи, варто зазначити, що під час підготовки фахівців для підрозділів Національної поліції України існує ряд особливостей, врахування яких науково-педагогічними та іншими особами, які приймають участь у підготовці фахівців, дозволить підвищити рівень набутих знань, умінь та навичок.

Список використаних джерел

1. Основи кримінального аналізу: підручник. Бабенко А.М., Заєць О.М., Некрасов В.А., Ісмайлов К.Ю., Пефтієв Д.О. та ін.; за заг. ред. Користіна О.Є., 2019. 296 с.

2. Яніцкі Мірослав. Оперативний кримінальний аналіз : навч.-практ. посіб. переклад Ігоря Родюка / за ред. Міжнародної організації з міграції – Республіка Польща, 2009. 86 с.

Кіреєва Ольга Сергіївна,
Національна академія Державної прикордонної служби України імені Богдана Хмельницького, кандидат психологічних наук, доцент

ПІДГОТОВКА КРИМІНАЛЬНИХ АНАЛІТИКІВ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НА БАЗІ НАЦІОНАЛЬНОЇ АКАДЕМІЇ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

На теперішний час кримінальний аналіз є одним з найефективніших аналітичних інструментів в протидії злочинній діяльності.

Так, відповідно статті 8 Закону України «Про оперативно-розшукову діяльність» підрозділи, які здійснюють оперативно-розшукову діяльність мають право безпосередньо проводити або ініціювати проведення кримінального аналізу [1].

Державна прикордонна служба України є першим правоохоронним органом в Україні, в якому, з метою здійснення кримінального аналізу, в оперативних підрозділах із 2008 року діють підрозділи кримінального аналізу.

Сьогодні підрозділи кримінального аналізу оперативних підрозділів Державної прикордонної служби України укомплектовані майже на 90 %, що сприяє високій ефективності виконання поставлених завдань.

Серед офіцерів і майбутніх офіцерів вважається престижним проходити службу в підрозділах кримінального аналізу оперативних підрозділів Державної прикордонної служби України.

Такого попиту на посади в підрозділах кримінального аналізу досягнуто шляхом проведення заходів популяризації цього напряму діяльності:

обмін досвідом;

залучення до конференцій міжнародного рівня;

висвітлення найбільш цікавих справ, по яких працювали кримінальні аналітики;

залучення до проведення занять стейкхолдерів із числа найкращих кримінальних аналітиків підрозділів кримінального аналізу оперативних підрозділів Державної прикордонної служби України [2].

Крім того, проходження служби в підрозділах кримінального аналізу оперативних підрозділів Державної

прикордонної служби України надає офіцерам можливість кар'єрного зростання, а також отримання додаткової грошової надбавки за аналітичну діяльність.

За останніх 15 років неодноразово відбувалися організаційно-штатні зміни підрозділів кримінального Державної прикордонної служби України, однак незмінними лишалися вимоги до особового складу даних підрозділів, а саме всі аналітики мають бути фахівцями вищого рівня.

Тому для забезпечення ефективної діяльності підрозділів кримінального аналізу оперативних підрозділів Державної прикордонної служби України дані підрозділи потребують підготованих фахівців-аналітиків.

У «Короткому тлумачному словнику керівника підрозділу кримінального аналізу» аналітик розглядається як посадова особа підрозділу кримінального аналізу, що володіє необхідними знаннями та досвідом аналізу управлінських ситуацій, підготовки аналітичних звітів, висновків та пропозицій [3].

В Державній прикордонній службі України підготовка кримінальних аналітиків оперативних підрозділів здійснюється на базі Національної академії Державної прикордонної служби України імені Богдана Хмельницького під час проходження військовослужбовцями спеціалізованого курсу оперативного кримінального аналізу.

Особливість підвищення кваліфікації кримінальних аналітиків полягає в тому, що слухачами є офіцери оперативно-розшукових підрозділів, які вже володіють певними знаннями і практичними навичками виконання професійних обов'язків, і можуть в силу цього критично ставитися до навчального матеріалу, прагнучи отримати саме те, що їм перш за все потрібно для професійної діяльності.

Тому, для забезпечення якісної підготовки кримінальних аналітиків всі викладачі мають практичний досвід роботи в оперативних підрозділах Державної прикордонної служби України і постійно проходять різноманітні курси підвищення кваліфікації у сфері кримінального аналізу не лише в Україні, а й за кордоном.

Для підготовки кримінальних аналітиків на базі кафедри спеціальних дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького облаштовано спеціальний комп'ютерний клас, який оснащено сучасною технікою і сучасним програмним забезпечення.

Спеціалізований навчальний курс підготовки кримінальних аналітиків «Оперативний кримінальний аналіз» розрахований на 210 навчальних годин та охоплює 12 навчальних тем. Основними видами занять даного курсу є лекції та практичні, у співвідношенні 20 % – лекції, 80 % – практичні заняття. Закінчується даний курс складанням комплексного екзамену, який складається з двох частин: теоретичної (тестування) та практичної (слухачі в рамках учбової ОРС виконують звіт кримінальною аналітика).

Під час проходження спеціалізованого курсу кримінальні аналітики вивчають:

поняття аналітичної діяльності, кримінального аналізу, види та форми кримінального аналізу;

сутність процесу кримінального аналізу, етапи та послідовність дій щодо здійснення кримінального аналізу з використанням наявної інформації та інформаційних ресурсів;

поняття та порядок формулювання гіпотез;

поняття та призначення схем зв'язків, перетину державного кордону, подій, діяльності, аналізу телефонних роздруківок, аналізу правопорушення, злочину тощо;

призначення та порядок застосування аналітичної техніки в процесі кримінального аналізу та комп'ютерного програмного забезпечення i2 «Analyst's Notebook» та «iBase», Microsoft Exel, представлення результатів аналітичних дій.

По закінченню проходження курсу кримінальні аналітики готові до самостійної роботи і мають практичні навички щодо:

– застосовування аналітичної техніки та комп'ютерного програмного забезпечення i2 «Analyst's Notebook» та «iBase», Microsoft Exel, здійснення імпорту (експорту) даних;

– використання відомчих баз даних та баз даних інших правоохоронних органів України, а також інших інформаційних ресурсів, зокрема «Clearview», «Artellence», «RuAssets», «Delta», «YouControl», АС «Електронний журнал» ДП «Український державний центр міжнародної освіти», Державного реєстру актів цивільного стану громадян, Єдиного державного реєстру судових рішень, ЄАІС Держмитслужби, тощо;

– здійснення пошуку особи у відкритих джерелах інформації;

– встановлення власника телефонного номеру з використанням наявних інформаційних ресурсів;

– оформлення і презентації результатів аналізу в цілому у вигляді аналітичних звітів та його окремих елементів у

вигляді схем, формулювання та аргументування на основі результатів аналізу своїх висновків й рекомендацій щодо можливих подальших дій, використовуючи для цього наявні підручні засоби та наочний матеріал.

Таким чином, після успішного закінчення спеціалізованого навчального курсу «Оперативний кримінальний аналіз» кримінальний аналітик готовий виконувати свої функціональні обов'язки у повному обсязі та самостійно.

Список використаних джерел

1. Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 року № 2135-XII / Відомості Верховної Ради України. 1992. № 22. Ст. 303.

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

3. Кіреєва О. С., Половников В. В., Фаріон О. Б. Короткий тлумачний словник керівника підрозділу кримінального аналізу : словник. Хмельницький : НАДПСУ, 2016. 68 с.

Крутік Юрій Вікторович,
заступник начальника управління – начальник першого відділу управління інформаційно-аналітичного забезпечення та кримінального аналізу Департаменту оперативно-розшукової діяльності Адміністрації Держприкордонслужби, кандидат наук з державного управління;
Головацький Володимир Григорович,
старший офіцер першого відділу управління інформаційно-аналітичного забезпечення та кримінального аналізу Департаменту оперативно-розшукової діяльності Адміністрації Держприкордонслужби

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ ПІДРОЗДІЛІВ КРИМІНАЛЬНОГО АНАЛІЗУ

2022 рік став водночас переломним і знаковим для історії нашої держави, з першої хвилини широкомасштабного

вторгнення російської федерації в Україну, що сталося вночі 24 лютого 2022 року, українське суспільство зрозуміло, що у довгостроковій перспективі ми постійно стикатимемося із загрозами для безпеки нашої держави та кожного її громадянина. Разом із цим, нікуди не зникли прояви протиправної діяльності, які були притаманні нашому суспільству раніше і усі суб'єкти сектору державної безпеки та оборони чітко усвідомлюють, що в подальшому збережеться тенденція використання злочинцями для здійснення протиправної діяльності все краще організованих та більш якісно спланованих схем злочинної діяльності.

Протидіяти належним чином військовій агресії російської федерації та проявам злочинності, яка постійно вдосконалюється, можна шляхом використання сил та засобів підрозділів кримінального аналізу. Світова практика показує, що за сучасних умов мінливого зовнішнього середовища, для ефективного виконання вищевказаних завдань потрібно системно проводити заходи щодо аналізу та оптимізації робочих процесів органів державної влади.

Як позитивний приклад здійснення аналізу та оптимізації робочих процесів органів державної влади України слід відмітити участь персоналу управління інформаційно-аналітичного забезпечення та кримінального аналізу Департаменту оперативно-розшукової діяльності Адміністрації Держприкордонслужби у проєкті «Підтримка ЄС у зміцненні інтегрованого управління кордонами в Україні (EU4IBM)». Дані заходи проводили міжнародні експерти із вдосконалення робочих процесів та співробітники Адміністрації Держприкордонслужби, дотримуючись міжнародно визнаної методології вдосконалення робочих процесів «Lean Six Sigma (LSS)», а також відповідно до Методики аналізу та оптимізації робочих процесів і процедур в органах виконавчої влади, розробленої Кабінетом Міністрів України.

За результатами проведення заходів щодо аналізу та оптимізації робочих процесів міжнародними експертами спільно із персоналом управління інформаційно-аналітичного забезпечення та кримінального аналізу Департаменту оперативно-розшукової діяльності Адміністрації Держприкордонслужби відпрацьовано звіт та рекомендації. В ході роботи міжнародні експерти погодились із персоналом управління інформаційно-аналітичного забезпечення та кримінального аналізу щодо необхідності вдосконалення процесу перевірки інформації по інформаційно-комунікаційних системах (реєстрах, базах даних) органів

державної влади та відкритих джерелах інформації. На сьогодні дані заходи не мають системного та уніфікованого характеру, що негативно відображається на швидкості проведення оперативного кримінального аналізу.

На даний час персонал підрозділів кримінального аналізу використовує в повсякденній діяльності близько 25 інформаційно-комунікаційних систем (реєстрів, базах даних) та 30 відкритих джерел інформації. Враховуючи курс держави на діджиталізацію, з часом кількість інформаційно-комунікаційних систем буде збільшуватись, відповідно і час на перевірку об'єктів зацікавленості значно зросте. На даний час перевірка оперативної інформації по інформаційних ресурсах та її подальша систематизація є одним із найбільш часозатратних процесів у ході оперативного кримінального аналізу. Підвищити ефективність даної роботи можна шляхом запровадження в державі єдиної інформаційної системи органів державної влади, з можливістю долучення до неї відомостей з інформаційних систем (баз даних) комерційних установ та відкритих джерел інформації. За умови реалізації в даній системі принципу «Один запит – комплексний результат» вона зможе значно підвищити ефективність роботи сектору державної безпеки і оборони, а саме:

1) зменшить час на перевірку інформації щодо громадян (їх транспортних засобів, телефонних номерів, об'єктів нерухомого майна, належних їм юридичних осіб, сплачених податків, наявності податкової заборгованості, судимостей, фактів притягнення до адміністративної відповідальності та інших оперативно значимих даних);

2) мінімізує можливий негативний вплив людського фактору в процесі перевірки інформації по окремих інформаційно-комунікаційних системах (введення при перевірці частково помилкових даних, не використання при проведенні перевірки окремих інформаційних ресурсів та інше);

3) забезпечить виявлення та притягнення до відповідальності більшої кількості осіб, які причетні до скоєння злочинів;

4) підвищить ефективність заходів із протидії транскордонній злочинності та зменшить рівень латентної злочинності;

5) покращить реалізацію превентивної функції кримінальної та адміністративної відповідальності;

6) підвищить рівень захисту державного суверенітету, територіальної цілісності та недоторканності державних кордонів;

7) мінімізує ризики втручання у внутрішні справи України;

8) покращить якість проведення заходів, які безпосередньо чи опосередковано забезпечують гарантування конституційних прав і свобод людини і громадянина;

9) забезпечить сталий розвиток громадянського суспільства, його демократичних інститутів;

10) сприятиме зміцненню політичної і соціальної стабільності в суспільстві;

11) сприятиме інтеграції України в європейський політичний, економічний, правовий простір та в євроатлантичний безпековий простір.

Надзвичайно важливо у єдиній інформаційній системі органів державної влади передбачити можливість для співробітників правоохоронних органів та спецслужб автоматизовано вивантажувати дані щодо оперативно значимих зв'язків особи (у формі таблиць та графічних схем), які стосуються (випливають із) наступних аспектів:

1) спільної причетності до протиправної діяльності;

2) спільних перетинів державного кордону України на транспортних засобах;

3) реєстрації за тою ж адресою, що й об'єкт зацікавленості;

4) спільного ведення підприємницької діяльності;

5) ведення спільного побуту (родинні зв'язки);

6) надання права вчиняти юридично значимі дії (оформлення доручення чи довіреності);

7) перереєстрації транспортних засобів;

8) спільного володіння нерухомим майном;

9) спільного навчання у закладах освіти;

10) спільного місця роботи;

11) спільної участі у тендерах;

12) поштових відправлень об'єкта зацікавленості;

13) «е-декларацій» осіб, уповноважених на виконання функцій держави або місцевого самоврядування;

14) податкових декларацій про майновий стан і доходи та інших даних.

В ході проведення заходів із вдосконалення робочого процесу організації і здійснення кримінального аналізу в Дерпжприкордонслужбі міжнародні експерти також підтримали

бачення персоналу управління інформаційно-аналітичного забезпечення та кримінального аналізу щодо доцільності внесення змін до алгоритму отримання доступу до інформаційно-комунікаційних систем (реєстрів, базах даних). На нашу думку, давно застаріла система отримання доступу до наявних у державі інформаційно-комунікаційних систем (реєстрів, базах даних), оскільки вона передбачає відпрацювання різного роду формалізованих документів (угоди, договори, заявки, зобов'язання, переліки посадових осіб та інші), які у друкованому чи електронному вигляді довго циркулюють між різними управлінськими ланками органів державної влади. На зміну діючій процедурі отримання доступів до інформаційно-комунікаційних систем доцільно запровадити оновлену, яка полягатиме у затверджені на рівні Кабінету Міністрів України стандартизованих переліків посадових осіб конкретного органу певного відомства, які можуть отримувати доступ до окремих підсистем єдиної інформаційної системи органів державної влади (з урахуванням норм посадових обов'язків). Доступ до цих ресурсів пропонується надавати адміністраторами єдиної інформаційної системи органів державної влади по запиту відповідного керівника органу (установи).

Разом із цим, доцільно змінити процедуру скасування доступу до вказаних інформаційних систем, на нашу думку, це можна реалізувати як окремий пункт інформаційного меню в особистому кабінеті користувача, з покладанням даних обов'язків на кожну особу яка користується даними системами (з можливістю формування звіту про виконання даного запиту адміністраторами).

Двадцять перше століття називають епохою «інформаційних технологій», оскільки вона відкриває надзвичайні можливості для інститутів, які здатні будувати ефективні моделі управління інформацією. Так, Україна стала першою державою у світі з цифровими паспортами, які мають таку ж юридичну силу, що й паперові документи. Запровадження в Україні єдиної інформаційної системи органів державної влади буде проривом, який дозволить значно підвищити якість роботи державних інститутів, оскільки інформація у сучасному світі являється стратегічним ресурсом, уміле розпорядження яким гарантує успіх у будь-якій сфері суспільного життя.

Більше двох століть тому англійський банкір, бізнесмен і фінансист Натан Ротшильд сказав всесвітньо відоме висловлювання: «Хто володіє інформацією – той володіє

світом» (воно стало крилатим після того, як його процитував Вінстон Черчилль), свою актуальність дане висловлювання зберігає й сьогодні.

Список використаних джерел

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

2. Яніцкі М. Оперативний кримінальний аналіз : навчально-практичний посібник / М. Яніцкі; переклад Ігоря Родюка / за редакцією Міжнародної організації з міграції – Республіка Польща, 2009. 86 с.

3. Кіреєва О. С. Короткий тлумачний словник керівника підрозділу кримінального аналізу / О. С. Кіреєва, В. В. Половников, О. Б. Фаріон // Словник : Видавництво НАДПСУ, 2016. 68 с.

4. Посібник з кримінального аналізу для кримінальних аналітиків ДПСУ // ОБСЄ. 2015. 176 с.

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

ПРОФІЛЬ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ КРИМІНАЛЬНОГО АНАЛІТИКА: КОНЦЕПТУАЛЬНІ ЗАСАДИ РОЗРОБЛЕННЯ

Кримінальний аналіз є основою Моделі правоохоронної діяльності, керованою аналітичною розвідкою (Intelligence-Led Policing, ILP), яка спрямована на інтеграцію інтелектуальних аналітичних підходів у правоохоронну діяльність, підвищення ефективності правоохоронних органів, шляхом збільшення ролі аналітичної розвідки в процесі прийняття рішень та планування. Така діяльність серед іншого вимагає наявності висококваліфікованих працівників, які володіють необхідними навичками та знаннями.

Разом з тим, не зважаючи на зростаючий запит правоохоронних органів України на працівників, що володіють компетентностями у сфері інформаційних технологій та кримінального аналізу, на сьогодні, відсутнє єдине бачення щодо необхідного рівня знань, навичок, досвіду, якостей та інших характеристик, які потрібні для ефективного виконання таких обов’язків.

Наявність такого бачення, зокрема у формі профілю професійної компетентності, є важливим для створення стандартизованого освітнього фреймворку, розроблення та впровадження ефективних програм навчання та підвищення кваліфікації відповідно до сучасних вимог та технологій, забезпечення практичної орієнтації та відповідності до вимог роботодавців, підвищення готовності випускників до виконання посадових обов'язків, формування професійної спільноти кримінальних аналітиків. Профіль професійної компетентності - комплексна характеристика посади, що містить визначення змісту виконуваної за посадою роботи та перелік спеціальних знань, умінь і навичок, необхідних працівнику для якісного виконання посадових обов'язків.

Отже, виникає необхідність визначення обсягу знань та навичок необхідного для виконання завдань, які стоять перед кримінальними аналітиками, зокрема в поліції. З цією метою автор спробував узагальнити в одному документі (додаток) перелік компетентностей, яким має володіти працівник поліції, на якого покладено функції здійснення кримінального аналізу, ґрунтуючись на міжнародній практиці та рекомендаціях, а також результатах особистих спостережень та використанні власного досвіду, набутого під час участі у проєктах з впровадження кримінального аналізу в Національній поліції України та роботи в підрозділах кримінальної поліції.

Створення профілю професійної компетентності сприятиме уніфікації, стандартизації та гармонізації сфери кримінального аналізу, покращенню співпраці між слідчими, оперативниками та аналітиками, професійному розвитку та популяризації цього виду професійної діяльності в суспільстві.

Додаток

Профіль професійної компетентності кримінального аналітика

І. ХАРАКТЕРИСТИКА ПОСАДИ

1.1. Мета посади:

Здійснення аналізу оперативних даних та інформації з метою встановлення фактів злочинної діяльності та фактів з нею пов'язаних, а також визначення напрямків для подальшого розслідування.

Здійснення аналізу інформації з метою виявлення трендів та закономірностей злочинності.

Сприяння в розробці та впровадженні стратегій та протоколів для протидії злочинності.

Загальна мета посади полягає в забезпеченні більш ефективного виявлення, аналізу, прогнозування та реагування на злочинність, з метою зменшення її рівня та покращення загальної безпеки в суспільстві.

1.2. Зміст виконаної за посадою роботи:

Здійснення детального аналізу злочинності, включаючи збір та обробку даних, виявлення злочинних тенденцій та встановлення можливих закономірностей.

Використання сучасних інструментів аналізу даних, таких як програми для статистичного аналізу, інструменти візуалізації даних, бази даних та аналітичні програми.

Розробка та вдосконалення методик аналізу злочинності для ефективного виявлення, запобігання та розкриття злочинів.

Виявлення ключових ареалів злочинності за видами злочинів, що потребують особливої уваги та пошук заходів з протидії.

Аналіз злочинної діяльності, встановлення важливої для розслідування інформації, зокрема можливих мотивів, для надання підтримки в розслідуванні злочинів та впровадженні профілактичних заходів.

Підготовка аналітичних продуктів для використання в кримінальних провадженнях та матеріалах оперативно-розшукових справ, публічних звітах та стратегічному плануванні боротьби зі злочинністю.

Моніторинг та оцінка ефективності запроваджених заходів та стратегій впливу на злочинність, а також розробка рекомендацій щодо подальших дій.

Пошук та аналіз даних з метою виявлення злочинності;

Взаємодія з іншими правоохоронними органами, організаціями та відомствами з питань аналізу злочинності.

ІІ. ВИМОГИ ДО РІВНЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ОСОБИ

2. Мінімальні загальні вимоги

2.1. Освітньо-кваліфікаційний рівень:

Бакалавр або магістр відповідної спеціальності.

2.2. Напрям підготовки (спеціальність):

Основними напрямами підготовки є підготовка за спеціальностями: правоохоронна діяльність, комп'ютерні науки та інформаційні технології, соціологія, економіка, право.

Певний досвід за відповідною спеціальністю може вважатися додатковою перевагою.

3. Спеціальні вимоги:

3.1. Досвід роботи:

Важливо, щоб кримінальний аналітик мав деякий досвід роботи в поліції або іншому правоохоронному органі, а також досвід виконання завдань з аналізу злочинності, інших даних та зв'язків.

