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, 1 листопада 2024 року)

Київ
2024

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, 1 листопада 2024 року)

Київ
2024

УДК 343.97(477)(06)
А437

Рекомендовано до друку науково-методичною радою Національної академії внутрішніх справ 19 грудня 2024 року (протокол № 11)

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, 1 листоп. 2024 р.) / [редкол.: С. С. Чернявський, Д. І. Овсянюк, В. В. Корольчук]. – Київ : Нац. акад. внутр. справ, 2024. – 183 с.

УДК 343.97(477)(06)

ЗМІСТ

ВІТАЛЬНІ СЛОВА

НАУКОВІ ДОПОВІДІ

НАУКОВІ ПОВІДОМЛЕННЯ

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

Шановні колеги!

Від імені ректорату Національної академії внутрішніх справ маю нагоду привітати учасників міжвідомчої науково-практичної конференції.

Приємно, що розгляд питань упровадження сучасної моделі поліцейської діяльності, керованої аналітикою, в академії набув системності. Для Національної поліції та інших сил правопорядку цей напрям є особливо актуальним в умовах воєнного стану.

Зацікавлену участь у заході, зокрема в онлайн форматі, беруть представники Міністерства внутрішніх справ, Національної поліції, Державної прикордонної служби, Служби безпеки України, Державного бюро розслідувань, інших правоохоронних структур, наукових установ, міжнародних організацій та провідні науковці.

Реалії сьогодення засвідчують важливість застосування силами безпеки кримінального аналізу в забезпеченні громадського порядку й безпеки, протидії злочинності з розробленням ефективних стратегій протидії новим загрозам на загальнодержавному й місцевому (регіональному) рівнях.

Ефективними інструментами в діяльності підрозділів НП України слугують методи стратегічного й тактичного аналізу, упровадження програмних рішень для досудового розслідування, міжнародна комунікація. Актуалізуються новітні підходи до захисту об’єктів критичної інфраструктури, аналізу фінансових потоків і медіаданих, застосування методів OSINT тощо. Зазначені й інші інновації будуть презентовані спікерами та стануть предметом обговорення з урахуванням уже апробованого війною досвіду їх цільового використання.

Проблемами розвитку кримінального аналізу опікується і наша академія: створено профільний аналітичний відділ (Центр кримінальної аналітики), на постійній основі триває підготовка наукових і навчально-методичних видань з цієї тематики, забезпечено проведення цільових наукових досліджень, конференцій і тренінгів, фахівці академії отримують патенти на винаходи й корисні моделі, надають методичну допомогу оперативним і слідчим підрозділам.

Переконаний, що сьогоднішній захід сприятиме підтримці та розширенню творчих контактів і взаємодії.

Бажаю успіхів у подальшій реалізації набутих знань на практиці!

Слава Україні!

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

Шановні колеги!

Від імені Національної поліції України хочу привітати Вас з початком роботи науково-практичної конференції, присвяченої питанням розвитку кримінального аналізу в правоохоронній сфері та подякувати організаторам за сприяння в організації підвищення рівня професійної підготовки працівників та формування кадрового потенціалу служби кримінального аналізу Національної поліції України.

На сьогоднішній день штатна чисельність підрозділів кримінального аналізу складає 474 посади з них 70 % посад – це аналітики. Протягом 2022–2024 років на місцевому рівні створено 44 сектори кримінального аналізу у відділах кримінальної поліції районних управлінь ГУНП в областях та м. Києві, з них у 2024 році створено 9. На регіональному рівні у січні поточного року створено сектор кримінального аналізу у ГУНП в АР Крим. Відбулись зміни в організаційно-штатній структурі у Вінницькій та Миколаївській областях, де відділи кримінального аналізу реорганізовано в управління, у Харківській області – створено відділ оперативного моніторингу, додатково введено більше 15 посад аналітиків в різних ГУНП.

Керівництво Національної поліції ставить перед службою кримінального аналізу складні та амбітні завдання. Так з початку року підрозділи кримінального аналізу залучались до розкриття більш ніж 12 тис. злочинів (досудове розслідування за яких закінчено), з них було вчинено у звітному періоді понад тис., зокрема 6 тис. тяжких та особливо тяжких злочинів. Опрацьовано більше 83 тис. запитів на проведення аналізу по 200 тис. об’єктів, по яких підготовлено понад 140 тис. аналітичних продуктів (в порівнянні з 2023 роком опрацьовано 35 тис. запитів по яких підготовлено 66 тис. аналітичних продуктів).

Зі свого боку ми забезпечуємо підтримку заходів з розбудови потенціалу аналітичної діяльності, залучаючи до цього як можливості Національної поліції, так і міжнародну технічну допомогу.

Сподіваюся сьогодні ми зможемо поділитися нашими досягненнями та презентувати перспективи.

Інтеграція в світовий правоохоронний простір, адаптація світових аналітичних норм і стандартів, універсальність кримінальних аналітиків та налаштованість на постійне професійне зростання й удосконалення є одними із основних пріоритетів служби кримінального аналізу.

Представники служби постійно демонструють приклад високої адаптивності, оперативності, професіоналізму у виконанні поставлених завдань та налаштованість на постійне професійне зростання й удосконалення.

Кримінальні аналітики продемонстрували, що здатні відшукати найприхованіші закономірності в діяльності кримінальних елементів, побудувати системні зв'язки в ситуаціях неочевидності. На сьогодні вже досить складно уявити розкриття особливо резонансних, тяжких та особливо тяжких кримінальних правопорушень без участі кримінальних аналітиків та відповідного проведення аналітичної роботи.

Вчасні та вдало проведені аналітичні дослідження сприяли розкриттю значної кількості резонансних злочинів, особливо «по гарячих слідах», затриманню злочинців та загальному посиленню тиску на криміналітет. Служба кримінального аналізу стала незамінною частиною процесу документування протиправної діяльності злочинців у сфері незаконного обігу наркотиків, зброї та вибухівки, торгівлі людьми тощо.

Служба кримінального аналізу у своєму розвитку орієнтується на успішні моделі протидії злочинності в інших країнах, передусім оцінюючи їх ефективність та можливість застосування в сучасних українських умовах.

Важливо зазначити, що розбудова потенціалу кримінального аналізу відбувається завдяки постійній взаємодії Національної поліції з зарубіжними партнерами та закладами вищої освіти зі специфічними умовами навчання, що належать до сфери управління Міністерства внутрішніх справ України, зокрема Національній академії внутрішніх справ.

Тому, хочу подякувати організаторам конференції та нашим міжнародним партнерам за допомогу в розвитку кримінального аналізу Національної поліції України.

Бажаю всім учасникам сьогоднішньої конференції плідної роботи.

Слава Україні!

Бутко Роман Юрійович,
начальник Департаменту кримінального аналізу Національної поліції України

Шановні колеги!

Сьогодні ми зібралися, щоб обговорити основні вектори розвитку кримінального аналізу в правоохоронній системі України та зосередитися на фундаментальних принципах, які рухають вперед кримінальний аналіз.

Кримінальний аналіз — це динамічна та багатогранна служба, яка вимагає постійного розвитку та адаптації до сучасних викликів.

Люди, знання, системи та джерела даних — це чотири стовпи, на яких будується майбутнє кримінального аналізу.

Кримінальний аналіз в сучасному світі є невід'ємною складовою правоохоронної діяльності. У світлі постійно зростаючих загроз, кримінальний аналіз стає необхідним інструментом, який дозволяє забезпечувати якісні рішення в сфері правопорядку та безпеки суспільства.

Підрозділи кримінального аналіз, одна із небагатьох сервісних (оперативно-аналітичних) служб. І саме ефективність та результативність аналітичної діяльності напряму залежить від побудови дієвої комунікації між аналітиком, слідчим та «оперативником»

Лише завдяки комплексному підходу ми зможемо протистояти новим загрозам, зберігаючи безпеку суспільства на високому рівні.

Чотири принципи які рухають вперед кримінальний аналіз: люди, знання, системи та джерела. Кожен з цих аспектів формує цілісну систему, що дозволяє нам ефективно аналізувати, прогнозувати та протидіяти злочинній діяльності.

1. Люди – наш основний капітал

Люди залишаються серцем будь-якої системи. Це не тільки аналітики й дослідники, але й співробітники правоохоронних органів, судової системи, наукових та освітніх інституцій. Ефективна підготовка фахівців з кримінального аналізу потребує постійного розвитку, в тому числі вдосконалення знань у таких галузях, як психологія, соціологія, криміналістика та інформаційні технології. Навчання має бути динамічним процесом, що забезпечує сучасні компетенції в

аналізі великих даних, роботі з новими технологіями та розробці аналітичних моделей.

2. Знання – рушійна сила аналітичних процесів

Знання в кримінальному аналізі постійно оновлюються: сучасні загрози еволюціонують, з'являються нові типи злочинної діяльності, і, відповідно, методи протидії повинні також змінюватися. Традиційні методи аналізу поступаються місцем моделям, побудованим на штучному інтелекті та машинному навчанні, що дозволяє виявляти складні схеми злочинності, прогнозувати ризики та підвищувати ефективність прийняття рішень. Таким чином, наше завдання — постійно накопичувати, систематизувати та поширювати знання, залучаючи нові підходи та відкриття.

3. Системи – інтеграція та автоматизація

Сучасний кримінальний аналіз потребує комплексних систем, що об'єднують різні джерела даних та забезпечують аналітику в реальному часі. Інтеграція між базами даних, системами обліку, комплексними системами відеоспостереження та відеоаналітики іншими засобами збору інформації забезпечує повну картину ситуації та пришвидшує процеси реагування. Автоматизація, у свою чергу, дозволяє знизити навантаження на аналітиків, даючи можливість автоматично виявляти аномалії, зв'язки та тенденції. Завдяки цьому ми підвищуємо оперативність роботи та зменшуємо ймовірність помилок.

4. Джерела – від традиційних до цифрових

Джерела даних – це основа будь-якого кримінального аналізу. Сучасні аналітичні процеси включають як традиційні джерела (покази, звіти, матеріали розслідувань), так і цифрові сліди, які залишаються в інтернеті, соціальних мережах, мобільних додатках та інших цифрових платформах. Забезпечення доступу до легальних та надійних джерел інформації, а також питання приватності та етики залишаються критично важливими у нашій сфері. Спільне використання джерел даних між відомствами та країнами дозволяє виявляти транскордонні злочини і краще розуміти глобальні тенденції у злочинній діяльності.

Завдяки своїй експертності у зборі, обробці та аналізі даних, аналітики здатні опрацьовувати великі масиви інформації, проводити специфічний пошук з різних джерел, а також співставляти відомості з метою виявлення ключових тенденцій і закономірностей. Для ідентифікації осіб

використовуються автоматизовані інформаційні системи, реєстри та банки даних державних органів, системи МВС, програмні рішення Департаменту інформаційно-аналітичної підтримки (ДІАП) та технології приватних ІТ-компаній.

Окрім зазначених функцій, Департамент кримінального аналізу виконує низку інших важливих завдань:

– **Ситуаційний цілодобовий аналіз**: постійний моніторинг та аналіз оперативної ситуації, супроводження розкриття злочинів по «гарячим слідам», що дозволяє оперативно реагувати на загрози.

– **Оперативний аналіз**: в межах кримінальних проваджень проводиться детальне дослідження окремих об'єктів, ситуацій та явищ, а також візуалізація отриманих даних у вигляді карт і схем, що сприяє прийняттю зважених управлінських рішень.

– **Відеоаналітичні дослідження**: підрозділ займається покращанням якості фото- та відеозображень, а також ефективною роботою із системами категорії «Безпечне місто», що дозволяє підвищити рівень безпеки в населених пунктах.

– **Дослідження тактичного рівня**: виявлення тенденцій та аномалій у певних сферах, що дозволяє націлити зусилля правоохоронних органів на ключові проблеми.

– **Реалізація проєкту SOCTA**: проведення стратегічної аналітики, що включає оцінку загроз і ризиків, а також рекомендації для вдосконалення політики у сфері безпеки.

– **Інформаційно-аналітичне супроводження**: забезпечення оперативно-розшукової діяльності підрозділів Національної поліції через надання оперативних аналітичних матеріалів, що сприяє ефективному виконанню службових обов'язків.

– **Протидія дезінформації та інформаційно-психологічним операціям рф:** здійснення на постійній основі моніторингу медіа, соціальних мереж, месенджерів та інших онлайн-ресурсів для виявлення фейкових новин, дезінформаційних кампаній і пропагандистських матеріалів; використання спеціальних аналітичних інструментів для аналізу та виявлення дезінформаційних трендів і джерел.

За останні два роки відзначається стрімка розбудова служби кримінального аналізу в Україні, що стало важливим кроком у зміцненні системи правопорядку. У рамках цієї ініціативи функціонують **25 підрозділів кримінального аналізу Національної поліції (регіональні підрозділи ІІ та ІІІ**

рівнів) та один сектор кримінального аналізу в Автономній Республіці Крим.

Створено також перші місцеві підрозділи кримінального аналізу, які продовжують розвиватися. Одночасно з цим відзначається збільшення кількості практичних аналітиків, що дозволяє запровадити нові підходи до удосконалення їх аналітичних навичок через системне навчання.

Для досягнення визначених цілей в аналітичному напрямку Департамент пройшов кілька етапів реорганізації. У межах цих змін було створено декілька нових структурних підрозділів Департаменту, включаючи відділ відеоаналітичних досліджень, що забезпечує якісний аналіз відеоматеріалів, відділ оперативного моніторингу для контролю за криміногенною ситуацією, а також відділ аналітики воєнних злочинів, що займається вивченням та документуванням військових злочинів.

Крім того, утворено відділ оцінювання загроз і стратегічного аналізу, який аналізує можливі ризики та загрози, відділ оперативної аналітики, що забезпечує аналіз оперативної інформації для підтримки правоохоронних органів у виконанні їхніх завдань, а також відділ міжнародного співробітництва, який відповідає за обмін аналітичною інформацією з міжнародними партнерами.

Указані зміни не лише передбачають підвищення ефективності роботи служби, але й забезпечують більш системний підхід до кримінального аналізу, що має критичне значення для підтримки правопорядку та безпеки в країні.

Бондар Володимир Сергійович,
кандидат юридичних наук, професор,
завідувач кафедри кримінального
процесу та криміналістики навчально-
гуманітарного інституту Національної
академії Служби безпеки України

ОСОБЛИВОСТІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ВИЯВЛЕННЯ, ДОКУМЕНТУВАННЯ ТА РОЗСЛІДУВАННЯ КРИМІНАЛЬНО ПРОТИПРАВНОЇ ДІЯЛЬНОСТІ ОРГАНІЗОВАНИХ ГРУП І ЗЛОЧИННИХ СПІЛЬНОТ

Результати аналізу матеріалів сучасної практики протидії організованій злочинності в Україні дає можливість виокремити основні тенденції використання її представників спецслужбами іноземних держав (насамперед, рф) у підривній діяльності проти нашої держави:

1) організація та координація підконтрольними «злодіями в законі» з числа вихідців з рф, країн Кавказу та Середньої Азії кримінально-протиправної діяльності місцевих організованих груп, спрямованої на загострення криміногенної обстановки в Україні, здійснення провокацій тощо;

2) координація кримінально-протиправної діяльності організованих груп у виправно-трудових установах України, спрямовані на формування стійких кримінальних осередків у місцях позбавлення волі та дестабілізацію їх роботи;

3) відрядження до України «злодіїв в законі» з числа вихідців з рф та інших країн колишнього СРСР для створення і координації діяльності організованих груп, спрямованої на штучне загострення криміногенної обстановки в регіонах держави;

4) використання можливостей представників вітчизняних та етнічних організованих груп для налагодження каналів нелегальної міграції громадян рф та інших держав через територію України до ЄС або легалізації та її території;

5) залучення представників організованої злочинності в Україні до створення та безпосередньої діяльності диверсійно-розвідувальних груп (ДРГ);

6) використання можливостей представників етнічних організованих груп для налагодження ремонту й відновлення на території інших держав російської військової техніки, пошкодженої в ході ведення бойових дій. Так, російсько-британський підприємець Т. Сомхішвілі (кримінальний авторитет «Тамаз Тобольський»), співзасновник та в минулому гендиректор російської нафтової компанії «Лукойл» виявився причетним до діяльності структур МО рф, що відновлюють боєздатність російських ВКС на потужностях Тбіліського авіаційного заводу, – не лише ремонту російських літаків, але й модернізації ракет класу «повітря-повітря».

Інформаційно-аналітичне забезпечення досудового розслідування кримінально-протиправної діяльності злочинних організацій та організованих груп представляє собою розгалужену складну систему, яка охоплює наступні напрями діяльності:

– аналіз зібраної органами правопорядку та Офісом Генерального прокурора статистичної інформації про стан, структуру та динаміку кримінальних правопорушень, скоєних злочинними спільнотами (ч. 4 ст. 255 Кримінального кодексу України – далі КК України);

– аналіз інформації про обставини, способи вчинення злочинів злочинними спільнотами;

– включення в процес аналізу та синтезу інформації, накопиченої в централізованих, статистичних, оперативних та інших обліках СБ України, МВС України, а також інших органів правопорядку;

– використання відомостей, що містяться в базах даних, якими володіють інші державні органи та недержавні установи та організації (державна казначейська служба, банківські установи, пенсійний фонд, державна міграційна служба, криптовалютні біржі, бази персоналізованого обліку доступу співробітника до інформаційних систем, бази даних систем відеонагляду за об’єктами, бази даних сеансів всіх видів послуг зв’язку, що надаються населенню, бази даних провайдерів, які здійснюють надання послуг Інтернет своїм користувачам та ін.);

– використання сучасних комунікацій для створення умов для логічного та технічного об’єднання різних інформаційних масивів при вирішення обліково-реєстраційних задач.

Водночас, під час досудового розслідування злочинів, учинених злочинними спільнотами взагалі та при проведенні тактичних операцій зокрема, оперативно-аналітична робота має

низки особливих властивостей. Специфічність вихідної інформації, її оперативної перевірки призводить до виникнення найскладнішої ситуації за двома основними аспектами:

1) необхідність відпрацювання надвеликого масиву різнопланової інформації з перспективою запиту, отримання та переробки додаткової інформації суб'єктів оперативно-розшукової діяльності, визначених ч. 3 ст. 5 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю»;

2) вимушена екстреність оперативно-розшукових заходів, негласних слідчих (розшукових) дій, слідчих (розшукових) дій з метою недопущення настання тяжких наслідків.

Аналітичний пошук здійснюється практично безперервно. Аналізуються факти, події, стосунки, зв'язки, співвідношення різних злочинних груп. Піддаються аналізу групи кримінальних проваджень. Запитується на аналізується інформація органів і установ виконання покарань та слідчих ізоляторів. Таким чином, на початковому етапі залежно від розглядуваних версій події окреслюється те чи інше коло осіб, можливо причетних до підготовки злочину злочинною спільнотою.

Створення, нормативне та технічне забезпечення діяльності інформаційної системи та її підсистем в яких обов'язково виділенні окремою категорією осіб причетних, або раніше причетних до організованої злочинності, їх кримінальні зв'язки, у тому числі з держслужбовцями та представниками правоохоронних органів, наявність нерухомого майна, або використання нерухомого майна яке належить іншим особам для злочинної діяльності або для зберігання предметів та речовин які можуть бути доказами злочинної діяльності, наявність або використання автомототранспорту, можлива наявність незареєстрованої зброї, обов'язкова систематизація компрометуючих даних отриманих від конфідентів та у ході здійснення оперативно-розшукових та оперативно-технічних заходах, факти притягнення особи що має відношення до організованої злочинності до кримінальної або адміністративної відповідальності.

Ефективність цієї системи обумовлена тим фактом що наповнення її баз це завдання не тільки спеціальних підрозділів (Департаменту стратегічних розслідувань, Департаменту кримінального аналізу Національної поліції України, відповідних підрозділів Служби безпеки України, а й всіх існуючих (наприклад, офіцер громади отримавши інформацію стосовно можливої причетності особи до організованої злочинності повинен

ініціативним рапортом, через керівництво, надіслати цю інформацію до компетентних оперативних підрозділів, які в свою чергу забезпечать надходження цієї інформації до інформаційної системи).

Використання ресурсів інформаційної системи та її підсистем повинно здійснюватися тільки в рамках оперативно-розшукової справи (контррозвідувальної справи) або кримінального провадження і тільки особою якою заведено оперативно-розшукову справу, або яка входить до складу слідчо-оперативної групи, створеної для розслідування кримінального провадження. Інформація про доступ до банку даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про особу, яка отримала доступ, та про обсяг даних, доступ до яких було отримано. Кожна дія особи щодо отримання інформації з інформаційних ресурсів, фіксується у спеціальному електронному архіві інформаційно-комунікаційної системи, за допомогою якої отримано відомості. В електронному архіві фіксуються прізвище, ім'я, по батькові, посада та номер спеціального жетона (в разі наявності), вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації особи, яка отримувала інформацію з інформаційних ресурсів, реєстрів та баз даних. Використання інформації отриманих із банків даних підсистем що містять відомості стосовно осіб причетних до організованої злочинності буде найефективнішою якщо вони будуть оброблені разом з інформацією, отриманою із баз даних Департаменту оперативно-технічних заходів (оброблених телефонних трафіків фігурантів), результатами оперативно-розшукових та оперативно-технічних заходів (у тому числі проведених Департаментом оперативних служб), контррозвідувальних заходів, оброблених та проаналізованих з залученням департаменту кримінального аналізу.

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

ЗАРУБІЖНИЙ ДОСВІД ВИКОРИСТАННЯ ПРАВООХОРОННИМИ ОРГАНАМИ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

На сьогоднішній день інформаційні технології з використанням технічних засобів фото- і кінозйомки, відеозапису у світі розвиваються швидкими темпами. Правоохоронні органи зарубіжних країн широко запроваджують новітні розробки в цій сфері у свою діяльність і для їх впровадження урядами країн виділяється достатньо коштів. В Україні темпи впровадження сучасних інформаційних технологій дещо відстають від світових. В першу чергу це пов'язано з обмеженим фінансуванням правоохоронних органів. Ще однією з причин є неналежним чином організоване співробітництво Національної поліції з місцевою владою. [1]

Розглянемо деякі напрями впровадження та використання систем відеоспостереження правоохоронними органами на прикладі деяких країн світу.

За даними поліції Сінгапуру, камери відеоспостереження допомогли розкрити понад 5000 злочинів з моменту їхньої появи у 2012 році. Уряд Сінгапуру настільки впевнений в успіху міського відеоспостереження, що прагне до 2030 року збільшити кількість камер з 90000 до 200000. Мережа камер відеоспостереження, відома як PolCam, охоплює такі місця, як житлові квартали, районні центри, автостоянки та інфраструктуру громадського транспорту.

Правоохоронці заявили, що камери відеоспостереження дуже ефективні в запобіганні фізичних злочинів, таких як випадки домагань, пов'язаних із кредитуванням без ліцензії, включно з крадіжками зі зломом, крадіжками автомобілів і пошкодженням майна. Ці злочини скоротилися більш ніж удвічі з 2015 по 2020 рік [2].

Згідно з даними поліції Сінгапуру, комплекти відеоспостереження PolCam не тільки допомагають стримувати і розкривати злочини, а й розширюють можливості поліції в плані ситуаційної обізнаності та дають змогу офіцерам оперативніше реагувати на інциденти, пов'язані з порушенням правопорядку на місцях. Система навіть дозволяє виявляти

підозрюваних: приклади включають виявлення підозрюваних, які починають бійку до прибуття офіцерів на місце події, або виклик підкріплення, якщо залучено багато людей. У кількох таких випадках офіцерам вдавалося заарештувати підозрюваних одразу після прибуття на місце.

Мережа відеокамер PolCam продовжує розвиватися завдяки новим можливостям, таким як вдосконалена технологія відеоаналітики для прискорення пошуку релевантних матеріалів.

Сполучене Королівство визнане світовим співтовариством лідером у сфері використання відеоспостереження для забезпечення публічної безпеки та розслідування злочинів, а Лондон часто називають світовою столицею відеоспостереження, і це не дарма. В місті встановлено сотні тисяч камер відеоспостереження, і середньостатистичний житель Лондона потрапляє в камери відеоспостереження 300 разів на день [3].

Відеоспостереження відіграє значну роль в охороні публічного порядку і сприяє поліції в справі розслідування злочинів. Запровадження систем відеоспостереження почалося в 1970-ті роки, бурхливе зростання кількості їхніх інсталяцій припало на 1990-ті роки і триває донині.