3.2. Перелік знань, необхідних для виконання посадових обов'язків:

Знання основ кримінального аналізу та НПА, що регулюють інформаційно-аналітичну діяльність;

Знання аналітичного циклу та його змісту;

Знання основ логіки;

Знання процесу виявлення, розслідування та розкриття злочинів;

Знання процедур та методів збору доказів та підготовки справ для суду;

Знання інформаційних технологій обробки даних та аналітичного ПЗ;

Знання основ кримінології, соціології та психології злочинності;

Знання кримінального права та кримінального процесу;

Знання методів дослідження;

Знання методів, технік пошуку та аналізу інформації.

3.3. Перелік умінь та навичок, необхідних для виконання посадових обов'язків:

Уміння мислити логічно та критично;

Уміння працювати з різними джерелами даних;

Уміння шукати інформацію, у тому числі методом OSINT та обробляти дані;

Уміння аналізувати та синтезувати інформацію;

Уміння виконувати статистичний аналіз даних;

Уміння вести документацію, готувати звіти та аналітичні документи, лаконічно формулювати аналітичні висновки та рекомендації, а також представляти результати аналітичних досліджень;

Уміти ідентифікувати та аналізувати закономірності у злочинності;

Комунікаційні навички для спілкування з іншими членами правоохоронних органів, свідками, підозрюваними та громадськістю;

Навички роботи з програмами для обробки, аналізу та візуалізації даних;

Вміння працювати в команді та координувати дії з іншими фахівцями з різних областей правоохоронної діяльності.

3.4. Інші вимоги до рівня професійної компетентності:

Здатність до постійного навчання та оновлення знань у сфері інформаційних технологій та кримінального аналізу;

Дисциплінованість та відповідальність у виконанні посадових обов'язків;

Здатність до прийняття швидких та обґрунтованих рішень у ситуаціях, що вимагають оперативності;

Високий рівень професійної етики та усвідомлення важливості дотримання законності та прав громадян;

Етичність та здатність до збереження конфіденційної інформації;

Креативність.

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

МОЖЛИВОСТІ ТА ПЕРЕВАГИ ВИКОРИСТАННЯ КЛАСИФІКАЦІЙНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Сучасні методи аналізу великих обсягів даних вимагають спеціалізованих інструментів. Традиційні текстові та табличні процесори, як MS Excel, обмежені у своїх можливостях обробки великих даних через великі витрати на апаратні ресурси та максимальну межу в 1 048 576 рядків, що зумовлено обмеженою архітектурою формату.

Типові завдання аналітика правоохоронного органу найчастіше перевищують зазначену межу та потребують вирішення питання масштабування. Використання офісних додатків на межі максимального обсягу створюють ризики відмови програмного забезпечення або невиправдано значного часу опрацювання.

У зв'язку з цим, Data Science надає перевагу більш пристосованим засобам, як Python та R. Створені спеціалізовані процесори даних, такі як Jupyter Notebook та DataSpell, абстрагують користувача від класичного програмування,

надаючи гнучкість та відсутність жорстких обмежень на обсяг даних. Ці інструменти, у поєднанні з бібліотеками на кшталт pandas та polars, забезпечують ефективне виконання завдань, зазвичай вирішуваних традиційними текстовими та табличними процесорами.

Додатково з'являється можливість використовувати фрагменти програмного коду для виконання специфічних аналітичних задач або перевикористання вже існуючих сценаріїв обробки. За допомогою середовищ опрацювання стало можливим впровадження у повсякденну аналітичну діяльність засобів штучного інтелекту. Моделі машинного навчання, на відміну від побудови глибоких нейронних мереж, інтуїтивно зрозумілі та не потребують надлишкових апаратних ресурсів для тренування.

Основним принципом підходу застосування моделей машинного навчання є відмова від створення алгоритму. Натомість для створення моделі надається зразок даних з промаркованим результатом (тренувальна вибірка). Для класифікаційних моделей типовим є маркування «ІСТИНА» (True) або «ХИБА» (False). Під час опрацювання тренувальних даних модель найкращим чином знаходить закономірності у даних та створює внутрішній порядок прийняття рішень. За умови надання достатньо різноманітної тренувальної вибірки, тренована модель набуває здатності до узагальнення та можливості роботи з даними, які раніше їй були невідомі. Таким чином тренована модель може бути перевикористана у аналогічних випадках.

Для прикладу пропонується розглянути модель виявлення помилок у написанні анкетних даних осіб. Дані про перетин державного кордону містять помилки, допущені операторами введення. Так, наприклад помилки «Олейнік – Олейник», «Ямпільський - Йампільський» мають місце при опрацюванні значних зрізів даних.

При перевірці великого датасету за участю 88000 осіб, виявлено ознаки схожості у ~2000 осіб (однакова дата народження та схоже написання імені та прізвища). Опрацювання такої кількості значень ручним способом вимагає значних часових витрат та підвищує ризик пропуску, а відмова від нормалізації призводить до втрати зв'язків під час аналізу зв'язків з використанням графічних засобів (наприклад i2 Analyst Notebook).

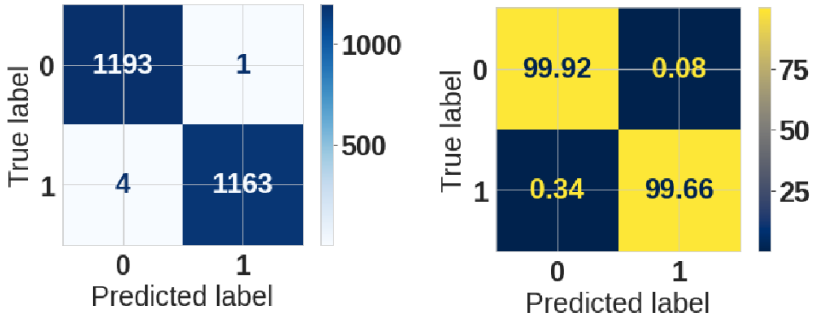
Для вирішення проблеми виявлення помилкових написань підготовлена тренувальна вибірка з промаркованими статусами для пар схожих осіб:

ПІ_особа1	ПІ_особа2	С_особа1	С_особа2	… інші ознаки	Статус
Саргалієва	Саргалієва	Жіноча	Жіноча	…	Одна особа
Іванов	Іванова	Чоловіча	Жіноча	….	Різні особи
…	…	…	…	…	…

З наявних даних сформовано ознаки схожості (features) для кожної з пар:

Опис ознаки	Назва ознаки	Пара осіб 1	Пара осіб 2	Інші пари
Маркований результат (чи одна особа)	target	0	1	…
Однакова стать	same_sex	1	1	…
Однаковий тип документа	same_doc_type	1	1	…
Однаковий номер документа	same_doc_num	0	0	…
Однакова країна походження	same_country	0	1	…
Співпадіння написання українською	same_ukr_full	0	0	…
Співпадіння написання англійською	same_eng_full	0	0	…
Зважена різниця написання прізвища	ukr_sname_diff	0.33	0.90	…
Зважена різниця написання імені	ukr_fname_diff	0.44	0.85	…

Після тренування з допомогою навчальної вибірки, модель машинного навчання може аналізувати нові дані, не потребуючи їх попереднього маркування. Вона здійснює автоматичні передбачення, визначаючи, чи є подана пара даних помилковим дублікатом однієї особи, чи належить вона до різних осіб. Це дозволяє швидко і точно ідентифікувати помилки.



Матриця помилок.

True label – дійсні значення, *Predicted label* – робота моделі

Результати валідації моделі вказують на достатню ефективність. Серед 2361 пар схожих анкет правильно визначено 2356 пар тотожних осіб.

Для задачі визначення тотожності осіб використана класифікаційна модель Decision Tree Classifier (Дерево рішень). Для схожих задач можливе використання більш надійних моделей, таких як: ансамблеві моделі – Random Forest (Випадковий ліс), моделі, що використовують градієнтний спуск виправлення помилки – lgbm (Light Gradient Boosting Machine), XGBoost (Extreme Gradient Boost).

Переваги класифікаціних моделей:

– самостійно формують кращий алгоритм для великої кількості факторів;

– придатні до перевикористання у аналогічних випадках;

– можливі для впровадження малими командами чи окремими аналітиками;

– не використовують зовнішні сервіси.

Недоліки класифікаційних моделей:

– потребують матеріал для навчання;

– залежать від помилок учителя;

– обмежені у передбаченні кількісних значень;

– менш ефективні ніж моделі глибокого навчання.

Наразі існують повні посібники для впровадження методів машинного навчання, в тому числі з наочною демонстрацією роботи моделей з використанням найбільш популярного програмного пакету sklearn: www.scikit-learn.org. Всесвітньою практикою набуття професійних навичок вважається участь у змаганнях аналітиків на платформі www.kaggle.com.

Використання класифікаційних моделей машинного навчання мають широкі можливості застосування у типових аналітичних задачах аналітика правоохоронного органу. Зокрема: визначення призначення колонок під час опрацювання таблиць з несталою структурою, визначення скорінгу використання конспіративних засобів зв'язку серед абонентів радіомоніторингу, визначення переліку господарських товариств з підвищеним ризиком до бюджетних злочинів, виділення найбільш перспективних об'єктів аналізу до оперативної перевірки, інші задачі, що потребують аналізу одночасно значної кількісті ознак з неочевидною кореляцією.

Впровадження моделей машинного навчання та сучасних середовищ опрацювання даних може значно підвищити швидкість та якість роботи аналітика правоохоронного органу, розшити спектр виконуваних задач, отримати нові підходи до здобуття аналітичної інформації.

Олексин Христина Любомирівна,
курсант навчально-наукового інституту № 3
Національної академії внутрішніх справ
Науковий керівник:
Мостепанюк Людмила Олександрівна,
доцент кафедри кримінального права
Національної академії внутрішніх справ,
кандидат юридичних наук, доцент

ТЕНДЕНЦІЇ КРИМІНАЛЬНО-ПРАВОВОГО ЗАХИСТУ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ

Як відомо, Конституцією України було проголошено захист прав і свобод людини і громадянина, а також забезпечення державного суверенітету і територіальної цілісності України, зокрема, належна охорона економічної та інформаційної системи, як важливих складових в нормальному функціонуванні державного апарату. Повне та досконале виконання цих простих завдань є підґрунтям для розбудови суспільства та держави і подальшої ефективної інтеграції нашої країни до Європейського Союзу. До того ж варто враховувати, що для виконання цих завдань невід'ємною складовою є ефективна діяльність правоохоронних органів, що потребує належного кримінально-правового захисту, особливо під час дії військового стану, який був введений на території України Указом Президента від 24.02.2022 р. Враховуючи вище зазначене, державою було взято

до уваги питання про механізм реконструкції системи правоохоронних органів з метою підвищення рівня ефективності їх діяльності, зокрема у випадку надзвичайної ситуації – обороноспроможності.

Так, у нестандартних умовах, для правоохоронних органів набирає актуальності проблема забезпечення законності та власний захист від протиправних посягань. Найнебезпечнішим проявом втручання в діяльність працівників правоохоронних органів є погроза або насильство (ст. 345 Кримінального кодексу України (далі – КК)), умисне знищення або пошкодження майна працівника правоохоронного органу (ст. 347 КК) а також посягання на життя працівника правоохоронного органу, члена громадського формування з охорони громадського порядку і державного кордону або військовослужбовця (ст. 348 КК). Вчинення вказаних злочинів суттєво відображається на підвищенні авторитету працівників правоохоронних органів, створює перешкоду на відтворенню високопоставлених соціально-правових стандартів, а також певним чином негативно впливає на ефективності їх діяльності. Так, оптимізація захисту працівників правоохоронних органів зі сторони держави за допомогою чинного кримінального законодавства дає змогу дослідити цю проблематику у ширших аспектах зі сторони загального та спеціального.

Теоретичним та практичним дослідженням різних аспектів кримінально-правової охорони працівників правоохоронних органів та дослідження кримінальної відповідальності за вчинення погрози або насильства в кримінальному законодавстві приділялася значна увага, а саме у працях таких авторів, як: Л.В. Сердюк, А.О. Цховребова, М.В. Стерехов, С.В. Антонов, В.Т. Дзюба, М.М. Комарницький, Л.В. Дорош, П.С. Єлизаров, М.П. Журавльов, С.В. Владимиренко, І. М. Залялової, І.М. Ізай, О.О. Кашкарова, В.А. Клименко, О.О. Книженко, В.О. Навроцький, А.М. Удод, І.М. Чуб, О.А. Чувакова, В.І. Осадчий, С.М. Школа, В.Г Кондратов та інші.

В даній праці нам необхідно спершу дослідити основні аспекти захисту працівників правоохоронних органів в Україні з урахуванням дії воєнного стану, недосконаліть та деякі прогалини чинного вітчизняного законодавства, а також кримінальну відповідальність, передбачену ст. 343, 345, 347, 348 КК України.

На сьогоднішній день, враховуючи дію військового стану, для України залишається важливим забезпечення внутрішнього

порядку та законності. Варто зауважити, що під час повномасштабного вторгнення росії, досить таки важко контролювати криміногенну обстановку в країні і забезпечувати ефективність розслідування різного роду кримінальних правопорушень, в тому числі – пов'язаних із посяганням на власну діяльність та авторитет. Від початку повномасштабного вторгнення, станом на 24 лютого 2023 року органами Національної поліції, за офіційними даними відкрито 48 тисяч кримінальних проваджень за фактами воєнних злочинів, вчинених окупантами. Саме тому на сьогодні на правоохоронні органи покладається значне навантаження, у зв'язку із чим ефективність діяльності значною мірою погіршується. Тому така діяльність потребує чіткого і всебічного кримінально-правового захисту для реалізації своєї професійної діяльності та убезпечення себе від незаконних посягань, як зі сторони громадян та, вірогідно, зі сторони окупантів. Тому доцільно буде говорити про кримінальну відповідальність за втручання в діяльність працівника правоохоронного органу, вчинення погрози або насильства щодо нього або членів його сім'ї у зв'язку із виконанням ним своїх службових обов'язків.

Згідно з положеннями КК, кримінально-правове реагування зі сторони держави на вчинення злочину відображається у виді кримінальної відповідальності та інших примусових заходів, що застосовуються за рішенням суду. Як відомо, кримінальна відповідальність посідає провідне місце, а з недавніх пір вважається єдиним заходом кримінально-правового реагування зі сторони держави на вчинення злочину. Тому в галузі права на теоретичному і практичному рівнях фахового право розуміння, кримінальна відповідальність виступає, як наслідок за вчинення протиправних дій які законодавець закріпив в КК України. В юридичній літературі є безліч визначень та тлумачень щодо кримінальної відповідальності. На думку С.М. Школи, якщо про визначення кримінальної відповідальності говорити з позиції загального і спеціального запобігання злочинів, то не можна не зауважити, що відповідальність для громадян насамперед є не обов'язком зазнати покарання, а можливістю держави (її правом) притягти до неї правопорушника [1, с. 149].

В основу визначення самої сутності та змісту кримінальної відповідальності в дослідженні насамперед поставлено офіційне розуміння даного терміну, що висвітлено в рішенні Конституційного суду України від 27 жовтня 1999 року

№ 9-рп/9 [2]. У вище зазначеному рішенні спочатку зазначалося, що кримінальна відповідальність є різновидом юридичної відповідальності, а її місце є досить таки важливим елементом у кримінально-правовому реагуванні держави на вчинення злочинів, але зміст даного поняття законодавчо є не визначеним. Вказане судове рішення є своєрідним алгоритмом, визначення сутності самого поняття кримінальної відповідальності, як засобу реагування на вчинення злочину. Опираючись на дану сутність визначеного поняття, ми можемо спостерігати, що в більшій кількості випадків розгляду справ судами, переважає притягнення винуватих осіб у вчиненні кримінального правопорушення саме до кримінальної відповідальності аніж застосування до них менш суворішого покарання кримінально-правового характеру.

Так, до прикладу за проведеним дослідженням А.О. Цховребова, щодо аналізу судових рішень за статтею 343 КК України, а саме, «Втручання в діяльність працівника правоохоронного органу, працівника державної виконавчої служби» у 100 % винесених рішень є притягнення саме до кримінальної відповідальності [3, с. 27]. За проведеним дослідженням інших заходів кримінально-правового характеру, таких як: звільнення від кримінальної відповідальності, застосування примусових заходів медичного чи виховного характеру за фактом втручання в діяльність працівника правоохоронного органу не було встановлено. Кримінальна відповідальність за своєю кримінально-правовою природою є однією із заходів кримінально-правового характеру, а не охоплює всі ці заходи, як вважалося раніше. Так, із визначенням в Україні кримінального проступку, що було розпочато в 2008 році та насамперед офіційним оприлюдненням в Концепції реформування кримінальної юстиції, злочин, передбачений ст. 343 КК, було визначено кримінальним проступком.

Особливість кримінальної відповідальності за погрозу або насильство щодо працівника правоохоронного органу полягає насамперед в тому, що вона є більш суворішою, а ніж за втручання в його діяльність. Адже здійснення погрози або насильства тягне за собою накладення судимості та є злочином, а не кримінальним проступком, який за своєю природою такого виду покарання не передбачає. Варто зазначити, що говорячи про вчинення даного кримінального правопорушення, ми вже розглядаємо його, як злочин а не як проступок. Відповідно за

вчинення якого правопорушник буде підлягати кримінальній відповідальності на загальних підставах.

На думку М.М. Комарницького, більше уваги досліджуваним злочинам, як передбаченим розділом XV Особливої частини КК України «Злочини проти авторитету органів державної влади, органів місцевого самоврядування та об'єднань громадян», так і передбаченим іншими розділами Особливої частини КК стало приділятися після набуття чинності КК 2001 р. [3; 4, с. 17]. Зокрема від початку дії воєнного стану на території України даній групі досліджуваних кримінальних правопорушень стала приділятися, ще більша увага зі сторони законодавців, адже злочини проти авторитету органів державної влади набули неабиякої актуальності.

Так у 2007 році, було захищено дисертацію для здобуття наукового ступеня кандидата юридичних наук з досліджуваної теми – І.М. Залялової «Кримінальна відповідальність за втручання в діяльність працівника правоохоронного органу» в даній роботі було досліджено загальні характеристики злочинних посягань здійснених щодо представників влади і громадськості. Зокрема, в дослідницькій роботі визначається, насамперед об'єкт даної досліджуваної групи злочинів, на основі чинного законодавства конкретизуються ознаки потерпілих, також береться до уваги і погроза та насильство, що розглядається автором, як спосіб вчинення передбачених законом посягань на представників влади [5, с. 18].

Розглядаючи праці деяких авторів ми знаходимо необхідні нам моменти для дослідження досить таки актуального питання. До того ж, питання про кримінально-правову охорону осіб чи їх близьких родичів у зв'язку із виконанням цими особами свого службового чи громадського обов'язку цікавлять не лише визначних науковців але і законодавчі органи. Так, у Верховній Раді України періодично з'являються законопроекти, що своєю характеристикою спрямовані на вдосконалення чи доповнення деяких статей чинного КК. Не виключенням є і досліджувані нами статті, а саме: 343, 345, 348 Особливої частини. У 2014 році був зареєстрований законопроект «Про внесення змін до деяких законодавчих актів України щодо регламентації положень Кримінального процесуального кодексу України», яким пропонувалося виокремити норми закріплені в чинному КК України а саме її статтю 379 Особливої частини, як таку, що містить в собі норми дискримінаційного характеру. Вище вказане положення обґрунтовується тим, що саме посягання на

життя людини не в залежності від її посади чи діяльності якою вона займається чи займалася, не може бути піддано різній за характером мірі покарання. У зв'язку із цим, органам державної влади, що мають правозастосовні повноваження, пропонувалося в таких випадках використовувати положення п. 8 ч. 2 ст. 115 КК, що передбачає відповідальність за умисне вбивство «особи чи її близької особи у зв'язку з виконанням цією особою службового або громадського обов'язку» [3].

Такі пропозиції та доповнення викликали в галузі юриспруденції серйозні заперечення. Адже пропозиції щодо даного випадку, можна вносити в санкції статей КК, які передбачають відповідальність за вбивство, погрозу чи заподіяння тілесних ушкоджень або знищення чи пошкодження майна потерпілим, що є представниками державної влади. Така кримінально-правова не визначеність, щодо оцінки посягання на представників органів державної влади чи виконання ними свої службових повноважень, зумовлені тим, що є певне збільшення складів кримінальних правопорушень, що передбачають собою відповідальність за насильницькі злочини чи злочини пов'язані із посяганням на осіб чи їх близьких родичів, у зв'язку із виконанням ними свого службового обов'язку.

Список використаних джерел

1. Школа С.М. Актуальні питання правоохоронної діяльності. *Питання кримінального права та кримінології* Дніпропетровський державний університет внутрішніх справ. С. 149–153. URL: http://www.pravoisuspilstvo.org.ua/archive/2012/6_2012/31.pdf.

2. Рішення Конституційного суду України 27 жовтня 1999 року Справа № 1-15/99, № 9-рп/99. URL: zakon.rada.gov.ua/laws/show/v009p710-99#Text.

3. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. з наступними змінами та доповненнями – від 27.01.2023. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

4. Комарицький М.М. Кримінально-правова охорона осіб чи їх близьких родичів у зв'язку з виконанням ними свого службового чи громадського обов'язку : дис… канд. юр. наук : 12.00.08 / Національна академія внутрішніх справ. Київ, 2017. с. 225.

5. Залялова І.М. «Кримінальна відповідальність за втручання в діяльність працівника правоохоронного органу» : автореф. дис... канд. юрид. наук : спец. 12.00.08. Київ, 2007. 18 с.