За оцінками фахівців CCTV.co.uk, до 2025 року в одному тільки Лондоні вже буде мільйон камер відеоспостереження – ця тенденція поширіться на всю країну. Станом на листопад 2020 року на 14 лондонців припадає одна камера відеоспостереження. Але в міру вдосконалення технологій і збільшення кількості населення, це співвідношення може змінитися до однієї відеокамери спостереження на 11 лондонців. За прогнозами аналітиків, до 2025 року в столиці Великої Британії вже буде нараховуватися 1 мільйон відеокамер спостереження [3].

Постійне підтвердження цього лідерства – наочні приклади того, як відеоспостереження робить вулиці безпечнішими, знижує страх громадян перед злочинністю і дає змогу виявляти та боротися з серйозними порушеннями закону. Відеоспостереження користується значною підтримкою громадськості країни.

Використання відеоспостереження з метою розслідування терористичної діяльності у Великій Британії викликало значний інтерес в усьому світі, і наразі безліч країн наслідують цей приклад у розвитку власних інфраструктур відеоспостереження.

Держава вельми активно інвестувала в системи відеоспостереження, що перебувають у віданні місцевої влади, і

в результаті ними виявилися оснащені більшість міських центрів [4].

Відеоспостереження довело свою ефективність у процесі сприяння поліцейським силам під час ідентифікації та пред'явлення обвинувачень особам, пов'язаним зі здійсненням злочинної діяльності, найсерйознішими проявами якої є тяжкі злочини і терористичні акти.

Розширення відеоспостереження, збір даних і застосування Китаєм так званої системи соціального рейтингу (кредиту довіри) викликають занепокоєння у країн, тісно пов'язаних із Китаєм, а також у тих країн, де розгорнуті китайські технології та інфраструктура.

На думку аналітиків, Китай використовує технології для посилення авторитарного правління завдяки близько півмільярда камер відеоспостереження (дані на 2022 рік), дедалі ширшому використанню програм розпізнавання облич і голосових відбитків, пристроям стеження за телефонами та одній з найбільших у світі баз даних ДНК.

Китайська поліція використовує систему відеоспостереження однієї з найбільших компаній, що виробляють камери, Hikvision для стеження за протестувальниками.

Hikvision розробила хмарний інструмент Infovision IoT, який «дає можливість розумного прийняття рішень у сфері безпеки» і надає послуги для полегшення роботи поліції. У технічних документах, підготовлених Hikvision, є опис сигналів тривоги, про які система повідомляє силовиків.

Крім таких варіантів, як «крадіжка», «порнографія» або «торгівля людьми», є описи сигналів, пов'язаних із протестами і демонстраціями. Це, зокрема, «збір натовпу для порушення порядку в громадському місці», «збір натовпу для нападу на державні органи», «незаконні збори, ходи, демонстрації» і навіть «погроза подачі петиції» і «Фалуньгун» (заборонений у Китаї релігійний рух). У документах немає докладного опису, як саме працюють ці сигнали, але серед варіантів реакції є виклик співробітників поліції.

Також у базі даних компанії Hikvision зберігаються обличчя та інші фізичні характеристики, які компанія дозволяє відстежувати своїм клієнтам. Різні особисті якості перераховані як частина «кадрового словника», включно з політичним статусом, релігією та етнічною приналежністю, а також фізичні

описи, як-от довге або коротке волосся або носіння окулярів, колір пальта, віковий діапазон і посмішка [5].

Китайська поліція тестує технологію розпізнавання людей за ходою, розроблену однією з китайських ШІ-компаній «Watrix». Вона використовує камери відеоспостереження та аналізує тисячі показників ходи людини, зберігаючи їх в базі даних. Програмне забезпечення може ідентифікувати людину на відстані 50 м від точки зйомки, навіть якщо в неї приховано обличчя або віна стоїть до відеокамери спиною [6].

Представники поліції заявили, що планують встановити камери відеоспостереження з програмою розпізнавання облич у громадських місцях (ресторани, магазини, розважальні центри, туристичні пам'ятки), а також у приватних місцях – житлових будинках, караоке-залах і готелях [7].

На сьогоднішній день Ізраїль перетворився на державу тотального стеження за своїми громадянами: незліченна кількість камер зовнішнього спостереження та інтернет-додатків фіксує буквально кожен крок, кожну дію в інтернеті, кожну покупку. Вся ця інформація зберігається у величезних базах даних.

Комісія з національної безпеки Ізраїлю затвердила нову регуляцію, яка фактично дає змогу поліції Ізраїлю вести масове стеження за громадянами без жодного контролю. Нові правила надають поліції безпрецедентні технологічні можливості в галузі контролю над переміщенням громадян. Мова йде про особливу систему відеозйомки, яка містить «комп'ютерний процесор, що дає змогу збирати й обробляти різні дані, зокрема зображення». Крім того, система «дає змогу здійснювати точну ідентифікацію об'єктів у режимі реального часу і вести спостереження за людьми».

Простими словами це ідентифікація людини за обличчям, що дає змогу вести за об'єктом безперервне комп'ютерне стеження. Місцезнаходження того, чий портрет опинився в системі, можна завжди визначити в режимі реального часу[8].

В сфері безпеки дорожнього руху поліція Ізраїлю використовує систему контролю дорожнього руху на основі ШІ.

Датчики, встановлені вздовж доріг, передаватимуть інформацію на комп'ютер із центральним процесором, що використовує штучний інтелект, який здатний автоматично аналізувати відео і виписувати штрафи за правопорушення.

З датчиків дорожнього руху, стаціонарних та мобільних смарт-камер у режимі реального часу дані передаватимуться до

диспетчерського центру для автоматичної розшифровки. Штрафні квитанції будуть виготовлені протягом кількох хвилин і надіслані порушникам.

Така система допоможе фіксувати правопорушення, які складніші для виявлення поліцейськими – перетин розмітки, керування автомобілем з використанням телефону тощо.

Цифрові штрафи включатимуть відеофіксацію правопорушення, включно з посиланням на відеоролик, що «підвищить справедливість і прозорість процесу» для порушників [9].

Інформаційні технології з використанням технічних засобів фото- і кінозйомки, відеозапису та технологій ШІ розвиваються дуже швидко в світі та знаходять своє застосування в правоохоронних органах різних країн.

Виходячи зі світового досвіду, основні тенденції розвитку систем безпеки з переліченими технологіями є такими: 1) масове впровадження штучного інтелекту в усі системи безпеки, біометричне розпізнавання осіб, пошук поведінкових аномалій у рухах людини, розвиток розумних систем керування дорожнім рухом, автоматичний пошук підозрюваних, автотранспорту в розшуку тощо; 2) сертифікація інтелектуальних систем відеоспостереження із заданими показниками точності розпізнавання, визначення координат об'єкта тощо; 3) запровадження нейронних мереж для забезпечення високих показників точності; 4) упровадження систем безпеки в усіх місцях масового скупчення людей та на транспорті [10].

Список використаних джерел

1. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду: метод. матеріали для працівників підрозділів поліції МВС України / В. А. Коршенко, М. В. Мордвинцев, Ю. В. Гнусов та ін. Харків : Харків. нац. ун-т внутр. справ, 2020. 34-40 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/5a48c83f-6d5b-4435-b9d4-0cbd34d42dc8/content.

2. До 2030 року кількість камер відеоспостереження в Сінгапурі збільшиться більш ніж удвічі. URL: https://worldvision.com.ua/k-2030-godu-kolichestvo-kamer-videonabludeniya-v-singapure-uvelichitsya-bolee-chem-vdvoe/.

3. Скільки камер відеоспостереження є в Лондоні? URL: https://cctv.co.uk/how-many-cctv-cameras-are-there-in-london/.

4. National CCTV Strategi, Graeme Gerrard, Garry Parkins, Ian Cunningham, Wayne Jones, Samantha Hill, Sarah Douglas, 2007. URL: https://www.viseum.co.uk/wp-content/uploads/2010/12/UKHomeOfficeCCTVStrategy.pdf

5. В Китае система видеонаблюдения Hikvision автоматически помогает силовикам отслеживать протестующих – The Guardian. URL: https://svtv.org/news/2022-12-29/v-kitae/.

6. Chinese police test gait-recognition technology from AI start-up Watrix that identifies people based on how they walk. URL: https://www.scmp.com/tech/start-ups/article/2187600/chinese-police-surveillance-gets-boost-ai-start-watrix-technology-can (дата звернення: 23.11.2024).

7. Хитой кузатув тармоғининг кенгайиб бораётгани иттифоқчилар ва савдо шерикларида хавотир уйғотмоқда URL: https://central.asia-news.com/ru/articles/cnmi_ca/features/2022/08/24/feature-01 (дата звернення: 22.11.2024).

8. Нова технологія дозволяє поліції Ізраїлю стежити за будь-ким і будь-коли

TheMarker URL: https://detaly.co.il/novaya-tehnologiya-pozvolyaet-politsii-sledit-za-kem-ugodno-i-kogda-ugodno/ (дата звернення: 22.11.2024).

9. Поліція Ізраїлю представляє систему контролю дорожнього руху на основі ШІ URL: https://mignews.net/news/lifestyle/policiya-izrailya-predstavlyaet-sistemu-kontrolya-dorozhnogo-dvizheniya-na-osnove-ii.html (дата звернення: 23.11.2024).

10. В.А. Коршенко, В.В. Чумак, М.В. Мордвинцев, Д.В. Пашнєв, Стан систем безпеки з використанням технічних засобів відеозапису та відеоспостереження: зарубіжний досвід, перспективи впровадження в діяльність національної поліції України,). ISSN 2617-2933 (Online). Право і безпека – Право и безопасность – Law and Safety. 2020. № 2 (77).

Буртак Артем Володимирович,
заступник начальника міжнародного відділу з обміну аналітичною інформацією Департаменту кримінального аналізу Національної поліції України;
Франчук Юлія Олександрівна,
старший інспектор міжнародного відділу з обміну аналітичною інформацією Департаменту кримінального аналізу Національної поліції України

ЕФЕКТИВНІСТЬ МІЖНАРОДНОЇ ВЗАЄМОДІЇ ТА СПІВПРАЦІ В СЛУЖБІ КРИМІНАЛЬНОГО АНАЛІЗУ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ МІЖНАРОДНОГО ОБМІНУ АНАЛІТИЧНОЮ ІНФОРМАЦІЄЮ

В умовах глобалізації та зростання транснаціональних загроз питання міжнародної взаємодії та співпраці в кримінальному аналізі стає надзвичайно важливим. Злочинні мережі, які часто діють за межами національних кордонів, ставлять перед правоохоронними органами нові виклики. Ефективний обмін аналітичною інформацією вимагає швидкої та надійної співпраці між державами, що є ключовим фактором для протидії виникаючим загрозам. Обмін інформацією між країнами щодо методів вчинення злочинів, результатів аналітичної діяльності, фактів скоєння злочинів та осіб, що їх вчинили, є необхідним для ефективної міжнародної співпраці в сфері кримінального аналізу.

Дослідження теми міжнародної взаємодії та співпраці в сфері кримінального аналізу є предметом уваги численних вчених та дослідників. Зокрема, О. Користін у своїй монографії розглядає впровадження інноваційних підходів у кримінальному аналізі в Україні [1, с. 150]. У свою чергу, колектив авторів у праці «Exploring crime analysis: Readings on essential skills» висвітлює виклики, з якими зіштовхуються працівники служби кримінального аналізу під час обміну інформацією на міжнародному рівні [2, с. 45]. Інші дослідники, наприклад, Сара Джонсон (Sarah Johnson), акцентує увагу на важливості безпеки інформаційних систем як ключового елемента міжнародної взаємодії [3, с. 78]. Крім того, проблеми, які стосуються

міжнародного обміну аналітичною інформацією, включають відмінності в законодавствах країн, мовні бар'єри, а також обмежений доступ до сучасних технологій [4, с. 142]. Дослідження вченого Лейка Кеннета також вказує на важливість розробки спільних стандартів для обміну даними [5, с. 33].

Слід зазначити, що міжнародна взаємодія відрізняється від міжнародної співпраці, оскільки перша акцентує увагу на інтеграції інформаційних систем та технологій для досягнення спільних цілей, тоді як друга охоплює ширший спектр відносин між країнами, включаючи юридичні, політичні та культурні аспекти. Україна активно співпрацює в сфері кримінального аналізу з понад 20 країнами. Найближчими партнерами є Польща, Литва, Латвія, Молдова, США, Іспанія, Німеччина, Нідерланди, Велика Британія та Естонія. Ці країни забезпечують підтримку через співпрацю в рамках Європолу та доступ до платформ, таких як SIENA (Secure Information Exchange Network Application), для безпечного обміну аналітичною інформацією. Усі країни не лише надають технічну підтримку, але й активно беруть участь у проведенні спільних тренінгів та обміні досвідом у сфері боротьби з кіберзлочинністю та організованою злочинністю.

Лише за рік кількість опрацьованих запитів на проведення кримінального аналізу, наданих в межах міжнародної співпраці зросла з 51 у 2023 році до 226 за 9 місяців 2024 року, або на 343 %.

Варто зазначити, що важливим елементом міжнародної взаємодії є використання мережевих платформ або додатків. Тому такі організації як Інтерпол, Європол і ООН, використовують кілька платформ для обміну аналітичною інформацією між країнами.

Дослідження показують, що такі інструменти є критично важливими для покращення взаємодії між правоохоронними органами різних країн [1, с. 12].

Варто зазначити, що платформи для обміну інформацією значно спрощують процес взаємодії між кранами, а також створюють додаткові можливості для підвищення ефективності кримінального аналізу на глобальному рівні [7, с. 97].

Станом на 2024 рік Україна обмінюється інформацією з наступними міжнародними організаціями та установами:

1) Інтерпол – Україна є членом Інтерполу і використовує його систему для обміну інформацією про злочинців, крадені автомобілі, наркотики та інші види злочинності [8].

2) Європол – Україна активно співпрацює з Європолом, маючи можливість отримувати та надавати інформацію через Інформаційну систему Європолу (EIS) та інші інструменти [9].

3) UNODC (United Nations Office on Drugs and Crime) – Україна співпрацює з ООН у питаннях боротьби з наркотиками і злочинністю, маючи доступ до аналітичних ресурсів і звітів [10].

4) SIENA – через партнерство з Європолом Україна використовує цю платформу для безпечного обміну конфіденційною інформацією з країнами ЄС та іншими партнерами [6, с. 90].

Слід виділити основні проблеми міжнародного обміну інформацією та можливі шляхи їх вирішення:

1) Різні закони про конфіденційність ускладнюють обмін персональними даними. Рішення: створення міжнародних стандартів, таких як GDPR (General Data Protection Regulation) – це стандарт Європейського Союзу для захисту персональних даних. Він встановлює правила для організацій щодо збору, обробки та зберігання персональних даних громадян ЄС, а також застосовується до міжнародних платформ для обміну інформацією [11].

2) Безпека даних і кіберзагрози. Вирішується через шифрування та використання безпечних платформ (наприклад, SIENA) [12].

3) Затримки в обміні інформацією через складні процедури. Рішення: автоматизація процесів обміну [13].

4) Різні формати даних. Рішення: уніфікація форматів і шаблонів звітів (аналітичних продуктів).

5) Політичні бар'єри. Рішення: міжнародні угоди для зниження політичної напруженості [14].

6) Фінансування – багато країн стикаються з обмеженими ресурсами для підтримки та розвитку технологій, необхідних для ефективного обміну аналітичною інформацією. Рішення: розробити міжнародні програми фінансування, які б підтримували країни з обмеженими ресурсами, надаючи їм доступ до технологій і навчальних програм.

Отже ми наголошуємо на тому, що важливо боротися з такими проблемами, як різні правові системи, технічні бар'єри, недостатня довіра між країнами, які ускладнюють міжнародний обмін інформацією та, як наслідок, боротьбу із транснаціональною злочинністю.

У світі, де кіберзагрози стають все більш складними та виразними, аналітика допомагає виявляти та аналізувати

кібератаки, знаходити вразливості і розробляти заходи для їх своєчасного запобігання та нейтралізації. Аналітика заглиблюється в сутність розвідувальних та контррозвідувальних операцій, допомагає відповідати на важливі питання та ухвалювати важливі рішення [1, с. 29]. Тому слід сказати, що боротьба із потенційними загрозами у сфері обміну інформацією є одним із пріоритетних питань, адже міжнародна співпраця вимагає надійності, швидкості передачі даних та відповідності стандартам захисту даних. Інформаційний обмін має враховувати специфіку правових норм різних держав, наприклад, стандарт GDPR у ЄС, який визначає вимоги до обробки та захисту персональних даних, важливих для ефективної комунікації між країнами

Ефективність міжнародної взаємодії та співпраці у сфері кримінального аналізу є надзвичайно важливою для успішної боротьби з транснаціональною злочинністю. Обмін інформацією та застосування кращих практик дозволяють країнам оперативніше реагувати на загрози, оптимізуючи використання своїх ресурсів і стратегій. Ключовими елементами цього процесу є гармонізація законодавства, розвиток технологій обміну даними та створення ефективних каналів комунікації між міжнародними організаціями та правоохоронними установами. Проте виклики, такі як мовні бар'єри, культурні розбіжності та питання кібербезпеки, продовжують залишатися актуальними, вимагаючи додаткових зусиль для їх подолання.

Список використаних джерел

1. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Швець Д., Бутко Р., Денисенко Б. та ін., за заг. ред. Користіна О.Є. - Київ: «ВАІТЕ», 2024. 444 с.

2. International Association of Crime Analysts. (2017). Exploring crime analysis: Readings on essential skills (3rd ed.). K. Gallagher, J. Wartell, S. Gwinn, G. Jones, & G. Stewart (Eds.). Overland Park, KS: Author.

3. Johnson, Sarah. (2019). Access to Information in Conflict Situations. International Journal of Law and Society, 11(2), 75–90.

4. Літвінов, М. (2020). Проблеми міжнародного обміну інформацією в кримінальному аналізі. Журнал кримінологічних досліджень, 8, с. 135–150.

5. Лейк, Кеннет. (2021). Спільні стандарти для міжнародного обміну даними. Монографія. Київ: Академія права.

6. Міжнародні угоди та їх роль у кримінальному аналізі. (2022). Журнал міжнародних відносин, 15(1), с. 78–92.
7. ООН. (2023). Звіт про глобальні зусилля у боротьбі з міжнародною злочинністю. Нью-Йорк: ООН.
8. Ukraine: INTERPOL General Secretariat statement. Режим доступу: https://www.interpol.int/News-and-Events/News/2022/Ukraine-INTERPOL-General-Secretariat-statement
9. Secure Information Exchange Network Application (SIENA).
Режим доступу: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena
10. UNODC Office in Ukraine. Make Ukraine safer from drugs, organized crime and corruption. Режим доступу: https://www.unodc.org/poukr/uploads/documents/UNODC_in_Ukraine_Factsheet/UNODC_in_Ukraine_Factsheet_EN.pdf
11. Interpol. Data Protection in Interpol. Режим доступу: https://www.interpol.int
12. Europol. SIENA - Secure Information Exchange Network Application.. Режим доступу: https://www.europol.europa.eu
13. European Commission. European Criminal Records Information System (ECRIS). Режим доступу: https://ec.europa.eu
14. UNODC. International Cooperation Against Transnational Organized Crime. Режим доступу: https://www.unodc.org

Василинчук Віктор Іванович,
доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ;
Поптанич Юрій Михайлович,
аспірант Національної академії внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЇ З МЕСЕНДЖЕРІВ ЯК ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

З впровадженням Всесвітньої павутини у 1990-х роках, а потім популяризацією соціальних медіа та смартфонів у 2000-х роках, кількість та якість інформації у відкритому доступі різко змінилися. Сьогодні будь-яка особа зі смартфоном

чи доступом до Інтернету може створювати та поширювати цифровий контент у всьому світі, хоча і різної якості, достовірності та прозорості. Зростаючий обсяг даних та швидкість передачі і обміну такими даними створили нові можливості для слідчих, що ведуть розслідування із використанням даних у відкритому доступі, збирати та аналізувати інформацію про міжнародні злочини та порушення прав людини. У той же час творці контенту тепер можуть поширювати дезінформацію та відносно легко маніпулювати цифровими даними.

Тому світова практика документування злочинів пішла іще далі та запровадила механізм фіксації цифрової інформації із відкритих джерел – протокол Берклі. Тобто документуванню підлягають не лише фактичні дані щодо спілкування між абонентами в месенджерах, а й інформація із відкритих джерел, з метою подальшої її використання в якості доказу для цілей правосуддя. [1, с. 21–22]

Особливо актуальним та дискусійним є питання використання у кримінальному провадженні в якості доказової бази інформації, яка передається абонентами за допомогою месенджерів (Viber, WhatsApp, Telegram, тощо).

Для фіксування слідів вчиненого або вчинюваного кримінального правопорушення правоохоронцям вкрай важливо оглянути вміст переписки месенджерів, які установлені на мобільному телефоні учасника кримінального провадження або іншому належному йому електронному пристрої.

Сама по собі переписка в месенджері не вважатиметься документом, оскільки це лише переписка між абонентами, яка за своїми ознаками тяжіє до звичайного спілкування (передачі інформації).

Для того, щоб переписка в месенджері набула ознак документу та могла слугувати доказом обставин вчинення кримінального правопорушення, її необхідно оформити процесуально правильно, так як того вимагає КПК України.

До процесуального оформлення виявлена на електронному пристрої інформація, що становить інтерес для органу досудового розслідування, може розглядатись лише як невід'ємна частина цього електронного пристрою, який, з огляду на вміст інформації, що в ньому зберігається, де-факто матиме статус речового доказу.

Відтак, для процесуального оформлення виявлених на електронному пристрої фактичних даних, які відображають

обставини вчинення кримінального правопорушення та можуть бути використані як доказ у кримінальному провадженні необхідно провести процесуальні дії із неухильним дотриманням вимог КПК України.

У відповідності до вимог ст. 86 КПК України доказ визнається допустимим, якщо він отриманий у порядку, встановленому цим кодексом [2].

Ст. 159 КПК України зазначає, що тимчасовий доступ до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення [2].

У випадку якщо власник електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку не обмежує доступ системою логічного захисту та надає добровільну на огляд вмісту інформації на його електронному пристрої, такий доступ може здійснюватися без ухвали слідчого судді.

Тимчасове вилучення майна також може відбутись під час обшуку чи огляду.

У разі необхідності слідчий чи прокурор вилучає за допомогою апаратно-програмних комплексів копії інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста.

У випадках, передбачених КПК України, хід і результати проведення процесуальної дії фіксуються у протоколі.

Тому після складення протоколу за результатами огляду переписки в месенджері установленого на електронному пристрої із дотриманням процедури визначеної КПК України (ухвала слідчого судді, обшук, добровільна згода, особистий обшук при затримані особи на підставі ст. 208 КПК України, інше) останній може використовуватись в суді, як окремий документ для встановлення необхідних обставин вчинення кримінального правопорушення, а не як речовий доказ.

Окрім процесуального закріплення переписки в месенджері за допомогою протоколу в арсеналі правоохоронних органів є можливість призначити судову комп'ютерно-технічну

експертизу. Під час проведення вказаної експертизи здійснюється відшукання, вилучення та систематизація необхідної інформації. Отримані внаслідок проведення експертизи фактичні дані фіксуються у висновку експерта та додатках до нього.

Зазначений спосіб збирання доказів є актуальним з огляду на те, що в практичній діяльності не завжди можливо детально оглянути кожен електронний носій за участю спеціаліста, наприклад у зв'язку з значною кількістю слідчих дій, що проводяться одночасно.

У подальшому, експерт може ефективно виконати завдання по аналізу даних по відповідним ключовим словам та відповідно до питань поставлених у постанові слідчого (прокурора).

Крім цього у випадках, якщо відомості про кримінальне правопорушення та особу, яка його вчинила, неможливо отримати шляхом проведення слідчих (розшукових) дій, слідчий за погодженням із прокурором або прокурор мають право звернутись до слідчого судді відповідного апеляційного суду із клопотанням про надання дозволу на проведення негласної слідчої (розшукової) дії у виді зняття інформації з електронних інформаційних систем, яка полягає у пошуку, виявленні і фіксації відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача лише в рамках розслідування тяжкого та особливо тяжкого злочинів. (3 ст. 264 КПК України) [2].

Результати проведеної негласної слідчої дії в даному випадку оформляються протоколом у відповідності до вимог КПК України.

Вказаний спосіб надає можливість отримати важливу для досудового розслідування інформацію (у вигляді аудіо-, відео-файлів, переписки) та документи (їх проекти), якими особи причетні до протиправної діяльності обмінювалися між собою під час підготовки, вчинення, приховування слідів кримінального правопорушень.

У подальшому отриману інформацію та доказову базу можна використати при проведенні слідчих (розшукових) дій (обшук, огляд, допит, тощо.), зокрема для виявлення та вилучення оригіналів документів, перевірки під час отримання показань свідка, потерпілого, підозрюваного, тощо.

Таким чином, до процесуального оформлення виявлена на електронному пристрої інформація, що становить інтерес для органів досудового розслідування, може розглядатись лише як невід'ємна частина цього електронного пристрою, який, з огляду на вміст інформації, що в ньому зберігається, де-факто матиме статус речового доказу.

Після складення протоколу за результатами огляду переписки в месенджері установленого на електронному пристрої із дотриманням процедури визначеної КПК України (ухвала слідчого судді, обшук, добровільна згода, особистий обшук при затримані особи на підставі ст. 208 КПК України, інше) чи відповідного протоколу, у разі проведення НС(Р)Д, чи отримання висновку експерта останні може використовуватись в суді, як окремий документ для встановлення необхідних обставин вчинення кримінального правопорушення, а не як речовий доказ.

Список використаних джерел

1. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових джерел/ практичний посібник – 2020 р.: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

2. Кримінальний процесуальний кодекс України, URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

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

ОСОБЛИВОСТІ ОНЛАЙН ШАХРАЙСТВА В УКРАЇНІ

On-line шахрайство є найбільш поширеним видом кіберзлочину. У загальній сукупності злочинів, протидія яким є пріоритетом в діяльності кіберполіції, більше третини складають кримінальні правопорушення, пов'язані із шахрайством, при вчиненні яких використовуються сучасні інформаційні та телекомунікаційні технології. Водночас, 84% шахрайств вчиняються саме у формі діяльності передбаченої частинами 3 та 4 ст. 190 ККУ, що ще раз підкреслює надзвичайну поширеність on-line шахрайства в Україні.

За методологією Європол IOCTA, із врахуванням значної різноманітності способів та засобів, що використовуються при

здійсненні платежів, розрізняється два види шахрайства з платежами: з використанням картки та без такої.

За сучасного стану найбільшим поширенням характеризуються загрози шахрайства з платежами, пов'язані з (*табл.1*): роздрібною торгівлею фізичними (51,4 %) та віртуальними товарами (40,6 %); конвертацією валют (криптовалют та електронних грошей) (46,6 %); а також позикою (46,6 %).

Експертами зазначається про певне загальне зниження масштабів поширення цієї групи загроз за останні роки, враховуючи і перші роки повномасштабного вторгнення, хоча окремі з них характеризуються меншим трендом до зниження масштабів, зокрема, пов'язані з: позикою, роздрібною торгівлею фізичними товарами, конвертацією валют (криптовалют та електронних грошей) та використанням паливних карток.

Таблиця 1

Загрози шахрайства з платежами без використання банківської картки

ВИДИ ЗАГРОЗИ ШАХРАЙСТВА З ПЛАТЕЖАМИ БЕЗ ВИКОРИСТАННЯ БАНКІВСЬКОЇ КАРТКИ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
2.1. пов'язане з транспортом – авіаквитки		23,3	-	-	-	33,91
2.2.пов'язане з транспортом – квитки на поїзд або автобус		30	-	-	-	34,00
2.3.пов'язане з транспортом - оренда автомобілів		22,6	-	-	-	31,83
2.4.пов'язане з позикою (послугою, орендою приміщення тощо)		46,6	-	-	-	37,43
2.5.пов'язане з веб-сайтами азартних ігор		37,1	-	-	-	33,67
2.6.пов'язане з роздрібною торгівлею – фізичні товари		51,4	-	-	-	39,52
2.7.пов'язане з роздр торг– віртуальні товари		40,6	-	-	-	36,66
2.8.пов'язане з конвертацією валют(криптовалют та електр грошей)		46,6	-	-	-	38,95
2.9. з використанням паливних карток		37,4	-	-	-	34,62
2.10.з використанням карток у роздрібній торгівлі продуктам		28,3	-	-	-	32,53
2.11. з використанням клубних карток		16,3	-	-	-	28,33
2.12.з використанням подарункових карток		18,3	-	-	-	28,60
2.13.з використанням ігрових карток		19,7	-	-	-	29,01
2.14. на ринку мобільного зв'язку		30,6	-	-	-	32,23
2.15.в сфері комп'ютерних ігор (внутрішньоігрові перекази)		29,7	-	-	-	30,02
2.16.пов'язане з букмекерськими послугами		28,3	-	-	-	31,29
2.17.пов'язане з «move to»		21,1	-	-	-	29,89

Зазначені види загроз шахрайства з платежами, без використання банківської картки, характеризуються і найвищим ризиком поширення у післявоєнний період, зокрема, пов'язані з: роздрібною торгівлею фізичними товарами (39,52 %), конвертацією валют (криптовалют та електронних грошей)

(38,95 %), позикою (37,43 %) та роздрібною торгівлею віртуальними товарами (36,66 %).

Водночас, було ідентифіковано 13 загроз, у якості різновиду поширення шахрайства з платежами, з використанням банківської картки (*табл. 2*).

Таблиця 2

Загрози шахрайства з платежами з використанням банківської картки

ВИДИ ЗАГРОЗИ ШАХРАЙСТВА З ПЛАТЕЖАМИ З ВИКОРИСТАННЯМ БАНКІВСЬКОЇ КАРТКИ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
3.1. Зняття готівки з банківських карт UA за межами UA		46,00				40,45
3.2.Зняття готівки з банківських карт UA в межах UA		63,70				42,23
3.3.Зняття готівки з іноземних банківських карток у межах UA		38,60				37,40
3.4.PoS-покупки з використанням скомпрометованої платіж карти		45,10				38,35
3.5.Шахрайство з платіжними картками: трешінг		30,90				33,40
3.6.Шахрайство з платіжними картками: фармінг		32,00				34,23
3.7.Шахрайство з платіжними картками: фішинг		52,30				42,80
3.8.Шахрайство з банкоматом: скіминг		37,40				35,67
3.9.Шахрайство з банкоматом: траппінг		29,10				33,04
3.10.Шахрайство з банкоматом: фантом		27,40				32,36
3.11.Шахрайство з банкоматом: jackpotting		26,90				32,17
3.12.Шахрайство з телефоном та інтернетом: вішинг		44,90				38,26
3.13.Шахрайство з телефоном та інтернетом: смішинг		38,60				36,06

За сучасного стану, враховуючи і перші роки повномасштабного вторгнення, найбільшим поширенням серед таких загроз характеризуються: зняття готівки з банківських карт UA в межах UA (63,70 %); шахрайство з платіжними картками (фішинг) (52,3 %); зняття готівки з банківських карт UA за межами UA (46,0 %); PoS-покупки з використанням скомпрометованої платіжної карти (45,1 %), а також шахрайство з телефоном та інтернетом (вішинг) (44,9 %).

Водночас, важливо зазначити про незмінність масштабів поширення зазначеної групи загроз за останні роки, враховуючи і перші роки повномасштабного вторгнення. Водночас, окремі загрози, характеризувалися певним трендом підвищення масштабів поширення: шахрайство з платіжними картками (фішинг); зняття готівки з банківських карт UA в межах UA; зняття готівки з банківських карт UA за межами UA.

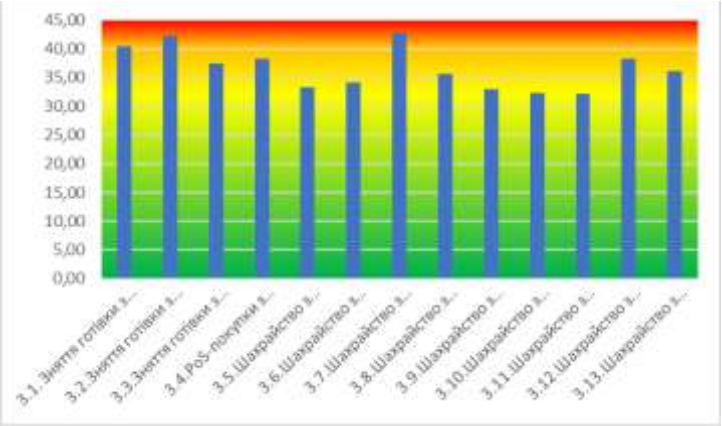


Рис. Оцінка ризиків поширення загроз шахрайства з платежами, з використанням банківської картки, у післявоєнний період

Оцінюючи ризики поширення групи загроз шахрайства з платежами, з використанням банківської картки, у післявоєнний період, такий же різновид шахрайства характеризуються найвищим ризиком (*рис.*): шахрайство з платіжними картками (фішинг) (42,8 %); зняття готівки з банківських карт UA в межах UA (42,23 %); та зняття готівки з банківських карт UA за межами UA (40,45 %).

Таким чином, шахрайство з платежами є найбільш поширеною загрозою у сфері кіберзлочинності, складаючи 67,10 % усіх випадків on-line шахрайства. Воно характеризується високим рівнем ризику і залишається важливою проблемою як до, так і після війни.

Денисенко Богдан Анатолійович,
експерт з питань організованої злочинності (Консультативна місія Європейського Союзу)

ІТ ІНФРАСТРУКТУРА ДЛЯ ВПРОВАДЖЕННЯ ILP

Процес реформування сектору цивільної безпеки є складним та багатогранним. Для досягнення бажаного результату, в процесі реформування необхідно орієнтуватись на

чітке бачення, модель, стратегію розбудови, а особливо – на спроможності.

Модель правоохоронної діяльності є основою, скелетом, навколо якого повинні вибудовуватись всі інші елементи системи, як от: інформаційні, аналітичні, робочі та управлінські процеси та можливості, таке інше. Важливо щоб всі елементи моделі були взаємосумісними та доповнювали один одного, розвивались комплексно. Модель по суті і є дороговказом, який допомагає сформулювати, сформувати бачення та стратегію розбудови, яка повинна відповідати потребам країни. Правоохоронна діяльність, керована аналітичною розвідкою (ILP) є моделлю правоохоронної діяльності, яка може забезпечити державі можливість ефективно протидіяти транснаціональній організованій злочинності та комплексно реагувати на виклики злочинності, та, відповідно, звертати увагу на вразливості для подальшого підвищення спроможносте – правоохоронної системи, та, відповідно, – держави.

Модель ILP є універсальною та лежить в основі будь якого підходу, який має на меті за найменших витрат ресурсів досягти максимального, найкращого результату. ILP є управлінським інструментом, що допомагає керівникові (або особі, що приймає рішення) приймати найбільш ефективне та результативне рішення щодо розподілу ресурсів (людських, у тому числі інтелектуальних, матеріальних, таке інше).

Крім застосування інструментів державного управління, аналітичних інструментів та можливостей, необхідно враховувати, створювати та застосовувати існуючі (у тому числі найбільш сучасні) IT технології та відповідні можливості відповідно до сформованої моделі правоохоронної діяльності. Аналітична розвідка (intelligence) є ключовим, базовим та центральним елементом формування моделі ILP. Впровадження ILP передбачає уніфікованого та комплексного підходу щодо збору, внесення, опрацювання, аналізу та поширення даних, інформації та, відповідно, аналітичної розвідки серед всіх правоохоронних органів. Що, в свою чергу, передбачає уніфікованого та комплексного підходу щодо формування баз даних, реєстрів, репозиторіїв, таке інше серед усіх правоохоронних органів (формування державного стандарту); спільної та взаємосумісної IT інфраструктури на рівні всієї держави (не може бути різних стандартів у державі, яка декларує напрям комплексного реформування та цифровізації на державному рівні); уніфікованих процесів (щодо збору,

внесення, опрацювання, аналізу та поширення даних, інформації, аналітичної розвідки) серед усіх правоохоронних органів, що передбачає існування уніфікованого бачення та розуміння даних процесів на всіх рівнях вертикально (від тих, хто збирає, вносить, опрацьовує та аналізує дані, інформацію, – до керівника, керівного складу найвищого рівня) та горизонтально (серед усіх державних органах).

Інформаційно-аналітична складова є достатньо дороговартісною та складною. У зв'язку з чим пропонується пройти наступні етапи перед впровадженням оновленої інфраструктури:

1) Створення уніфікованого понятійного апарату. Всі учасники процесу (ті хто вносять (збирають), опрацьовують та аналізують інформацію, керівники та виконавці, таке інше) повинні стандартизовано підходити до всіх процесів роботи з даними, інформацією, говорити «однією мовою».

2) Функціональний аудит бізнес-процесів (робочих процесів) з інформаційного менеджменту (щодо збору інформації, її внесення та опрацювання, аналітичних процесів та прийняття управлінських рішень) задля визначення найбільш ефективної та результативної моделі.

3) Перегляд, переналаштування, та/або новий дизайн IT можливостей (IT інфраструктури (фізичного обладнання, програмного забезпечення та інформаційних технологій, таке інше), та відповідних процесів регулювання з управління інформацією, баз даних, реєстрів, таке інше).

IT можливості повинні відповідати реальним робочим процесам, потребам аналітиків та завданням, які перед ними ставляться керівництвом (або тими хто приймає рішення щодо проведення аналітичного дослідження).

Інтегроване, комплексне бачення щодо впровадження реформ передбачає поєднання ряду реформ в рамках уніфікованого підходу. Відповідно, ILP, як основа, повинна впливати на розвиток похідних процесів та продуктів, як от SOCTA та EMPACT (або їх альтернативи), а не навпаки.

Звіт щодо оцінки загроз серйозної та організованої злочинності (SOCTA), як аналітичний продукт є результатом впровадження ILP, його (цей звіт) неможливо повноцінно та якісно сформувати в умовах домінування моделі традиційної правоохоронної діяльності, або неповноцінного чи часткового впровадження ILP. Цей звіт передбачає «зріз» стану загроз станом на той момент, коли він формувався. Основною його

метою є визначення поточних тенденцій, які змінюються з часом. Для цього необхідно мати відповідну ІТ інфраструктуру, інтегровані бази даних, адаптовані процеси збору, аналізу та розповсюдження інформації, аналітичної розвідки, таке інше, для того щоб можливо було отримати цей звіт наближено до реального часу. У той же час, EMPACT (європейська міждисциплінарна платформа проти кримінальних загроз), побудований навколо політичного циклу ЄС щодо боротьби з організованою та серйозною міжнародною злочинністю (EU Policy Cycle), що є ні чим іншим, ніж адаптацією циклу аналітичної розвідки (intelligence cycle) до політичного процесу застосування бачення щодо серйозної та організованої злочинності, отриманої в результаті формування звіту SOCTA. Звіт SOCTA і є першим етапом цього циклу (EU Policy Cycle). Цикл аналітичної розвідки (intelligence cycle) є основою ILP.

Отже, SOCTA та EMPACT є результатом впровадження ILP. ILP є основою, скелетом для SOCTA та EMPACT. Тому, формування звіту SOCTA та участь у EMPACT передбачає повноцінне та комплексне впровадження ILP.

У той же час, необхідно пам'ятати, що немає універсального бачення та стратегії розбудови моделі. Задля цього проведення так званого внутрішнього аудиту щодо інформаційного менеджменту, перегляд та переналаштування бізнес-процесів (робочих процесів), є ключовим та надає можливість розбудувати ту модель ILP, яка б відповідала реальним потребам правоохоронної системи. ILP тільки тоді буде давати свої повноцінні результати, коли всі елементи будуть працювати навколо сучасних та адаптованих інформаційно-аналітичних можливостей безперебійно, ефективно та результативно, як єдиний механізм, орієнтований на результат. Результатом у цьому випадку є підвищення спроможностей правоохоронної системи щодо ефективної боротьби з організованою злочинністю, протидія транснаціональній організованій злочинності та можливість ефективно, результативно та комплексно реагувати на виклики злочинності. У той же час, модель ILP є універсальною та може бути адаптованою до більшості управлінських процесів. Впровадження дієвої моделі ILP є основою для подальшого комплексного реформування правоохоронних органів.

Кардашевський Юрій Романович,
доктор філософії в галузі права,
керівник відділу внутрішнього
контролю Національного агентства
з питань запобігання корупції

КІБЕРЗЛОЧИННІСТЬ У БАНКІВСЬКІЙ СФЕРІ

Значна частина кіберзлочинів вчиняється фінансово мотивованими злочинцями. Таким злочинцям, які займаються торгівлею на кримінальних ринках або вимаганням грошей від своїх жертв, потрібні певні кошти чи інші фінансові інструменти для здійснення та отримання прибутку від своєї діяльності. У «реальних» злочинах це, швидше за все, була б готівка в місцевій або вільно конвертованій валюті, але кіберзлочинцям, які працюють у цифровому світі, потрібне цифрове рішення.

Фінансова активність, перш за все, пов'язується з отриманням швидкого прибутку і мінімізацією ризиків для самих кіберзлочинців, та набуває самих різних форм (*табл. 1*):

– фінансові шахрайства: *використання фішингу, скіммінгу, та інших методів для отримання доступу до банківських рахунків та кредитних карток*;

– фінансові транзакції від жертв до злочинців та між злочинцями: *використання новітніх банківських послуг та сучасних фінансових інструментів*.

Водночас важливими аспектами фінансової активності кіберзлочинців є відмивання коштів та фінансування тероризму, що певним чином пов'язується не лише з матеріальним збагаченням, а й з формуванням ринку кримінальних послуг у кіберпросторі.

За сучасного стану найбільшим поширенням характеризуються загрози шахрайства з платежами (67,10 %), водночас є значною фінансова активність, пов'язана з платежами від жертв до злочинців (60,90 %). Такий тренд зберігався упродовж останніх років та є характерним також у післявоєнний період, зокрема: значним рівнем ризику у майбутньому характеризуються шахрайство з платежами (45,37 %) та фінансова активність, пов'язана з платежами від жертв до злочинців (44,42 %).

Таблиця 1

Фінансова активність кіберзлочинців

ВИДИ ФІНАНСОВОЇ АКТИВНОСТІ КІБЕРЗЛОЧИНЦІВ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
Шахрайство з платежами		67,10				45,37
Фінансова активність пов'язана з платежами між злочинцями		47,10				40,78
Фінансова активність пов'язана з платежами від жертв до злочинців		60,90				44,42
Відмиванням коштів		48,00				41,61
Фінансування тероризму		32,30				36,45

Серед фінансових інструментів, що використовують жертви шахрайства, найбільшим поширенням характеризуються традиційні – банківські перекази (66,0 %) та використання платіжних карток – 64,3 %), тренд високого рівня за якими, зберігається упродовж останніх років та характеризується найвищим рівнем ризику у післявоєнний період (*табл. 2*).

Водночас, високим рівнем використання також визначаються платежі від жертв злочинів, що здійснюються шляхом купівлі предметів та речей (50,9 %) та з використанням криптовалют (48,6 %). При цьому, значним поширенням характеризується шахрайське поповнення мобільного рахунку (43,7 %) та використання електронних грошей (42,6 %).

Таблиця 2

Рівень ризиків фінансової активності за платежами від жертв до злочинців

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
5.1.Банківські перекази		66,00				43,70
5.2.Платіжна картка		64,30				43,91
5.3.Шляхом поповнення мобільного рахунку		43,70				38,18
5.4.Шляхом покупки якогось предмету, речі		50,90				40,54
5.5.Системи оплати ваучерами (наприклад, paysafecard)		27,40				33,38
5.6.Використання електронних грошей		42,60				39,74
5.7.Використання криптовалюти		48,60				41,35

Співвідношення активності використання різних фінансових інструментів жертвами шахрайства, залишається сталим як упродовж останніх років, так і відповідно таким самим чином характеризується тренд у післявоєнний період.

Значною у кіберпросторі є фінансова активність, що пов'язана з платежами між злочинцями (47,1 %). Серед фінансових інструментів, що використовуються для здійснення платежів між злочинцями, найбільшим поширенням характеризуються – грошові мули (60,9 %), використання банківських карток (60,9 %) та банківські перекази (56,9 %). Водночас, упродовж останніх років тренд високого рівня зберігався більше за грошовими мулами та характеризується найвищим рівнем ризику у післявоєнний період (*табл.3*).

Таблиця 3

Рівень ризиків фінансової активності за платежами між злочинцями

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
4.1. Грошові мули (дропи)	-	60,9				45,62
4.2. Банківські перекази	-	56,9				42,14
4.3. Банківська картка	-	60,6				43,08
4.4. Системи оплати ваучерами (наприклад, paysafecard)	-	31,4				34,92

Багато кіберзалежних злочинів в певний момент породжують фіатну валюту з регульованим фінансовим сектором, незалежно від того, чи вона отримана із скомпрометованого банківського рахунка жертви чи з банкомату, зараженого шкідливим програмним забезпеченням. Доступ до цих коштів часто становить значно більший ризик, ніж дії, спрямовані на те, щоб перевести їх під контроль злочинців. Саме тут з'являється потреба в послугах третьої сторони – «грошових мулів».

«Грошові мули» – це найняті, або в деяких випадках введені в оману особи, які приймають або забирають кошти від імені злочинців. Наприклад, «грошові мули» можуть відкривати нові банківські рахунки або використовувати існуючі для

отримання коштів з рахунків, скомпрометованих банківськими троянськими програмами. Потім кошти перераховуються на інші рахунки, можливо, ті, що безпосередньо контролюються злочинцями, або забираються і передаються злочинцям в інший спосіб, наприклад, через бюро, що надають грошові послуги, за невелику частину коштів у вигляді оплати за такі послуги.

Для вербування нічого не підозрюючих «грошових мулів» використовуються різні шахрайські схеми. Більшість з них, принаймні спочатку, вважають, їх найняли на оплачувану роботу в легальній компанії. Інші «грошові мули» повністю усвідомлюють свою діяльність і є її співучасником. Таких «грошових мулів» часто можна знайти на кримінальних форумах. Вони пропонують свої послуги в обмін на частину прибутку. Професійні «грошові мули» часто є добре організованими і працюють в координованих групах.

Найчастіше «грошовими мулами» стають люди з невеликим доходом або які взагалі не мають регулярного доходу, наприклад студенти або безробітні і люди, які вперше приїхали до певної країни. У деяких європейських країнах існує значний фінансовий стимул займатися такою діяльністю.

Такій діяльності частково сприяє легкість відкриття нових рахунків, особливо в деяких європейських країнах, де є багато банків, що дозволяють клієнтам відкривати рахунок в режимі онлайн без потреби фізично відвідувати відділення або подавати документи, що посвідчують особу.

Тренд у майбутньому щодо традиційних банківських фінансових послуг хоча і є відносно меншим за рівнем ризику, у порівнянні з використанням грошових мулів, все ж у перспективі оцінюється експертним середовище на рівні вищому 40 % і зниження рівня ризику є лише відносним, у порівнянні з використанням грошових мулів.

Користін Олександр Євгенійович,
доктор юридичних наук, професор,
головний науковий співробітник
Державного науково-дослідного
інституту МВС України

РОЗВИТОК СТРАТЕГІЧНОЇ АНАЛІТИЧНОЇ КОМПОНЕНТИ В ДІЯЛЬНОСТІ ОРГАНІВ ПРАВОПОРЯДКУ

Давно стало очевидним, що правоохоронна практика, зокрема, протидія злочинності потребує оновлення, інновації, оптимізації за рахунок позитивних змін саме на рівні її аналітичного забезпечення. Водночас з появою сучасних інформаційних й телекомунікаційних технологій в умовах глобальної експансії злочинності, враховуючи характер, складність та обсяги кримінальних викликів, правоохоронні органи потребують принципової зміни методології та підходів, які визначають важливість використання методів аналітичної роботи не лише як інструменту збирання доказів, а також як ресурсу стратегічного менеджменту, прогнозування на основі оцінювання ризиків, підвищення спроможностей та виявлення вразливостей – упровадження повноцінних проактивних інструментів аналітичної розвідки.

Розвідувальна компонента аналітичної діяльності потребує постійного удосконалення аналітичної практики та обізнаності керівної ланки органів та підрозділів Національної поліції України щодо специфіки використання аналітичних матеріалів у процесі ухвалення управлінських та процесуальних рішень. Саме тому особливо важливим є зосередження уваги на концепціях та ключових процесах поліцейської діяльності у сфері інтелектуальної аналітичної роботи, а також кращого розуміння аналітиками й, особливо, керівниками правоохоронних підрозділів нової парадигми у сфері поліцейської діяльності.

Загалом сьогодні в тренді вітчизняних безпекових концепцій, стратегій та планів є ризик-орієнтований підхід, стратегічний аналіз, прогнозування тощо. Дійсно це виклики часу і сучасного підходу до організації діяльності органів правопорядку. Успіх інноваційного розвитку інформаційно-аналітичної діяльності сьогодні є результатом спільних зусиль. І це не лише сучасні аналітичні інструменти, технічне обладнання, хоча вони теж важливі.