Панченко Євгеній Вікторович,
начальник 4-го управління
Департаменту кіберполіції Національної поліції України

ДОСВІД КІБЕРПОЛІЦІЇ В РОЗСЛІДУВАННІ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ВІРТУАЛЬНИМИ АКТИВАМИ

Департамент кіберполіції, починаючи від часу створення як окремого структурного підрозділу в системі Міністерства внутрішніх справ, а потім Національної поліції України [3], почав стикатися з віртуальними активами (криптовалютами), що використовували у своїй діяльності представники злочинного світу, зокрема хакери, кібер-анархісти, послідовники ідей Сатоші Накамото [1, 2].

Досвід, здобутий за час роботи Департаменту, є важливим для обміну та поширення серед інших підрозділів Національної поліції України, правоохоронних органів та правозастосовних інституцій. Безперечно, важливим цей досвід буде і в наукових, навчальних посібниках, підручниках та інших матеріалах.

На сьогодні найбільшою проблемою, виходячи зі здобутих результатів практичної роботи, бачиться відсутність належного правового регулювання сфери віртуальних активів в України. Україна втрачає сотні мільйонів доларів доходів бюджету через відсутність регуляції [4], а правоохоронна ланка діє не системно та опирається на загальні норми, що містять відсилки до розуміння віртуальних активів як речей. Тому надалі мова піде саме про практики та підходи щодо вилучення та арешту віртуальних активів, що потребують негайної регуляції в Україні, а також запроваджені в інших країнах.

Арешт активів, що зберігаються на гаманцях сервісів, якими керують постачальники послуг віртуальних активів (VASP), наприклад, криптобіржі, може бути відносно простим, якщо правоохоронні органи мають необхідні законодавчі повноваження, суди, здійснюючи свої повноваження, ухвалюють унормовані рішення, а VASP визнають юрисдикцію цієї країни.

Проте активи, що зберігаються на особистих гаманцях, часто становлять більшу проблему. Їх успішне вилучення вимагає ретельної підготовки, коректного поводження з даними та їх аналізом. У зв'язку з чим, весь процес вилучення слід розділити на 6 етапів:

1. Підготовчий.
2. Ідентифікація.

3. Вилучення.
4. Арешт.
5. Зберігання.
6. Управління.

Розглянемо кожен з етапів окремо, опишемо його особливості та ризики, що можуть виникати.

Перший етап (підготовчий). Незалежно від того, йдеться мова про невідкладну слідчу (розшукову) дію чи заплановану, правоохоронні органи мають бути готові до можливого вилучення віртуальних активів. Це передбачає створення та керування стандартними операційними процедурами (інструкціями) і політиками, що регулюють підхід організації до арешту віртуальних активів, включаючи розуміння та пом'якшення фінансових, операційних, репутаційних і юридичних ризиків.

Урегульована та апробована правова політика повинна чітко визначати та регулювати наступне:

– законодавчі підстави та порядок вилучення й арешту активів;

– перелік мінімально необхідних для залучення осіб, зобов'язання кожного з них і відповідальність на кожному етапі;

– визначене та затверджене програмне та апаратне забезпечення;

– перелік кваліфікаційних вимог до працівників, залучених до проведення заходів із вилучення;

– процес надання внутрішнього схвалення планових і невідкладних заходів з вилучення віртуальних активів.

Усе програмне та апаратне забезпечення мають підтримувати найновіші політики безпеки, проходити тестування та, що не менш важливо, відповідати загальноприйнятим стандартам протоколу, такому як «BIP 39». Стандарт «BIP 39» є проектним документом для впровадження функцій або інформації в Bitcoin. Використання загальноприйнятих стандартів гарантує, що, якщо підтримку гаманця буде припинено, інший гаманець, що працює за стандартом протоколу, може бути використаний для відновлення доступу до активів [5].

Найважливішою частиною будь-якого підготовчого етапу є налаштування гаманців, що контролюються правоохоронними органами, і їх постійна готовність до використання: створення та налаштування гаманців на місці конфіскації завжди має бути останнім варіантом. Через їх граничну чутливість доступ до приватних ключів і початкових значень відновлення має бути суворо захищеним, але надаватися принаймні двом особам у

підрозділі, щоб запобігти єдиній точці компрометації. Резервні копії початкових фраз «Шаміра» служать подібній меті. Shamir – це процес протоколу безпеки, у якому від 12 до 24 початкових слів поділяються на три або більше окремо записаних колекцій, що можна зберігати в різних місцях. Щоб відновити гаманець, потрібно знову зібрати фрази разом [6].

На підготовчому етапі також слід розглянути державно-приватне партнерство з VASP і постачальниками депозитарного (custodial) зберігання віртуальних активів, що нормативно визначені для допомоги в реалізації цілей конфіскації, що реалізовують правоохоронні органи. Правоохоронним органам може знадобитися придбати та утримувати різні активи, наприклад, Ethereum, щоб заплатити за газ (комісію), якщо гаманець підозрюваного містить великий портфель токенів, але не нативний (рідний) актив Ethereum. Державно-приватні партнерства також можуть допомогти правоохоронним органам проводити подальші продажі або аукціони конфіскованих віртуальних активів через авторитетну та регульовану компанію (VASP).

Другий етап (ідентифікація). Ідентифікація віртуальних активів на етапі правозастосування – це уміння, яким повинен володіти кожен працівник у правоохоронній структурі, принаймні на базовому рівні. Крім цього, потрібно мати навички щодо виявлення апаратних і паперових гаманців, ресурсів відновлення доступу до віртуальних активів, а також методів, за допомогою яких ці предмети можна приховати. Компактні та невибагливі гаманці для холодного зберігання можна легко сплутати з канцелярським приладдям і не помітити під час обшуку. Працівники також мають бути обережними у поводженні з ідентифікованими предметами: оскільки вони можуть містити надзвичайно конфіденційну інформацію, таку як необроблені приватні ключі чи початкові коди відновлення (seed-фрази). Їх слід поміщати в непрозору упаковку, щоб запобігти випадковому захопленню камерами, що носять на тілі, або іншими записуючими пристроями під час проведення обшуку, а також фіксації іншими залученими до процесуальної дії особами.

Технічний персонал і ті, хто має досвід цифрової криміналістики, повинні бути готові проводити огляд техніки (ноутбуків, настільних комп'ютерів і мобільних пристроїв) на місці, намагаючись зібрати дані та ідентифікувати програми, що можуть вказувати на використання віртуальних активів або

нещодавню історію доступу до VASP. Більш повні та ретельні цифрові криміналістичні експертизи згодом повинні проводитися в судово-медичних установах.

Третій і четвертий етапи (вилучення та арешт). Щодо віртуальних активів, вилучення фізичного об'єкта (флеш-накопичувач, спеціалізований холодний гаманець) не завжди означає наявність повного контролю над віртуальними активами, що зберігаються на них. Щоб конфіскація була завершена успішно, правоохоронні органи повинні підписати транзакції та отримати власні приватні ключі від віртуальних активів.

Місце конфіскації становить найбільший ризик: помилки, такі як відправка активів за неправильною адресою або помилкова плата за газ, можуть бути незворотними. Щоб запобігти таким ризикам, процес конфіскації має здійснюватися через «систему запобіжників», коли двоє співробітників узгоджують кожен крок із заздалегідь визначеним контрольним списком, як зазначено в політиці вилучення.

Процес конфіскації має бути ретельно зафіксований як у письмовій формі, так і, якщо це можливо, з використанням аудіо- та відеозаписувальних пристроїв, на що можна посилатися пізніше або використовувати як докази. Такі записи стануть у нагоді під час обґрунтування конкретних рішень. Через їх надзвичайну чутливість, запис фраз відновлення або приватних ключів варто здійснювати з дотриманням правил подальшої конфіденційності та чіткого управлінням доступом до зафіксованого матеріалу.

Незважаючи на те, що наведені вище принципи можуть бути широко застосовані до різних засобів зберігання віртуальних активів, не всі вилучення однакові, і використовувані процеси можуть суттєво відрізнятися залежно від типу ідентифікованого віртуального активу чи засобу його зберігання. Наприклад, пошук закритого ключа на паперовому гаманці вимагатиме іншого підходу до відновлення гаманця з вихідних кодів відновлення. Хоча спеціально підготовлені засоби для вилучення не можуть охоплювати всі поточні та майбутні варіанти зберігання віртуальних активів, вони повинні чітко визначити процеси, за допомогою яких віртуальні активи не можуть бути вилучені на місці події через технічні труднощі, і які доступні варіанти збереження ідентифікованих активів мають правоохоронці натомість.

Будь-які активи, вилучені безпосередньо з пристроїв, таких як настільні комп'ютери, ноутбуки та мобільні телефони,

смартфони тощо, вимагають особливої обережності. Зважаючи на важливість збереження цифрових доказів, з ними має працювати лише персонал, навчений сортуванню цифрових пристроїв у реальному часі. Баланс між захистом віртуальних активів і збереженням доказів необхідно контролювати та керувати ним з обережністю. Правова основа цього процесу має вирішальне значення як для встановлення винних осіб, так і для їх успішного затримання та арешту.

П'ятий етап (зберігання). Зберігання віртуальних активів під час процесу збору доказової бази та розгляду кримінального провадження пов'язане з певними ризиками. Значна частина дискусій щодо зберігання віртуальних активів обмежується програмним і апаратним забезпеченням для зберігання активу. Як такий, він не відображає унікальних вимог правоохоронних і державних органів, де організаційний контроль доступу, можливості аудиту та відшкодування цих активів є пріоритетними. Незважаючи на судові вимоги щодо правил ланцюга постачання, програмне та апаратне забезпечення споживчого рівня для роботи віртуальними активами часто створюються з єдиною точкою доступу, що викликає додаткові ризики втрати, відмови та зловживання.

Використання VASP і спеціалізованих зберігачів – організацій, що забезпечують безпечне довгострокове зберігання криптовалют від імені установ – може зменшити ці ризики. Зокрема, зберігачі часто мають надійні положення щодо роботи з інституційними інвесторами, чиї вимоги до постачальника послуг подібні до вимог правоохоронних органів або державних інституцій.

«Не ваші ключі, не ваша віртуальні активи» – це аксіома у світі криптовалюти, і використання кастодіальних послуг означає відмову від певного контролю над активами. Однак правоохоронні органи зазвичай покладаються на безпечних третіх сторін: адже автотранспорт, вилучений поліцією, зазвичай, зберігається на спеціальних майданчиках, а готівка, вилучена у великих розмірах, – у банках і фінансових установах.

Вибір методу зберігання не слід робити легковажно, і один варіант не підходить для всіх ситуацій. Організації знайдуть різні рішення, що добре підходять для їх цілей і юридичних зобов'язань. Але ключовим є те, що рішення про те, як зберегти віртуальні активи, приймаються на основі інформації від широкого кола зацікавлених сторін і як частина організаційної політики.

Шостий етап (управління).

Останній етап управління активами тісно пов'язаний з обраними умовами на п'ятому етапі (зберігання активів). Як вже відомо, на минулому етапі найбільше суперечок точиться між програмним та апаратним зберіганням, а також кастодіальним управлінням активами, що здійснюється третіми особами.

Обираючи будь-який з варіантів особистого зберігання (некастодіального), правоохоронні органи стикнуться з проблемами подвійної сплати комісії (газу) за транзакції під час вилучення активу, а також його подальшого переказу на гаманці, підконтрольні організаціям, що будуть здійснювати управління активами від імені держави, що є небажаним.

У випадку кастодіального зберігання, коли активи відразу переходять в управління VASP, потреба для подальшого переміщення може і не виникнути, коли VASP одночасно уповноважений на управління активами після їх вилучення.

Підсумовуючи викладене, на сьогодні найскладніше питання під час розслідування злочинів, пов'язаних з віртуальними активами, у проблемі відсутності належного регулювання цього інституту. Отже, описані вище етапи є власним баченням спільноти та автора щодо бажаного стану справ у роботі з віртуальними активами в правоохоронній схемі.

Список використаних джерел

1. The recording of crypto assets in the System of National Accounts – Interim guidance. Working paper 3.3. 8 July 2020. 22 p.

2. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 9 p.

3. Кіберполіція України. ВікіпедіЯ – Вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Кіберполіція_України.

4. Бюджет втратив 3 млрд грн податків від діяльності криптобірж // Бюро економічної безпеки: державний сайт України. 02.08.2023. URL: https://esbu.gov.ua/news/biudzhet-vtratyv-3-mlrd-hrn-podatkiv-vid-diialnosti-kryptobirzh.

5. Жидко А. А. Дослідження блокчейн технологій для обробки і передачі інформації з використанням криптографічних методів шифрування даних. 80 с.

6. P. Luo, A. Yu-Lun Lin, Z. Wang, M. Karpovsky. Hardware Implementation of Secure Shamir's Secret Sharing Scheme (англ.) // HASE '14 Proceedings of the 2014 IEEE 15th International Symposium on High-Assurance Systems Engineering : Proceeding. Washington, DC, USA: IEEE Computer Society, 2014. P. 193–200. doi: 10.1109/HASE.2014.34.

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

НОВІ ВЕКТОРИ РОБОТИ КРИМІНАЛЬНОГО АНАЛІЗУ В УМОВАХ ВОЄННОГО СТАНУ

Передусім слід зазначити, що до широкомасштабного вторгнення російських військ робота підрозділів кримінального аналізу базувалася здебільшого на участі в розслідуванні шахрайств, серійних крадіжок та інших загально кримінальних злочинів, однак все змінилося в одну мить і аналітик змушений був почати діяти у незвичному для нього полі.

Так, за короткий час служба адаптувалася до умов бойових дій та змогла в повній мірі виконувати поставлені завдання під час блекаутів, повітряних тривог та обмежень комендантської години.

У короткі терміни були створені умови для ефективної роботи: налагоджено комунікацію з іншими правоохоронними органами України, організовано комунікацію аналітиків 24/7, забезпечено обмін інформацією з іншими країнами.

Окремо було вирішено питання розміщення аналітиків на декількох локаціях з метою мінімізації впливу раптового нападу ворога.

Перед кримінальними аналітиками постали нові завдання, які були пов’язані з наступною аналітичною діяльністю:

– аналіз інформації з відкритих джерел про військовослужбовців агресора, які діяли на території України, в тому числі моніторинг інформації про рух або скупчення військових формувань на певній території країни;

– опанування новітніх методів аналізу, в тому числі картографування та геопросторовий аналіз;

– збір та аналіз інформації про процеси, які відбуваються на окупованих територіях;

– аналіз інформації про громадян України, які можуть бути причетні до колаборайної діяльності (ст. 111-1 ККУ);

– протидія інформаційно-психологічним операціям ворога (ІПСО);

– боротьба з поширенням інформації про переміщення, рух або розташування Збройних Сил України (ст. 114-2 ККУ). [1]

За умови забезпечення вищепереліченого, аналітик стає майже незамінним при документуванні злочинів такого характеру.

Тому тепер є можливість поділитися деякими результатами аналітичної роботи.

У доповіді є можливість окреслити лише маленьку частину успішних аналітичних досліджень нашого підрозділу, який у тісній співпраці з декількома міжнародними командами аналітиків, продемонстрували високі результати роботи.

Завдяки скрупульозній роботі вдалося встановити осіб, причетних до обстрілу житлових будинків у місті Чернігові навесні 2022 року.

Після встановлення азимута падіння снарядів було вирахувано декілька вірогідних місць запуску снарядів.

Коли території були деокуповані, поліцією були проведені опитування місцевих мешканців на предмет розміщення військових формувань у їх населених пунктах. У результаті проведених заходів визначені артилерійські формування, причетні до обстрілів. Далі, шляхом перевірки інформації з відкритих джерел, були ідентифіковані причетні до злочину особи.

Другий приклад залучення аналітиків стосується воєнних злочинів, учинених на території одного з населених пунктів Київської області.

Завдяки аналізу інформації про техніку, яку використовували росіяни, були виявлені матеріали, що підтверджують участь військового формування на території інших напрямів, починаючи з 2014 року. Це дало підґрунтя для ідентифікації можливих військовослужбовців, що могли користуватись танками, а також їх командирів, які безпосередньо віддавали наказ.

У третьому випадку першочергово було отримано інформацію про участь громадянина однієї з інших держав у військових формуваннях рф, що діють на території України. Завдяки найпростішому OSINT-аналізу були отримані першочергові відомості для ідентифікації такої особи. У подальшому вдалося встановити підрозділ, де іноземець проходив службу, перевірено причетність до воєнних злочинів аналогічного спрямування, перевірено його спільників.

Кожне повідомлення про злочин відпрацьовано та структуровано за декількома десятками параметрів. Визначені військові формування, ймовірні позивні, місце скоєння злочину. За можливістю проаналізовано військову техніку, яка перебуває у розпорядженні частини. Зібрано відомості з соціальних сторінок. Додано відомості від потерпілих, у тому числі і тих, хто виїхав з країни.

Уся вказана інформація структурована в декількох десятках графіків та даних для ефективного пошуку як за місцем скоєння злочину, так і за параметрами злочинця чи свідченнями жертви.

Саме така основа із зібраних даних дає можливість проводити аналіз навіть у випадках складних та великих за обсягом розслідувань.

З початку широкомасштабного вторгнення російської федерації до поліції надходять тисячі повідомлень про зникнення громадян. До них належать повідомлення родичів, які втратили зв'язок з рідними, а також повідомлення про зникнення людей на окупованих територіях.

Людську трагедію, спричинену війною, використовують кримінальні елементи з метою приховання злочинної діяльності та інсценування її під воєнні злочини.

Ураховуючи викладене, питання розшуку безвісти зниклих є одним із пріоритетних напрямів роботи, у якій кримінальні аналітики беруть активну участь. 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.

Отже кримінальний аналіз продовжує розвиватися і нові вектори участі в виявленні доказів та документуванні злочинів, що з'явилися в умовах війни, стають ключовими чинниками успішного виконання завдань.

Список використаних джерел

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

Разєнков Євген Валерійович,
начальник відділу проєктного
та ризикового менеджменту
Департаменту інформаційно-
аналітичної підтримки Національної
поліції України

УПРОВАДЖЕННЯ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ СИСТЕМИ ОЦІНКИ SOCTA (ПУБЛІЧНИЙ СЕГМЕНТ)

З метою реалізації положень статті 3 Угоди про асоціацію між Україною та Європейським Союзом (далі – ЄС) щодо зміцнення співробітництва в «боротьбі з різними формами транснаціональної організованої злочинності» в Міністерстві внутрішніх справ України та Національній поліції України впроваджується методологія «Оцінка загрози з боку особливо небезпечних форм організованої злочинності» (Serious and Organised Crime Threat Assessment, SOCTA) [1].

Розпорядженням Кабінету Міністрів України від 16 вересня 2020 року № 1126-р, схвалено Стратегію боротьби з організованою злочинністю, однією із цілей якої є розробка оцінки загроз, визначення кількості стратегічних цілей та виконання комплексних планів заходів, спрямованих на запобігання організованій злочинності та боротьбу із злочинними організаціями [2].

За ініціативою Консультативної місії Європейського Союзу в Україні, Постановою Кабінету Міністрів України від 26 січня 2022 року № 59 «Деякі питання запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна» (далі – Постанова) утворено міжвідомчу робочу групу з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна, до складу якої включено представника Департаменту кримінального аналізу Національної поліції України (далі – ДКА) [3].

Відповідно до Постанови на Національну поліцію було покладено функції з реалізації практичної частини методології SOCTA.

SOCTA є продуктом системного аналізу інформації правоохоронців про кримінальну діяльність і групи, що становлять загрозу для ЄС, та полягає у збиранні, узагальненні

та оцінюванні загроз організованої злочинності, а також тяжких та особливо тяжких злочинів.

Згідно з пунктом 4 Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України (далі – Департамент, ДІАП), затвердженого наказом Національної поліції України від 31 січня 2020 року № 77 (зі змінами), Департамент є відповідальним підрозділом за організацію (здійснення) розроблення, упровадження, супроводження (адміністрування) інформаційних систем, комп'ютерних технологій, телекомунікаційних мереж та систем зв'язку для забезпечення діяльності органів (підрозділів) поліції [4].

З метою збору та консолідації даних у сфері боротьби з тяжкими злочинами й організованою злочинністю в Україні за методологією SOCTA, ДКА запропоновано керівництву Національної поліції та в подальшому узгоджено, створення фахівцями ДІАП виключно для потреб поліції на базі інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» (далі – система «ІПНП») тестової інформаційної підсистеми «SOCTA», яка б дозволила щомісячно проводити збір і узагальнення інформації про викриті підрозділами Національної поліції організовані групи та сфери їх злочинної діяльності.

Так, з метою вивчення методик збирання та порівняння інформації, а також ознайомлення з прикладом розробки запитальника для збирання необхідної інформації, як основи для подальшої її аналітичної обробки, відповідно до рішення Голови Національної поліції України та за погодженням Міністра внутрішніх справ, представником Департаменту було здійснено службове відрядження до Агентства Європейського Союзу із співробітництва у сфері правоохоронної діяльності (EUROPOL) (далі - Агентство) (м. Гаага, Королівство Нідерландів).

З урахуванням отриманих відомостей щодо методології Європолу, ДІАП, згідно вимог Агентства до структури запитальника, по узгодженню із ДКА, на базі системи «ІПНП» розроблено апаратно-програмний комплекс – інформаційну підсистему «SOCTA», призначену спростити збір даних та пришвидшити їх порівняння та аналіз.

За дорученням Голови Національної поліції України від 30.12.2022 № 9452/01/27-2022 «Про введення в тестову експлуатацію інформаційної підсистеми «SOCTA» інформаційно-

комунікаційної системи «Інформаційний портал Національної поліції України», інформаційну підсистему «SOCTA» з 01.01.2023 введено в тестову експлуатацію.

Вказана інформаційна підсистема автоматизує окремі механічні процеси під час збору та аналізу інформації SOCTA, скорочує час у десятки разів та надає можливість виключення людського фактору з недопущення механічних помилок під час роботи з надвеликим масивом даних, тим самим забезпечуючи реалізацію проєкту SOCTA, у перспективі проведення аналітики стратегічного рівня.