Перш за все, це питання комплексне і в розвинених правоохоронних системах реалізується в межах відповідних моделей, на основі упровадження відповідної філософії та культури. Обравши шлях євроінтеграції, українські правоохоронні органи визначились із упровадженням самої сучасної моделі ILP. Комплекс питань, які необхідно вирішувати у зв'язку з цими процесами є багатоаспектним і непростим.

Проактивна поліцейська діяльність, закладена в поняття ILP, вимагає від аналітиків, політиків, керівників правоохоронних органів та інших осіб, що відповідають за прийняття рішень, нових навичок і компетенцій. Це також означає необхідність обізнаності осіб, що приймають рішення, про можливості проведення аналізу та про те, як використовувати його результати.

Намір передбачення конкретної загрози, зокрема, розглядається через визначення майбутніх поведінкових патернів (зразків, шаблонів, моделей, систем) для посилення на проактивному компоненті. Перехід до формату INTELLIGENCE був частково простимульований бажанням посилити проактивний підхід, який використовують для ефективного запобігання деструктивним явищам замість традиційного реагування на вчинені протиправні дії. Для того, щоб вжити власне запобіжні заходи, і потрібен проактивний підхід. Проактивність, натомість, вимагає наявності компонента передбачуваності, якщо характеризуємо загрозу. Якщо діяльність є унікальною за своєю природою, ми навряд чи матимемо можливість визначити певні майбутні події через те, що нам потрібна «історія», аналогічні інциденти, зв'язок між якими можливо простежити, встановивши певну залежність.

Незважаючи на можливість виникнення певних відхилень у короткостроковій перспективі, більшість тенденцій та проблем залишаються незмінними до моменту прийняття рішення про вжиття дієвих заходів. Значення патернів є особливо важливим, вони є «ядром» так званого першого закону INTELLIGENCE: *найбільш чітким індикатором потенційної злочинної діяльності є аналогічні дії, що вчиняються зараз*.

Особи, які проявили певні можливості та скористалися ними, будуть продовжувати доти, поки їх не зупинять, і таким чином можливим стане визначення патерну конкретної повторюваної діяльності. Стратегічний менеджмент патернів (обставини інцидентів та поведінкова специфіка) буде

оптимальним форматом, на відміну від індивідуальних розслідувань.

Суто з аналітичного погляду, ідентифікація патернів (обставини інцидентів та поведінкова специфіка) є першим кроком на шляху до запровадження проактивного підходу. Навіть дескриптивний (описовий) аналіз патернів щодо вчинених у минулому злочинів може бути використаний для прогнозування майбутньої динаміки. Також існує думка, що безперервність ланцюга подій, які характеризують досліджуваний патерн, може бути порушена лише вжиттям відповідних заходів.

Інша складова комбінованого процесу прогнозування в контексті INTELLIGENCE – вплив на тих, хто приймає рішення. Базовою у цьому випадку є аксіома аналітичної розвідки: аналітична розвідка, що не впливає на мислення того, хто приймає рішення, не є справжньою аналітичною розвідкою.

Водночас жодним чином не применшується цінність підтримки процесу розслідування, надання консультацій та іншої, не менш важливої роботи, яку виконують аналітики, але аналітична розвідка – це процес формування знань.

Загалом проактивна діяльність в правоохоронній сфері означає запобіжні дії, які здійснюються до того, як виникають проблеми або загрози. Це підхід, що фокусується на попередженні небезпек, а не на реагуванні на вже існуючі інциденти. Проактивні заходи можуть включати:

– аналіз ризиків: *оцінка потенційних загроз і вразливостей для визначення можливих джерел небезпеки*;

– моніторинг: *постійне спостереження за ситуацією для виявлення будь-яких підозрілих або потенційно небезпечних дій*;

– планування: *розробка та впровадження планів дій на випадок надзвичайних ситуацій, включаючи навчання співробітників і проведення тренувань*;

– профілактика: *вживання заходів для усунення або зниження ймовірності виникнення загроз, наприклад, встановлення систем безпеки, оновлення програмного забезпечення, посилення контролю доступу*;

– освіта та підготовка: *проведення навчальних програм для персоналу з метою підвищення їх обізнаності щодо безпеки та здатності ефективно реагувати на потенційні загрози*.

Проактивна діяльність допомагає мінімізувати ризики і забезпечити більш надійний захист від можливих небезпек.

Аналітика відіграє ключову роль у проактивній діяльності. Вона дозволяє ідентифікувати, оцінювати та прогнозувати потенційні загрози, а також розробляти ефективні стратегії для їх попередження. Розглядають наступні способи, як аналітика використовується у проактивній діяльності:

1. *Оцінка ризиків:* Аналітичні інструменти допомагають визначити слабкі місця в системах безпеки, оцінити ймовірність виникнення різних загроз і визначити їх можливі наслідки. Це дозволяє приймати обґрунтовані рішення щодо пріоритетних заходів безпеки.
2. *Моніторинг даних:* Системи аналітики збирають і аналізують великі обсяги даних у реальному часі для виявлення аномалій, підозрілих дій або потенційних загроз. Це дозволяє оперативно реагувати на можливі інциденти ще до їхнього виникнення.
3. *Прогнозування загроз:* Використовуючи історичні дані та сучасні алгоритми, аналітичні системи можуть прогнозувати майбутні загрози та тренди, що дозволяє розробляти превентивні заходи.
4. *Оптимізація ресурсів:* Аналітика допомагає ефективно розподіляти ресурси безпеки, визначаючи найбільш критичні області, які потребують уваги. Це забезпечує максимальну ефективність захисних заходів при обмежених ресурсах.
5. *Підтримка прийняття рішень:* Аналітичні дані надають обґрунтовану інформацію для прийняття стратегічних рішень щодо безпеки, включаючи вибір технологій, політик і процедур.
6. *Розробка політик та процедур:* На основі аналітики можна розробляти політики та процедури, що забезпечують ефективне попередження загроз і реагування на них.

Загалом, аналітика є невід’ємною складовою проактивної діяльності в сфері діяльності органів правопорядку та безпеки в цілому.

Крутік Юрій Вікторович,
кандидат наук з державного управління,
заступник начальника управління –
начальник першого відділу управління
інформаційно-аналітичного
забезпечення та кримінального аналізу
Департаменту оперативно-розшукової
діяльності Адміністрації Державної
прикордонної служби України

ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ КРИМІНАЛЬНОГО АНАЛІЗУ

Організована злочинність, поряд із війною, є однією з найсерйозніших загроз для безпеки та стабільності України. Ця форма злочинності має складну структуру, високий рівень конспірації та значні ресурси, що ускладнює її виявлення та розслідування. За таких обставин ефективна боротьба з нею можлива лише за умови використання сучасних методів, а саме кримінальний аналіз, який дозволяє систематизувати інформацію, виявляти закономірності та прогнозувати дії злочинців.

У різних країнах світу визначення кримінального аналізу дещо різниться, про те всі вони відображають глобальні стандарти та підходи до кримінального аналізу, які застосовуються. Зокрема, Міжнародна асоціація кримінальних аналітиків (IACA) визначає кримінальний аналіз як:

«Процес аналізу даних з метою виявлення закономірностей та тенденцій злочинної діяльності, який сприяє підтримці прийняття рішень у правоохоронній діяльності».

У США кримінальний аналіз також визначається як:

«Застосування аналітичних методів до даних про злочини з метою виявлення тенденцій, закономірностей і створення інформації, необхідної для прийняття рішень у правоохоронній діяльності».

Європейський Союз надає своє визначення кримінального аналізу:

«Кримінальний аналіз – це систематичний підхід до збирання, обробки та аналізу інформації, що використовується для розслідування та запобігання злочинів, а також для підтримки стратегічних та оперативних рішень у правоохоронних органах».

Основними завданнями кримінального аналізу є підтримка правоохоронних органів у розслідуванні злочинів,

прогнозуванні майбутніх злочинних подій та розробці стратегій для їх запобігання.

Ключовими елементами кримінального аналізу є:

1) систематичність: кримінальний аналіз є структурованим процесом, що вимагає послідовності та методичності у зборі та в обробці даних;

2) аналітичні методи: використання різноманітних аналітичних технік, а саме: статистичний аналіз, аналіз тенденцій, профілювання, картографування, аналіз великих даних (Big Data), OSINT та інше;

3) підтримка прийняття рішень: аналіз забезпечує інформацію, необхідну для прийняття обґрунтованих рішень у розслідуванні злочинів та запобіганні злочинності;

4) інформаційний обмін: обмін інформацією між правоохоронними органами є критично важливим для ефективної протидії злочинності та забезпечення безпеки громадян.

Саме теракти 11 вересня 2001 року в США є трагічним нагадуванням про важливість ефективного обміну інформацією між правоохоронними та розвідувальними органами. Краща координація і взаємодія могли б дозволити виявити підготовку до атак і запобігти їм. США зробили значні кроки для поліпшення цих процесів, що є важливим для інших країн в їхніх зусиллях щодо забезпечення національної безпеки.

Деякі з причин важливості цього обміну:

швидкість реакції: злочини часто перетинають межі регіонів або навіть країн. Обмін інформацією дозволяє правоохоронним органам реагувати швидко на злочинну діяльність, що сталася в іншому регіоні або країні;

підвищення ефективності розслідування: обмін інформацією дозволяє різним правоохоронним органам об’єднати свої зусилля та ресурси для ефективного розслідування злочинів. Він допомагає установлювати зв’язки між різними злочинами та злочинцями, що допомагає розкрити широкі мережі злочинності;

запобігання злочинам: обмін інформацією дозволяє правоохоронним органам отримувати інформацію про потенційні загрози та тенденції злочинності, що допомагає їм приймати запобіжні заходи для запобігання злочинам;

збільшення публічної довіри: ефективний обмін інформацією між правоохоронними органами сприяє підвищенню довіри громадськості до правоохоронної системи,

оскільки він демонструє їх здатність до співпраці та взаємодії в боротьбі зі злочинністю.

Прикладом ефективного обміну інформацією між правоохоронними органами є система «Fusion Centers» у США. Ці аналітичні центри є місцями, де представники різних правоохоронних агентств, включаючи ФБР, Департамент безпеки США, місцеву поліцію та інші, обмінюються інформацією про потенційні загрози безпеці. Це дозволяє підвищити швидкість реакції на загрози та спільно координувати дії для запобігання злочинам і терористичним актам.

Існують такі фактори, які сприяють досягненню найкращих результатів кримінального аналізу, а саме:

інтеграція з іншими джерелами інформації: кримінальний аналіз стає більш ефективним, коли він інтегрується з іншими джерелами інформації, а саме: дані зі служби 102, записи відеоспостереження, реєстри та документи відомств та інші джерела, що містять релевантну інформацію;

використання технологій: сучасні технології, а саме аналітика даних, штучний інтелект, машинне навчання, можуть значно підвищити швидкість і точність аналізу даних, допомагаючи виявляти патернів та зв'язки, які можуть залишитися непоміченими людським оком;

співпраця між аналітиками та оперативниками: ефективний обмін інформацією та співпраця між аналітиками, які відповідають за обробку даних, та оперативниками, які проводять розслідування на місці події, є ключовим для успішного виявлення злочинів;

постійне навчання та адаптація: злочинні схеми постійно змінюються, технології розвиваються, отже ефективність кримінального аналізу вимагає постійного навчання та адаптації до нових викликів і технологій;

етичність та дотримання законності: використання кримінального аналізу повинно ґрунтуватися на принципах етичності та дотриманні законності, щоб запобігти можливим порушенням прав людини та порядку.

Найкращі результати досягаються, коли ці фактори поєднуються, а аналіз використовується як частина широкої стратегії боротьби зі злочинністю.

З досвіду запровадження кримінального аналізу у Державній прикордонній службі України, який розпочався у 2008 році, можна стверджувати, що кожен правоохоронний

орган на шляху впровадження такої системи буде стикатися з такими проблемами та викликами:

Технічні проблеми. Застаріла матеріально-технічна база правоохоронних органів. Відсутність сучасного, як правило, коштовного програмного забезпечення та обладнання значно ускладнює проведення якісного аналізу даних.

Організаційні проблеми. Відсутність чіткої організаційної структури та координації між різними відомствами призводить до неефективного використання ресурсів та дублювання функцій. Крім того, бракує єдиної бази даних, що ускладнює обмін інформацією між правоохоронними органами.

Проблеми підготовки кадрів. Низький рівень підготовки аналітиків та відсутність систематичного навчання є серйозною перешкодою для ефективного проведення кримінального аналізу. Також, відсутність мотивації та належного матеріального заохочення призводить до низької продуктивності праці.

На теперішній час в Україні практично у кожному правоохоронному органі є підрозділ, подібний до підрозділу кримінального аналізу. Зусилля цих підрозділів потрібно об'єднати для подальшого швидкого розвитку системи кримінального аналізу в Україні. У зв'язку з цим доцільно рухатися у таких напрямках:

Технологічні інновації. Впровадження сучасного програмного забезпечення та обладнання є необхідним кроком для підвищення ефективності кримінального аналізу. Зокрема, використання систем штучного інтелекту та машинного навчання дозволить серед іншого:

автоматизувати процес обробки великих обсягів даних (Big Data), що надходять з різних джерел та виявляти складні закономірності та аномалії;

якісно та швидко прогнозувати злочинну діяльність, що забезпечить правоохоронним органам більш ефективно розподіляти свої ресурси та проводити профілактичні заходи;

автоматизувати багато рутинних завдань, а саме обробка звітів, перевірка даних у базах, аналіз відеозаписів тощо. Це звільняє час аналітиків для виконання більш складних завдань, що потребують людського втручання.

Організаційні зміни. Необхідність створення єдиної координаційної структури, яка забезпечуватиме ефективну взаємодію між різними правоохоронними відомствами. Це може бути досягнуто шляхом створення єдиної бази даних та розробки чітких регламентів і процедур для проведення

кримінального аналізу. Таке інтегроване рішення дозволить об'єднати всі доступні ресурси та дані в одному місці, забезпечуючи швидкий і безперебійний доступ до інформації для різних правоохоронних органів, та автоматизувати багато рутинних завдань, таких як збір та аналіз даних. Це значно підвищить ефективність роботи, знизить дублювання даних, покращить координацію дій між різними відомствами та знизить витрати на управління даними та інформаційними системами у довгостроковій перспективі. Прикладами розвинутих країн з інтегрованими системами, окрім США, є Сполучене Королівство Великої Британії та Північної Ірландії, Канада, Федеративна Республіка Німеччина, Австралія.

Підвищення кваліфікації кадрів. Важливо запровадити систематичне навчання та підвищення кваліфікації для аналітиків. Це може включати спеціалізовані тренінги, участь у міжнародних конференціях та обмін досвідом з колегами з інших країн. Також слід впровадити мотиваційні програми для підвищення продуктивності праці аналітиків. Інвестування у навчання та розвиток аналітиків є важливим елементом успішної діяльності правоохоронних органів.

Отже, якщо одночасно інвестувати у ресурси — знання, системи, джерела та людей, кримінальний аналіз стане найефективнішим елементом у боротьбі не лише з організованою злочинністю, а й загалом у системі правоохоронної діяльності. Це сприятиме підвищенню рівня безпеки та правопорядку в країні.

Список використаних джерел

1. Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України: навчальний посібник / Кірєєва О.С., Крутік Ю.В., Махлай О.М., Треус А.С. Хмельницький: НАДПСУ, 2022.

2. Exploring Crime Analysis: Readings on Essential Skills (3rd ed): paper book / International Association of Crime Analyst, Overland Park, Kansas, USA, 2017.

3. UNODC. Criminal Intelligence: Manual for Analyst (2011). Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

4. Taylor, B., & Boba, R. (2013). The Integration of Crime Analysis into Patrol Work: A Guidebook. U.S. Department of Justice, Office of Community Oriented Policing Services.

5. Крутік Ю.В., Головацький В.Г. Шляхи підвищення ефективності роботи підрозділів кримінального аналізу. Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України: тези міжвідомчої науково-практичної конференції, 11 серпня 2022 р. / Національна академія внутрішніх справ, 2022. С. 106–110.

6. Крутік Ю.В., Головацький В.Г. Перспективи розвитку системи кримінального аналізу в Україні. Освітньо-наукове забезпечення діяльності складових сектору безпеки й оборони України: тези XII Всеукраїнської науково-практичної конференції, 26 листопада 2020 р. / Національна академія Державної прикордонної служби України імені Б. Хмельницького, 2020. С. 299–303.

7. Кримінальний аналіз та інформаційно-аналітичне забезпечення, як елементи ILP моделі правоохоронної діяльності. Імплементація ILP моделі в Україні: матеріали круглого столу, 15 березня 2023 р. / Одеський державний університет внутрішніх справ, 2023. С. 22–26.

Лемешко Юрій Олександрович,
начальник управління кримінального аналізу Головного управління Національної поліції в Харківській області;
Серватовський Андрій Володимирович,
заступник начальника відділу аналітичної роботи управління кримінального аналізу Головного управління Національної поліції в Харківській області

ІДЕНТИФІКАЦІЯ ПІДРОЗДІЛІВ РФ ПІД ЧАС ОКУПАЦІЇ ХАРКІВСЬКОЇ ОБЛАСТІ

З початком повномасштабного вторгнення військами рф на територію України, частина територій Харківської області потрапила під окупацію. Військові злочинці армії рф, які перебували на українській землі вчиняли ряд злочинів, такі як: організації катівень, порушення звичаїв ведення війни.

Внаслідок чого постало питання як же взагалі довести присутність вказаних осіб на території України, ідентифікувати особистість, зібрати достатньо достовірної інформації, яка підтверджує її автентичність.

Можна виділити 2 методи ідентифікації військових рф:

1. З'єднання абонентів телекомунікацій, отримана в операторів мобільного зв'язку. (Використовуючи інформацію українських операторів, стало можливим виявляти мобільні пристрої, якими користувалися військовослужбовці рф (+7…, +8…) на окупованій території, їх місцезнаходження, контакти, локалізацію та зв'язки з колаборантами.)

2. Ідентифікація особи за фотозображенням. (однин із ключових методів ідентифікації, завдяки якому можна визначити часткові дані про особу на основі її профілів у соціальних мережах. У процесі ідентифікації також використовуються дані, отримані з месенджерів, таких як Telegram, Viber та WhatsApp, які зареєстровані на абонентські номери військових злочинців. Завдяки такій синергії різних джерел інформації, вдається ідентифікувати конкретних осіб, встановлювати їхні зв'язки, а також підтверджувати присутність на окупованій території.)

Починаючи з кінця шестидесятих років, розпізнавання облич стало однією з найбільш досліджуваних тем комп'ютерного зору та біометрії. Вказана технологія одна з найшвидше розвиваючих у сфері штучного інтелекту та комп'ютерного зору. З кожним роком все більше знаходиться застосування її можливостей в багатьох галузях, починаючи з систем безпеки до маркетингу та охорони здоров'я.

То що це таке та як же працює технологія розпізнавання облич?

Система розпізнавання обличчя – це технологія, яка здатна ідентифікувати особу на цифровому зображенні і порівняти риси обличчя заданого зображення з обличчями, які зберігаються в базі даних.

Система аналізує та ідентифікує особу по так званому «відбитку особи», або «вузлових точках», до якої відносяться відстані між очима, ширина носа, глибина очниці. Завдяки мережі камер відеоспостереження, механізми ідентифікації обробляють широкий перелік параметрів, включаючи вік, колір очей та волосся.

Сьогодні технологія розпізнавання облич використовується в більшості розвинених країн, допомагаючи підтримувати порядок в громадських місцях, підвищує рівень розкриття злочинів, полегшує пошук людей і дозволяє робити ще дуже багато всього іншого.

Перевагами застосування цієї технології є безпека (пошук злочинців, запобігання крадіжкам в магазинах, тощо), зручність, економія часу, простота використання.

Створення системи інтелектуального ідентифікування облич довело, що відбиток особи – це унікальний код, який є індивідуальним для кожної людини та може бути зчитано на відстані.

Для чого це потрібно?

В першу чергу для ідентифікації та затримання злочинців (на жаль, їх не стало менше, і вони чудово вміють ховатися). У деяких країнах технології ідентифікування облич застосовують для контролю порушень правил дорожнього руху. Наприклад, для притягнення до відповідальності пішоходів, які переходять вулицю в недозволеному місці або водіїв, які розмовляють телефоном під час руху.

Наразі існує кілька провідних систем і програм розпізнавання облич, які відрізняються високою точністю, швидкістю та різноманітними можливостями застосування:

1. Clearview AI
2. Face++ (Megvii)
3. Amazon Rekognition
4. Microsoft Azure Face API
5. NEC NeoFace
6. Face ID (Apple)
7. Cognitec Systems
8. AnyVision
9. Trueface
10. OpenFace

Вказані ресурси використовуються в різних сферах (для забезпечення безпеки, в наукових і дослідницьких проектах, для розблокування смартфонів і аутентифікації в додатках, для контролю доступу в урядових установах) але всі мають щонайменше 1 спільну рису: висока точність розпізнавання. Системи розпізнавання облич постійно вдосконалюються, стаючи більш точними, швидкими та інтегрованими з іншими технологіями.

То як же це працює і чим може стати нам у нагоді? На реальному прикладі покажемо вам, як система розпізнавання облич допомагає в зборі доказової бази та розкритті злочинів.

Після отримання фото через месенджери наступним кроком стало використання технології розпізнавання облич для ідентифікації осіб у соціальних мережах. За допомогою відкритих

джерел та програмного забезпечення (ClearView, Artellence, FaceChek, Search4face) вдалося автоматично порівняти отримані зображення з базами даних профілів у соцмережах, таких як «Вконтакте», «Однокласники» та «Facebook».

Використання технології розпізнавання облич допомогло встановити зв'язок між отриманими фото і сторінками в соціальних мережах, де були присутні анкетні дані: імена, дати народження, місця проживання та інша важлива інформація. Це дозволило більш точно ідентифікувати військових рф та зібрати докази їх діяльності на окупованих територіях.

Поєднавши отримані часткові дані з різних джерел, маємо змогу встановити повні анкетні дані особи, включаючи прізвище, ім'я, дату народження та місце проживання. Ця інформація отримана завдяки базам даних, доступним у мережі інтернет, що дозволило детально перевірити особу, зібрати додаткові відомості про її діяльність, зв'язки та можливу причетність до військових злочинів. Систематизація таких даних зробила процес ідентифікації більш ефективним і точним, що суттєво підвищило якість розслідувань.

Після деокупації виявлено значну кількість військової документації, залишеної підрозділами рф. Серед них журнали особового складу, книги хворих та інші документи, що містили важливу інформацію. Це дозволило ідентифікувати конкретні підрозділи, які перебували на Харківщині під час окупації, і простежити їх маршрути під час наступу. Отримані дані дали змогу встановити військових за інформацією, залишеною в документах, і провести порівняння з наявною базою, щоб визначити повні анкетні дані осіб, їх рід військ та інші деталі, які стали важливими для подальших розслідувань.

Після встановлення анкетних даних осіб важливим етапом стало порівняння отриманої інформації з документами, які стали доступні після деокупації. До таких документів належали захоплені військові журнали, списки особового складу, дані з пропускних пунктів та інші матеріали, що використовувались російськими підрозділами на окупованих територіях. Під час звірки підтверджувалися особисті дані військових рф, встановлювалися їх звання, підрозділи, маршрути пересування та місця розташування. Це допомогло ідентифікувати тих, хто був причетний до вчинення військових злочинів, організації катівень та порушення звичаїв ведення війни.

Отже як можемо простежити, система розпізнання облич допомогла поєднати інформацію, отриману з різних джерел, швидше та ефективніше ідентифікувати військових злочинців рф.

Технологія розпізнавання облич є потужним інструментом, який відкриває нові можливості в різних галузях. Збалансований підхід до розвитку технологій розпізнавання осіб, з урахуванням етичних стандартів і правової бази, дозволить створити безпечне й справедливе суспільство, де інновації слугуватимуть на благо кожного.

Список використаних джерел

1. Методичні рекомендації щодо організації та проведення кримінального аналізу підрозділами Національної поліції 132 України, затверджені Головою Національної поліції України Клименком Ігорем 11 травня 2021 року (вих. ДДЗ від 26 травня 2021 року № 6516/01/33-2021)
2. Face Detection and Recognition: Theory and Practice (Wiley, 2016) – S. Z. Li
3. FaceNet: A Unified Embedding for Face Recognition and Clustering. – F. Schroff, D. Kalenichenko, J. Philbin, 2015
4. Наукова праця «Дослідження методів розпізнавання облич при використанні мобільних технологій», Левенець Т. В., Кравець І. О., 2016
5. Алгоритм розпізнавання обличчя людей на базі згорткової нейронної мережі // Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління», Вип. 1 (32), 2018, Тимошин Ю. А., Орленко С. П.

Макарова Олена Павлівна,
кандидат психологічних наук, доцент,
доцент кафедри криміналістики
та судової експертології ННІ № 1
Харківського національного
університету внутрішніх справ

УДОСКОНАЛЕННЯ МЕТОДОЛОГІЇ КРИМІНАЛЬНОГО АНАЛІЗУ В КОМПЛЕКСНІЙ СУДОВО-ПСИХОЛОГО-ПСИХІАТРИЧНІЙ ЕКСПЕРТИЗІ

Вдосконалення методології кримінального аналізу в процесі проведення комплексної судово-психолого-психіатричної експертизи є важливим кроком для підвищення точності й ефективності судових розслідувань. Цей процес потребує врахування кількох ключових напрямків, серед яких:

удосконалення збору та обробки даних, інтеграція міждисциплінарних підходів, використання сучасних технологій та інструментів кримінального аналізу, міжнародний досвід і стандарти, підвищення кваліфікації експертів, аналіз поведінкових моделей та психічних станів.

Розглянемо їх більш детально. *Удосконалення збору та обробки даних*- створення ефективних механізмів збору даних про психічний стан обвинуваченого та його поведінкові особливості. Використання цифрових технологій, аналітичних платформ та баз даних дозволить знизити ризики втрати важливої інформації та покращити її точність. *Інтеграція міждисциплінарних підходів* – забезпечення тісної співпраці між криміналістами, психіатрами, психологами та іншими фахівцями, що беруть участь у комплексній експертизі. Об'єднання різних методів і підходів сприятиме більш комплексній і всебічній оцінці психічного стану обвинуваченого та його поведінки. *Використання сучасних технологій та інструментів кримінального аналізу*-сучасні інформаційні технології, такі як штучний інтелект та великі дані (Big Data), можуть допомогти виявляти складні закономірності у злочинній поведінці, а також оцінювати зв'язок між психічними розладами та протиправними діями. *Міжнародний досвід і стандарти* – запозичення кращих практик із країн Європейського Союзу та інших юрисдикцій, де існує розвинута практика кримінального аналізу та проведення судово-психіатричних експертиз, може сприяти вдосконаленню української методології. Це включає впровадження нових стандартів якості та навчання фахівців. *Підвищення кваліфікації експертів* – систематичне навчання та обмін досвідом між експертами з кримінального аналізу та судово-психіатричної експертизи є необхідним для забезпечення високого рівня професіоналізму й обізнаності про новітні методики. *Аналіз поведінкових моделей та психічних станів* – розвиток методик, що дозволяють глибше аналізувати поведінкові моделі осіб з психічними розладами, може допомогти в більш точному встановленні їх здатності до осмислених протиправних дій.

Загалом, шляхи вдосконалення методології кримінального аналізу в рамках судово-психолого-психіатричної експертизи включають впровадження новітніх технологій, інтеграцію міждисциплінарних підходів, розвиток міжнародної співпраці та підвищення кваліфікації фахівців. Це сприятиме більшій

точності експертиз, підвищенню рівня правосуддя та ефективності правоохоронної системи.

Аналіз кримінальних справ, що вимагають експертної оцінки психічного стану обвинуваченого, супроводжується низкою основних проблем: *Відсутність єдиних методичних стандартів.* Оцінка психічного стану обвинуваченого часто проводиться з використанням різних підходів та методів, що може призводити до неоднозначних висновків. Відсутність уніфікованих стандартів для судово-психіатричної та психологічної експертизи ускладнює порівняння результатів та їх застосування в судовому процесі. *Складність визначення психічного стану на момент вчинення злочину.* Однією з основних проблем є ретроспективна оцінка психічного стану обвинуваченого на момент вчинення злочину. Зміни у психічному стані між моментом вчинення правопорушення і часом проведення експертизи можуть ускладнити об'єктивний аналіз і вплинути на результати. *Недостатність інформації для аналізу*. У багатьох випадках експертам бракує повної або достовірної інформації про попередні психічні розлади обвинуваченого, медичні історії хвороби, умови життя чи інші важливі аспекти. Це може призвести до неповної оцінки його психічного стану та вплинути на точність експертного висновку. *Вплив суб'єктивного фактору.* Експертна оцінка психічного стану містить суб'єктивні елементи, оскільки кожен експерт може інтерпретувати ті самі симптоми або поведінкові прояви по-різному. Це може створювати суперечливі висновки щодо осудності або ступеня відповідальності обвинуваченого. *Зловживання з боку обвинувачених*. У деяких випадках обвинувачені можуть симулювати психічні розлади або маніпулювати своїм психічним станом, щоб уникнути відповідальності або отримати більш м'яке покарання. Виявлення симуляції потребує ретельного аналізу і додаткових спеціалізованих тестів, що не завжди проводиться належним чином. *Міждисциплінарні бар'єри.* Взаємодія між юристами, слідчими та судовими експертами часто ускладнена через відмінності в розумінні правових та медичних аспектів кримінальних справ. Це може призводити до неправильного формулювання питань до експертів або недооцінки важливих психіатричних факторів під час розслідування. *Незабезпеченість належними ресурсами.* Недостатність матеріальних і кадрових ресурсів для проведення повноцінної судово-психолого-психіатричної експертизи також є проблемою. У деяких випадках

експерти не мають доступу до сучасних інструментів або методик, що обмежує точність висновків. *Обмежена тривалість експертизи.* Час, відведений для проведення судово-психіатричної експертизи, часто є обмеженим, що не дозволяє здійснити ґрунтовний аналіз. Це може бути критичним, особливо у складних випадках, де психічний стан обвинуваченого потребує тривалого спостереження та комплексного підходу.

Розв'язання цих проблем вимагає вдосконалення методологічних підходів, тіснішої співпраці між експертами та правоохоронними органами, а також впровадження сучасних технологій і наукових досягнень у процес судових експертиз.

Кримінальний аналіз відіграє важливу роль в оптимізації процесу судово-психолого-психіатричної експертизи та виявленні причинно-наслідкових зв'язків між психічними розладами і протиправними діями. Його роль можна розглядати через кілька ключових аспектів: *Систематизація та структуроване представлення інформації.* Кримінальний аналіз дозволяє зібрати та систематизувати велику кількість різнорідної інформації, що надходить від різних джерел – слідчих органів, медичних установ, свідків та інших учасників справи. Це допомагає експертам отримати чітку та повну картину подій, пов'язаних зі злочином, а також краще розуміти психологічний і психічний стан обвинуваченого. Така структуризація даних прискорює процес проведення експертизи та підвищує її точність. *Виявлення закономірностей у поведінці обвинуваченого*. Кримінальний аналіз дозволяє досліджувати не лише конкретні факти, але й їх контекст та поведінкові моделі обвинуваченого, які могли вплинути на вчинення злочину. Аналіз минулих дій, соціального середовища, психологічних особливостей та взаємодії з іншими людьми дає можливість експертам оцінити, чи могли певні психічні розлади стати каталізатором протиправної поведінки. *Встановлення причинно-наслідкових зв'язків.* Один із найважливіших аспектів кримінального аналізу – це виявлення та підтвердження причинно-наслідкових зв'язків між психічними розладами та злочинами. Наприклад, чи вплинули симптоми психічного захворювання (галюцинації, манія, депресія тощо) на сприйняття обвинуваченим реальності та його здатність розуміти наслідки своїх дій. Кримінальний аналіз допомагає з'ясувати, наскільки значущим був вплив психічних розладів на злочинну поведінку, що важливо для визначення ступеня відповідальності обвинуваченого. *Оцінка мотивів та емоційних*

факторів. Кримінальний аналіз також сприяє глибшому розумінню мотивів злочину. Це може допомогти експертам встановити, чи мав обвинувачений злочинні наміри або його дії були результатом імпульсивного пориву, спричиненого психічними розладами. Розуміння мотиваційних факторів є ключовим при визначенні осудності особи та її здатності контролювати свої дії. *Допомога у створенні прогнозів щодо подальшої поведінки.* Кримінальний аналіз також може використовуватися для прогнозування майбутньої поведінки обвинуваченого, що важливо при визначенні заходів впливу або реабілітації. Якщо виявлено, що певний психічний розлад є суттєвим фактором ризику для повторення протиправної поведінки, це може бути враховано при виборі заходів безпеки або лікування. *Інтеграція сучасних методів та технологій* Сучасні технології кримінального аналізу, включаючи системи обробки даних можуть значно оптимізувати процес судово-психіатричної експертизи. Вони дозволяють автоматично виявляти патерни в поведінці, пов'язані з психічними розладами, що раніше могли залишатися непоміченими, тим самим підвищуючи точність висновків. *Підтримка правосуддя через більш обґрунтовані експертні висновки*

Кримінальний аналіз дозволяє зробити експертні висновки більш обґрунтованими та аргументованими. Це особливо важливо для судів, які повинні ухвалювати рішення на основі комплексної інформації, що включає психологічний та психіатричний стан обвинуваченого. Чітке розуміння зв'язку між психічними розладами та злочином дозволяє суддям приймати більш справедливі рішення.

Таким чином, кримінальний аналіз не тільки оптимізує процес судово-психолого-психіатричної експертизи, але й значно сприяє встановленню причинно-наслідкових зв'язків між психічними розладами та злочинами, забезпечуючи більш обґрунтовані судові рішення та підвищуючи ефективність правосуддя.

Підводячи підсумки можемо визначити, що у процесі проведення комплексної судово-психолого-психіатричної експертизи виникає низка важливих проблем, серед яких відсутність уніфікованих методичних стандартів, складність ретроспективної оцінки психічного стану обвинуваченого та нестача інформації для повноцінного аналізу. Крім того, кримінальний аналіз відіграє ключову роль в оптимізації експертного процесу, систематизуючи інформацію, виявляючи

поведінкові закономірності та встановлюючи причинно-наслідкові зв'язки між психічними розладами та протиправними діями. Для підвищення ефективності експертизи необхідно вдосконалювати методологію кримінального аналізу, впроваджувати сучасні технології та підвищувати кваліфікацію фахівців. Ці заходи сприятимуть більш точним і обґрунтованим експертним висновкам, що допоможе правосуддю ухвалювати справедливі рішення.

Список використаних джерел

1. Гусєва В. О. Сучасні можливості психологічних експертиз під час розслідування кримінальних правопорушень, вчинених проти працівників правоохоронних органів. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* 2021. № 3 (95). С. 256–267. https://doi.org/10.33766/2524-0323.95.256-267

2. Макарова О.П. Теоретико правові засади проведення судово психіатричної експертизиу кримінальному провадженні. Право і безпека .ХНУВС Науковий журнал No 3(90) 2023. 244 с. С. 190–200. https://doi.org/10.32631/pb.2023.3.16

3. Kryvoruchko, L., Pylyp, V., Makarova, O. (2023). Peculiarities of the activity Ukrainian law enforcement agencies of in ensuring the rights and freedoms citizens in the conditions of the legal regime martial laws. *Amazonia Investiga,* 12(64).

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

АКТУАЛЬНІ ПИТАННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КРИМІНАЛЬНОГО АНАЛІЗУ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

Розвиток кримінального аналізу в Україні є необхідним елементом боротьби зі зростаючою складністю злочинності, обумовленою соціально-політичними змінами та повномасштабною збройною агресією росії. Інтеграція інноваційних аналітичних технологій та методів дозволяє правоохоронним органам ефективніше аналізувати, прогнозувати та попереджувати злочини, що сприяє зміцненню громадської безпеки. Сьогодні кримінальний аналіз динамічно розвивається, відповідаючи на нові виклики через застосування передових аналітичних методів, які сприяють ефективнішому розслідуванню і

проактивному підходу в безпековій стратегії, інтегруючись у міжнародний аналітичний простір і підвищуючи ефективність роботи правоохоронців.

Серед основних напрямів подальшого розвитку кримінального аналізу, які потребують першочергової уваги, на нашу думку можна виділити наступні:

Впровадження моделі ILP (Intelligence-Led Policing)

Впровадження моделі Intelligence-Led Policing (ILP), або «правоохоронної діяльності, керованої аналітикою», є одним із ключових напрямів подальшого розвитку правоохоронної системи України. Intelligence Led Policing – це сучасна модель, яка передбачає інкорпорування аналітичної розвідувальної функції в загальну місію правоохоронної системи [1]. Модель ILP спрямована на забезпечення більш цілеспрямованого та проактивного підходу до протидії злочинності через зосередження уваги на зборі, обробці, аналізі та використанні інформації для прийняття рішень у правоохоронній сфері. Це впровадження є особливо актуальним в умовах нових безпекових викликів, зокрема пов'язаних збройною агресією росії та гібридними загрозами. Проактивний підхід в Intelligence-led policing не тільки дозволяє підвищити ефективність виявлення та протидії загрозам, але й сприяє формуванню більш гнучких та адаптивних систем державного управління [2]. Така діяльність серед іншого вимагає наявності висококваліфікованих працівників, які володіють необхідними навичками та знаннями [3].

Освіта та підвищення рівня професійної підготовки аналітиків

Знання, навички та досвід працівників, які здійснюють кримінальний аналіз, зокрема вміння володіти аналітичними інструментами та методами, розуміння проблеми, тенденцій і явищ у сфері, у якій проводяться дослідження є одним з найважливіших компонентів аналітичної діяльності [4]. Отже, підготовка кадрів для кримінального аналізу є одним з найважливіших аспектів його розвитку. В Україні активно розвиваються освітні програми для аналітиків. Зокрема, у Національній академії внутрішніх справ реалізуються програми підвищення кваліфікації, спеціалізації та тренінги, а також здійснюється поглиблене вивчення аналітичних інструментів у рамках навчальних програм для здобувачів вищої освіти. 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 [5].

Розширення використання інформаційно-аналітичних технологій

Інформаційно-аналітичні технології значно розширили можливості кримінального аналізу: програми для обробки, аналізу та візуалізації великих обсягів інформації, відео- аудіо- аналітика, геоінформаційні системи а також методи та інструменти OSINT [6] дозволяють швидко збирати й аналізувати дані, вчасно надавати інформацію для підготовки рішень у правоохоронній сфері. Сучасні підходи також включають використання технологій машинного навчання для вирішення аналітичних задач, що сприяє швидшому реагуванню на кримінальні загрози, якіснішому прогнозуванню, автоматизації рутинних задач та зниженню ризиків аналітичних помилок.

Міжнародне співробітництво

Активна співпраця з міжнародними партнерами, зокрема Консультативною місією Європейського Союзу, є важливою складовою розвитку кримінального аналізу в Україні. Тренінги, обмін досвідом, конференції та участь у міжнародних проєктах дозволяють впроваджувати найкращі практики у сфері кримінального аналізу в Україні.

Завдяки міжнародній співпраці, Україна інтегрується у світовий аналітичний простір, що підвищує рівень професійної підготовки та покращує координацію з іншими державами у боротьбі зі злочинністю.

Перспективи

Отже, кримінальний аналіз в Україні має значні перспективи розвитку. Першочергові завдання включають широке впровадження ILP, міжнародне співробітництво, підвищення ефективності аналітичних підрозділів через подальше впровадження нових технологій та методів, використання штучного інтелекту, якісну підготовку аналітиків та підвищення кваліфікації. Існує потреба у розвитку національних стандартів, що регулюють кримінальний аналіз та забезпечують єдиний підхід до аналітичної роботи у всіх правоохоронних органах.

Сьогодні кримінальний аналіз відіграє ключову роль у забезпеченні безпеки, орієнтуючись на попередження злочинів і підвищення ефективності реагування на загрози. Таким чином, розвиток кримінального аналізу в Україні є стратегічним

напрямком, який значно посилює здатність правоохоронних органів відповідати на нові виклики.

Список використаних джерел

1. Користін О.Є., Пефтієв Д.О., Пеньков С.В., Некрасов В.А. Довідник керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою / ILP : навчальний посібник. К: «Видавництво Людмила», 2019. 120 с.

2. Худенко Д.М. Публічні (відкриті) дані та проактивний підхід в ILP. Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VIII Міжнар. наук.-практ. конф. (м. Дніпро, 15 березня 2024 р.) ; у 2-х ч. Ч. І. Дніпро : ДДУВС, 2024. С. 423–425.

3. Овсянюк Д.І. Профіль професійної компетентності кримінального аналітика: концептуальні засади розроблення. Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України : 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. С. 78–82.

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

5. Бутко, Р.Ю. Розвиток системи кримінального аналізу в діяльності Національної поліції України в сучасних умовах Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України : 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. С. 19–25.

6. Денисенко, Б.А. Методологічні засади OSINT. Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України : 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. С. 44–48.

Овчаренко Едуарда Вікторівна,
головний інспектор відділу оперативної аналітики Департаменту кримінального аналізу Національної поліції України

ДОСЛІДЖЕННЯ ФІНАНСОВИХ ТРАНЗАКЦІЙ ТА ВИЯВЛЕННЯ РОСІЙСЬКИХ АКТИВІВ ФАХІВЦЯМИ ПІДРОЗДІЛІВ КРИМІНАЛЬНОГО АНАЛІЗУ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Аналіз фінансових транзакцій включає в себе порівняння, ретельний та поглиблений аналіз усієї наявної банківської інформації про фінансові транзакції та грошові потоки в цілях сприяння досудовому розслідуванню у кримінальних провадженнях, у яких внаслідок протиправної діяльності отримано незаконний дохід (актив).

Так, при аналізі фінансових транзакцій ключовими завданнями для аналітиків є:

– відстеження руху коштів на банківських рахунках суб'єкта;

– встановлення місцезнаходження, переміщення, використання коштів, одержаних внаслідок вчинення суспільно-небезпечного діяння;

– встановлення джерела незаконного походження коштів;

– встановлення взаємозв'язків між рахунками та особами, яким ці рахунки належать;

– виявлення злочинних доходів;

– встановлення методів приховання чи маскування незаконного походження коштів тощо.

Отже, щоб виявити ознаки злочинної діяльності в масиві даних банківських документів, необхідно провести детальний та послідовний аналіз отриманих первинних документів, при цьому важливо забезпечити систематичну підготовку та коректне оформлення даних, що дозволить ефективно обробляти великі масиви даних.

Етапи підготовки та опрацювання даних:

1. Оцінка наявних виписок:

1.1. Визначення структури наданих документів та їх форматів (наприклад, PDF, Excel).

1.2. Виявлення можливих розбіжностей у форматах для подальшої уніфікації.

2. Уніфікація форматів файлів:

2.2. Конвертація даних до єдиного формату (Excel) для полегшення аналізу.

2.3. Стандартизація структури інформації для всіх файлів (однакові назви та послідовність стовпців).

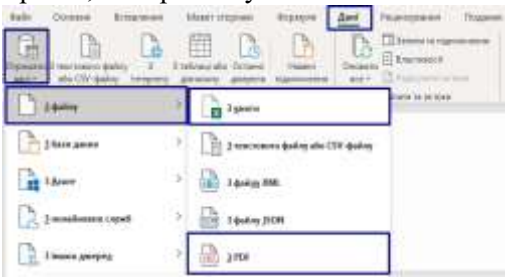
3. Виконання об’єднання всіх даних в один масив для подальшої обробки.

4. Використовуючи IBM i2 Analyst’s Notebook відобразити дані у вигляді timeline.

5. Візуалізація даних у вигляді схеми та в табличному форматі з використанням зведених таблиць.

Для створення одноманітної структури та перетворення всіх файлів у формат Excel та їх подальше об’єднання можна використовувати можливості Power Query та Microsoft Excel, а саме:

1. Завантажити наявні файли у Power Query. Якщо документи надані у PDF-форматі, використовуємо можливість імпорту PDF-файлів через Power Query. У випадку Excel-документів або CSV-файлів, додаємо їх безпосередньо або імпортуємо одночасно кілька файлів із папки для автоматичного об’єднання.

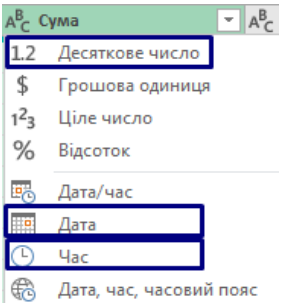


2. Використовуючи окремі функції програмного забезпечення Microsoft Excel, або ж мову формул M в Power Query необхідно провести очистку даних та їх систематизацію по конкретним стовбцям.

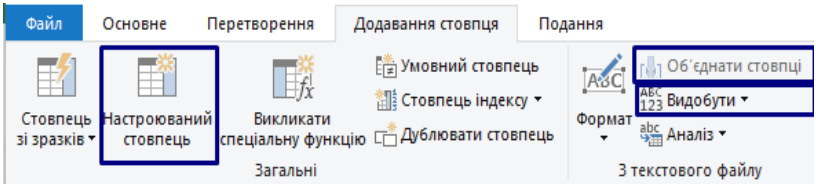
До прикладу налаштування форматів даних:

Стовбці із зазначенням сум транзакцій мають бути налаштовані у числовому форматі. Необхідно враховувати локалізацію даних – коми або крапки, як роздільники у числових значеннях.

Стовбці з датами та часом також мають бути налаштовані у відповідних форматах для їх подальшого використання.

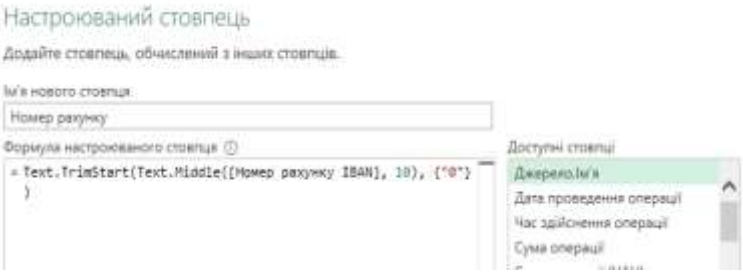


Об’єднання та розділення стовпців, додавання настоюваних стовпців дасть можливість створення більш структурованої таблиці з розподіленням по стовбцям отримувачів та відправників коштів, їх номери рахунків та призначень платежів.



За допомогою додавання настроюваного стовпця із зазначенням відповідної формули, за необхідності можна видобути номер рахунку з номера рахунку в форматі IBAN:

= Text.TrimStart(Text.Middle([Номер рахунку IBAN], 10), {"0"})

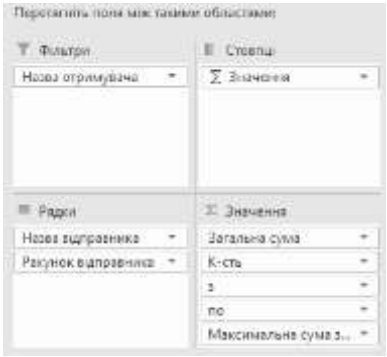


Для масової заміни тексту в стовпцях з зазначенням найменування відправників та отримувачів коштів, використовуючи наведений нижче код в Power Query можна провести очищення даних:

```
let
СписокЗамін = {
   {"ТОВАРИСТВО З ОБМЕЖЕНОЮ
ВІДПОВІДАЛЬНІСТЮ", " ТОВ "},
    {"ПРИВАТНЕ ПІДПРИЄМСТВО", "ПП"},
    {"Фізична особа - підприємець", " ФОП "}
        },
ЗаміненіДані = List.Accumulate(
    СписокЗамін,
```

```
        #"Попередній крок",
        (таблиця, пара) =>
          Table.ReplaceValue(
              таблиця,
              пара{0},
              пара{1},
              Replacer.ReplaceText,
              {"Найменування платника", "Найменування
отримувача"})
        )
    in
      ЗаміненіДані
```

Примітка Можливе внесення замін у даному коді використовуючи власний список та заповнюючи значення, яке необхідно знайти та значення на яке необхідно замінити знайдене у перших та других подвійних лапках відповідно.*



Після сформування вихідного масиву даних з чіткою структурою, створюється зведена таблиця (PivotTable) із відповідним налаштуванням, шляхом перетягування потрібних назв колонок (вихідної таблиці) до областей «Фільтри», «Стовпці», «Рядки», «Значення». Зведені таблиці забезпечують структурований підхід до аналізу великих обсягів даних.

При умові здійснення налаштування полів зведеної таблиці вищевказаним чином для відправників та отримувачів коштів отримаємо таблицю в якій буде підраховано загальну суму, кількість проведених транзакцій, періоди їх проведення та максимальна сума за одну транзакцію.