Список використаних джерел

1. Угода про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої. URL: https://www.kmu.gov.ua/storage/app/sites/1/ugoda-pro-sociaciyu/TITLE_I.pdf.

2. Про схвалення Стратегії боротьби з організованою злочинністю. 2020. URL: https://zakon.rada.gov.ua/laws/show/1126-2020-%D1%80#Text.

3. Деякі питання запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна: Постанова Кабінету Міністрів України від 26 січня 2022 р. № 59. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-zaprovadzhennya-v-diyalnist-centralnih-organiv-vikonavchoyi-vladi-sistemi-ocinki-socta-ukrayina-59-260122.

4. Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України. 2020. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Struktura/Polohena11.pdf.

Рибальченко Людмила Володимирівна,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент;
Бандурін Владислав Віталійович,
курсант ННІППФПНП
Дніпропетровського державного
університету внутрішніх справ

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Правове забезпечення інформаційних технологій в правоохоронній діяльності є важливим фактором існування та роботи правової системи в Україні та світі.

В епоху всеохоплюючого домінування комп'ютерних технологій усі галузі життя та держави мали адаптуватись до сучасних і постійно мінливих наслідків прогресу.

У результаті, така стара та консервативна сфера як правоохоронна юридична діяльність так чи інакше, була вимушена адаптуватись до нових правопорушень та викликів цифрового світу.

Цей аспект стосується створення та виконання правової основи для використання інформаційних технологій поліцейськими органами. Це включає в себе встановлення стандартів збереження та передачі інформації, захисту особистих даних, а також правила використання спеціальних інструментів для розслідування злочинів у цифровому просторі.

Україна, як європейська держава має надзвичайно потужний комп'ютерний розвиток, який, в порівнянні з сусідніми країнами вищий, але не достатній, щоб вийти на рівень країн-домінантів як США чи Японія.

Однак, можна чітко стверджувати, що наша держава йде в правильному напрямку та має надзвичайно серйозні перспективи розвитку в інформаційних технологій.

У сфері кібербезпеки наша держава має певне відставання від провідних країн світу, серйозні недоліки і прогалини у роботі та законодавчому фундаменті.

Розглянемо основні елементи міжнародної системи інформаційної безпеки:

– міжнародні доктринальні документи універсального характеру, присвячені інформатизації, інформаційному суспільству та інформаційній безпеці;

– міжнародні стандарти у галузі інформаційної безпеки;

– міжнародні професійні (спеціалізовані) установи, які займаються питаннями інформаційної безпеки у різних галузях;

– міжнародно-регіональні інститути та структури, які створюються інтеграційними об'єднаннями (на прикладі, ЄС);

– інститути, що створюються військово-політичними організаціями (на прикладі НАТО);

– національні доктрини, концепції та стратегії [1].

Серед основних юридичних актів, які регулюють діяльність органів по забезпеченню в Україні кібербезпеки є «Доктрина інформаційної безпеки України» від 25 лютого 2017 року, основні положення в якому вказують на мету : «…Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу рф в умовах розв'язаної нею гібридної війни…» [2].

На міжнародній площині такими актами є Будапештська Конвенція про кіберзлочинність, Стандарти Інтернет-безпеки ІКТ (ITU-T X.800 – X.809), Стратегія кібербезпеки Європейського Союзу, Конвенція про кіберзлочинність Африканського Союзу.

Для такої воюючої країни як Україна питання кібербезпеки є вирішальним в реаліях сучасної війни.

Насамперед, слід зазначити, що можливості та здібності вітчизняних кіберпідрозділів значно розширились, однак і завдання та цілі українського цифрового фронту значно збільшилися.

У підсумку, інформаційна безпека України не лише важлива, але і критично необхідна для забезпечення стабільності, захисту прав та економічного розвитку країни. Комплексні заходи для зміцнення інформаційної безпеки мають бути в центрі національної стратегії та політики.

Список використаних джерел

1. Формування міжнародної системи інформаційної безпеки: економічні орієнтири для України. URL: http://www.economy.nayka.com.ua/?op=1&z=4457.

2. Доктрина інформаційної безпеки. URL: https://www.president.gov.ua/documents/472017-21374.

Рибальченко Людмила Володимирівна,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент
Павлій Максим Андрійович,
курсант ННІППФПНП
Дніпропетровського державного
університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ ПІД ЧАС ВІЙНИ

У сучасних умовах військово-політичних конфліктів, інформація стала важливим інструментом, здатним вирішувати завдання без застосування фізичної сили. Інформаційна війна та гібридні конфлікти надають можливість впливати на ситуацію, шляхом впливу на громадську думку та підсилення внутрішніх суперечностей. Це підкреслює важливість інформаційної грамотності, оскільки низький рівень аналізу та сприйняття інформації може призвести до втрати критичної здатності формування та мислення власної думки.

Інформаційна безпека означає ступінь захищеності інформаційного середовища суспільства, особистості та організацій від негативних наслідків, що можуть виникнути внаслідок навмисних, несанкціонованих або неумисних маніпуляцій інформацією. Рівень інформаційної безпеки держави визначається стійкістю основних сфер її життєдіяльності – економіки, науки, технологій, управління, оборони, громадської свідомості та інших – до потенційно небезпечних впливів на інформаційному рівні.

Інструментами інформаційної війни проти України є такі методи: пропаганда, маніпулювання, спроби вплинути на громадську думку, психологічний і психотропний вплив, поширення чуток, блокування мовлення на телебаченні та радіо, вилучення українських каналів із ефіру на окупованих територіях, дезінформація та поширення фейкових новин, а також розповсюдження провокаційної інформації.

Відзначено, що війна породжує психологічні виклики, які можна розділити на чотири групи: виклики для українського суспільства, вплив на ментальне здоров’я окремих осіб, вплив

на психологічний стан і благополуччя, а також виклики для українських психологів як професіоналів у цій галузі [1, с. 345].

Забезпечення інформаційної безпеки вимагає підвищення рівня інформаційної грамотності, створення умов для розвитку особистості в умовах інформаційного суспільства та захисту від різних інформаційних загроз. Сучасний процес формування держави включає створення нового політичного стану, національного відродження, міжнародних відносин, усунення військових конфліктів, економічної суперечності, суперечки національного та релігійного спрямування, збільшення рівня злочинності,політичну конкуренцію та інші аспекти.

Важливість систем інформаційної безпеки в державі підкреслюється, таким чином, що необхідно адаптувати її захист до змін зовнішніх та внутрішніх впливових чинників

Заходи для запобігання впливу на інформаційне середовище, електронні ресурси і системи управління державою, особливо в контексті проведення війни, є основним завданням для забезпечення інформаційної безпеки та національної безпеки держави.

Національна безпека є невід'ємною частиною суверенітету та незалежності країни. Важливо акцентувати увагу на ролі системи забезпечення інформаційно-військової безпеки в Україні. Ця концепція включає не лише зовнішню політику, а й всі галузі, що гарантують правильне функціонування держави. Крім захисту інформаційного простору, нашим завданням є військовий відпор агресорові, який вже має значний досвід. У війні в інформаційному просторі ключовим стає взаємодія із різними верствами населення на рівні інформаційної та психологічної взаємодії. На сьогодні інформаційна війна набула гібридного характеру та включає в себе застосування інформаційних технологій на практиці. Щодо воєнних та політичних цілей, особливого значення набувають інформаційно-психологічні операції і дії [2, с. 25].

Економічна безпека означає, наскільки національна економіка може залишатися міцною та стійкою перед внутрішніми і зовнішніми загрозами. Вона дозволяє досягати високої конкурентоспроможності у світовому економічному середовищі та забезпечувати стале та збалансоване зростання. Оцінка якості національної економіки та ефективності економічної політики держави в цій сфері важлива, і в умовах

зростаючих загроз, спричинених агресією Росії проти України, має особливе значення, тому постійний моніторинг її рівнів та потенційних загроз є надзвичайно актуальним.

В перші місяці повномасштабної війни, стабільність економічної безпеки України була гарантована завдяки наявним резервам та внутрішній стійкості, оперативній координації заходів на рівні регіонів і місцевих громад, громадській ініціативності та єднанню громадян перед загрозою російської агресії, а також завдяки значній підтримці з боку міжнародного співтовариства.

У зв'язку з переходом російської агресії до війни на виснаження, прямий вплив бойових дій на економіку став інтенсивнішим через цілеспрямовані атаки на ключову інфраструктуру країни, виснаження фінансових резервів населення і підприємств, збільшення економічних нерівностей, що виникли під час конфлікту, та застосування ворожих гібридних методів впливу. Ця ситуація підкреслює важливість впровадження спеціалізованої політики держави для боротьби з різними ризиками у сфері економічної безпеки в умовах війни. Ця політика має базуватися на оперативному моніторингу викликів і загроз економічній безпеці та аналізі їх наслідків [3, с. 97].

Список використаних джерел

1. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. Іва-на Франка, 2017. 725 с

2. Артемов В. Ю. Інформайційно-воєнна безпека як елемент національної безпеки України 2022. С. 21–29.

3. Онопрієнко С.Г. Функції забезпечення інформаційної безпеки публічного адміністрування в Україні за умов повномасштабної збройної агресії Російської Федерації. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2022. Київ. С. 95–98.

Ротт Ангеліна Олександрівна,
курсант навчально-наукового інституту № 3
Національної академії внутрішніх справ
Науковий керівник:
Литвин Вікторія Вікторівна,
старший науковий співробітник наукової
лабораторії з проблем превентивної
діяльності та запобігання корупції
навчально-наукового інституту № 3
Національної академії внутрішніх справ,
кандидат юридичних наук

ВИЯВИ АГРЕСІЇ У СТУДЕНТІВ В УМОВАХ ВОЄННОГО СТАНУ

На жаль, на сьогоднішній день досі триває воєнний стан в країні. Це неабиякий стрес для дорослих, а, тим паче, для підлітків і юнаків. Для агресії чи агресивного стану стрес є одним з чинників їх виникнення. Нам може здаватися (як би це дивно не було чути), що ми змогли адаптуватися до військових дій, не піддаємося її впливові та в нас з'явилася стресостійкість до будь-яких подій, які відбуваються в нашому житті. На жаль, це дійсно часткова правда, гортаючи новини у гаджетах чи читаючи в газетах, ми вже знаємо, що можемо побачити погані новини та вважаємо, що це не залишає слідів у нашій психіці та пам'яті. Та, люди це живі істоти з душею, які схильні проявляти емпатію, переживання, співчутливість. Також, зараз підвищена емоційна чутливість у дорослих людей. Враховуючи, що у підлітки та юнаки мають сензитивність, що насамперед характеризується їх віковим періодом, в цей час вони знаходяться на межі з дитиною та дорослим. Враховуючи це, вони можуть бути ще більш вразливі в цей час до стресу, який проявлятиметься в прямій агресії.

Для початку треба зрозуміти, що немає тільки поганих чи позитивних емоцій. Також, варто зазначити, що всі ситуації та люди індивідуальні, але їх можна розділити на певні групи. Тож коли виникає певна ситуація, людина інтуїтивно обирає емоції, які їй здаються правильними в той момент. В основі агресії лежить потреба. Коли маємо потреби, задовольняючи їх, ми робимо певні дії. Дуже часто агресію людина використовує як захист, у людини може спрацьовувати інстинкт самозбереження та інструментом його буде агресія.

Тож, дамо визначення терміну агресія. Агресія – це поведінка, яка спричинює шкоду іншим людям або самій

людині. Агресія проявляється у побитті інших людей, у вербальних образах, погрозах, ворожих насмішках, жартах, а також містить непрямі форми фізичної та вербальної агресії (бойкот, ворожа міміка та жестикуляція). Також можна надати таку характеристику цьому визначенню, що у психології агресія – зумовлена переживанням фрустрації ворожа поведінка стосовно іншої особи або групи осіб. Агресію розглядають або як інстинкт, або як наслідок фрустрації, або як соціальне научіння. Агресію класифікують за різними критеріями [1].

За формами вияву:

а) відверта агресія – агресор завдає фізичної шкоди або погрожує завдати таку шкоду;

б) стосункова агресія – агресор завдає шкоди в соціальному плані, наприклад, ігноруючи або принижуючи партнера, пліткуючи про нього, вдаючись до наклепів тощо.

За метою:

а) реактивна, або ворожа агресія – спрямована на спричинення шкоди іншій особі;

б) проактивна, або інструментальна агресія – спрямована на досягнення певних цілей (отримання бажаного об'єкта, привілею або простору) [2].

Останнім часом увагу дослідників привертає нова форма агресії – «кібертретирування» (cyberbullying). Під ним розуміють форму поведінки, яка полягає у розсиланні повідомлень агресивного та образливого характеру з використанням нових інформаційних та комунікаційних технологій (інтернет, мобільний телефон) [2].

Вияву агресії можуть передувати також інші чинники та причини окрім раніше перерахованих. Візьмемо до уваги мирний час, стрес теж можу бути присутній в житті студентів. Вони вступають у доросле життя, потрапляють у новий колектив де мусять починати з нуля своє знайомство та адаптацію. Також новий стиль життя, переїзд від батьків , вибір професії екзамени. Все це може викликати в них стрес. І це буде нормальним явищем, адже це нормально відчувати стрес коли відбуваються такі великі зміни у житті.

Також виокремлюють такі причини, що впливають на нашу агресію:

– соціум;

– гени;

– сім’я, оточення [3].

Завдання кожної людини – правильно підібрати форму слів та озвучити свою потребу, здійснити певну активність.

Будь-який симптом з’являється в результаті отриманої енергії від потреби у задоволенні. Це і є агресія. Тому потрібно вчитися висловлювати свої потреби прямо та зрозуміло.

Для подалання агресії та набуття вміння керувати нею психологи радять знайти зручний для вас спосіб регуляції.

Наприклад:

1. Фізичні вправи та свіже повітря, навіть незначне фізичне навантаження на свіжому повітрі – найкращий спосіб розслабитись. Це перше й основне, про що згадують усі без винятку фахівці.

2. Візуалізація. Якщо ви перебуваєте в стані агресії, рекомендовано звилайними олівцями заштрихувати аркуш паперу, розірвати аркуш, бити грушу тощо.

3. Почуття гумору. Якщо ви маєте добру уяву, можна представити собі порушника вашого душевного спокою в якій-небудь комічній ситуації, кумедному вигляді або безглуздій позі.

4. Аналітичне мислення. Аналітичне відтворення події, що відбулася [3].

Слід розуміти, що вияв агресії, яка шкодить не лише оточуючим, а й вам – ознака низької емоційної саморегуляції. У такому випадку людині важко контролювати себе в пориві гніву, тому слід звернутися до психолога з метою опанування навичками безконфліктного спілкування та регуляції емоційного стану.

Список використаних джерел

1. Агресія. URL: https://healthcenter.od.ua/psyhichne-zdorovya/agresiya/.

2. Агресія (психологія). URL: https://vue.gov.ua/%D0%90%D0%B3%D1%80%D0%B5%D1%81%D1%96%D1%8F_(%D0%BF%D1%81%D0%B8%D1%85%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F).

3. Агресія у відносинах: причини та види. URL: https://holdyou.net/news/agressiya-otnosheniya.

Сайипов Руслан Чаримурадович,
аспірант кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ
Науковий керівник:
Томма Роман Павлович,
доцент кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ЗЛОЧИННІСТЬ В ОБОРОННО-ПРОМИСЛОВОМУ КОМПЛЕКСІ УКРАЇНИ ЯК ОБ'ЄКТ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Забезпечення безпеки особи, суспільства та держави від загроз злочинних посягань – найбільш пріоритетне завдання всіх інститутів державної влади в Україні. Так, у ст. 1 Основного закону Україна визначена як суверенна і незалежна, демократична, соціальна, правова держава, а у ст. 3 – людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю, права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави, а держава відповідає перед людиною за свою діяльність [1]. Важливість згоди на визнання суверенності й незалежності на рівні однієї з ключових установчих норм Українського суспільного договору важко переоцінити. Однак ще важче її дотримати, реалізувати, утримати, а надто в умовах гострих викликів воєнно-політичного, інформаційного, соціально-економічного характеру, грубого, агресивного, з порушенням норм міжнародного права, силового втручання іноземних держав у внутрішні справи України, відвертого посягання на її територіальну цілісність, недоторканість кордонів. І саме в цих умовах стає очевидною значущість потужностей вітчизняного оборонно-промислового комплексу.

Оборонно-промисловий комплекс України входить до складу сектору безпеки і оборони, головним завданням якого є забезпечення оперативних спроможностей сил та засобів сектору безпеки і оборони шляхом постачання нових і модернізації наявних зразків озброєння, військової та спеціальної техніки. Відповідно до закону України «Про національну безпеку України» (2018 р.) такий комплекс включає в себе сукупність органів державного управління, підприємств, установ і організацій промисловості та науки, що розробляють,

виробляють, модернізують і утилізують продукцію військового призначення, надають послуги в інтересах оборони для оснащення та матеріального забезпечення сил безпеки і сил оборони, а також здійснюють постачання товарів військового призначення та подвійного використання, надання послуг військового призначення під час виконання заходів військово-технічного співробітництва України з іншими державами [2].

Сучасний оборонно-промисловий комплекс України є тією галуззю економіки, яка не лише репрезентує чи не найбільш інноваційні компоненти системи господарства, а й формує науково-виробничий базис суверенізації державної влади у її спроможності забезпечити потреби Українського війська у техніці, озброєнні як факторів посилення обороноздатності країни [3].

Однак службові особи у такій сфері нерідко вдаються до злочинних порушень покладених на них обов'язків, пов'язані тіньовими схемами з представниками органів державної влади, контролюючими органами, військово-комерційними структурами й організованими злочинними угрупованнями, спрямовуючи на конвертацію мільйонних прибутків із залученням законних й фіктивних суб'єктів господарської діяльності з послідуючим відтоком капіталу за межі країни. Злочинність в оборонно-промисловому комплексі підриває засадничі структури національної безпеки, підвищуючи масову віктимність народу України щодо злочинів агресії, воєнних та інших злочинів [3].

Це все призводить до посилення загрози національній та економічній безпеці держави, що особливо відчутно в умовах воєнного стану. Зокрема, згідно з офіційною статистикою, протягом п'ятирічного періоду (2018–2022 рр.) було зареєстровано 264 839 кримінальних правопорушень економічної спрямованості загалом, з яких 5285 – у сфері оборони, що складає близько 2 % від загального обсягу економічної злочинності, а направлено до суду з обвинувальним актом – лише 2522. Динаміка економічних кримінальних правопорушень у сфері оборони у 2022 р. засвідчила найнижчі показники ряду (за виключенням базисного 2018 р.). Темп приросту, розрахований ланцюговим способом у 2022 р. склав – -15,9 %, що пов'язано з воєнним станом. Водночас найвищим цей показник був у 2020 р. – +32,6 %. Загалом для динаміки відтворення економічних кримінальних правопорушень у сфері оборони характерні щорічні коливання позитивних і негативних значень темпів зростання і приросту відповідно із генеральною тенденцією до їх зростання [4; 5].

У той же час, кількість виявлених кримінальних правопорушень у сфері економіки знижувалася впродовж 2014–2022 рр. (за винятком 2018 року), зокрема динаміка задокументованих організованих груп і злочинних організацій відповідного спрямування зменшилася на 33,0 %, закінчених провадженням кримінальних правопорушень – на 27,0 %, що фактично засвідчує суттєве послаблення оперативно-розшукових позицій у протидії економічній злочинності. Негативною також є динаміка щодо викритих угруповань з корумпованими (-6,0 %), міжрегіональними (-53,0 %) і транскордонними (-48,0 %) зв'язками. Згідно з офіційними звітами Бюро економічної безпеки, показник розкриття тяжких та особливо тяжких злочинів у сфері господарської діяльності, учинених у кваліфікованих формах співучасті, коливається в межах від 30 до 50 % за щорічного зростання залишку кримінальних проваджень відповідної категорії, у яких не прийнято кінцевого процесуального рішення. Матеріали, зібрані в межах оперативно-розшукових справ, використано як докази лише в 31,4 % (проведених негласних слідчих (розшукових) дій – у 34,3 %) проваджень, що загалом вказує на недооцінку можливостей використання аналітичних, оперативно-технічних, агентурно-оперативних та інших інструментів збирання доказів.

Характерним для оборонно-промислового комплексу є кваліфіковане приховування слідів та ознак кримінально караних діянь (частка латентної злочинності у цій сфері складає 70–80 %) шляхом використання мережі різних господарюючих суб'єктів недержавного сектору, що займаються господарською діяльністю у військовій сфері, підроблення проектно-кошторисної, реєстраційної та дозвільної документації, ігнорування норм і правил безпеки, неправомірного доступу до інформації в автоматизованих телекомунікаційних мережах, застосування удосконалених технологій відмивання злочинних доходів, що значно ускладнює своєчасне виявлення й документування таких правопорушень.

Відтак, протидія злочинності в оборонно-промисловому комплексі України постає однією з ключових задач у комплексі забезпечення національної безпеки, підвищення обороноздатності країни, посилення захищеності громадян, а досягнутий за роки незалежності ступінь криміналізації цієї галузі не залишає сумнівів у необхідності розгортання широкомасштабного, системного кримінально-обструктивного й оперативно-розшукового впливу.

Список використаних джерел

1. Конституція України від 28.06.1996 р. URL: http://zakon5.rada.gov.ua/laws/show/254к/96-вр.
2. Про національну безпеку України: Закон від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355.
3. Кожушко С. О. Феномен злочинності в оборонно-промисловому комплексі України. *Вісник Кримінологічної асоціації України*. 2020. № 1 (22). С. 224–233.
4. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора України*. URL: http://www.gp.gov.ua/ua/stat.html.
5. Кримінальна ситуація в Україні: основні тенденції. 2021 рік : монографія / авт. кол.: М. Г. Вербенський, О. Г. Кулик, І. В. Наумова та ін.; за заг. ред. докт. юрид. наук, проф. М. Г. Вербенського. Вінниця : ТВОРИ, 2022. 340 с.