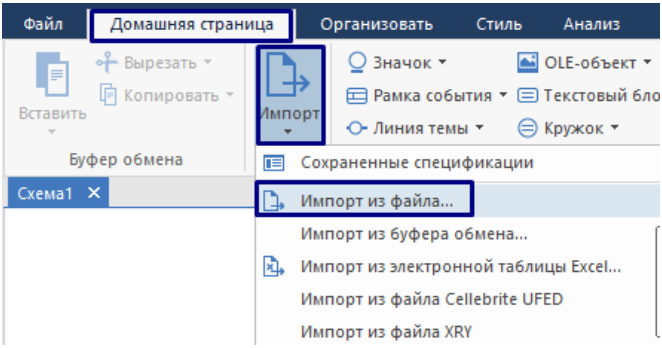
Використовуючи сортування таблиці по стовбцю «загальна сума» у зведеній таблиці відображаємо дані за спаданням, для чіткого розуміння отримувачів та відправників коштів які здійснили перерахування на найбільші суми.

Іншою частиною аналізу фінансових операцій є відображення даних у timeline:

1. Відкриваємо I2 Analyst`s Notebook вибираємо в меню «Імпорт», «Імпорт із файлу…».

2. Обираємо відповідний файл, який має бути збережений у форматі Книга Excel 97-2003 (*.xls).

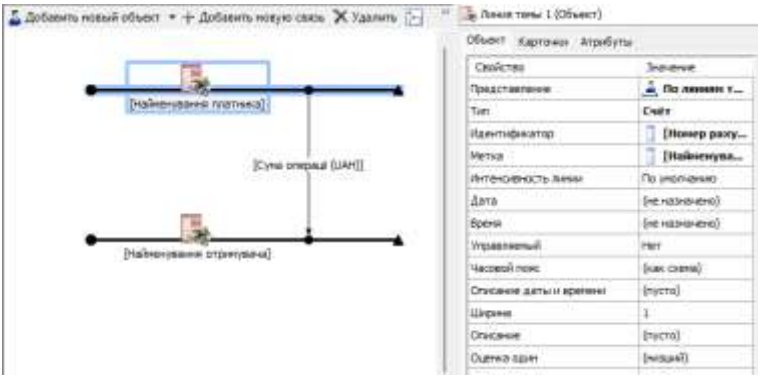
3. Вибираємо «Створити нову специфікацію» та натискаємо «ОК»



4. Здійснюємо основні налаштування, визначаємо заголовки таблиці та обираємо «Послідовність транзакцій»

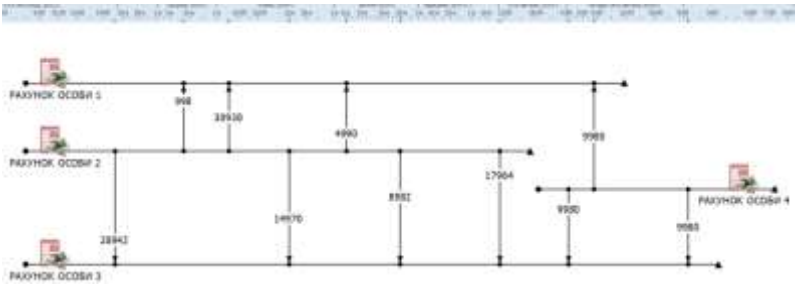
5. Отримаємо вікно формування схеми, в якій шляхом перетаскування відповідного стовпчика формується сама схема.

6. Натискаємо Імпорт.



В подальшому після проведення систематизації даних в I2 Analyst`s Notebook отримуємо схему із зазначенням сум

переказів коштів та їх відображенням у часі, що дозволяє виявити ключові взаємозв'язки між учасниками транзакцій.



Окушко Андрій Васильович,
кандидат юридичних наук, заступник начальника управління протидії кіберзлочинам в м. Києві Департаменту кіберполіції Національної поліції України;
Орлов Роман Русланович,
старший оперуповноважений управління протидії кіберзлочинам в м. Києві Департаменту кіберполіції Національної поліції України

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ. РОЗРОБЛЕННЯ МОДЕЛЕЙ ДЛЯ ПРОГНОЗУВАННЯ ЗЛОЧИНІВ І ДОПОМОГИ В ПРОФІЛЮВАННІ ЗЛОЧИНЦІВ

У сучасному кримінальному аналізі застосування штучного інтелекту (ШІ) стає дедалі більш актуальним, оскільки технології швидко розвиваються і пропонують нові можливості для підвищення ефективності розслідувань. Однією з ключових областей, де ШІ демонструє свої переваги, є прогнозування злочинів. Використання алгоритмів машинного навчання для аналізу великих обсягів даних з історії злочинності дозволяє виявляти патерни та закономірності, які можуть бути використані для запобігання злочинам. Наприклад, аналітики можуть використовувати дані про час, місце та типи злочинів, щоб створити моделі, які прогнозують, де і коли може статися новий злочин. Це дозволяє правоохоронним органам більш

ефективно розподіляти ресурси та проводити превентивні заходи

Дослідження показують, що завдяки використанню таких технологій можна суттєво знизити рівень злочинності в певних районах. Наприклад, у містах, де впроваджено системи прогнозування злочинів, спостерігається зменшення кількості правопорушень на 20–30 %. Однак, поряд із цими позитивними результатами виникають і певні виклики. Одним із найбільших ризиків є упередженість алгоритмів, які можуть відображати соціальні та економічні нерівності. Якщо дані, на яких базуються моделі, містять упередження, це може призвести до дискримінаційних практик у правоохоронній діяльності [1, с. 2].

Впровадження штучного інтелекту (ШІ) в кримінальний аналіз може стати ключовим чинником у підвищенні ефективності правоохоронних органів. Першим кроком є збір та аналіз великих обсягів даних, які можуть включати історичні дані про злочини, соціально-економічну інформацію, дані з соціальних медіа та навіть інформацію про події в реальному часі. Це дозволяє створити базу для навчання алгоритмів машинного навчання, які можуть виявляти патерни та кореляції, що допомагають у прогнозуванні злочинності. Наприклад, алгоритми можуть аналізувати, які фактори впливають на збільшення певних видів злочинів у певних районах, що дозволяє правоохоронним органам ефективніше планувати свої дії.

Наступним етапом є розробка моделей для профілювання злочинців. Використовуючи дані про попередні злочини, алгоритми можуть допомагати у визначенні психологічних та соціальних характеристик злочинців, що сприяє кращому розумінню мотивації та поведінки правопорушників. Це може бути особливо корисно в розслідуваннях, де важливо швидко отримати інформацію про можливих підозрюваних [2, с. 5].

Крім того, важливо інтегрувати системи ШІ у вже існуючі правоохоронні системи. Це може включати автоматизацію процесів, таких як обробка заяв про злочини або аналіз свідчень, що зменшує навантаження на персонал. Застосування технологій комп’ютерного зору для аналізу відео з камер спостереження також може суттєво підвищити оперативність розслідувань [3, с. 2].

Проте впровадження ШІ в кримінальний аналіз повинно супроводжуватися дотриманням етичних стандартів і забезпеченням прозорості алгоритмів, щоб уникнути упередженості та дискримінації. Це вимагатиме активної

співпраці між технологами, правоохоронними органами та громадськістю. В цілому, штучний інтелект має потенціал для значного покращення кримінального аналізу, створюючи більш безпечне і справедливе суспільство.

Отже, впровадження штучного інтелекту в кримінальний аналіз відкриває нові горизонти для правоохоронних органів, дозволяючи суттєво підвищити ефективність розслідувань і запобігання злочинності. Використання алгоритмів машинного навчання для аналізу великих обсягів даних, прогнозування злочинів та профілювання злочинців сприяє виявленню патернів, які можуть залишатися непоміченими традиційними методами. Це, в свою чергу, дозволяє правоохоронцям більш проактивно реагувати на потенційні загрози, оптимізуючи розподіл ресурсів та підвищуючи безпеку громад [4, с. 3].

Однак, разом із перевагами виникають і серйозні виклики, зокрема етичні питання, пов'язані з приватністю, упередженістю алгоритмів та можливими зловживаннями. Для забезпечення відповідального використання технологій важливо встановити чіткі етичні норми та регуляції, які гарантують прозорість і підзвітність систем ШІ. Співпраця між технологами, правоохоронними органами та громадськістю є ключовою для формування довіри до нових технологій і уникнення негативних наслідків [5, с. 2].

Таким чином, штучний інтелект має потенціал стати незамінним інструментом у боротьбі зі злочинністю, однак його використання повинно супроводжуватися уважним аналізом і розумінням етичних аспектів. Тільки так можна забезпечити баланс між безпекою суспільства і правами громадян, створюючи справедливу та безпечну правову систему.

Список використаних джерел

1. Сергій Гайда. ChatGPT: виклик чи нові можливості для університетської освіти (перші кроки кафедри ТМВД у використанні штучного інтелекту) URL: https://nltu.edu.ua/index.php/novyny/item/1568-chatgpt-vyklyk-chy-novimozhlyvosti-dlia-universytetskoi-osvity-pershi-kroky-kafedry-tmvd-u-vykorystannishtuchnoho-intelektu.

2. Штучний інтелект як технологія створення автоматизованих інтелектуальних систем. URL: https://er.knutd.edu.ua/bitstream/123456789/5044/1/20160428-29_TEZY_V3_P349.pdf.

3. Переваги та недоліки застосування штучного інтелекту у сферах управління. URL: http://elartu.tntu.edu.ua/

bitstream/lib/25207/2/MSNK_2018v2_Pelcher_M-Advantages_and_lack_of_application_72-73.pdf.

4. Штучний інтелект (AI): Що це таке і чому це важливо? URL: https://www.everest.ua/ai-platform/analytics/shtuchnij-intelekt-ai-shho-ce-take-i-chomu-ce-v/.

5. N. Wirth, (2018). Hello marketing, what can artificial intelligence help you with? International Journal of Market Research. 435-438. URL: https://doi.org/10.1177/1470785318776841.

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

МЕТОДИ ТА ПІДХОДИ ОПРАЦЮВАННЯ ТАБЛИЦЬ З'ЄДНАНЬ АБОНЕНТІВ ЗВ'ЯЗКУ ПІД ЧАС РОЗСЛІДУВАННЯ ТА РОЗКРИТТЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Значна кількість розслідувань пов'язана зі здійсненням тимчасового доступу до даних операторів рухомого (мобільного) зв'язку в частині історичних записів про з'єднання з іншими абонентами, фактів обміну повідомленнями, реєстрації мережі інтернет, використання переадресації дзвінків. В закордонних публікаціях також відомі як CDR (від англ. «*call data records*»). Відомості, отримані в результаті виїмки, можуть бути використані в процесі дослідження події правопорушення, підтверджуючи чи спростовуючи обставини, що підлягають доказуванню. Законодавець визначає загальний порядок здійснення доступу до таких даних, визначаючи їх як охоронювану законом таємницю – інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

Типовий зміст такої інформації складається з табличних записів, що містять відомості про дату та час події, тип з'єднання, цільового абонента та використаного пристрою, другого учасника розмови або використану IP-адресу, інформацію про використану станцію зв'язку.

Сукупність записів надає можливість здійснювати широке коло аналітичних звітів. Типовими задачами є підтвердження

фактів з'єднань, уточнення дати та часу подій, оцінювати переміщення та перебування абонента у періоди, що становлять інтерес для доказування, підтвердження використання певного пристрою.

Окремими напрямками можна виділити опрацювання цих даних з метою встановлення місцезнаходження розшукуваного або виявлення інших епізодів злочинної діяльності, інших співучасників правопорушення.

Методи та підходи до аналізу записів:

Найбільш поширеними є використання табличних процесорів для пошуку окремих записів відповідно критеріїв дати та часу або ідентифікаторів абонентів, що становлять інтерес; формування впорядкованих варіаційних вибірок для виявлення значень, що повторюються частіше (найближче коло спілкування, ділянки місцевості, які відвідуються частіше); виявлення перетинів множин (встановлення переліку спільних співрозмовників, спільного використання пристроїв зв'язку, тощо).

Структура отриманих даних може бути опрацьована з використанням інших статистичних методів, методів аналізу часових рядів або аналізу графів зв'язків. Розширені підходи можуть бути надлишковими для працівників, які безпосередньо залучені до розслідування, але доцільними для формування системних рішень. Також при створенні аналітичних систем чи програмного забезпечення можуть бути використані методи машинного навчання.

Пропонується розділити сценарії опрацювання записів про з'єднання на типові та похідні (розширені, комбіновані).

Типові аналітичні задачі:

Типові аналітичні задачі є інтуїтивно зрозумілими, популярними та покликані відповідати на питання, що перші виникають при дослідженні таких даних. За складність умовно можна виділити задачі:

– щодо одного абонента (перебування у місці злочину, підтвердження використання пристрою, підтвердження з'єднань, що відносяться до обставин вчинення правопорушення);

– порівняння двох абонентів (підтвердження попереднього знайомства співучасників, фактів зв'язків між собою, тривалості знайомства);

– дослідження зв'язків групи абонентів (побудова схем зв'язків, виявлення та оцінки зв'язків осіб, що поєднують співучасників або мають зв'язки з потерпілим).

Основними недоліками типових підходів є абсолютне сприйняття кількісних показників, не врахування особливостей поведінки для кожного з досліджуваних абонентів, обмежена здатність до розширення.

Похідні аналітичні задачі:

Похідні (або розширені) аналітичні задачі можуть полягати у комбінації методів, бути менш очевидними, але мають здатність до виділення закономірностей та фактів, що неможливо досягнути іншим способом або у розумний строк. Умовно можна виділити:

- прикладні статистичні зведення;
- геопросторовий аналіз;
- обернений аналіз співрозмовників;
- зважений аналіз зв'язків;
- застосування алгоритмів машинного навчання.

Здійснення *статистичних зведень* щодо календарних періодів, днів тижня та часу доби з подальшим застосуванням таких зведень до окремої вибірки записів (щодо абонента, станції зв'язку, окремого співрозмовника) дають смогу швидко оцінити характер таких зв'язків. Зв'язки в нічний час або у вихідні дні можуть вказувати на більш особистий характер, тоді як схильність до зв'язків в робочі години – навпаки. Календарні графіки дають змогу оцінити загальні закономірності, що можуть вказувати на зміни у звичній поведінці, повторюваності та періодичності. Певна складність у формуванні зведень виникає через різну «ціну» або «вагу» періодів доби та тижня, зокрема через очікувану різницю у активності вночі або у вихідні дні. Проблема зваженості може бути вирішена нормалізацією даних, що досліджуються, введенням маски ваг відповідно частот кожного з періодів, застосування методів ковзного вікна, тощо.

Зважаючи на загальну концепцію формування окремого запису, яка також полягає у фіксації розташування базової станції зв'язку, це відкриває окремий напрямок *геопросторового аналізу*. Встановлення відвідування абонентом місця вчинення злочину за весь період перевірки не може бути досягнуто класичними методами, оскільки потребує порівнянь всіх зафіксованих ділянок перебування з місцем злочину. Невизначеність дати орієнтовного відвідування створює значні обтяження у вигляді збільшення кількості записів, що потребують перевірки, а також знання місцевості щодо якої здійснюється перевірка. Окрему складність додає невизначеність

відстані обслуговування базових станцій розташованих в різних умовах (рельєфу, щільності покриття, навантаження мережі). Системно задачі геопросторового аналізу можуть бути вирішені застосуванням алгоритмів пошуку спільних сусідів (KNN), оптимізації порівнянь вибірок (апроксимація, використання дерев пошуку), використанням моделей передбачення відстані обслуговування (PathLoss алгоритм, обернено-пропорційна функція, інші методи, що використовуються при побудові мереж). Застосування вирівнювання вибірки та інтерполяції ділянки перебування абонентів дозволяє виявляти можливі зустрічі співучасників злочину, визначення ділянок та їх тривалості, при цьому забезпечивши повну автоматизацію.

Обернений аналіз співрозмовників полягає у здійсненні тимчасового доступу до записів, де абонент, що становить інтерес значився співрозмовником. Зворотня таблиця надає можливість застосувати вже існуючі методи для визначення осіб з кола оточення підозрюваного, які також перебували у ділянках, що становлять інтерес для розслідування. Такий підхід спрощує забір даних та не потребує здійснення запитів щодо всієї множини співрозмовників.

Однією з проблем релевантної візуалізації схем зв'язків або оцінки ступеню зв'язку двох абонентів є орієнтація на кількісні показники з'єднань. Переважно абоненти мають різні вподобання щодо способів зв'язку та різну активність. Використання *зваженої оцінки зв'язків* для кожного окремого абонента дозволяє правильно оцінити його роль у схемі зв'язків або надати більш наближену оцінку щодо ступеню зв'язку з іншим абонентом.

Іншим напрямком автоматизації є застосування алгоритмів *машинного навчання*. Зокрема, алгоритми класифікації (RF, LGBM, XGBoost) та алгоритми кластеризації (DBSCAN, HDBSCAN, HC, KNN, Radius-based KNN) дозволяють визначати групу базових станцій, що обслуговують ділянку з подальшим уточненням місцезнаходження через перекриття ділянок обслуговування; виявлення дійсного кола зв'язків шляхом відсіювання кластеру «дрібних» співрозмовників.

Перспективи розвитку напрямку аналітики з'єднань:

Зважаючи на зростаючу складність аналітичних задач, збільшення використання VoIP телефонії, що схиляє до більшої роботи в напрямку геопросторового аналізу, виникає потреба у створенні повторюваних алгоритмів, які забезпечать необхідний рівень абстракції кінцевого користувача (слідчого,

оперуповноваженого), без необхідності розуміння внутрішньої логіки.

Також значна кількість задач потребує впровадження підходів автоматизації у прийнятті рішень (визначенні переліку дійсного кола зв'язків, припущень щодо наявності зустрічей, формування груп базових станцій, що обслуговують окрему географічну ділянку). Це може бути забезпечено впровадженням комплексних моделей здатних до внесення змін, налаштувань та навчання на тренувальних вибірках.

Популяризація використання сучасних підходів може бути забезпечена наданням кінцевим користувачам ефективних та зрозумілих програмних додатків та проведенням достатньої просвітницької роботи щодо сценаріїв та орієнтовних результатів використання таких інструментів.

Системне впровадження запропонованих методів дозволить значно збільшити ефективність використання даних отриманих в результаті тимчасового доступу до відомостей операторів рухомого (мобільного) зв'язку, скоротити витрати часу аналітиків, здобути додаткові відомості, що сприятимуть розслідуванню.

Паламарчук Іван Васильович,
кандидат юридичних наук, головний спеціаліст Департаменту правового забезпечення Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів (АРМА)

ПЕРЕДУМОВИ ПІДГОТОВКИ АНАЛІТИКІВ ДЛЯ ВИКОНАННЯ ЗАВДАНЬ З ВИЯВЛЕННЯ ТА РОЗШУКУ АКТИВІВ

Невід'ємною складовою державного механізму формування та реалізації як внутрішньої так і зовнішньої політики держави є складові загального механізму держави, зокрема, якими є органи державної влади та їх службові і посадові особи.

Відомо, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1].

Тому догматичним є той факт, що інтерес держави, який спрямований на забезпечення економічного добробуту України –

є превалюючим. Превалювання такого інтересу є цілком логічним, у зв'язку з тим, що таким чином забезпечується фінансування різних інтересів держави від функціонування яких залежать, у тому числі і рівень забезпечення в Україні прав людини (інтереси держави в обороні, безпеці і т.д.).

Встановлено, що публічні службовці, зокрема, представляючи державу діють виключно в її інтересах, у зв'язку з чим сумлінно, компетентно, вчасно, результативно і відповідально виконують службові повноваження та професійні обов'язки [2].

Також, слід зазначити, що неефективний розподіл видатків на оборону України є одним із основних ризиків у сфері воєнної безпеки [3].

Доречно також зазначити, що успіх реалізації Стратегії воєнної безпеки України залежить, зокрема, від:

єдності, патріотизму та готовності держави і суспільства до захисту, зокрема, демократичного ладу, незалежності, суверенітету та територіальної цілісності України;

рівня довіри українського суспільства до органів, зокрема, виконавчої влади в Україні, дієвої протидії корупції, політичної та правової культури в суспільстві, розвитку, зокрема, доброчесного суспільства, об'єднаного як повагою до сил оборони, так і повагою до закону;

достатності економічного розвитку держави для нарощування можливостей оборонної промисловості щодо розроблення, виробництва і постачання силам оборони новітнього озброєння, військової та спеціальної техніки [3].

Отже, задля реалізації визначених державою завдань, серед центральних органів виконавчої влади, що реалізовують та формують різні види державних політик, які є невід'ємними складовими внутрішньої та зовнішньої політики України, функціонує Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів (АРМА).

АРМА в установленому законом порядку здійснює виявлення активів (діяльність із встановлення факту існування активів, на які може бути накладено арешт у кримінальному провадженні, чи у справі про визнання необґрунтованими активів та їх стягнення в дохід держави) та їх розшук (діяльність із визначення місцезнаходження активів, на які може бути накладено арешт у кримінальному провадженні, чи у справі про

визнання необґрунтованими активів та їх стягнення в дохід держави) [4].

Тим паче, змістом Комплексного плану [5] впровадження такого процесуального учасника, кримінального провадження, який по суті в межах визначених повноважень забезпечував би виконання завдань цифрового забезпечення кримінального провадження, є «цифровий детектив», що на теперішній час та із урахуванням прогнозування подальшого розвитку таких правовідносин по суті є доцільним, послідовним та необхідним в таких реаліях. При цьому, виконання подібних функцій за своїми можливостями та набутою практикою можуть здійснювати відповідні структурні підрозділи АРМА (з питань виявлення та розшуку активів).

Варто зазначити, що АРМА інтенсивно впроваджує цифрові технології у сфері виявлення та розшуку активів, постійно взаємодіє в цьому напрямі з усіма правоохоронними органами, а також з компетентними структурами за кордоном. В АРМА створено ІТ-лабораторію, діяльність якої спрямована саме на аналіз даних з будь-яких цифрових носіїв інформації [6].

Продовжуючи слід зазначити, що кінцевим результатом діяльності АРМА з питань реалізації державної політики віднесеної до сфери його повноважень є подальше здійснення управління такими активами (які було виявлено та розшукано і на які було в установленому законом порядку накладено арешт та передано в управління АРМА) на умовах ефективності, а також збереження (за можливості – збільшення) їх економічної вартості [4].

Також, доречно зазначити, що якість виконання поставлених перед АРМА державою завдань, які виражаються в реалізації, зокрема, інтересу держави у вигляді забезпечення економічного добробуту України – залежав, залежить та буде залежати від виконання працівниками АРМА зазначених законом [2] вимог при реалізації своїх повноважень.

При цьому наслідком виконання АРМА своїх повноважень є «результативність», яка може виражатися й в економічному ефекті від діяльності АРМА – відношення отриманого результату до касових видатків із Державного бюджету України на діяльність АРМА.

Результативність подальшого виконання АРМА своїх повноважень в інтересах держави також залежить від відповідального підходу до формування та забезпечення

передумов для реалізації державної політики, що відноситься до сфери повноважень АРМА.

Тому, таким підходом (як одним із основних) є формування у майбутнього покоління, зокрема, здобувачів відповідного рівня та ступеня освіти:

навичок конструктивної міжособистісної та суспільної взаємодії, яка ґрунтується на взаємоповазі, обміну досвідом і співпраці;

впровадження принципів солідарності та турботи про спільне благополуччя, яке у тому числі забезпечується прищепленням набутих (при реалізації державної політики у сфері виявлення, розшуку та управління активами одержаними від корупційних та інших злочинів) результативних для суспільства та держави знань і навичок для забезпечення ідеї безперебійного правонаступництва держави з реалізації політики в зазначеній сфері.

Таким чином, з метою забезпечення передумов для подальшої реалізації державної політики, що відноситься до сфери повноважень АРМА, та забезпечення збереження набутих знань та практичних навичок з реалізації зазначеної державної політики та на їх основі забезпечити примноження та збільшення результатів майбутніми поколіннями (в ідеях реалізації справи всього Українського народу) нагально необхідним є передача та поширення таких знань та навичок серед здобувачів вищої освіти у галузях знань дотичних до державної політики, що реалізується АРМА. Як приклад, під час участі в наукових заходах, що проводяться на базі закладів вищої освіти; налагодженням взаємодії із закладами вищої освіти, із відповідним укладенням угод про співробітництво та партнерство на досягнення зазначеної ідеї, і т.п.

Доречно зазначити, що задля подальшого забезпечення ідеї безперервності реалізації державної політики, яка відноситься до сфери повноважень АРМА доцільним є здійснення фундаментального налагодження взаємодії з різними освітніми платформами, що по суті може забезпечити підготовку та профорієнтацію майбутніх наступників нинішніх працівників АРМА, на досягнення зазначеної ідеї.

З огляду на викладене, підготовка аналітиків для забезпечення виконання завдань з питань виявлення та розшуку активів, що здійснюється АРМА, має починатися із створення передумов для забезпечення безперервності реалізації державної політики, віднесеної до сфери повноважень АРМА, зокрема,

висвітленими способами, що є шляхом до сформування в суспільстві превентивної аксіоми «все предикатне майно – буде повернуто державі та суспільству» – в ідеях реалізації справи всього Українського народу!