Сальніков Ігор Іванович,
начальник 3-го управління
(організаційно-контрольної роботи
та забезпечення діяльності) Департаменту
кримінального аналізу Національної
поліції України

ЗАПРОВАДЖЕННЯ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ СИСТЕМИ ОЦІНЮВАННЯ ЗАГРОЗ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ ТА ТЯЖКИХ ЗЛОЧИНІВ ЗА МЕТОДОЛОГІЄЮ SOCTA

З метою реалізації затвердженої у 2015 році Стратегії національної безпеки України та зобов'язань, узятих Урядом за Угодою про асоціацію між Україною та ЄС, держава повинна вжити заходів щодо імплементації циклу ЄС – EMPACT [1].

EMPACT (*European Multidisciplinary Platform Against Criminal Threats*) – це Європейська мультидисциплінарна платформа проти злочинних загроз, тобто комплексний підхід до внутрішньої безпеки, що включає сукупність заходів від контролю зовнішніх кордонів, поліцейської діяльності та митного контролю до управління інформацією, навчання й профілактики, це своєрідний механізм об'єднання правоохоронних принципів чи концепцій ЄС та України.

EMPACT має чотирирічний цикл і складається з чотирьох кроків:

Крок 1: Оцінка тяжкої та організованої злочинності (SOCTA)

Крок 2: Визначення пріоритетів злочинності

Крок 3: Оперативні плани дій

Крок 4: Незалежна оцінка

Україною вжито низку заходів з виконання взятих на себе зобов'язань перед ЄС у сфері протидії тяжкій та організованій злочинності. Так, у 2020 році Кабінетом Міністрів України схвалено Стратегію боротьби з організованою злочинністю, яка визначає напрями розвитку системи боротьби з організованою злочинністю та механізми реалізації державної політики у цій сфері в сучасних умовах. [2]

Зокрема, Стратегією передбачено три етапи реалізації стратегії.

На першому етапі здійснюється оцінка загроз тяжких злочинів та організованої злочинності (SOCTA Україна).

На другому етапі за результатами проведеної оцінки визначаються стратегічні цілі і розробляються комплексні плани заходів.

Третій етап передбачає виконання зазначених вище комплексних планів заходів.

SOCTA – це продукт системного аналізу інформації правоохоронців про кримінальну діяльність і групи, що становлять загрозу для ЄС, щоб допомогти керівникам у визначенні пріоритетів серед загроз організованої злочинності.

До завдань, які стоять перед SOCTA Україна, слід визначити такі:

проведення аналізу тенденцій організованої злочинності;

здійснення аналізу сфер діяльності організованих груп і злочинних організацій (далі – ОГ і ЗО);

узгодження цілей та завдань з протидії організованій злочинності;

аналіз законодавства у сфері протидії організованій злочинності;

оцінка ефективності здійснення заходів з протидії ОЗ;

аналіз можливостей досягнення цілей та виконання завдань;

інші заходи організаційного та аналітичного характеру;

Реалізація проєкту оцінки тяжкої та організованої злочинності за методологією Європейського поліцейського офісу SOCTA Україна здійснюється у 3 етапи:

1. Підготовчий (організаційно-методичний, первинний збір інформації);
2. Обробка та внесення даних до ІП «SOCTA»;
3. Аналіз та оцінка зібраних даних.

На сьогодні завершено І (підготовчий) етап упровадження оцінки загроз SOCTA Україна. До його результатів можна віднести те, що в січні 2022 року Кабінетом Міністрів України затверджено склад та Положення міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна, *до якої зокрема входять представники МВС, Національної поліції, ДПС, СБУ, ДБР, ОГП, БЕБ, НАБУ, РНБО та інших*. Крім того схвалено Порядок збирання і узагальнення інформації та здійснення оцінювання загроз організованої злочинності та тяжких злочинів відповідно до системи оцінки SOCTA Україна» [3].

Міністерством внутрішніх справ і Національною поліцією забезпечено функціонування вищезгаданої міжвідомчої робочої групи, на засіданнях якої визначено 4-річний період оцінювання загроз організованої злочинності за методологією SOCTA – 2019–2022 роки; затверджено, запропоновані Національною поліцією, типові форми облікових карток щодо організованої групи та/або злочинної організації, злочинної спільноти та щодо сфер злочинної діяльності [4].

У результаті проведених підрозділами кримінального аналізу звірок відомостей, отриманих з регіонів, та матеріалів щодо протидії організованій злочинності, наданих Офісом генерального прокурора України, визначено перелік кримінальних проваджень відносно ОГ і ЗО, які було направлено до суду в період з 2019 по 2022 роки, та які підлягають оцінці за методологією SOCTA.

Також відбулося затвердження запропонованого Національною поліцією переліку сфер злочинної діяльності, які будуть вивчатися у ході проведення оцінювання загроз організованої злочинності та тяжких злочинів відповідно до системи оцінки SOCTA Україна, а також органів, відповідальних за заповнення відповідних облікових карток [5].

Розпочато тестову експлуатацію ІТ-рішення зі збору інформації.

Крім того, у грудні 2022 року в структурі Департаменту кримінального аналізу створено 4-й відділ (оцінки загроз та стратегічного аналізу) 1-го управління (аналітичного), на який покладено завдання щодо проведення стратегічного кримінального аналізу, у т. ч. у межах проєкту SOCTA.

На даний момент триває 2-й етап реалізації проєкту, який передбачає обробку та внесення даних до інформаційної підсистеми «SOCTA».

Зокрема, з метою автоматизації процесу збору даних про викриті ОГ і ЗО розроблено відповідне ІТ-рішення – Інформаційну підсистему ІПНП України «SOCTA». Слід зазначити, що в більшості країн ЄС дотепер працівники поліції збирають відомості в ручному форматі за допомогою таблиць програми Excel.

Інформаційна підсистема ІПНП України «SOCTA» – це спільний проєкт Департаменту кримінального аналізу та Департаменту інформаційно-аналітичної підтримки, який розпочав тестову експлуатацію із залученням працівників інших оперативних підрозділів Національної поліції на центральному рівні.

На виконання підпункту 2 пункту 4 протокольного рішення, ухваленого на засіданні Міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна [6] та за дорученням Міністерства внутрішніх справ України розроблено проєкт наказу Міністерства внутрішніх справ України «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «SOCTA» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України».

Зазначений проєкт наказу погоджений в Міністерстві цифрової трансформації України, Державній службі зв'язку та захисту інформації України, Уповноваженого Верховної Ради України з прав людини та направлений до Міністерства юстиції України для державної реєстрації.

У структурі ІП «SOCTA» передбачено 2 форми облікових карток (запитальників):

1. Облікова картка щодо організованої групи та/або злочинної організації, злочинної спільноти, яка заповнюється окремо на кожну організовану групу та/або злочинну організацію, злочинну спільноту.

2. Облікова картка щодо сфер злочинної діяльності, яка заповнюється окремо на кожну сферу злочинної діяльності,

причому кожна сфера злочинної діяльності оцінюється за визначеним переліком індикаторів.

Зазначені картки створені у формі запитальників, що містять індикатори, які дозволяють цілісно зрозуміти та оцінити рівень організованої злочинності.

Методологія оцінювання використовує змішаний підхід, який складається з якісних та кількісних методів аналізу та набору чітко визначених показників для виявлення та уточнення найбільш загрозливих кримінальних явищ.

На підставі зібраних даних остаточно ухвалено перелік кримінальних проваджень відносно ОГ і ЗО, які було направлено до суду у період з 2019 по 2022 роки та які підлягають оцінці за методологією SOCTA. Також визначений перелік пріоритетних сфер злочинної діяльності.

До переліку пріоритетних сфер злочинної діяльності, які підлягають оцінці за методологією SOCTA, входять:

Торгівля людьми *(сексуальна експлуатація, трудова експлуатація, торгівля дітьми, тощо)*

Нелегальна міграція

Незаконний обіг наркотичних засобів *(коноплі – трава, смола та інше, кокаїн, героїн, синтетичні наркотики, нові психоактивні речовини (НПР) та прекурсори, наркомісткі лікарські препарати, тощо)*

Кіберзлочинність *(кіберзалежна злочинність, сексуальна експлуатація дітей в Інтернеті, шахрайство з безготівковими розрахунками, тощо)*

Фальсифікація товарів *(у галузі харчової промисловості, фармацевтична галузь, тощо)*

Порушення авторського права і суміжних прав

Корупція

Легалізація (відмивання) майна, одержаного злочинним шляхом

Зловживання (корупція) в спорті

Незаконна діяльність з організації або проведення азартних ігор, лотерей

Екологічна злочинність *(незаконний обіг відходів, торгівля зникаючими видами, тощо)*

Підроблення грошей, цінних паперів, білетів державної лотереї, марок акцизного податку чи голографічних захисних елементів

Незаконна діяльність з підакцизними товарами *(алкоголь, тютюн, нафтопродукти, тощо)*

Рейдерство
Підроблення документів
Вимагання *(рекет, шантаж)*
Незаконний обіг вогнепальної зброї
Викрадення людей
Вбивство
Встановлення або поширення злочинного впливу
Злочини проти власності *(крадіжка, грабіж, розбій, привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем, тощо)*
Незаконне заволодіння транспортними засобами
Культурні цінності та артефакти
Шахрайство

Важливо зазначити, що якість кінцевого аналітичного продукту залежить від якості внесених у підсистему даних. З метою оптимізації процесу внесення даних та контролю за їх якістю в центральному органі управління поліцією та Головних управліннях Національної поліції в областях та м. Києві створено робочі групи, на які покладений цей обов'язок. До складу таких робочих груп включені співробітники слідчих, оперативних та аналітичних підрозділів.

Основним вимогами до членів робочої групи є те, що співробітники, які включені до робочих груп, повинні мати достатній рівень знань про криміногенну ситуацію в регіоні, особливості розслідування та документування кримінальних правопорушень, учинених організованими групами та злочинними організаціями, а також мати навички роботи з великими обсягами інформації, складання аналітичних документів.

З метою забезпечення повного та своєчасного внесення даних до облікових карток ІП «SOCTA» працівниками Департаменту кримінального аналізу підготовлено відповідний методичний посібник, постійно проводилась роз'яснювальна робота по внесенню інформації, проведено ряд занять з членами робочих груп, детально роз'яснено обсяг інформації, необхідний для внесення по кожному з індикаторів, а також зазначено джерела отримання такої інформації.

Після внесення даних до ІП «SOCTA» буде проведено 3-й етап проєкту – опрацювання отриманої інформації, її аналіз та підготовлено відповідний аналітичний звіт, який готуватиме міжвідомча аналітична група.

Звіт буде включати аналітичні висновки, що сформують політичні пріоритети, які трансформуються в стратегічні

правоохоронні цілі. Затверджені стратегічні цілі стануть основою для розроблення комплексних планів заходів.

На четвертому засіданні Міжвідомчої робочої групи з координації запровадження в діяльності центральних органів виконавчої влади системи оцінки SOCTA Україна, затверджено методологію оцінювання загроз серйозної та/або організованої злочинності в Україні (SOCTA Україна), яка розроблена Міжвідомчим науково-дослідним центром з проблем боротьби з організованою злочинністю.

Список використаних джерел

1. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text.

2. Розпорядження Кабінету Міністрів України від 16 вересня 2020 року № 1126-р «Про схвалення Стратегії боротьби з організованою злочинністю». URL: https://zakon.rada.gov.ua/laws/show/1126-2020-%D1%80#Text.

3. Постанова Кабінету Міністрів України від 26 січня 2022 року № 59 «Деякі питання запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна». URL: https://zakon.rada.gov.ua/laws/show/59-2022-%D0%BF#Text.

4. Протокол № 1 засідання Міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна від 02 листопада 2022 року.

5. Протокол № 2 засідання Міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна від 11 січня 2023 року.

6. Протокол № 3 засідання Міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна від 23 червня 2023 року.

7. Протокол № 4 засідання Міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна від 02 листопада 2023 року.

Севрук Володимир Геннадійович,
провідний науковий співробітник
відділу організації наукової діяльності та
захисту прав інтелектуальної власності
Національної академії внутрішніх справ,
доктор юридичних наук, доцент

ОКРЕМІ НАПРЯМИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ЗЛОЧИНАМ, ЩО ВЧИНЯЮТЬСЯ ОРГАНІЗОВАНИМИ ГРУПАМИ І ЗЛОЧИННИМИ ОРГАНІЗАЦІЯМИ, ЯКІ СФОРМОВАНІ НА ЕТНІЧНІЙ ОСНОВІ

Актуальною і нагальною проблемою в Україні є протидія етнічній організованій злочинність. Відповідно, реалії сьогодення спонукають правоохоронні органи протидіяти злочинам, що вчиняються організованими групами і злочинними організаціями, які сформовані на етнічній основі, шляхом використання нових методів, засобів, а особливо інформаційних технологій та сучасних телекомунікаційних засобів, що мають глобальний масштаб впливу, і відходити від застосування застарілих методів [1, с. 572]. Етнічна організована злочинність існує в усіх країнах і регіонах та має свій напрям й різниться лише мірою згуртованості, що залежить від історичних, етнічних, економічних, соціальних шляхів розвитку того чи іншого суспільства: [2, с. 344; 3, с.76].

Ефективність протидії злочинності, попередження, виявлення та припинення злочинів, зокрема вчинених членами організованих злочинних груп та злочинних організацій, які сформовані на етнічній основі, насамперед залежить від належного інформаційно-аналітичного забезпечення діяльності оперативних підрозділів кримінальної поліції [4].

Базовими елементами та засобами реалізації інформаційно-аналітичної діяльності виступають інформаційні системи, системи зв’язку та передачі даних, сучасна інформаційно-телекомунікаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, правові,

організаційні засоби. Це знайшло втілення у ст. ст. 25−27 Закону України «Про Національну поліцію» [5; 6].

Як слушно відзначає С. О. Павленко, що інформаційно-аналітичне забезпечення оперативно-розшукової діяльності – відіграє ключову роль в організації діяльності оперативних підрозділів щодо тактики протидії передусім організованим формам злочинності [7, с. 117].

Виокремлено сучасні можливості інформаційно-аналітичного забезпечення діяльності правоохоронних органів щодо протидії злочинам, що вчиняються організованими групами і злочинними організаціями, які сформовані на етнічній основі, зокрема забезпечення системи відеоспостереження, що полягає у фіксації правопорушення, часу та осіб, які його вчинили, методиці ідентифікації людини за параметрами мовних сигналів; алгоритми автоматизованої цифрової фотозйомки, цифрового відео- та звукозапису (з моделюванням фотопортретів осіб, які брали участь у вчиненні злочину), алгоритми ідентифікації людини на основі біометричних ознак з розпізнаванням облич.

Констатовано, що основною причиною незадовільного стану інформаційно-аналітичного забезпечення щодо протидії злочинам, що вчиняються організованими групами і злочинними організаціями, які сформовані на етнічній основі, є організаційний характер, що проявляється у відсутності єдиної системи щодо збору, накопичення, аналізу, узагальнення та використання інформації. Наразі правоохоронними органами України ще не створено умов, які б дозволяли ефективно використовувати високі інформаційні технології і телекомунікаційні системи під час протидії злочинам, що вчиняються організованими групами і злочинними організаціями, які сформовані на етнічній основі. У зв’язку з цим наявна проблема, яка полягає у відсутності процедур і робочих методологій у сфері збирання, оброблення, аналізу та, що не менш важливо, поширення/розповсюдження даних/звітів щодо таких організованих груп і злочинних організацій.

Ураховуючи неналежний стан інформаційно-аналітичного забезпечення протидії злочинам, що вчиняються організованими групами і злочинними організаціями, які сформовані на етнічній основі, сталу тенденцію до збільшення інформаційних ресурсів та активне її освоєння кримінальними структурами, розвиток на базі

високих інформаційних технологій спеціалізованого програмного забезпечення, запропоновано такі напрями інформаційно-аналітичної роботи з підвищення ефективності виявлення та документування злочинів, що вчиняються організованими групами і злочинними організаціями, які сформовані на етнічній основі, а саме: запровадження сучасних інформаційних і телекомунікаційних технологій; створення на рівні профільних департаментів і служб МВС України спеціалізованих інформаційно-аналітичних підрозділів; об'єднання наявних систем в універсальні комплекси (мережі); забезпечення функціонування системи безпеки та захисту інформації в автоматизованих інформаційно-пошукових системах; удосконалення підготовки і перепідготовки кадрів для інформаційно-аналітичних підрозділів МВС України.

Отже, підсумовуючи вище викладене, слід наголосити, що це не боротьба з особами певної національності, це захист інтересів законослухняних громадян від злочинців, які об'єдналися за етнічною ознакою При цьому не можна заперечувати факт, що звичаї етносу не завжди можуть збігатися з прийнятими в суспільстві неписаними законами, і навіть із нормами, викладеними у Кримінальному кодексі [8, с. 67].

Список використаних джерел

1. Севрук В. Г. Протидія злочинам, що вчиняються організованими групами і злочинними організаціями, які сформовані на етнічній основі: теорія та практика: монографія. Київ: «Видавництво Людмила», 2022. 1092 с.

2. Севрук В. Г. Протидія організованій злочинності циганських етнічних угруповань на території України. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1. С. 343-350. URL: http://nbuv.gov.ua/UJRN/boz_2012_1_41.

3. Sevruk V. Ethnic crime in Ukraine. Юридичний часопис Національної академії внутрішніх справ України. 2016. № 1 (11). С. 73–83.

4. Пічкуренко С. І., Кацан Л. О. Щодо деяких аспектів використання підрозділів кримінальної розвідки в інформаційно-аналітичному забезпеченні діяльності кримінальної поліції. Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції: зб. наук. статей за

матеріалами доп. Всеукр. наук.-практ. семінару (Львів, 23 берез. 2018 р.) / упоряд. А. В. Баб'як, В. В. Сеник, Т. В. Магеровська. Львів: ЛьвДУВС, 2018. С. 128.

5. Про Національну поліцію: Закон України від 02 лип. 2015 р. № 580-VI. Відомості Верховної Ради. 2015. № 40−41. Ст. 379.

6. Єсімов С. С. Юридична природа інформаційно-аналітичної діяльності Національної поліції. ІТ право: проблеми і перспективи розвитку в Україні: конф. (Київ, 18 листоп. 2016 р.). URL: http://aphd.ua/publication-151/.

7. Павленко С. О. Основи оперативно-розшукової тактики : монографія. Київ : Людмила, 2022. 624 с.

8. Sevruk V. Definition and classification of the ethnic crime in Ukraine. European Reforms Bulletin: scientific peer-reviewed journal. 2016. № 1. P. 64–68.

Семенюк Ірина Юріївна,
здобувач ступеня вищої освіти магістра
Національної академії внутрішніх справ
Науковий керівник:
Школьніков Владислав Ігорович,
старший викладач кафедри
інформаційних технологій
та кібербезпеки Національної академії
внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ФОРМУВАННЯ ІМІДЖУ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

Правоохоронні органи України, а саме Національна поліція, доволі молодий орган виконавчої влади, сформований у 2015 року та працює над створенням позитивного іміджу та довіри населення. Сучасні інформаційні технології слугують важливим фактором в побудові асоціації і гарного враження суспільства, а також відіграють ключову роль у підвищенні прозорості та відкритості діяльності державного органу.

Система інформаційного забезпечення НП України – це сукупність взаємопов'язаних та взаємодіючих організаційних елементів та технічних засобів, яка здійснює інформаційне забезпечення НП України.

Інформацією ж, згідно закону України, слід вважати будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1].

Без інформації немає процесу управління, без неї неможливо сформулювати цілі управління, оцінити ситуацію, визначити проблеми, спрогнозувати розвиток подій, підготувати управлінські рішення, проконтролювати їх виконання. Сфера охорони правопорядку є надзвичайно динамічною, комплексною, вона потребує постійного вдосконалення, взаємодії правоохоронних структур, що можливе тільки при належному інформаційному забезпеченні [2, с. 240]

Інформаційні технології дозволяють правоохоронним органам надавати публічний доступ до важливих даних та статистики, таких як злочинність, результати розслідувань та інші показники діяльності. Також через соціальні медіа та веб-портали надаються відповіді на запитання та пояснення щодо різних аспектів роботи. Це дозволяє громадськості слідкувати за роботою поліції, розуміти принципи роботи правоохоронців та аналізувати їхні досягнення та виклики, а також сприяє зближенню поліції та громади.

Інформація, надана поліцією, є надзвичайно важливою для громадян, оскільки вона забезпечує обізнаність та допомагає відчути впевненість у сфері правопорядку та безпеки. Важливість цієї інформації виявляється у декількох ключових аспектах:

1. Інформованість про поточні події. Інформація від поліції надає можливість бути в курсі актуальних ситуацій, подій та розслідувань, що стосуються їхнього регіону чи міста.

2. Забезпечення особистої безпеки. Інформація про потенційні загрози, правила поведінки в екстремальних ситуаціях, а також рекомендації щодо запобігання злочинам допомагають громадянам уникнути небезпек та захистити себе та свою власність.

3. Важливість участі громадян у боротьбі зі злочинністю. Інформація від поліції може мотивувати громадян брати активну участь у спільноті, надаючи свідчення, надсилаючи важливі повідомлення та долучаючися до громадських ініціатив у сфері безпеки.

4. Сприяння довірі до правоохоронних органів. Публікація достовірної та об'єктивної інформації сприяє формуванню довіри громадян до поліції як інституції, що працює на благо суспільства.

5. Підвищення ефективності реагування на кризові ситуації. Громадяни, інформовані про правила та порядок дій у небезпечних ситуаціях, можуть швидше та ефективніше реагувати на надзвичайні ситуації [3].

Усе це свідчить про те, що інформація, яку надає поліція, є важливим чинником у формуванні відчуття безпеки, впевненості та довіри у суспільстві. Громадяни, будучи обізнаними, можуть більш ефективно співпрацювати з правоохоронними органами у забезпеченні загальної безпеки та правопорядку.

Інформаційна взаємодія системи Міністерства внутрішніх справ України та громадян є надзвичайно важливим аспектом сучасного управління правопорядком та забезпечення громадської безпеки.

Ключовим органом, на який покладено функції з формування інформаційних ресурсів Національної поліції в областях є управління інформаційно-аналітичної підтримки, яке є структурним підрозділом Головного управління НП (ГУНП) в області, що організовує і здійснює заходи, спрямовані на забезпечення правоохоронної діяльності органів поліції області.

Провідними напрямками його діяльності є:

– збір, обробка, накопичення та зберігання статистичної, оперативно-розшукової, криміналістичної та архівної інформації; створення, розвиток та організація експлуатації автоматизованих та інтелектуальних інтегрованих інформаційних систем, розвиток корпоративної інформаційної мережі ГУНП в області;

– інформаційне забезпечення підрозділів поліції, надання інформації фізичним та юридичним особам, ведення обліків правопорушників, злочинів, скоєних на території області, криміналістичних та оперативних обліків;

– упровадження сучасних інформаційних технологій та інформаційних систем у діяльність підрозділів ГУНП в області;

– формування державної і відомчої статистичної звітності про стан законності на території області та результати діяльності підрозділів ГУНП в області [4].

Оптимізація вирішення завдань пошуку, відбору та систематизації інформації, необхідної в діяльності поліції, базується на конструкті єдиного інформаційного простору системи МВС України, який логічно визначити як сукупність спеціалізованих баз і банків даних, технологій їх ведення та використання, інформаційно-телекомунікаційних систем і мереж, суб'єктів інформаційно-аналітичної діяльності, які функціонують на основі єдиних принципів і за загальними правилами

забезпечують інформаційну взаємодію системи Міністерства внутрішніх справ України і громадян [5].

Отож, імідж правоохоронних органів безперечно формується завдяки думці громадян. Суспільна думка є важливим критерієм оцінки діяльності правоохоронців, оскільки вона відображає взаємодію та взаєморозуміння між правоохоронцем та особою. Повага до правопорядку та довіра до правоохоронних органів є фундаментальними складовими ефективної роботи поліції. Тому надання важливої інформації та встановлення відкритого діалогу між правоохоронцями і громадою через різноманітні комунікаційні канали є невід'ємною частиною створення позитивного іміджу правоохоронних органів. Взаєморозуміння та партнерство між ними створюють міцний фундамент для підвищення ефективності та якості правопорядку в сучасному суспільстві.

Список використаних джерел

1. Про інформацію : Закон України від 25 червня 2016 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 651. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

2. Державне управління: Навч. посіб./Мельник А.Ф., Оболенський О.Ю., Васіна А.Ю., Гордієнко Л.Ю.; За ред. А.Ф. Мельник. К.: Знання-Прес, 2003. 240 с.

3. Про Національну поліцію : Закон України від 05 жовтня 2016 р. № 580-VIII. Відомості Верховної Ради України. 2015. № 40–41. ст. 379. URL: https://zakon.rada.gov.ua/laws/show/580-19.

4. Про затвердження Порядку організації доступу до інформаційних ресурсів під час інформаційної взаємодії між Міністерством внутрішніх справ України, Державною міграційною службою України та Державною прикордонною службою України : Наказ МВС України від 26.09.2013 № 920 URL: http://zakon3.rada.gov.ua/laws/show/z1771-13.

5. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 23 грудня 2016 року / упорядник Т. В. Магеровська / Львів: ЛьвДУВС, 2017. 313 с.

Сивун Андрій Сергійович,
начальник 5-го відділу (відеоаналітичних досліджень) 1-го управління (аналітичного) Департаменту кримінального аналізу Національної поліції України

ВІДЕОАНАЛІТИЧНІ ДОСЛІДЖЕННЯ – НОВИЙ НАПРЯМ КРИМІНАЛЬНОГО АНАЛІЗУ

У сучасних реаліях розвитку інформаційних технологій, комп'ютерної техніки люди дедалі більше починають користуватися новими можливостями цифрового світу.

Кримінальний аналіз – це досить молода служба в підрозділах Національної поліції України, яка почала відразу користуватися всіма новітніми технологіями, техніками та ресурсами, які раніше або не досліджувались, або не використовувались через незнання їх повних можливостей.

Дослідження відеоматеріалів проводиться постійно підрозділами Національної поліції, починаючи з появи перших камер відеоспостережень, а з розбудовою масштабних систем відеоспостереження поліція отримала можливість розкривати злочини майже в режимі онлайн.

Оскільки нові технології, які приносять результат під час розслідування, неможливо було ігнорувати, аналітики стали першопроходьцями в даному векторі розвитку.

На сьогоднішній день підрозділи кримінального аналізу щодня на професійному рівні користуються системами відеоспостереження та аналізують сотні терабайт відеоматеріалів, тому напрям відеоаналітичних досліджень був лише питанням часу та потребував певного поштовху.

На жаль, цим поштовхом стала війна. Підрозділи кримінального аналізу розкрили весь свій накопичений потенціал у секторі відеоаналітики саме з повномасштабним вторгненням – а це аналіз великих масивів відео, геопросторовий аналіз, аналіз маршрутів руху, у тому числі військової техніки ворога, розпізнання воєнних злочинців, мародерів, диверсантів, покращення відеоматеріалів, спростування дезінформації, що набувала суспільного резонансу та сіяла деморалізацію і паніку (ІПСО).

Додатковим поштовхом було надходження надвеликої кількості відео для аналізу. Кількість відеоматеріалу на одного аналітика з початку війни зростає у геометричній прогресії.

Тільки Департамент кримінального аналізу проаналізував більше 200 терабайтів матеріалів по воєнних та інших злочинах. Аналітики показали ефективність результатів своєї роботи, а тому потреба в аналітичних продуктах зросла.

Наразі в Департаменті кримінального аналізу сформовано новий відділ – відеоаналітичних досліджень, який не просто займається профільною аналітикою, а спирається на аналіз великих за обсягом відеоматеріалів, здійснює розпізнання виявлених на відео суб'єктів та об'єктів, встановлення та аналіз маршруту руху, покращення якості відео- та фотозображень, візуалізацію результатів роботи з метою їх подальшого використання [1].

Для аналізу великих за обсягом відеоматеріалів використовуються спеціалізовані програмно-аналітичні платформи, що дають змогу швидко аналізувати великі масиви відео. Дані платформи спеціалізуються на індексації завантажених відеоматеріалів з подальшим розбиттям їх на певні класи об'єктів, з якими аналітики в подальшому працюють.

Аналітики здійснюють постійний OSINT-аналіз для виявлення публікацій, що можуть викликати суспільний резонанс, з установленням причетних до них осіб. Зазвичай, підрозділи кримінального аналізу перші виявляють дані публікації та відпрацювавши їх, уже надають готові матеріали, що можуть принести результати.

За допомогою унікальних ресурсів, єдиних інтеграційних платформ регіональних систем відеоспостереження та знань аналітиків проводиться детальний аналіз пересування осіб злочинців, потерпілих, транспортних засобів та інших об'єктів по всій території України.

З розвитком технологій штучного інтелекту аналітики отримали змогу здійснювати покращення відеоматеріалів, особливо здійснених у темну пору доби. Це питання завжди було актуальним, адже більшість злочинів учиняються в нічний час, злочинці розуміють, що можуть використовувати це як перевагу, а тому отримання для правоохоронних потреб ресурсів, які дозволяють із цим боритися, очікувало свого часу. Окрім відеоматеріалів, покращенню піддаються і фотоматеріали. Оскільки сам напрям покращення вважається новим, виникають і перші проблеми – такі як опрацювання відеоматеріалів, отриманих з камер відеоспостереження з можливістю нічного бачення, або просто статичних камер.

Геопросторовий аналіз не новий напрям аналітики, особливо для підрозділів Національної поліції, але починаючи з лютого 2022 року, необхідність у ньому почала зростати в геометричній прогресії. Аналітики по всій Україні почали відпрацьовувати OSINT-джерела для виявлення місць розташування ворожої техніки, особового складу армійських підрозділів рф, місць їх дислокації, а також пошуку місць ворожих ракетних ударів. Зазвичай, для проведення даного виду аналізу використовуються OSINT-ресурси, але інколи виникає потреба використання ресурсів з можливістю отримання супутникових знімків на певній місцевості та у конкретну дату.

Потрібно зазначити, що всі вище перелічені нові напрями аналітики майже ніколи не застосовуються окремо, відеоаналітичні дослідження – це комплекс заходів, якій у собі охоплює якнайбільшу кількість методик та ресурсів для отримання швидкого, повного та ефективного результату.

Останнім етапом аналізу завжди є візуалізація результатів роботи. За результатами проведених аналітичних заходів вся інформація узагальнюється у відповідному форматі для подальшої її реалізації замовниками або особами, які отримають аналітичний продукт. Уся отримана та опрацьована в результаті аналітичних досліджень інформація повинна бути викладена у зрозумілій для замовника формі. Цією формою може бути відеоряд, схема, аналітичний звіт або будь-який інший аналітичний документ [2].

Підбиваючи підсумки, варто зауважити, що попит на аналітичні продукти спонукає до розвитку. Чисельна кількість аналітиків збільшується з кожним роком, як наслідок збільшується і обсяг роботи, кількість ресурсів та рівень знань аналітиків.

Усі наведені вище види робіт не є новими, проте обставини, у яких поліція опинилася після повномасштабного вторгнення, збільшили потребу в їх використанні та створили мотивацію для розвитку. Як ми можемо бачити, даний напрямок аналізу набирає обертів, збільшуючи спектр аналітичних можливостей, завдяки чому з кожним днем стає все кориснішим для підрозділів Національної поліції та суспільства.

Список використаних джерел

1. Наказ Національної поліції України від 27 квітня 2023 року № 340.

2. Методичні рекомендації щодо організації та проведення кримінального аналізу підрозділами Національної поліції

України, затверджені Головою Національної поліції України Клименком Ігорем 11 травня 2021 року (вих. ДДЗ від 26 травня 2021 року № 6516/01/33-2021).

Тихонова Олена Володимирівна,
професор кафедри економічної безпеки
та фінансових розслідувань НАВС,
доктор юридичних наук, професор

ОСОБЛИВОСТІ ВИЗНАЧЕННЯ ПАТЕРНІВ У ТАКТИЧНОМУ КРИМІНАЛЬНОМУ АНАЛІЗІ

Тактичний кримінальний аналіз, як один з видів кримінального аналізу, полягає в аналізі злочинності та кримінальних правопорушень на конкретній території за невеликий проміжок часу, за певним видом кримінального правопорушення чи протиправної діяльності певної групи. В його межах визначаються тенденції розвитку злочинності, встановлюються місця концентрації кримінальних правопорушень, визначаються шаблони кримінальних правопорушень, встановлюються профіль підозрюваного та жертви, визначаються напрями діяльності із розслідування та збору оперативної інформації. Підвищенню ефективності використання результатів тактичного кримінального аналізу сприяє встановлення патернів, якими характеризується кримінальна активність на певній території.

Основою для встановлення патерну може слугувати час (дата і день тижня, а також кількість днів між зафіксованими інцидентами), географічне розташування (локації (міські, приміські або сільські), види діяльності, характерні для визначеного місця (комерційні, промислові, житлові райони), висотність, наближеність до інших житлових (або нежитлових) будівель тощо).

Під час вивчення тенденцій кримінальної активності можуть бути виявлені такі патерни:

– «Серія» – два чи більше подібних кримінальних правопорушення, вчинених тою самою особою чи групою осіб, які діють за попередньою змовою (наприклад, грабіжник «зазирає» у шість аптек за три місяці й завжди викрадає наркотичні знеболюючі речовини; гвалтівник шукає жертв-жінок, представляючись брокером зі здачі нерухомості в оренду та заманюючи їх у порожні квартири; одна банда здійснює

напади на дванадцять компаній, приміщення яких розташовані в діловому);

– «Хвиля» – серії кримінальних правопорушень, інтервал між якими настільки короткий, що вони ;

– «Гаряча здобич» («Hot Prey») – патерн, що характеризується однотипністю постраждалих (наприклад, із наближенням місцевих виборів на посаду мера громадяни, які підтримують одного кандидата, починають масово повідомляти про акти вандалізму, вчинені щодо їхніх домівок та); авто

– «Гарячий об'єкт» («Hot Product») – патерн, що характеризується однотипністю вкраденого майна (наприклад, відкривається новий ломбард, який скуповує використовувані мобільні телефони, за які розраховуватиметься готівкою – рівень крадіжок мобільних телефонів різко зростає);

– «Гаряче місце» («Hot Place») – патерн, у межах якого всі інциденти відбуваються в одному й тому самому місці (наприклад, кінотеатр подовжує години показу кінофільмів. Протягом чотирьох місяців з моменту такого оголошення молодиками, які «тусуються» на парковці для автомобілів, було скоєно 8 нападів);

– «Гаряче середовище» («Hot Setting») – патерн, що характеризується однотипністю місця інциденту (наприклад, крадіжки мідних труб та проводки з будівельних майданчиків у всьому місті);

– «Рецидивні злочини» («Hot Incidents») – певні місця, люди, види діяльності настільки ідентичні, що одну справу важко відрізнити від іншої.

Під час аналізу патернів для найбільш повної їх характеристики доцільним є отримання відповідей на низку питань, зокрема:

✓ Що? (тип та характеристики злочину; послідовність подій; діяння осіб, що брали участь у події).

✓ Де? (конкретне місце; тип місцевості; середовище; маршрут підходу та відходу (місце першого контакту, місце вчинення кримінального правопорушення, місце виявлення); напрям пересування; географічне прогресування патерну; територіальна близькість інших пов'язаних або споріднених подій).

✓ Коли? (час доби; день тижня; тиждень місяця; місяць року; сезон; кількість днів між подіями).

✓ Хто? (правопорушник (характеристика особи правопорушника; автомобіль; діяльність до та після

правопорушення; мотив); потерпілий (характеристика особи потерпілого; діяльність до та після).

✓ Як? (Modus operandi – спосіб вчинення кримінального правопорушення) (знаряддя; нанесені ушкодження; шкода, заподіяна майну; «почерк» (к правопорушник вчиняє кримінальне правопорушення; що незвичного в тому, яким способом правопорушник; що унікального в тому, яким способом правопорушник вчиняє кримінальне правопорушення).

✓ Чому? (чому саме це кримінальне правопорушення; чому саме ця ціль; чому саме цей час; чому саме це місце; чому саме цей спосіб вчинення кримінального правопорушення).

Запропонований підхід дозволить отримати найбільш достовірні результати при аналізі патернів, а це, у свою чергу, дозволить встановити актуальні тенденції злочинності, місця концентрації вчинення кримінальних правопорушень, а також напрацювати оптимальні тактичні заходи із затримання злочинців, виявлення ризиків та попередження конкретних правопорушень, ідентифікації ризиків, тенденцій та зон, найбільш вражених злочинною активністю.

Фаста Марина Олександрівна,
курсант навчально-наукового інституту № 1
Національної академії внутрішніх справ;
Марков Михайло Миколайович,
професор кафедри оперативно-розшукової
діяльності Національної академії внутрішніх
справ, кандидат юридичних наук, доцент

КРИМІНАЛЬНИЙ АНАЛІЗ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ТА ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

Кримінальний аналіз є діяльністю працівників Національної поліції та інших правоохоронних органів України з використання інтелектуального програмного забезпечення та системного підходу щодо збору відповідної інформації, аналітичного вивчення певних характеристик, тенденцій з метою встановлення взаємозв'язків між фактами, подіями, явищами, суб'єктами та об'єктами, оптимізації управління правоохоронними органами на державному, територіальному рівні та під час вирішення конкретних задач протидії злочинності [1].

Важливою частиною кримінального аналізу є співпраця між правоохоронними органами України та іншими зацікавленими сторонами, такими як компанії, які надають послуги в Інтернеті, технічні спеціалісти та експерти. Результатом цього співробітництва є ефективне виявлення та припинення кіберзлочинів, що забезпечує безпеку в Інтернеті та захист прав людей [2].

Практичне застосування оперативними підрозділами органів Національної поліції України методу кримінального аналізу вже підтвердило його високу ефективність у багатоепізодних провадженнях, що охоплювали велику територію, включаючи значну кількість подій і суб'єктів злочинних угрупувань зі складною структурною побудовою. У цих випадках традиційні методи відстеження та асоціювання фактів були недостатньо ефективними і, тому використання кримінального аналізу в теперішній час є ефективний і заслуговує відповідної уваги та подальшої розробки у майбутньому.

Залежно від рівня аналітичного продукту існують три види кримінального аналізу: оперативний, тактичний і стратегічний.

Метою збирання та аналізу інформації на різних етапах є створення та перевірка гіпотез і висновків щодо минулих, теперішніх і майбутніх протиправних дій і передачу зацікавленої особи чіткої інформації, що стосується проведення оперативно-розшукових заходів та слідчих (розшукових) дій. Інформація, залежно від одержувача, має планувальний, оцінювальний, керівний або контрольний характер. Його предметом є довгострокові цілі, визначення пріоритетів і стратегій боротьби зі злочинністю на підставі глибоких досліджень [3].

Обробка великих масивів інформації можлива лише при використанні інтелектуальних технологій, які зменшують мозкове навантаження оперативного працівника, слідчого та допомагають їм під час прийняття оперативного чи процесуального рішення.

Правоохоронні органи України користуються спеціалізованою програмою IBM i2, яка забезпечує аналітика потужним аналізом і надає допомогу можливості візуалізації задля підвищення продуктивності аналітики. У сфері кримінального аналізу i2, як правило, застосовується із програмними продуктами iBase, iBridge, iGlass, Analyst's Workstation тощо.

До глобальних пошукових систем відносяться: Googl, Bing, Yahoo, Rambler, Shukalka, Piplтта інші.

На цей час кримінальні аналітики органів Національної поліції України мають доступ до таких інформаційних ресурсів:

– Єдина інформаційна система МВС (ІПС);

– Інформаційний портал НПУ;

– Національна автоматизована інформаційна система МВС;

– Інформаційна система Відеоконтроль-Рубіж;

– Державний реєстр обтяжень рухомого майна (ДРОРМ) МЮУ;

– Державний реєстр речових прав МЮУ;

– ІПТС «АРКАН» тощо.

Наразі, через повномасштабне вторгнення РФ, кримінальними аналітиками створюються багато новітніх інформаційних продуктів, програм, технологій та ресурсів, які потрібні у сучасний період для превентивних заходів, протидії ІПСО та інших негативних наслідків, які виникають в теперішній час.

Комплексне використання інформаційних ресурсів одночасно з набутиминавиками дає свої позитивні результати також і під час інформаційного протистояння.

У зв'язку з російською агресією та ситуацією, яка склалася в державі, було б доцільно розширити доступ до інформаційних ресурсів, які створили та використовують підрозділи кримінального аналізу Національної поліції України у своїй діяльності.

Такими інформаційними ресурсами, які створили підрозділи кримінального аналізу Національної поліції за необхідності могли б користуватися не тільки працівники оперативних і слідчих підрозділів Національної поліції, а й інші правоохоронні органи України, які здійснюють оперативно-розшукову діяльність відповідно до статті 5 Закону України «Про оперативно-розшукову діяльність» .

Також, на нашу думку, необхідно налагодити більш міцну співпрацю та взаємодію з обміну інформаційними ресурсами, з міжнародними організаціями та інституціями, які здійснюють боротьбу із міжнародною та транснаціональною організованою злочинністю та протидіють іншим викликам сьогодення (збройні конфлікти, терористичні акти, нелегальна міграція).

Упровадження інформаційно-аналітичних програм, передових технологій та інших продуктів інформаційного призначення у діяльність оперативних і слідчих підрозділів Національної поліції, а також інших правоохоронних органів

України, які роблять свій внесок у безпеку держави, захисту її територіальної цілісності та суверенітету, доводять свою ефективність і потребують подальшого розвитку та сприяння з боку держави.

Список використаних джерел

1. URL:https://dspace.lvduvs.edu.ua/bitstream/1234567890/3723/3/%D1%84%D0%B5%D0%B4%D1%87%D0%B0%D0%BA%20%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D0%BA%D1%80%D0%B8%D0%BC%20%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D1%83.pdf.

2. Власюк О. В. Використання кримінального аналізу у боротьбі зі злочинністю: виникнення та становлення. Університетські наукові записки. 2012. No 4 (44). С. 351–356.

3. Власюк О. В. Використання кримінального аналізу в оперативно- розшуковій діяльності. Бюлетень Департаменту оперативної діяльності Адміністрації Державної прикордонної служби України. 2012. No 6. С. 82–85.

Федчак Ігор Андрійович,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ В МОДЕЛІ ЗДІЙСНЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ, ОРІЄНТОВАНОЇ НА ПЕВНУ ПРОБЛЕМАТИКУ (Problem-Oriented Policing)

Однією з позитивних проактивних (упереджувальних) поліцейських практик зарубіжних країн є відома в усьому світі модель «Проблемно-орієнтованої поліцейської діяльності» (Problem-Oriented Policing, POP). Дана модель спрямована на подолання першопричин злочинності та порушення громадського порядку. Дана модель реалізовується через поглиблене застосування методології вирішення проблем SARA, яку розробив Г. Гольдштейн (H. Goldstein) у 1979 році. Назва методології SARA – це абревіатура, що позначає чотири кроки, які поліція має дотримуватися при реалізації моделі Problem-Oriented Policing: (S) сканування операційного середовища, (A)

аналіз (поглиблений аналіз наявних кримінологічних відомостей) з метою виявлення проблем, (R) реагування (підготовка індивідуальних до кожної проблеми заходів реагування) та (A) аналітична оцінка (оцінка результативності застосовуваних контрзаходів для нейтралізації проблем).