Список використаних джерел

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР : станом на 17 жовт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

2. Про запобігання корупції : Закон України від 14.10.2014 № 1700-VII : станом на 17 жовт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text.

3. Стратегія воєнної безпеки України «ВОЄННА БЕЗПЕКА – ВСЕОХОПЛЮЮЧА ОБОРОНА» : Указ Президента України від 25.03.2021 № 121/2021 : станом на 17 жовт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text.

4. Про Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів : Закон України від 10.11.2015 р. № 772-VIII : станом на 17 жовт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/772-19#Text.

5. Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки : Указ Президента України від 11.05.2023 р. № 273/2023 : станом на 17 жовт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/273/2023#Text.

6. АРМА сприяє реалізації проєкту «Цифровий детектив». URL: https://arma.gov.ua/news/typical/arma-spriyae-realizatsii-proektu-tsifroviy-detektiv.

Панченко Євгеній Вікторович,
начальник 4-го управління (оперативно-аналітичного забезпечення та аналізу відкритих джерел) Департаменту кіберполіції Національної поліції України

КРИПТОВАЛЮТИ Й ЕЛЕКТРОННІ ГРОШІ ЯК ІНСТРУМЕНТИ ФІНАНСОВОЇ АКТИВНОСТІ КІБЕРЗЛОЧИНЦІВ

Експертним середовищем кіберполіції було оцінено окремі загрози, що характеризують фінансову активність кіберзлочинців.

Використовуючи криптовалюти у якості платежів від жертв злочинів, найбільша активність стосується: Bitcoin (53,7 %), USDT (46,9 %) та Ethereum (40,6 %) (*табл. 1*).

Таблиця 1

Рівень ризиків платежів від жертв до злочинців за видами криптовалют

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ: криптовалюта	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
7.1.Bitcoin		53,70				40,05
7.2.Ethereum		40,60				37,44
7.3.Ripple		26,00				32,63
7.4.Monero		28,00				33,38
7.5.BNB		29,40				32,09
7.6.USDT		46,90				38,12
7.7.USDC		32,00				33,50
7.8.Zcash		23,40				31,76
7.9.Dash		25,10				31,89
7.10.Litecoin		30,60				32,59

Bitcoin найпопулярніша валюта для здійснення розрахунків між злочинцями, наприклад, під час придбання або оренди інструментів або послуг для вчинення кіберзлочинів у цифровому підпіллі. Це єдина валюта, яку приймають в більшості магазинів у Darknet та автоматизованих магазинів карток, і валюта, яку вимагають як викуп у майже у всіх сьогоднішніх атаках з використанням програм-вимагачів або DoS-атаках.

Незважаючи на те, що використання Bitcoin у злочинних цілях залишається ключовим фактором, що сприяє злочинній поведінці в мережі Інтернет, у цифровому підпіллі зростає активність інших криптовалют.

Monero – з'явилася у 2014 році. Більша частина зростаючої популярності Monero пов'язана з додатковими функціями безпеки та конфіденційності, які вона пропонує; транзакції не можуть бути віднесені до конкретного користувача/адреси, всі монети, що використовуються в транзакції, «приховані» за замовчуванням, а історії транзакцій є приватними. Monero зараз приймають у низці ринків в Darknet, а в 2017 році з'явилася перша програма вимагач – Kirk, в якій викуп потрібно було сплатити у криптовалюті Monero.

Ethereum – «smart-контракти» Ethereum можуть стати інструментом для бізнес-моделі «злочин як послуга». Поки що цього не сталося, але принаймні певні ринки в Darknet приймають Ethereum для здійснення платежів і покупок.

Zcash – це ще одна криптовалюта, яка забезпечує підвищений рівень конфіденційності для своїх користувачів, приховуючи як одержувача транзакції, так і суму транзакції.

Інші види криптовалют також використовуються для здійснення платежів від жертв злочинів до злочинців, але відносно зазначених вище видів цей рівень є дещо нижчим (23,4 %–29,4 %).

Упродовж останніх років тренд за видами криптовалют, що використовуються для здійснення платежів від жертв злочинів до злочинців, залишається без особливих змін.

У післявоєнний період залишається переважно без змін співвідношення щодо використання найбільш поширених видів криптовалют для здійснення платежів від жертв злочинів до злочинців, а найвищий рівень ризику передбачається щодо Bitcoin (40,05 %), USDT (38,12 %) та Ethereum (37,44 %).

При використанні електронних грошей, у якості платежів від жертв злочинів до злочинців, найчастіше використовуються системи: EasyPay (47,1 %), PayPal (42,0 %), а також Webmoney (35,4 %) та Qiwi (32,6 %) (*табл. 2*).

У післявоєнний період залишається переважно без змін співвідношення щодо використання найбільш поширених систем електронних грошей для здійснення платежів від жертв злочинів до злочинців, а найвищий рівень ризику передбачається щодо: EasyPay (37,88 %), PayPal (35,73 %), Webmoney (34,27 %).

Таблиця 2

Платежі від жертв до злочинців за видами електронних грошей

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ: електронні гроші	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
6.1.Webmoney		35,40				34,27
6.2.PerfectMoney		28,60				33,46
6.3.ЮMoney		25,40				32,06
6.4.Qiwi		32,60				33,34
6.5.PayPal		42,00				35,73
6.6.Advanced Cash		26,60				32,47
6.7.Payeer		27,70				33,16
6.8.Skrill		26,30				32,44
6.9.EasyPay		47,10				37,88

Інші системи електронних грошей також використовуються для платежів від жертв злочинів до злочинців, але відносно зазначених вище систем цей рівень є дещо нижчим (25,4 %–28,6 %).

Використовуючи криптовалюти у якості платежів між злочинцями найбільш поширеними також є Bitcoin (54,9 %), USDT (45,4 %) та Ethereum (43,4 %) (*табл. 3*). Інші види криптовалют також використовуються для платежів між злочинцями, але відносно зазначених вище видів цей рівень є дещо нижчим (27,7 %–34,6 %).

Таблиця 3

Рівень ризиків платежів між злочинцями за видами криптовалют

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ: криптовалюти	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
4.14. Bitcoin		54,90				41,35
4.15. Ethereum		43,40				38,12
4.16. Ripple		29,70				33,52
4.17. Monero		30,90				34,59
4.18. BNB		33,40				33,26
4.19. USDT		45,40				39,14
4.20. USDC		34,60				34,86
4.21. Zcash		28,00				32,72
4.22. Dash		27,70				32,62
4.23. Litecoin		32,00				33,46

Такий же тренд за видами криптовалют, що використовуються для здійснення платежів між злочинцями, зберігався упродовж останніх років. Більше того, відзначається певне збільшення масштабів використання Bitcoin, USDT та Ethereum навіть у період воєнного стану.

Рівень ризиків у післявоєнний період характеризується збереженням співвідношення між активністю використання різних видів криптовалют та підвищенням у платежах між злочинцями USDC (33,5 %) та Monero (33,38 %).

При використанні електронних грошей, у якості платежів між злочинцями, найчастіше використовуються системи: EasyPay (46,6 %), PayPal (42,6 %), а також Webmoney (34,0 %), Qiwi (32,0 %) та PerfectMoney (31,4 %) (*табл. 4*). Інші системи електронних грошей також використовуються для платежів між злочинцями, але відносно зазначених вище систем цей рівень є дещо нижчим (26,3 %–30,3 %).

Такий же тренд за видами систем електронних грошей, що використовуються для здійснення платежів між злочинцями, з перевагою EasyPay та PayPal, зберігався упродовж останніх років.

Таблиця 4

Рівень ризиків платежів між злочинцями за видами електронних грошей

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ: електронні гроші	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
4.5. Webmoney	-	34,00				35,14
4.6. PerfectMoney	-	31,40				34,32
4.7. ЮMoney	-	28,90				33,08
4.8. Qiwi	-	32,00				34,81
4.9. PayPal	-	42,60				36,99
4.10. Advanced Cash	-	26,30				33,05
4.11. Payeer	-	30,30				33,62
4.12. Skrill	-	26,60				32,33
4.13. EasyPay	-	46,60				37,94

Водночас у післявоєнний період щодо використання окремих найбільш поширених систем електронних грошей для здійснення платежів між злочинцями, експертним середовищем передбачається зниження рівня ризику їх використання, у

порівнянні з іншими системами, хоча все ще відносно більшим рівнем ризику: EasyPay (37,94 %), PayPal (36,99 %).

Таким чином, криптовалюти активно використовуються в злочинних схемах. Найчастіше використовуються Bitcoin (53,7 %), USDT (46,9 %), Ethereum (40,6 %), а також інші види криптовалют, що займають значну частку (23,4 %–29,4 %). У післявоєнний період очікується зниження ризику для Bitcoin, USDT, Ethereum, але підвищення ризику для інших криптовалют.

Електронні гроші є значним компонентом у платежах від жертв злочинів, особливо такі системи, як EasyPay (47,1 %) і PayPal (42,0 %). Зазначається прогноз зниження рівня ризику для найпоширеніших систем електронних грошей у майбутньому, але підвищення для інших систем.

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

КЛЮЧОВІ НАПРЯМИ РОЗВИТКУ ТАКТИЧНОГО КРИМІНАЛЬНОГО АНАЛІЗУ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У 2024 РОЦІ

Департамент в своїй діяльності на постійній основі займається збором та аналізом інформації про кримінальну ситуацію, з метою забезпечення ефективного контролю та протидії злочинності.

Метод дослідження конкретної події обставин чи сукупності факторів, які призвели до кримінальної події або можуть сприяти її розвитку – називається ситуаційний аналіз.

Основні завдання ситуаційного аналізу:

– визначення контексту події: дослідження зовнішніх обставин, що могли сприяти злочину (наприклад, соціально-економічні, політичні, культурні умови);

– виявлення мотивів і причин: аналіз факторів, які призвели до злочинного діяння, включаючи психологічні, соціальні та економічні передумови;

– ідентифікація залучених осіб і груп: вивчення профілю осіб, які брали участь у події, включаючи їхню історію, можливі зв’язки, роль і мотиви;

– оцінка ризиків та наслідків: прогнозування потенційних негативних наслідків або ескалації ситуації, а також ризиків повторення подібних подій;

– аналіз середовища та локації: вивчення географічних і соціальних характеристик місцевості, де сталася подія, для розуміння, як це могло вплинути на скоєння злочину.

Ситуаційний аналіз дозволяє не тільки дослідити факти, але й глибоко вникнути у соціальні, психологічні та культурні аспекти подій, що є важливими для побудови комплексної системи протидії злочинності.

Ситуаційний і тактичний аналізи в кримінальному аналізі тісно взаємопов'язані, оскільки обидва спрямовані на розуміння конкретних подій, однак кожен з них підходить до аналізу з різних кутів та рівнів деталізації.

Тактичний аналіз – це процес збору, обробки та інтерпретації інформації для ухвалення оперативних рішень у короткостроковій перспективі. Він зосереджується на дослідженні конкретних ситуацій, подій або умов, які можуть безпосередньо вплинути на поточні цілі та завдання. Основною метою тактичного аналізу є швидке реагування на зміни у зовнішньому та внутрішньому середовищі для досягнення конкретних результатів або забезпечення конкурентної переваги.

На вибір цілей дослідження впливає поточний стан Держави, яка перебуває в стані повномасштабного вторгнення та супутні з цим станом ризики, які змінюють сфери, в яких злочинці виявляють «запит» суспільства та окремих громадян, що мають переважно економічне та соціальне підґрунтя.

В умовах цифрової трансформації все більше інформації збирається з різних джерел: від соціальних мереж до інтернет-платформ і камер спостереження.

Також слід урахувати прогнозування в реальному часі. Завдяки новітнім технологіям аналітики можуть спостерігати за подіями, які відбуваються просто зараз, і робити прогнози. Це надзвичайно важливо для управління ризиками та для швидкої реакції на будь-які зміни.

Сучасний світ сповнений непередбачуваних загроз, таких як терористичні акти, кіберзлочинність або раптове зростання певних видів злочинів. Тактичний аналіз дозволяє оперативно оцінювати ситуацію, аналізувати ризики та координувати дії різних підрозділів у реальному часі.

Умови сьогодення вимагають від поліції максимальної уваги до потреб громадян. Знання про місцеві проблеми, їх

глибокий аналіз і можливість впливу на криміногенну ситуацію на місцевому рівні забезпечують громадянам більший рівень безпеки та спокою.

Попри значні переваги, тактичний аналіз стикається з викликами – від забезпечення конфіденційності особистих даних до постійного оновлення аналітичних інструментів. Тим не менш, впровадження сучасних методів у цей процес дозволяє національній поліції адаптуватися до нових реалій та забезпечувати безпеку громадян у швидкозмінному світі.

Актуальність тактичного аналізу не можна переоцінити. Оперативний аналіз ситуації підвищує точність і швидкість прийняття рішень, дає змогу краще адаптуватися до змінних умов.

Слід звернути увагу на проблемні питання, з якими можна зіштовхнутись. Перш за все, це обробка величезних обсягів даних. Завдяки доступу до значних масивів даних поліція може швидко аналізувати великі обсяги інформації, що надходить з різних джерел. Це дозволяє аналізувати закономірності та підвищувати ефективність запобіжних заходів.

Аналіз великих даних (Big Data) при складанні тактичного аналізу має важливе значення для підвищення його якості та точності.

Взагалі аналіз великих масивів даних в правоохоронній сфері має сфери застосування:

– прогнозування злочинності: Big Data допомагає аналізувати злочини на основі місця, часу, та інших факторів, створюючи прогнози для запобігання злочинам;

– виявлення патернів: дозволяє розкривати закономірності та зв’язки між подіями, особами та локаціями;

– слідкування за соціальними мережами та комунікацією: аналіз даних з соцмереж допомагає відстежувати підозрілу активність та взаємозв’язки між групами чи окремими особами;

– реагування в режимі реального часу: системи аналізу великих даних, інтегровані з міськими камерами спостереження, GPS трекерами;

– ідентифікація ризиків та злочинців: штучний інтелект допомагає в аналізі великих за обсягом даних, для визначення осіб, які потенційно можуть вчинити злочини.

Виклики, які виникають при обробці великих масивів даних:

– конфіденційність даних та етичні питання;

– великі обсяги даних вимагають значних ресурсів для їх обробки;

– захист від кібератак для забезпечення цілісності даних;

Для обробки великих даних (Big Data) зазвичай використовуються спеціалізовані інструменти, які дозволяють зберігати, аналізувати та візуалізувати великі обсяги інформації. Ось кілька ключових інструментів:

Apache Hadoop: комплекс програмних рішень для зберігання та обробки великих даних у розподіленому середовищі.

Apache Spark: Потужна платформа для обробки даних у реальному часі з підтримкою машинного навчання, що забезпечує швидший аналіз у порівнянні з Hadoop.

NoSQL бази даних:

MongoDB: Документо-орієнтована база для неструктурованих даних.

Cassandra: База даних для великих розподілених систем із високою доступністю.

Elasticsearch: Інструмент для пошуку та аналізу великих обсягів даних у реальному часі. Часто використовується разом із Kibana (плагін з відкритим кодом для візуалізації даних).

Apache Kafka: Платформа для обробки потокових даних у режимі реального часу, яка дозволяє швидку передачу великих обсягів даних між системами.

Power BI: Інструмент для інтерактивної візуалізації даних, який допомагає створювати наочні графіки та звіти, роблячи аналіз зручнішим.

Ці інструменти дозволяють комплексно обробляти, аналізувати та візуалізувати великі масиви інформації, що є важливим для досліджень.

Однак в поліції наразі активно використовується Power BI, через інтуїтивно зрозумілий інтерфейс та простоту в використанні.

Отже повертаючись до проведення тактичного аналізу - якість аналітики та прогнози прямо залежать від того, наскільки правильно й уважно були оброблені вихідні дані. Якщо з самого початку інформація була відфільтрована неправильно або некоректно інтерпретована, на виході можна отримати помилкові висновки, що можуть призвести до неефективних або навіть шкідливих рішень. Тому кожен етап обробки має бути ретельно продуманим, а результати – перевіреними на точність.

Зрештою, результат залежить від того, як ретельно були виконані всі етапи. Якісно оброблені великі обсяги даних не лише покращують аналітику, але й дозволяють поліції швидше

реагувати, краще планувати ресурси та навіть передбачати події, що значно покращує безпеку та захищеність громадян [1, с. 25].

Слід зазначити, шо масив інформації про кожен факт кримінального правопорушення проти громадян України є дуже масштабним і потребує застосування великого об'єму ресурсів.

Отже, підвищення ефективності тактичного аналізу через впровадження сучасних технологій, інтеграцію аналітичних методів і поліпшення процесів прийняття рішень має вирішальне значення для безпеки суспільства [2, с. 60]. У світі, де загрози стають дедалі більш різноманітними та складними, тактичний аналіз виступає як один із ключових інструментів для забезпечення громадського порядку та безпеки.

Також слід звернути увагу на підготовку фахівців у сфері аналітики. Сучасні аналітики повинні володіти не лише знаннями з класичних методів дослідження, але й бути ознайомленими з новими технологіями, такими як обробка даних, програмування та статистичний аналіз. Інвестиції в освітні програми, тренінги та семінари можуть забезпечити високий рівень кваліфікації кадрів, що, в свою чергу, підвищить якість аналітичних досліджень.

Список використаних джерел

1. Барандич В.І. Важливість використання тактичного кримінального аналізу в діяльності аналітичних підрозділів Національної поліції України. Збірники наукових праць, матеріали конференцій (семінарів, круглих столів). М. Київ, Національна академія внутрішніх справ, 2022. 26 с. URL: http://elar.naiau.kiev.ua/jspui/handle/123456789/24787/

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

Сивун Андрій Сергійович,
начальник 2-го відділу (відеоаналітичних досліджень) 1-го управління (аналітичного) Департаменту кримінального аналізу Національної поліції України

ІНТЕГРАЦІЯ ПРОГРАМНИХ РІШЕНЬ ДЛЯ ВІДЕОАНАЛІТИКИ: ВІДЕОЗВІТИ ЯК СУЧАСНИЙ ІНСТРУМЕНТ АНАЛІТИКИ

В сучасному світі, де технології швидко розвиваються, розслідування злочинів стає все більш складним завданням для правоохоронних органів. Для ефективного виявлення, документування та розслідування злочинів необхідно використовувати інформаційно-аналітичне забезпечення, яке включає в себе різноманітні методи та підходи.

З розвитком технологій штучного інтелекту та розширення можливостей спеціалізованого програмного забезпечення аналітики отримали змогу виділити окремий, але не новий напрям роботи – відеоаналітичні дослідження (відеоаналітика).

Виокремлення нового напряму досліджень зумовлено стрімким розвитком комплексних систем відеопостереження, які вже побудовані та є невід'ємною складовою роботи підрозділів Національної поліції України.

Дані системи відіграють важливу роль у забезпеченні громадського порядку, плануванні заходів, а також розкритті злочинів. Найбільш ефективними та результативними є комплексні системи відеоспостереження камери яких включають у себе можливості аналітики – розпізнавання облич, предметів, номерних знаків транспортних засобів тощо.

Наразі, в Україні встановлено та функціонує **понад 64 тис.** камер відеоспостереження у **більш ніж 700** відомих нам окремих системах, з яких **більше 41 тис.** камер під'єднані до системам «Безпечне місто/Регіон», **понад 7 тис.** відомчих камер та **більше 18 тис.** камер інших суб'єктів господарювання (в т. ч. приватні). Якщо розглядати інформацію відносно камер відеоспостереження, які мають аналітичний функціонал, то це **більше 7 тис.** камер з функцією розпізнавання номерних знаків транспортних засобів та **1,5 тис**. камер з можливістю розпізнавання облич.

На сьогодні, кожен підрозділ кримінального аналізу у регіоні має безпосередній доступ до даних з камер відеоспостереження, але окрім перегляду звичайного відеоматеріалу або фіксацій, аналітик проводить також великий обсяг роботи для забезпечення ефективного результату.

Окремо, для опрацювання надвеликих масивів відеоматеріалів різних форматів Департаментом кримінального аналізу отримано доступ та забезпечується постійна розбудова технічної спроможності програмного продукту **BriefCam Investigator for Teams** з модулем **REVIEW SCC**.

Програмний продукт **BriefCam** дозволяє проводити аналітику по камерам відеоспостереження в яких вона відсутня або приватних камер відеоспостереження доступ до яких забезпечується відповідними підрозділами досудового розслідування та передається для аналізу. Завдяки цьому, програмний продукт продемонстрував свою ефективність в роботі не тільки по загальним злочинам, але й в новому напрямку – розслідування воєнних злочинів.

У Департаменті кримінального аналізу забезпечено місця попереднього сховища відеоматеріалів наданих для аналізу із загальним об’ємом у **640 ТВ** (з урахуванням RAID) та здійснено модернізацію старого обладнання призначеного для обробки (індексування) відеоматеріалів, що збільшило можливість для збереження індексованих матеріалів з **49 ТВ до 547 ТВ** (з урахуванням RAID) – тепер це дозволяє використовувати потенціал програмного забезпечення на повну потужність.

Наразі, у Департаменті кримінального аналізу тривають відповідні заходи щодо побудови **комплексної системи захисту інформації** програмного продукту «BriefCam», що сприятиме подальшому створенню відповідних положень та інструкцій щодо залучення аналітика як спеціаліста для аналізу відеоматеріалів у кримінальному провадженні.

Окрім цього напряму, відслідковується позитивна тенденція розвитку систем зберігання даних у регіональних підрозділах кримінального аналізу, на даний момент відомо про **понад 1 000 ТВ** загального об’єму наявних та налаштованих зовнішніх мережевих сховищ по всій території України.

Роль аналітика в аналізі камер відеоспостереження для розкриття злочинів є критично важливою, оскільки він сприяє збору та інтерпретації інформації, яка в майбутньому може слугувати в якості доказів, які можуть бути вирішальними для

встановлення фактів злочину та встановленню правопорушників. Основні аспекти роботи аналітика в цьому контексті включають:

Аналіз маршрутів пересування – аналітик може відслідковувати переміщення підозрюваних осіб або транспортних засобів, використовуючи кілька камер спостереження, що дозволяє визначити маршрут втечі, місце знаходження підозрюваних або місця, пов'язані зі злочином.

Сучасні системи також мають власні, додаткові, аналітичні здібності, які розроблені та встановлені у програмне забезпечення. Це надає змогу системі автоматично побудувати маршрут руху, проаналізувати дані з різних камер фіксації за певний проміжок часу порівнявши з іншими камерами без застосування додаткових маніпуляцій з експортом, встановити так звані «Hot Spot» перебування транспортного засобу та інші функції.

Даний функціонал хоч і полегшує роботу, але не заміняє роботу аналітика, адже злочинці використовують номерні знаки, які належать іншим транспортним засобам або взагалі не числяться за жодним із зареєстрованих транспортних засобів, тому потрібно проводити аналіз місць появи та зникнення автомобіля, його стоянок та місця ночівлі. Із появою новітніх камер з покращеною якістю аналітик із застосуванням спеціалізованих програмних продуктів може тепер встановлювати осіб пасажирів по фіксації транспортного засобу.

Розпізнання підозрілих осіб і подій – аналітик ретельно переглядає записи з камер відеоспостереження для виявлення підозрілої поведінки осіб, транспортних засобів, та інших об'єктів пов'язаних зі злочином. Він може використовувати програмні засоби для аналізу великого масиву відеоданих, або такі, що можуть здійснювати корекцію відеоматеріалу. Сучасні алгоритми програмного забезпечення дозволяють аналізувати та структурувати величезні обсяги відеоданих, що значно прискорює пошук релевантної інформації під час довготривалих розслідувань.

Програми для розпізнавання облич дозволяють встановлювати підозрюваних, свідків або жертв на відеозаписах з камер відеоспостереження або мобільних пристроїв (у тому числі боді-камер поліцейських). Сучасні алгоритми здатні порівнювати обличчя з фотографіями у соціальних мережах, де аналітик може проводити додатковий аналіз для встановлення як самої особи, так і найближчого кола родичів, друзів, колег по роботі або злочинних зв'язків.

Деякі програмні продукти дозволяють встановлювати та порівнювати осіб навіть при не якісній зйомці, здійснивши кадрування певного відеоматеріалу із застосуванням як звичайного програмного забезпечення типу Adobe, так і спеціалізованого із методами корекції – AmpedFive.