Концептуальні та практичні аспекти функціонування моделі правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing), досліджували зарубіжні учені зокрема: Г. Голдштейн (H. Goldstein), Дж. Хінкл (J. Hinkle), Д. Вайсбурд (D. Weisburd), К. Телеп (C. Telep), М. Скотт (M. Scott), С. Кірбі (S. Kirby) та інші учені [1, с. 91–92]. Попри те, що науковцями та практичними співробітниками правоохоронних органів різних країн сформовано теоретичне та практичне підґрунтя реалізації моделі правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing), проте існує необхідність висвітлити значення та роль у її реалізації кримінальної-аналітичної діяльності.

У рамках моделі здійснення правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing) кримінальний аналіз відіграє вирішальну роль. Так, кримінальні аналітики тісно співпрацюють із кадровими співробітниками поліції, на яких покладено обов'язки виявлення, викриття та розслідування конкретних злочинних проявів з метою збору інформації про проблеми у їх службовій діяльності. Зібрану інформацію кримінальні аналітики піддають ретельному та поглибленому аналітичному дослідженню. Проблема, яку аналізують кримінальні аналітики може бути і короткостроковою, проте модель здійснення правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing), здебільшого використовують для розв'язання довготривалих проблем, які потребують стратегічного підходу до їх вирішення. Тож вирішальне значення для вирішення проблем відіграє етап аналізу, що має критичне значення для дослідження сутності проблем та її детермінант.

Неналежний аналіз сутності проблеми може призвести до неправильного визначення заходів з реагування з метою вирішення проблеми. Крім того, перехід від фази сканування відразу до фази вжиття заходів реагування в рамках моделі SARA без проведення відповідного поглибленого аналізу й оцінки за результатами вжитих заходів, по суті, буде нераціональним витрачанням ресурсів у короткостроковій і довгостроковій перспективі. Це особливо стосується тих випадків, коли відповідь

на проблему полягає в посиленні присутності поліції (наприклад, посилене патрулювання), що не завжди є ефективним, і може спричинити переміщення злочинної активності до інших подібних районів, чи об'єктів, або повернення проблеми після перекидання ресурсів в інше місце.

Зрештою, одним із найважливіших чинників для ефективної правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing), є наявність в аналітиків часу для фактичного дослідження проблеми, або проблем в поєднанні із аналізом даних, щоб гарантувати повне аналітичне охоплення контексту проблеми. Проблеми неможливо аналізувати повною мірою без урахування відповідного контексту. Саме в цьому аспекті правоохоронна діяльність, орієнтована на певну проблематику (Problem-Oriented Policing), часто перетинається з правоохоронною діяльністю, орієнтованою на потреби громад: від громадян, і власників бізнесу у відповідному районі може знадобитися інформація стосовно місцевих особливостей традицій та культури, а також справжнього масштабу проблеми, яка поширена у тих чи інших територіальних громадах.

Найкраще користь від цієї моделі можна проілюструвати багатьма реалізованими проектами, а також численними посібниками, розробленими, опрацьованими й опублікованими Центром із питань правоохоронної діяльності, орієнтованої на певну проблематику (Center for Problem-Oriented Policing/POP Center), за фінансування з боку Бюро з питань правоохоронної діяльності, орієнтованої на певну проблематику, Міністерства юстиції США. На сьогодні доступно 92 посібники з питань правоохоронної діяльності, орієнтованої на певну проблематику, у яких розглянуто деякі з найбільш поширених проблем злочинності, заходів реагування та інструментів, які можуть використовувати й застосовувати на практиці ті, хто має справу з подібними проблемами. Деякі з цих тем охоплюють проблеми вандалізму, крадіжок із проникненням, підробки медичних рецептів, незаконного заволодіння транспортними засобами та крадіжок з авто на паркувальних майданчиках, підліткового хуліганства в громадських місцях, хуліганств поряд із розважальними закладами тощо. У кожному посібнику наведено рекомендації щодо розв'язання проблем, включаючи інформацію та підходи, які кримінальні аналітики можуть використовувати для одержання належного розуміння й оцінки проблем, які справляють вплив на стан криміногенної ситуації.

Кримінальна аналітична діяльність відіграє важливе значення для успішності правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing). Аналітики, які працюють у рамках цієї моделі, вносять різноманітні внески, які використовуються впродовж усього процесу застосування методології SARA. Можна впевнено стверджувати, що без кримінального аналізу модель правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing), не набула б такого поширення та не справляла б такий значний позитивний вплив на розв'язання проблем злочинності й порушення громадського порядку, як це є сьогодні.

Як висновок слід зазначити, що дослідження та висвітлення позитивного зарубіжного досвіду упереджувального (проактивного) впливу на повторювані проблеми, які справляють вплив на стан криміногенної ситуації становить підвищений інтерес для профілактичної правоохоронної складової діяльності вітчизняних правоохоронних органів. Сформований та апробований зарубіжний досвід застосування ефективних та дієвих контрзаходів до повторюваних проблем є суттєвим резервом інституційних знань, застосування яких за аналогією також може призвести до сутнісних змін у стані справ щодо проблемно-орієнтованої правоохоронної діяльності, провідну роль у реалізації якої відіграє кримінально-аналітична складова [2, с. 85].

Список використаних джерел

1. Федчак І.А. Концептуальні основи сутності та змісту моделі правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing). «Ампаро» 2023. № 2. Запорізький національний університет. С. 90–96. URL: DOI https://doi.org/10.26661/2786-5649-2023-2-12.

2. Федчак І. А. Практичні аспекти вирішення проблем злочинності під час реалізації моделі діяльності поліції, орієнтованої на певну проблематику (Problem-Oriented Policing). Науковий журнал «Juris Europensis Scientia». 2023. № 3. С. 82–85. URL: DOI https://doi.org/10.32782/chern.v3.2023.17.

Ханькевич Андрій Миколайович,
викладач спеціальної кафедри № 4
Інституту підготовки юридичних кадрів
для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого,
кандидат юридичних наук, професор

РОЗВІДУВАЛЬНА АНАЛІТИКА ЯК ІНСТРУМЕНТ У СФЕРІ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Сьогодні аналітика пронизує майже кожен аспект людського життя, надаючи цінну інформацію, оптимізуючи процеси та дозволяючи приймати більш обґрунтовані рішення. Її подальший розвиток і застосування мають потенціал стимулювання інновацій та вдосконалення в широкому спектрі галузей.

Разом із тим, окремою сферою використання аналітики стоїть безпековий сектор держави. Сьогодні як ніколи важливо, щоб організації, що діють у безпековому секторі держави, приймали зважені та дієві рішення, засновані на аналітиці, яка базується на фактах.

Російсько-українська війна, політичні та фінансово-економічні кризи показали ціну невиправданих очікувань, і сьогодні безпекові питання актуальні у всіх галузях держави. У той час, коли державні відомства, установи та організації прагнуть безпеки в дуже нестабільні часи, дані та аналітика забезпечать їм міцний фундамент і впевненість, необхідні для досягнення успіху з мінімізованим ризиком.

Аналітика у безпековому секторі держави відіграє важливу роль й використовується у різних сферах. Зокрема, у сфері національної безпеки вона сприяє виявленню та аналізу загроз з боку терористичних організацій і державних терористичних утворень, завчасно виявляє «слабкі місця» у сфері інформаційних технологій та мережевої безпеки, що може призвести до негативних наслідків, таких як втрата даних, порушення конфіденційності, пошкодження комп'ютерних систем або мереж, фінансові втрати, а також може бути спрямована до вчинення кіберзлочинів або кібершпигунства.

Розвідувальна аналітика грає критичну роль і є невід'ємною частиною роботи Служби безпеки України (далі – СБУ) як суб'єкта розвідувального товариства і розвідувального органу [1]. Вона сприяє її підрозділам й органам бути більш

ефективними у своїй діяльності, забезпечувати національну безпеку та запобігати зовнішнім та внутрішнім загрозам.

Розвідувальна аналітична діяльність є однією з основних складових інформаційно-аналітичної роботи СБУ (п.1 ч.1 ст. 24 ЗУ «Про Службу безпеки України»), а також процесом пізнання, здійснюваного під час добування, аналітичної обробки та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України (ч. 2 ст.2 ЗУ «Про контррозвідувальну діяльність») [2; 3].

Зміст розвідувальної аналітичної роботи слід розглядати в набагато ширшому аспекті – не тільки як діяльність спеціалізованих суб'єктів в області інформаційно-аналітичного забезпечення, а й як органічну функцію, до реалізації якої причетні всі діючі оперативні співробітники й слідчі СБУ.

Розвідувальна аналітика сприяє виявленню інтересів та загроз у сфері розвідувальної активності іноземних держав, допомагає у розробці стратегій та планів захисту країни.

Результати аналітичних досліджень й аналітичні звіти є надважливими під час оцінки геополітичних ризиків, вирішення міжнародних конфліктів, налагодження дипломатичних відносин й прийняття виважених рішень у сфері зовнішньої політики та національної оборони.

Роль розвідувальної аналітики в діяльності СБУ невпинно зростає, насамперед внаслідок стрімкого розвитку сфери телекомунікацій, мережі Інтернет та мобільних портативних пристроїв, без яких складно уявити сучасну людину, й правопорушника зокрема, що зумовлює виникнення в інформаційному і часовому просторі додаткової інформації, яка потенційно може мати значення для контррозвідувальної діяльності.

Розвідувальна аналітика забезпечує інтелектуальну підтримку процесу підготовки та виконання завдань, покладених на СБУ. В сучасних умовах ефективне використання результатів розвідувальної аналітики стає одним із ключових складових, який визначає успішність чи провал контррозвідувальної діяльності.

Загалом розвідувальна аналітика в СБУ становить собою процес, що передбачає збір, оцінку, зіставлення, аналіз й репрезентацію інформації про відповідні об'єкти й створює можливість обрання співробітниками СБУ проактивного

підходу до реагування на проблеми та ризики у сфері контррозвідувальної діяльності.

У доповнення до того, що розвідувальна аналітика може бути використана для забезпечення відповідної підтримки контррозвідувальних, розвідувальних або оперативно-розшукових заходів, процесу досудового розслідування тощо, її цінність полягає також у забезпеченні раціонального управління та розподілу ресурсів СБУ.

Інструменти розвідувальної аналітики – це різноманітний і багатогранний арсенал наукових методів опрацювання інформації, який залежить від сфери застосування, предмета дослідження і поставлених завдань. В його основі завжди лежать методи наукового аналізу та синтезу, системного й багатофакторного аналізу тощо. Широко використовуються методи узагальнення, класифікації, сценарного прогнозування, моделювання, включно зі створенням складних моделей, багатовимірного позиціонування, фреймування, аналогій та онтологічного спрощення. Цей різноманітний набір інструментів у сфері функціонування розвідувальної аналітики допомагає повніше і глибше досліджувати різні аспекти предмета його аналізу.

Відповідно до змісту ключового терміну «аналітика», як його викладено у численних теоретичних джерелах, можна представити концепцію використання аналітичного інструментарію у розвідувальній аналітиці через такі підходи як:

1. Підхід, спрямований на засвоєння та використання знань, який може бути охарактеризований як складна система інформації, що складається з розгалужених компонентів. Цей підхід створює складну структуру знань, яка об’єднує пізнавальні та практичні аспекти і залучає аналітичні методи для набуття знань. Він служить інструментом для перетворення інтуїтивних уявлень у систематичний та логічний план. Цей підхід також може бути розглянутий як прикладна галузь, що формує компетентності аналітиків-професіоналів [4; 5].

2. Структурно-методологічний підхід описує сукупність принципів, які керують методами організації та технологічними аспектами розумової активності, будь-то індивідуальна або колективна. Цей підхід також афішує збірність методів, що надають можливість знаходити прихований сенс у текстах та складних соціально-політичних та економічних процесах [5].

3. Діяльнісний підхід можна розглядати як спеціалізовану сферу, яка відповідає певним цінностям і вищим стандартам управлінських організацій, або окремих осіб, які мають за мету

отримання інформації про практичні виклики, що стоять перед управлінням, та шляхи їх вирішення за допомогою застосування аналітичних методів. Це також можна охарактеризувати як галузь діяльності, яка стрімко розвивається та базується на опрацюванні інформації за допомогою аналітичних методів для задоволення термінових потреб держави, суспільства, окремих організацій та підприємств. Цей підхід слугує основою інтелектуальної, логічної та розумової діяльності, спрямованої на вирішення практичних завдань. На його основі функціонує принцип «випередження явищ», що дозволяє прогнозувати майбутній стан об'єкта аналізу [4; 6].

4. Управлінський підхід можна сприймати як впливовий шар інтелектуальної культури, який використовується керівництвом будь-якого суспільства для злагодженого управління соціальними процесами. Цей підхід також може бути описаний як адаптивна стратегія збирання інформації з метою прийняття управлінських рішень в умовах обстановки, що постійно змінюється [5].

Засоби та методи, які у комплексі складають інструментарій розвідувальної аналітики, в разі їх комплексного використання дозволяють:

– встановлювати індивідуальну або групову приналежність осіб до діяльності, що становить загрозу державній безпеці України;

– виявляти приховані взаємозв'язки між фігурантами зазначеної діяльності;

– досліджувати фактори та їх співвідношення, які певним чином впливають на стан державної безпеки України;

– визначати ризики та здійснювати прогнози стосовно розвитку подій, що можуть впливати на стан державної безпеки України;

– надавати загальні та цільові рекомендації для здійснення подальших контррозвідувальних заходів.

Таким чином, в інструментарії розвідувальної аналітики розкривається його глибша сутність, яка виходить далеко за межі роботи простого експерта у вузькій галузі знань. Інтелектуальні ресурси і досвід практичної діяльності охоплюють широкий спектр сфер, і не обмежуються вузькоспеціалізованими областями. Розвідувальна аналітика, наділена різноманітним набором інтелектуальних інструментів, які дають змогу адекватно досліджувати природу явищ і процесів, здатна виявляти приховані фактори, тенденції та закономірності у потоках первинної інформації, а також слугує дієвим способом розроблення обґрунтованих гіпотез для своєчасного прийняття управлінських

рішень у процесі прогнозування потенційних протиправних проявів (або їх недопущення та нейтралізації), спрямованих на нанесення шкоди державній безпеці України.

За умови ефективного використання наявного інтелектуального потенціалу та впровадження Службою безпеки України у сферу контррозвідувальної діяльності сучасних аналітичних методик опрацювання інформації, апробованих на практиці спецслужбами провідних країн світу, є серйозною зброєю в арсеналі зазначеної Служби.

Список використаних джерел

1. Про розвідку : Закон України від 17.09.2020 № 912-IX URL: https://zakon.rada.gov.ua/laws/show/912-20#Text.

2. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text.

3. Про контррозвідувальну діяльність : Закон України від 26.12.2002 № 374-IV. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text.

4. Сурмін Ю.П. Аналітика державного управління: сутність і тенденції розвитку. URL: http://academy.gov.ua/ej/ej5/txts/ 06sypdsv.htm.

5. Дяченко Н.П. Методологічне забезпечення інформаційно-аналітичної діяльності органів державної влади та органів місцевого самоврядування. URL: http://www.kbuapa.kharkov.ua/ e-book/ tpdu/2013-4/doc/3/02.pdf.

6. Філіпова Л.Я., Захарова І.В. Аналітична складова інформаційної діяльності: уточнення сутності, ознак і процесів. Вісник ХДАК. Випуск 28, 2009. С. 44–52.

Худенко Дмитро Миколайович,
ветеран Національної поліції України

ПОНЯТТЯ І ТИПОЛОГІЯ АНАЛІТИЧНИХ ПОМИЛОК У КРИМІНАЛЬНОМУ АНАЛІЗІ

Відомо, що слово «помилка» вживають у декількох значеннях: 1. Неправильність у підрахунках, написанні слова і т. ін. // Неправильність, неточність у якому-небудь механізмі, пристрої, в якійсь схемі, карті і т. ін. 2. Неправильність у вчинках, діях і т. ін. // Неправильна думка, хибне уявлення про когось, щось [1, с. 118].

Одним із предметів вивчення логіки та когнітивістики, як науки, є логічні та когнітивні помилки. Свого часу Аристотель комплексно вивчив логічні помилки та класифікував їх на

паралогізм і софізм [2, с. 10]. Як і раніше, сьогодні багато дослідників працюють над питанням помилок, результатом чого, є велика кількість описаних їх різновидів, робота з вивчення та класифікації триває.

Сформовані знання про помилки було запозичено до правової науки, зокрема, до оперативно-розшукової психології, кримінального процесу та криміналістики. Враховуючи те, що кримінальний аналіз, виник в Україні, як міждисциплінарна наукова течія, яка поєднує положення згаданих теорій, стає за можливе запозичити необхідні знання для подальшого вивчення феномену помилок у роботі особи, яка проводить кримінальний аналіз.

В протоколі Берклі в контексті дотримання принципу неупередженості йде мова про когнітивні викривлення на етапі процесу виявлення інформації в циклі розслідувань з використанням цифрових даних [3, с. 55–56]. Однак, не розкривається широко суть, поняття та типи таких помилок.

У настанові ОБСЄ з поліцейської діяльності на основі оперативних даних та інформації [4] відсутня інформація про помилки.

Чинне національне законодавство використовує термін помилка в 112 законах [5]. Загалом можна зустріти наступні терміни: помилка; помилка І роду; помилка ІІ роду; помилка пілота; помилка персоналу; помилка області регулювання; технічна помилка; методологічна помилка; програмно-апаратна помилка та інші.

В академічних джерелах з кримінального аналізу найбільш докладно вивчено представниками одеської поліцейської школи кримінального аналізу саме логічні помилки, ними зверталась особлива увага на правдивість або помилковість, достовірність або недостовірність, підтвердження чи непідтвердження інформації [6, с. 49; с. 60]. Представниками львівської школи кримінального аналізу також розглядались логічні помилки та одними з перших наведено приклад інструменту, який допомагає виявити помилки, але в геометричних розрахунках [7, с. 101; с. 210–-2011; с. 242–243]. Питання про помилки також висвітлено у колективних працях Г.В. Заєць, О.М. Заєць [8], Ю.В. Крутіка, В.Г. Головацького [9], В.Ю. Калугіна, М.М. Феськова [10] та інших.

У структурі наукових знань про кримінальний аналіз згаданий феномен безпосередньо пов’язаний з принципом об’єктивності та неупередженості. Він також знаходить свій

прояв у девіації або недопустимих відхиленнях у поведінці особи, яка проводить кримінальний аналіз.

Особливої актуальності дане питання набуває з появою наукового інтересу до інформаційних технологій, зокрема, програмування та штучного інтелекту, де створюють та використовують шаблони або еталони для дослідження певних сутностей в кримінальному аналізу.

Дійсно, у практиці кримінального аналізу зустрічаються помилки, допущені ініціатором запиту в написанні назви об'єкту або дат, помилки через неуважність або втому під час проведення кримінального аналізу, некомпетентність у інтерпретації або неправильне використання статистики, помилки в нормалізації або обробці даних тощо.

Метою нашого дослідження є формулювання дефініції - аналітична помилка в кримінальному аналізі та визначення їх типів.

Під аналітичними помилками в кримінальному аналізі пропонуємо розуміти різновид помилок когнітивного, фактичного, логічного, фізіологічного, програмно-апаратного або технічного характеру, суть яких полягає в невідповідності між реальним станом сутності та визначеним еталоном або у визначені еталону.

В залежності від природи аналітичної помилки умовно виділимо п'ять їх основних типів – когнітивні, фактичні, логічні, фізіологічні, програмно-апаратні або технічні.

Так, когнітивні помилки виникають через обмеження здатності людини в обробці інформації або людського сприйняття інформації. Вони можуть включати упередження, стереотипи, а також помилки у висновках, які зумовлені природніми обмеженнями пам'яті, уваги та іншими психологічними факторами. Ці помилки або викривлення можуть неусвідомлено впливати на прийняття рішень, створюючи потенційні перешкоди для об'єктивності.

Фактичні помилки відбуваються, коли аналіз ґрунтується на недостовірних або неправильних даних. Ними можуть бути, наприклад, неадекватні покази свідків, невірні дані з місця події або виявлення злочину, граматичні помилки в службовій документації тощо.

Логічна помилка, яка є важливим фактором у кримінальному аналізі, виникає як наслідок невірного логічного умовиведення, нерідко через помилкове поєднання причин і наслідків, або некоректних висновків із наявною інформацією.

Фізіологічні помилки пов'язані з індивідуальними особливостями особи, яка проводить кримінальний аналіз. Це може включати різні психічні розлади чи проблеми зі здоров'ям, такі як порушення зору або метаморфопсія – викривлення сприйняття розмірів. Вони мають суттєвий вплив на дослідження та можуть вимагати проведення обов'язкового щорічного медично-профілактичного огляду особи, яка проводить кримінальний аналіз.

Програмно-апаратні помилки виникають через неправильне функціонування або взаємодію між програмним забезпеченням та апаратним обладнанням. Ці помилки можуть стосуватися некоректної роботи обладнання, такого як комп'ютери та спеціалізовані пристрої, або програмного забезпечення, яке використовується для збору, аналізу та обробки даних у рамках досудового розслідування чи оперативно-розшукової діяльності. Програмно-апаратні помилки можуть призводити до неправильних результатів аналізу, затримок у обробці даних або неправильного інтерпретування результатів досліджень.

Технічні помилки пов'язані з технічними несправностями або неправильним використанням обладнання. Окрім фізичних дефектів, вони також можуть виникати через недостатній рівень кваліфікації або навичок користувачів. Їх виправлення ефективно здійснюється через злагоджену співпрацю між відповідними спеціалістами та експертами, а також завдяки ретельному контролю за якістю проведених досліджень.

У кримінальному аналізі важливо розуміти ці типи помилок, щоб мінімізувати їхній вплив на результат оперативно-розшукової діяльності, досудового розслідування та прийняття загальноуправлінських рішень. Кожна з них може зіграти фатальну роль в аналізі і здатна нашкодити та принести невідворотну шкоду, як особі, яка проходить по матеріалах оперативно-розшукової справи чи кримінального провадження, або територіальній громаді, так і особі, яка проводить кримінальний аналіз.

Кожен тип помилки вимагає індивідуального підходу до їх усвідомлення, ідентифікації та коригування. До методів кримінального аналізу з недопущення та усунення помилок можна віднести, наприклад: контроль з боку безпосереднього керівника; використання декількох методів кримінального аналізу та мінімум трьох інструментів, які здатні забезпечити вивчення предмету кримінального аналізу; надання завдання для переоцінки отриманих у результаті кримінального аналізу

висновків; здобуття інформації з нових джерел у випадку її безповоротної втрати за допомогою проведення додаткового кримінального аналізу; отримання інформації, яку не враховано з того ж джерела шляхом проведення повторного кримінального аналізу; відвід або обґрунтована відмова від подальшого проведення кримінального аналізу; опис помилки та звернення до відповідної служби підтримки чи експертів чи спеціалістів; самоконтроль; щорічний медично-профілактичний огляд; оновлення програмного забезпечення тощо.

Найбільш складними вважаємо ситуації полігамності помилок тобто, коли існує декілька різнорідних помилок, або ж проведення кримінального аналізу в умовах дефіциту часу чи невизнання помилок.

Також ситуацію з усвідомлення, ідентифікації та коригування помилок може ускладнювати умисна протидія з боку володільця джерела або державних інституцій, які мають прямий вплив на нього. Так, у серпні 2023 року внесений до держдуми рф законопроект, передбачає надання права спецслужбам на доступ, зміну та видалення інформації у російських базах даних. Планується, що нові положення набудуть чинності з 1 березня 2024 року.

Отже, аналітичні помилки в кримінальному аналізі – це різновид помилок когнітивного, фактичного, логічного, фізіологічного, програмно-апаратного або технічного характеру, суть яких полягає в невідповідності між реальним станом сутності та визначеним еталоном або у визначені еталону. В залежності від природи аналітичної помилки основними їх типами є когнітивні, фактичні, логічні, фізіологічні, програмно-апаратні або технічні помилки.

Список використаних джерел

1. Словник української мови : [в 11 т.] / АН Української РСР, Ін-т мовознав. ім. О. О. Потебні ; редкол.: І. К. Білодід (голова) [та ін.]. Т. 7. Київ : Наук. думка, 1976. 723 с.

2. Логіка юридична: навчально-методичний посібник (у схемах і таблицях) / за наук. ред. проф. В. С. Бліхара. Львів: ПП «Арал», 2018. 172 с

3. Протокол Беркли по ведению расследований с использованием открытых цифровых данных. Женева: Организация Объединенных Наций, 2022. 87 с. URL: https://www.ohchr.org/sites/default/files/2022-12/Berkeley-Protocol-Russian.pdf.

4. Руководство ОБСЕ по полицейской деятельности на основе оперативных данных и информации. Відень: ОБСЕ, 2017 104 с. URL: https://www.osce.org/files/f/documents/a/9/357211.pdf.

5. Результат пошуку / Термінологія. URL: https://zakon.rada.gov.ua/laws/main?find=2&dat=00000000&sp=%26sp%3D%3Adark&user=ud72edbc0-a0f0-4ed5-82f1-9b0ab166a6e4&text=&textl=1&bool=and&org=0&typ=1&yer=0000&mon=00&day=00&dat_from=&dat_to=&datl=0&numl=2&num=&minjustl=2&minjust=.

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

7. Федчак І.А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

8. Заєць Г.В. Актуальні проблеми критичного мислення й аналітичної діяльності в умовах воєнного стану / Г. В. Заєць, О.М. Заєць // Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 825–828.

9. Крутік Ю.В., Головацький В.Г. Шляхи підвищення ефективності роботи підрозділів кримінального аналізу // Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України: матеріали міжвідом. наук.-практ. конф. (Київ, 11 серп. 2022 р.) / [редкол.: С. С. Чернявський, Д. І. Овсянюк, В. В. Корольчук]. Київ : Нац. акад. внутр. справ, 2022. С.106–110.

10.Калугін В.Ю., Феськов М.М. Значення достовірності інформації в ході аналітичної діяльності // Південноукраїнський правничий часопис. 2023. № 1. С. 217–221. DOI https://doi.org/10.32850/sulj.2023.1.38.

Швед Альона Сергіївна,
курсант навчально-наукового інституту № 3
Національної академії внутрішніх справ
Науковий керівник:
Гузенко Євгеній Володимирович,
доцент кафедри тактичної підготовки
навчально-наукового інституту № 3
Національної академії внутрішніх справ,
кандидат психологічних наук,доцент

СИСТЕМА ЗАХИСТУ НАСЕЛЕННЯ ТА ТЕРИТОРІЙ ВІД НАДЗВИЧАЙНИХ СИТУАЦІЙ

Безпека є найосновнішою потребою людини, і Конституція України визначає її як одну з найвищих соціальних цінностей. Безпека людини є частково універсальним показником реалізації її прав і свобод, забезпечення захищеності від небезпеки. Це один з головних показників якості та рівня життя людини.

У наш час є багато небезпек, від яких ми маємо бути готові захищатись. Одна з таких небезпек – вогонь, який вийшов із-під контролю і здатний викликати значні руйнівні та смертоносні наслідки. Ми знаємо, що вогонь здавна супроводжував людину, дарував тепло, допомагав зберегти їжу від псування, розчищав бур'яни, добував метал. Уміння користуватися вогнем наділило людину відчуттям незалежності від від циклічної зміни тепла та холоду, світла і темряви. Вогонь є важливим емоційним символом і фактором соціальної єдності.

Однак пожежа, що вийшла з-під контролю, може мати серйозні руйнівні та плачевні наслідки.

Отже, пожежна безпека (ст. 2 Кодексу цивільного захисту України) – це відсутність неприпустимого ризику виникнення і розвитку пожеж, які супроводжуються неконтрольованим процесом знищування або пошкодження вогнем майна, під час якого виникають чинники, небезпечні для живих істот та навколишнього природного середовища [1].

Пожежа знищує матеріальні цінності, загрожує життю та здоров'ю людей, довкіллю. Тож проблема пожеж стає глобальною за своїми масштабами, торкаючись не тільки національних, а й міжнародних інтересів. Про це свідчать катастрофа на Чорнобильській АЕС, тривалі пожежі на нафтових

об’єктах Іраку як наслідок війни у Перській затоці, горіння великих лісових масивів [2].

Тому, забезпечення пожежної безпеки є обов’язковою складовою виробничої та іншої діяльності посадових осіб, працівників підприємств, установ, організацій і підприємців. Органи державного пожежного нагляду контролюють стан пожежної безпеки, вдаючись до різних санкцій (відмова у виданні дозволу на початок роботи або оренду приміщень, штрафи, призупинення експлуатації приміщень, споруд, устаткування, об’єктів тощо) [3].

Технічна безпека набуває все більшого значення в нашому житті як комплекс дій, спрямованих на те, щоб складне технічне обладнання проектувалося, виготовлялося та експлуатувалося відповідно до необхідних вимог для безаварійної роботи та відповідності умовам навколишнього середовища [5].

Техногенна безпека – це відсутність ризику виникнення аварій та/або катастроф на потенційно небезпечних об’єктах, а також у суб’єктів господарювання, що можуть створити реальну загрозу їх виникнення. Техногенна безпека характеризує стан захисту населення і територій від надзвичайних ситуацій техногенного характеру. Забезпечення техногенної безпеки є особливою (специфічною) функцією захисту населення і територій від надзвичайних ситуацій [4].

З великої кількості надзвичайних ситуацій техногенного характеру маємо транспортні аварії та катастрофи, несподіване руйнування будинків, аварії на електроенергетичних, комунальних системах життєзабезпечення, очисних спорудах і гідродинамічні аварії.

Техногенні небезпеки погіршують здоров’я людей, призводять до травм або загибелі, матеріальних витрат і деградації природного середовища. Захист від техногенних небезпек здійснюється вдосконаленням джерел небезпек, збільшенням відстані між джерелами небезпек і об’єктами захисту, застосуванням захисних засобів (колективних та індивідуальних) [4].

Як відомо, наша планета існує вже 4,5 мільярда років. Весь цей час на його поверхні постійно відбувалися складні фізико-хімічні процеси, виникало життя, формувалися насичені киснем атмосфери. Сьогодні наука досягла дуже високого рівня і може передбачити багато стихійних лих. Безсумнівно, незабаром ми навчимося їх попереджати...але той самий технологічний

прогрес породив багато слів, у тому числі таких термінів, як «техногенна катастрофа».

Аналізувавши всю інформацію та підсумовуючи сказане, ми маємо зрозуміти, що ми повинні ставитися дбайливо до власного життя, до життя наших друзів, близьких і рідних, людей навколо. Життя у всіх складається по-різному, тому що кожна людина має свої погляди, відчуття, цінності, здібності. Цінність життя людини – у неповторності її особистості, її талантів, її мрій і можливостей. Історія розкриває нам неймовірну різноманітність життя наших предків. Сучасність показує таке ж різноманіття життя кожної сучасної людини.

Список використаних джерел

1. Кодекс цивільного захисту України. Закон України № 5403-VI від 02.10.2012. URL: https://protocol.ua/ua/kodeks_tsivilnogo_zahistu_ukraini_1.

2. Пожежна безпека в Україні URL: https://pro-op.com.ua/article/1013-pojejna-bezpeka.

3. Основні поняття та визначення пожежної безпеки URL: https://pervozvanivka.silrada.org/osnovni-poniattia-ta-skladovi-pozhezhnoi-bezpeky/.

4. Пожежна безпека URL: https://bsm.com.ua/index.php/advanced-stuff/pozhezhna-bezpeka/124-pozhezhna-bezpeka.

5. Типологія аварій на потенційно-небезпечних об’єктах URL: https://elearn.nubip.edu.ua/mod/book/tool/print/index.php?id=418094&chapterid=150971.

Шишкін Ігор Ігорович,
начальник відділу міжнародного співробітництва з обміну аналітичною інформацією Департаменту кримінального аналізу Національної поліції України

ЗАЛУЧЕННЯ ПІДРОЗДІЛІВ КРИМІНАЛЬНОГО АНАЛІЗУ ДЛЯ ПОШУКУ РОСІЙСЬКИХ АКТИВІВ І ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЕКОНОМІЧНОЇ СПРЯМОВАНОСТІ

У сучасних умовах розслідування злочинів економічної спрямованості набуває особливого значення, оскільки економічні злочини можуть мати серйозний вплив на економічну стабільність країни та впровадження прозорих та ефективних

економічних політик. Аналітики виявляються ключовими учасниками цього процесу, оскільки вони застосовують передові методи аналізу великих обсягів фінансових даних, виявляють невідомі зв'язки та патерни, що допомагають не лише виявити злочинців, але й уникнути подібних порушень у майбутньому. Їхні високоспеціалізовані навички та здатність оперативно реагувати на зміни у фінансовому середовищі забезпечують ефективне функціонування системи розслідування, навіть в умовах що склались після повномасштабного вторгнення рф.

За спільними оцінками Міністерства економіки та Київської школи економіки станом на початок 2023 року загальні втрати України у війні склали близько 400 мільярдів доларів. Тому, з початку війни весь аналітичний сектор правоохоронних органів, починаючи від поліції і закінчуючи Службою безпеки України, зосередив свої зусилля задля виявлення російського бізнесу на території України [1].

Як результат станом на початок 2023 року було накладено арешти на рухоме і нерухоме майно підприємств РФ на загальну суму близько 38 млрд грн [2].

Враховуючи такі дані, важливу роль у роботі українських аналітиків щодо пошуку російських активів почала відіграла консолідована робота з міжнародними інституціями та участь у міжнародних проектах, адже до приховування російських капіталів та створення тіньових схем відмивання «брудних» коштів бізнесу держави-агресора були залучені команди досвідчених юристів-міжнародників, експертів у сфері економіки.

В свою чергу, аналітики в умовах війни, ситуації обмежених ресурсів, зосередили свою увагу на двох напрямах:

1) Пошуку в Україні активів, які належать рф та її громадянам, які підтримують агресію.

2) Виявлення закордонних активів агресора: участь у зборі доказової бази задля подальшої конфіскації та передачі Україні.

Завдяки цій роботі вдалося перевірити низку підсанкційних осіб країни-агресора, встановити їх активи на території України. Крім того, з початку війни аналітики долучилися до проекту Офісу Генерального прокурора України «Task Force» - Міжвідомчої робочої групи з питань притягнення до відповідальності осіб, причетних до агресії проти України, розшуку, виявлення та арешту активів, а також об'єктів права власності рф та її резидентів. За результатами цієї міжнародної співпраці робочій групі вдалося заморозити значні активи росіян, навіть не зважаючи на прихований вплив російського капіталу на лобіювання інтересів

російських політичних кіл в Україні через, так званих, агентів впливу, та відповідно поширення російських наративів.

Зауважу, що у роботі підрозділів аналітики важлива увага приділяється плануванню аналітичного дослідження. Така діяльність аналітика спрямована, в першу чергу, на визначенні ключових індикаторів:

1. Виявлення активів політично значущих осіб держави-агресора, які мають офіційно зареєстровані активи на власне ім'я на території України.

2. Встановлення підприємств, що мають зв'язки з військово-промисловим комплексом росії.

3. На регіональному рівні – виявлення пов'язаних фірм – лідерів з отримання доходів за своїм основним видом діяльності.

4. Підтвердження приналежності виявлених активів до фігуранта розслідування.

Після виконання цих кроків перед аналітиком постають виклики здійснення загальної оцінки активу, необоротних та оборотних, прибутків та видатків, а також визначення кола осіб, які мають права на активи, в тому числі реальних та бенефіціарних власників, де в першу чергу, увага зосереджується на наявності фірм-прокладок та офшорних трастів.

Підсумовуючи очевидно, що попит на аналітичні продукти у сфері розслідування злочинів економічної спрямованості показує зростання з початку повномасштабного вторгнення. Такий стан справ вимагає від аналітиків рішучих дій із застосування не лише класичних методів кримінального аналізу, а й залучення додаткової інформації за рахунок можливостей міжнародних партнерів та використання сучасних методів аналізу та реєстрів.

Список використаних джерел

1. Звіт про прямі збитки інфраструктури та непрямі втрати економіки від руйнувань внаслідок військової агресії Росії проти України станом на червень 2023 року. URL: https://damaged.in.ua/damage-assessment.

2. Звіт Національної поліції України про результати роботи у 2022 році. URL: https://www.kmu.gov.ua/news/zvit-natsionalnoi-politsii-ukrainy-pro-rezultaty-roboty-u-2022-rotsi.

Яровий Кирило Васильович,
кандидат юридичних наук, викладач
кафедри інформаційних технологій
та кібербезпеки навчально-наукового
інституту № 1 Національної академії
внутрішніх справ

ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ПРАВООХОРОННИМИ ОРГАНАМИ В ПРОТИДІЇ ЗЛОЧИННОСТІ

У сучасному світі, де технологічний прогрес швидко розвивається, правоохоронним органам потрібно шукати нові підходи та інструменти для протидії злочинності. Розслідування та розкриття злочинів є складноструктурованим завданням, яке вимагає великої кількості часу та ресурсів. Однак, роль технологій штучного інтелекту у роботі правоохоронних органів стає все більш вагомою.

У свою чергу, за допомогою технології штучного інтелекту можливо автоматизувати процес обробки значної кількості інформації. Наприклад, ідентифікувати схожі правопорушення на основі їхніх характеристик, розпізнати обличчя та відбитки пальців правопорушників, у тому числі виявлення підозрюваних осіб в місцях масового скупчення людей.

Впровадження інформаційних технологій, у тому числі технологій штучного інтелекту, є важливим елементом розвитку соціально-економічної, науково-технічної, оборонної, правової та інших видів діяльності у сферах, що мають загальнодержавне значення. Відсутність концептуальних засад державної політики у сфері штучного інтелекту унеможливлює створення та розвиток конкурентного середовища у зазначених сферах [1].

Однак, порушене питання потребує чіткого нормативно-правового регулювання, яке має відповідати етичним і правовим нормам, для збереження балансу між ефективною правоохоронною системою та захистом прав і свобод громадян.

У сучасному світі використання технологій штучного інтелекту у різних сферах життєдіяльності набуває надзвичайної популярності. Однак, що насьогодні, відсутнє загальноприйняте тлумачення визначення «штучного інтелекту», що свідчить про необхідність впровадження новітніх підходів до використання зазначеної технології, у тому числі правоохоронними органами.

Слід зазначити, що існування різних поглядів на тлумачення поняття «штучний інтелект» вводить громадськість в оману щодо суті визначення та призводить до неналежного його використання.

На законодавчому рівні під штучним інтелектом 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 [1].

У свою чергу, на нашу думку штучний інтелект необхідно розуміти, як галузь науки й техніки, метою якої є створення комп'ютерних систем і програм, здатних аналізувати та обробляти дані, робити висновки, виконувати завдання в автоматизованому режимі, взаємодіяти з навколишнім середовищем у спосіб, подібний людському розуму.

Технології штучного інтелекту дозволяють ефективно вирішувати різноманітні завдання у різних сферах життєдіяльності. Наприклад, штучний інтелект широко використовують у сфері освіти, економіки, медичного обслуговування, охорони навколишнього середовища, державного управління та правозастосовної діяльності.

У свою чергу, технології штучного інтелекту використовуються й правоохоронними органами у протидії злочинності.

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

У сфері кібербезпеки технологія штучного інтелекту використовується для виявлення, запобігання та нейтралізації інформаційних загроз, створення національних інформаційних систем і продуктів щодо захисту інформаційно-комунікаційних та автоматизованих систем.

Насьогодні, органи правопорядку країн Європейського Союзу активно впроваджують організаційні та правові заходи з метою запобігання та протидії правопорушенням у галузі сучасних технологій та інформаційних систем [2].

В області криміналістики, інструменти штучного інтелекту активно використовуються з метою генерації та видачі

експертних оцінок у межах судової експертизи, здійснення практики судової експертології та ДНК-аналізу.

Водночас штучний інтелект правоохоронні органи використовують для:

– виявлення та фіксації фактів, що містять ознаки кримінального злочину, у тому числі, виявлення порушень природоохоронного характеру, таких як браконьєрство, незаконний видобуток корисних копалин та незаконна рубка лісу;

– ідентифікація осіб та власників транспортних засобів у разі вчинення ними правопорушення на дорогах;

– проведення повітряних розвідок, шляхом використання безпілотників,
в бойових ситуаціях підрозділами особливого призначення;

– здійснення пошуку людей, які загубилися в лісі або у горах.

У тому числі, штучний інтелект активно використовується у процесі розробки автоматизованих систем, баз даних, алгоритмів для виявлення кримінальних правопорушників «по гарячих слідах», прогнозування кримінальних правопорушень та ідентифікації потенційних жертв злочинів, та в інших напрямках роботи правоохоронних органів.

Використання штучного інтелекту має як позитивні можливості, так і потенційні загрози, зокрема в сфері кримінальної активності та порушення прав і свобод громадян.

Досягнення у розвитку штучного інтелекту можуть використовуватися для вчинення злочинів, зокрема в галузі інформаційних відносин, і можуть також представляти безпосередню загрозу правам та законним інтересам людини, суспільства і держави.

Технології штучного інтелекту дозволяють ефективно вирішувати різноманітні завдання у правоохоронній сфері. Однак використання технологій штучного інтелекту правоохоронними органами у протидії злочинності потребує відповідного правового регулювання.

З урахуванням викладеного, пропонуємо наступні напрями реформування правового регулювання використання штучного інтелекту наступним чином:

– розглядати штучний інтелект як можливого суб’єкта та об’єкта в рамках правових відносин;

– розглядати штучний інтелект як незалежного учасника правових відносин, який здатний аналізувати і оцінювати важливість своїх дій та вчинки інших осіб;

У зв’язку з цим, постає необхідність упровадження чіткого регуляторного механізму для штучного інтелекту в нових сферах і вирішення проблем, пов’язаних із його використанням у межах правового поля.

Отже, відповідно до вищевикладеного, можна зробити такі **висновки:**

– визначення терміну «штучний інтелект» залишається неоднозначним, що може створити плутанину та призвести до некоректного використання цієї технології;

– правові аспекти використання штучного інтелекту не належним чином досліджені, що може призвести до значних проблем та невизначеності у сфері юридичного регулювання цієї технології.

– штучний інтелект активно сприяє розвитку цифрової економіки, проте виникають серйозні питання, які вимагають належних юридичних гарантій для безпечного функціонування систем.

З метою вирішення зазначеної проблематики необхідно розробити правову базу, що дозволить забезпечити належний контроль та захист в контексті використання штучного інтелекту. Відповідна правова база дозволить створити умови, в межах яких використання технологій штучного інтелекту може функціонувати безпечно та ефективно, сприяючи правоохоронним органам у протидії злочинності.

Список використаних джерел

1. 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-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220.

2. Конвенція про кіберзлочинність: Законом України від 07.09.2005 № 2824-IV URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

Наукове видання

АКТУАЛЬНІ ПИТАННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КРИМІНАЛЬНОГО АНАЛІЗУ В ПРАВООХОРОННІЙ СИСТЕМІ УКРАЇНИ

Матеріали
міжвідомчої науково-практичної конференції
(Київ, 17 листопада 2023 року)

Відповідальні упорядники:
Віктор КОРОЛЬЧУК, Дмитро ОВСЯНЮК

Комп'ютерна верстка *Яни ШУМКО*

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 10.11.2023. Формат 60x84/16. Папір офсетний.
Обл.-вид. арк. 9,75. Ум. друк. арк. 9,07
Тираж 20 прим.