Слід зазначити, що наразі аналітики використовують не тільки закордонні програмні продукти, такі як **Clearview AI**, **Briefcam** чи **ProHawk**, а й розробки українських фахівців, такі як **BigDataPeople** від **Artellence**, систему **Face-check** та **інтеграційну платформу відеоспостереження та відеоаналітики** Національної поліції України, які розроблено фахівцями Департаменту інформаційно-аналітичної підтримки.

Також, слід відокремити інформацію отриману у ході OSINT, яка також поєднується та оцінюється в залежності від вихідних даних або даних, які аналітик знаходить у ході свого аналітичного дослідження.

Зниження рівня хибних спрацьовувань – системи відеоаналітики можуть генерувати велику кількість хибних спрацьовувань. Аналітик відіграє роль у фільтрації даних, відкидаючи нерелевантні або неправильні сигнали, щоб зосередитись на ключових моментах, які стосуються злочину.

У ході відпрацювання злочинів по «гарячих слідах» аналітик може аналізувати надвеликі масиви інформації з камер відеоспостереження та надавати ключову інформацію, яка пришвидшить пошук особи причетної до скоєння.

Так, у співпраці з оперативними підрозділами, які опрацьовують приватні камери відеоспостереження аналітичним підрозділам можуть надавати інформацію з місця події, наприклад, що автомобіль, класу седан, сірого кольору здійснював заїзд у двір у певний проміжок часу. Аналітик, за наявності камер відеоспостереження може провести швидкий аналіз та встановити транспортний засіб, здійснити його попередній аналіз (для спростування або підтвердження), встановити маршрут та останні фіксації, встановити власника або особу користувача, та надати дані для подальшого відпрацювання оперативним підрозділам, які продовжують роботу на місцях.

Відновлення хронології подій (відеозвіти) – один із ключових етапів розслідування злочину, адже це створення точного часового ланцюга подій. Аналітик допомагає відновити події у правильній послідовності, аналізуючи записи з різних камер та отриманої від оперативних підрозділів інформації, щоб скласти цілісну картину того, що відбулося.

Відеозвіти у розслідуванні – це детально підготовлені звіти, які включають аналіз і поєднання матеріалів, засновані на попередньому вивченні відеоматеріалів, отриманих з камер спостереження, мобільних пристроїв (у тому числі боді-камер поліцейських) або інших джерел. Вони використовуються для демонстрації послідовності дій (бездіяльності) суб'єктів або подій, які відбулись у певний проміжок часу.

Раніше більшість інформації, отриманої у ході розслідування, збиралась у певні схеми, які збирались та склеювались на столах або стінах для встановлення повної картини, а вже з початком розвитку технологій схеми почали створювати в електронному вигляді як у звичайному MS Power Point, так і в спеціалізованих IBM i2 із можливістю імпорту інформації.

Схеми і на сьогодні залишаються актуальними під час проведення розслідувань, адже вони допомагають підрозділам досудового розслідування розуміти повну картину для прийняття правильних процесуальних рішень. Тому їх роль у правоохоронній системі не зникає та залишатиметься ще довгий проміжок часу.

Однак, статистика демонструє нам тенденцію того, що з кожним роком попит саме на складені відеоматеріали як у хронології, так і за результатами досліджень зростає.

Для прикладу, щоб орієнтуватись на схемі зазвичай потрібно бути присутнім під час її складання, або попросити особу, яка орієнтується швидко ввести в суть схеми та справи (при цьому, зазвичай, не все можна вмістити у схемі). Самостійне вивчення схеми може зайняти багато часу, а також, можна не звернути увагу на ключові деталі. Відеозвіт може вирішити більшу частину даних проблем.

Правильно відтворена хронологія матеріалів, викладена у відео, може надати розуміння повної картини тижнів розслідування, адже для складання відеозвіту попередньо може бути написаний відповідний «сценарій», який охопить всі необхідні матеріали як для оперативних працівників та слідства, так і для керівництва.

Дані матеріали надають розуміння не тільки повноти картини, а й при правильній підготовці не потребують у коментуванні та пояснені іншими особами.

Структура та вимоги до відеозвітів залишаються майже тими самими, що і до звичайних аналітичних документів:

1. Повинна бути побудована **чітка структура звіту**, яка складається зі вступу, викладенні матеріалу, висновків, за

наявності рекомендації (у випадку хронології – вступ та основні події).

2. **Логічність та послідовність** – кожен етап аналізу має логічно витікати з попереднього. Будь-яка гіпотеза чи твердження повинні бути підкріплені фактами або аргументами.

3. **Об'єктивність та неупередженість** – аналіз має бути об'єктивним, базуватися на фактах і неупереджених оцінках. Особисті думки або суб'єктивні припущення повинні бути чітко відокремлені від фактичного аналізу та не зазначатись у ньому.

4. **Законність** – матеріали для аналізу отримані у законний спосіб.

5. **Точність** – не потрібно використовувати не перевірену або вигадану інформацію.

6. **Мова та стилізація мови** – мова повинна бути нейтральною, за необхідності із використанням юридичної термінології. Без складних термінів для сприйняття яких треба звертатись до додаткового пошуку.

7. **Фокусування** – не потрібно охоплювати всю відому інформацію, потрібно зосередитись на ключових питаннях.

8. **Джерело** – за необхідності, можемо зазначати джерело інформації на фрагментах викладених у звіті.

9. **Редагування та коректура** – інформація повинна бути ретельно перевірена та оговорена із замовником матеріалу на відповідність змісту та охоплення всіх моментів.

Синиціна Юлія Петрівна,
кандидат технічних наук, доцент,
доцент кафедри інформаційних
технологій Дніпровського державного
університету внутрішніх справ

ВИКОРИСТАННЯ КРИМІНАЛІСТИЧНИХ ОБЛІКІВ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ ВЛАСНОСТІ

Використання різних видів криміналістичних обліків при розслідуванні кримінальних правопорушень залежить від завдань та етапів розслідування, а також слідчої ситуації, що склалася на певний момент. У зв'язку з різноманітність криміналістичних обліків та їх функціональним призначенням у слідчих (дізнавачів) виникають питання щодо використання інформації, що міститься в них у конкретній слідчій ситуації. Криміналістикою не можливо передбачити кожну слідчу ситуацію та дії слідчого щодо її

вирішення, але розробка рекомендацій щодо можливостей використання криміналістичних обліків у типових ситуаціях розслідування є перспективним напрямком підвищення результативності слідчої діяльності.

Під типовою слідчою ситуацією розуміють абстраговану штучна модель, що відображає стан наявної у слідчого інформації про обставини злочину й обставини, що склалися на відповідному етапі розслідування [1]. Інформація, що міститься у криміналістичних обліках використовується, в основному, на початковому етапі розслідування. У залежності від слідчої ситуації, використовується сукупність інформаційних даних, що містяться у базах даних як інформаційно-довідкового призначення, так і оперативно-розшукових обліках.

Розглянемо типові слідчі ситуації розслідування злочинів проти власності та можливість використання інформаційних баз даних для їх вирішення. У типовій слідчий ситуації, що є найбільш несприятливою для розслідування, а саме: є ознаки злочину (залишені матеріальні сліди, зникло майно), відсутні свідки та очевидці, особа злочинця невідома. Для вирішення основного завдання розслідування – встановлення особи злочинця у такій ситуації використовуються криміналістичні обліки залежно від виду слідів, виявлених на місці події. При виявленні слідів рук, вони перевіряються за дактилоскопічним обліком, а саме автоматизованою інформаційно-пошуковою системою «Дакто 2000». Якщо особа була раніше засуджена або затримана та її дактилокарта є у базі даних перевірка слідів, вилучених на місці події, дає позитивні результати. В залежності від вилучених при огляді місця події слідів, у цій ситуації, поряд з дактилоскопічним використовуються обліки слідів взуття, знарядь зламу та інструментів, транспортних засобів та ін. Всі означені сліди вносяться до інформаційної підсистеми «СЛІД» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» (далі – ІПНП) та перевіряються за даними цієї системи. Облік у зазначеній системі ведеться за такими категоріями: фотозображення слідів рук; фотозображення слідів підошов взуття; фотозображення слідів знарядь зламу; фотозображення слідів структури матеріалу (рукавичок); фотозображення слідів протекторів шин транспортних засобів; мультимедійна інформація (фото-, відео-, звукозапис) щодо осіб, які причетні до вчинення кримінального правопорушення; мультимедійна інформація (фото-, відеозапис) обстановки події, що сталася;

інформація про кулі, гільзи і патрони зі слідами зброї; інформація про об'єкти біологічного походження; інформація про інші вилучені матеріальні об'єкти, які були знаряддям вчинення кримінального правопорушення та зберегли на собі його сліди або містять інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [2].

При розслідуванні злочинів проти власності перевірка здійснюється майже по всіх зазначених категоріях. На наш погляд, недостатньо уваги приділяється слідам біологічного походження, особливо при розслідуванні крадіжок та майнових злочинів, не пов'язаних із застосуванням насилля. Це пов'язано з значною вартістю проведення молекулярно-генетичних досліджень для виділення із слідів біологічного походження профіля ДНК та його внесення в базу даних.

Крім цього, в даній ситуації за даними інформаційних підсистем ІПНП «Особа» та «Оперативно-довідкова картотека» перевіряються всі особи, які проживають у районі вчинення кримінального правопорушення та були раніше засуджені за вчинення злочинів проти власності. Серед них особливу увагу приділяють тим з них, які нещодавно повернулись з місць позбавлення волі та не мають постійного заробітку. Також перевіряються за обліками викрадені речі, особливо якщо серед них є номерні речі або культурні цінності, що підлягають реєстрації в окремій інформаційній підсистемі.

Типова слідча ситуація, у якій присутні ознаки кримінального правопорушення, є свідки (очевидці), які запам'ятали правопорушника та можуть його описати та впізнати, або є його відеозображення, зафіксоване відеокамерою спостереження. У цьому випадку зі слів свідків-очевидців потрібно скласти суб'єктивний портрет підозрюваного за допомогою автоматизованого програмного комплексу «Фоторобот». Складений композиційний портрет може бути перевірений автоматизованою системою портретної ідентифікації «Портрет». Система також дозволяє завантаження зображень, отриманих з відеокамер спостереження, графічних файлів та сканерів. Незважаючи на відносно невелику вартість та простоту у використанні цієї ідентифікаційної системи, вона поки що не знайшла застосування на центральному рівні. Окремі підрозділи її використовують, але база зображень правопорушників є незначною, а звідси й ідентифікаційні можливості встановлення злочинця за його зображенням зменшуються. Окрім цієї системи,

на сьогодні існує достатня кількість програмних продуктів розпізнання обличчя людини, що вже знайшли апробацію на практиці. Наприклад, прикордонники за допомогою американської програми розпізнавання обличчя «Clearview AI» змогли встановити особи понад 10 тисяч осіб, які брали участь у воєнних злочинах російської федерації [3].

Також можливо використання даних інформаційної підсистеми «Розшук» ІПНП, що містить інформацію про осіб, які ухиляються від відбування покарання або переховуються від слідства чи зникли безвісти. В інформаційній підсистемі «Пізнання» ІПНП містяться відомості про підозрюваних, підсудних та осіб, які ухиляються від вироку суду або відбування покарання; зниклих безвісти; осіб, які не здатні через стан здоров'я чи вік повідомити інформацію про себе; невпізнаних трупів.

Більш сприятливою для розслідування є типова слідча ситуація, коли особу правопорушника встановлено, але не затримано і його місцезнаходження невідомо. У цій ситуації випадку потрібне комплексне використання інформації оперативно-розшукових обліків та інформаційно-довідкових обліків на центральному та регіональному рівнях. Також можуть використовуватись інформаційні бази інших відомств, зокрема: Державної міграційної служби, СБУ, прокуратури, НАБУ та ін. Поряд з цим, можливо використання баз даних різних підприємств та організацій, банківської системи, медичних установ, транспортних підприємств тощо.

У сприятливій для розслідування типовій слідчій ситуації коли є ознаки кримінального правопорушення та особу затримано з викраденим майном при його вчиненні. В такій ситуації особа перевіряється для встановлення: можливого вчинення ним інших кримінальних правопорушень за інформаційною підсистемою «Особа», вчинення правопорушень у минулому за інформаційною підсистемою «ОДК». Інформація зазначених підсистем при наявності судимості, містить дані про час і місце затримання, прояви агресивності, протидії працівникам поліції, наявності при затриманні викрадених речей, наркотичних засобів, зброї тощо, а також особистісну інформацію: спосіб життя, звички, нахили, стосунки з членами сім'ї, товаришами, колегами по роботі, сусідами тощо.

Проаналізувавши можливості використання криміналістичних обліків при розслідуванні кримінальних правопорушень проти власності, можна зазначити, що об'єм необхідної інформації визначається слідчим залежно від слідчої

ситуації, що склалась на певному етапі, об'єму та значимості вилучених об'єктів та наявності інших фактичних даних, що знаходяться у матеріалах кримінального провадження. Від швидкого та професійного використання інформації, що міститься в криміналістичних обліках на початковому етапі залежить успіх всього розслідування.

До основних перспективних напрямів дослідження потрібно віднести:

1. Інтеграція інформаційних систем для обміну даними: Розвиток і впровадження єдиних платформ для зберігання та обміну інформацією між правоохоронними органами, що спростить доступ до криміналістичних обліків та прискорить процес розслідування.

2. Використання технологій штучного інтелекту та машинного навчання: Застосування AI та ML для автоматизованого аналізу великих обсягів даних, що містяться в криміналістичних обліках, дозволить швидше і точніше ідентифікувати підозрюваних та встановлювати зв'язки між злочинами.

3. Розширення використання біометричних даних: Застосування обліків відбитків пальців, зразків ДНК, голосових відбитків та інших біометричних параметрів для ідентифікації підозрюваних та злочинців, а також розширення баз даних з біометричною інформацією.

4. Цифровізація криміналістичних обліків та архівів: Перехід до електронного зберігання даних, що дозволяє зменшити час пошуку інформації, забезпечити доступ до архівних даних з будь-якого місця та підвищити безпеку інформації.

5. Розробка нових методів аналізу криміналістичних даних: Впровадження інноваційних методів ідентифікації та аналізу об'єктів, зокрема методів, що використовують спектральний аналіз, обробку зображень та тривимірне моделювання.

6. Посилення міжнародної співпраці: Налагодження обміну даними з міжнародними правоохоронними організаціями, що дозволить ефективніше розслідувати злочини транснаціонального характеру та оперативніше використовувати міжнародні криміналістичні обліки.

7. Підвищення кваліфікації працівників правоохоронних органів: Регулярне навчання та тренінги для слідчих та експертів з використання сучасних криміналістичних інструментів і баз даних, що дозволить підвищити ефективність їх роботи.

8. Розвиток автоматизованих систем розпізнавання осіб та транспортних засобів: Застосування систем, які аналізують дані з камер спостереження та ідентифікують обличчя або транспортні засоби, що фігурують у злочинах, дозволить оперативно виявляти зловмисників.

9. Аналіз поведінкових моделей злочинців: Використання великих обсягів даних для створення моделей поведінки злочинців, що дозволить прогнозувати їхні дії та місця вчинення нових злочинів, сприяючи попередженню злочинів.

10. Законодавча адаптація до нових технологій: Оновлення нормативної бази, що дозволить офіційно застосовувати новітні технології та методи роботи з криміналістичними обліками під час розслідування злочинів, забезпечуючи їхню юридичну силу та захист прав людини.

Список використаних джерел

1. Єфімов М.М. Типові слідчі ситуації при розслідуванні кримінальних правопорушень проти моральності. *Прикарпатський юридичний вісник*. 2018. Вип. 1 (22), т. 5, ч. 2, С. 111–115.

2. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «СЛІД» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України: Наказ Міністерство внутрішніх справ України від 16.03.2020 № 257 станом на 14 серп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/z0319-20#Text.

3. Сайт Межа: Новини URL: https://mezha.net/ua/bukvy/za-dopomohoiu-systemy-rozpiznavannia-oblych-prykordonnyky-vstanovyly-ponad-10-tysiach-osib-prychetnykh-do-voiennykh-zlochyniv/.

Стрілецький Максим Олександрович,
начальник 2-го відділу (аналітики воєнних злочинів) 4-го управління (ситуаційного аналізу) Департаменту кримінального аналізу Національної поліції України

РОЛЬ OSINT У ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ В УКРАЇНІ

Open-source Intelligence – це розвідка на основі відкритих джерел. Але така назва не є звичною для кіберсвіту, тому зазвичай вживається формулювання «OSINT».

Сама назва говорить про те, що під час проведення розвідки використовуються виключно відкриті джерела, які доступні усім. Тим паче, що зараз в Інтернеті можна зібрати величезні масиви даних і без застосування методів, що акумулюють інформацію у незаконний спосіб.

Термін OSINT також охоплює інформацію, яку можна знайти в різних форматах медіа. Попри те, що ми зазвичай асоціюємо його з текстом, до цього поняття також включають зображення, відео, вебінари, публічні виступи та конференції.

Для чого OSINT в умовах сьогодення?

Протокол Берклі – це практичний посібник з ефективного використання цифрової інформації з відкритим вихідним кодом при розслідуванні порушень міжнародного кримінального права, права людини та гуманітарного права.

Це перший набір глобальних керівних положень щодо використання цифрових даних, які є у відкритому доступі, як доказів у міжнародних розслідуваннях щодо порушень прав людини.

Документ містить стандарти знаходження, збирання, зберігання, перевірки та аналізу контенту із соцмереж та інших відкритих джерел.

Які навички необхідні для OSINT?

Привабливість OSINT полягає в тому, що він може бути використаний, як для технічних процесів, так і загалом для розвитку людини. Стосовно навичок, то по-перше – це базове розуміння використання програмного забезпечення (мінімально браузер). По-друге – це звісно посидючість, тому що збір інформації потребує часу. Ще один важливий момент. Має бути присутня креативність, адже я часто в своїй роботі стикався із ситуаціями, коли ти робиш все правильно, застосовуєш правильні інструменти, але все одно не можеш добратися до суті.

Тоді потрібно знаходити креативні підходи, шукати дотичні об’єкти або події, що неопосередковано стосуються цього об’єкта. Ну і звісно бажання розвиватися, тому що цифровий світ розвивається дуже активно і створюються нові програмні рішення, нові підходи до збору інформації. Це потребує базових навичок у програмуванні, хоча вони не є ключовим і, в принципі, можуть прокачуватись паралельно.

Наскільки важливим є наявність технічного бекграунду у людини? Знання в програмуванні, налаштуванні відповідних систем?

Все залежить від задач, що стоять перед дослідниками. Для більш простіших нам може бути достатньо лише смартфону. Якщо ж ми говоримо про якийсь більш серйозний підхід, то тут дійсно потрібно прокачувати технічні навички, але, як я вже сказав, це можна робити паралельно. Тобто наявність або відсутність технічного бекграунду критично не впливає на роботу, але якщо це приватний детектив, якому потрібно все зробити для того, щоб провести розвідку обережно і без розкриття себе, то тут потрібен хоча б мінімальний технічний бекграунд.

Хто використовує OSINT?

OSINT використовується різними людьми та організаціями для різних цілей. Ось кілька прикладів:

Розвідувальні організації використовують OSINT для збору інформації про потенційні цілі, такі як конкуренти або вороги.

Кібербезпекові фахівці використовують OSINT для виявлення кіберзагроз, таких як фішингові атаки, розвідка і зломи.

Журналісти використовують OSINT для розслідування новинних історій.

Бізнесмени використовують OSINT для дослідження ринку, конкурентів і потенційних клієнтів.

OSINT також використовується окремими людьми для різних цілей, таких як:

Вивчення історії або культури.

Знаходження інформації про продукти або послуги.

Розслідування злочинів.

Етапи розвідувального процесу

Підготовка: На цьому етапі визначаються потреби та вимоги завдання, такі як визначення цілей і вибір найкращих джерел для пошуку необхідної інформації.

Збір: Це ключовий етап, під час якого здійснюється первинний збір даних та інформації з різних джерел.

Обробка: На цьому етапі зібрані дані організовуються, перевіряються та зіставляються для подальшого аналізу.

Аналіз та обробка: Цей етап включає інтерпретацію зібраної інформації з метою виявлення закономірностей та створення висновків. Підготовка звіту містить відповідь на розвідувальне питання та рекомендації для подальших дій.

Поширення: На останньому етапі результати представляються перед зацікавленими сторонами у вигляді

письмових звітів, графіків, рекомендацій і т. д. Вони відповідають на розвідувальні запитання та надають інформацію для подальших дій.

Пасивний та активний OSINT

Пасивний підхід передбачає, що ви не взаємодієте активно з об'єктом дослідження. Ви лише збираєте інформацію з відкритих джерел, використовуючи загальнодоступні дані. Важливо розуміти, що на пасивному етапі ви не вступаєте в активний контакт з особами в онлайні, такими як коментування, обмін повідомленнями, додавання в друзі тощо.

Приклади пасивного OSINT:

Пошук інформації в Інтернеті за допомогою пошукових систем.

Аналіз соціальних мереж.

Читання новинних статей.

Отримання доступу до публічних баз даних.

Активний підхід передбачає пряму взаємодію з об'єктом дослідження, таку як додавання до списку друзів на соціальних мережах, коментування публікацій, відправлення повідомлень іт. д.

Приклади активного OSINT:

Використання інструментів для збору інформації з соціальних мереж.

Спілкування з людьми в Інтернеті.

Використання інструментів для виявлення прихованої інформації.

Вибір між пасивним та активним OSINT залежить від ваших конкретних потреб. Якщо ви шукаєте інформацію, яка вже доступна публіці, пасивний OSINT є хорошим варіантом. Якщо вам потрібна інформація, яка недоступна публіці, активний OSINT може бути більш ефективним.

ВАЖЛИВІСТЬ «OSINT» У ДОКУМЕНТУВАННІ

В умовах війни доступ до окупованих або тимчасово неконтрольованих територій обмежений, а документування ймовірних порушень там – небезпечне, або й неможливе. Слідчим, прокурорам, адвокатам і суддям може бракувати досвіду роботи з деякими особливими категоріями надтяжких порушень, як-то воєнні злочини або злочини проти людяності.

Саме в цьому випадку аналітики воєнних злочинів допомагають встановити низку важливих деталей, зокрема:

1. **Військові підрозділи та їхня активність**. Чи видно на відео чи фотографіях військовослужбовців у формі. Чи можливо ідентифікувати форму, відзнаки, техніку.

2. **Можливі військові цілі**. Після визначення місця проведення військової операції, інформація з відкритих джерел може допомогти встановити, чи були там або поруч можливі військові цілі. З належними навичками ви можете визначити військові цілі з використанням картографічних інструментів і супутникових знімків високої роздільної здатності, перевіряючи наявність військових об'єктів або споруд, а також визначаючи крупну військову техніку: вантажівки, танки, бронетехніку та літальні апарати.

3. **Активність цивільних**. Куди саме припав удар – у житловий район, точку евакуації, багатоквартирний будинок, лікарню чи деінде? Чи видно десь цивільних осіб, наприклад, дітей або літніх людей? Що вони роблять? Чи дозволяють відкриті джерела візуально порахувати кількість цивільних осіб – живих або мертвих?

4. **Ідентифікація озброєння**. Постраждалі, які знімали місце подій, часто оприлюднюють зображення залишків зброї або іншої військової техніки онлайн. До них відносяться уламки ракет або снарядів, гільзи, касетні боєприпаси, упаковки тощо. Ідентифікація цієї зброї може допомогти встановити, чи був удар непропорційним або невибірковим та в подальшому допомогти встановити безпосередньо виконавців вказаного злочину (командирів підрозділу).

Список використаних джерел

1. Dehtiarova Y. Як OSINT впливає на війну в Україні? [Електронний ресурс] / Yuliana Dehtiarova // itedu.cente. – 2022. – Режим доступу до ресурсу: https://itedu.center/ua/blog/articles/osint/?srsltid=AfmBOooGkcfk0Cb_A5SDyxlzlsWzJPrA8FZTxGNgx2luA1fyOGcdwiHV.

2. Старосек А. OSINT в Україні: хто і як допомагає фронту під час війни? [Електронний ресурс] / Артем Старосек // Українська правда. – 2023. – Режим доступу до ресурсу: https://www.pravda.com.ua/columns/2023/01/23/7386112/.

3. ECOFCC. OSINT і його роль у сучасному світі [Електронний ресурс] / ECOFCC // EUROPEAN CENTER OF FINANCIAL CRIME COUNTERACTION – Режим доступу до ресурсу: https://ecofcc.org/2023/08/21/osint-earth/.

Треус Андрій Сергійович,
начальник управління інформаційно-аналітичного забезпечення
та кримінального аналізу Департаменту оперативно-розшукової діяльності Адміністрації Державної прикордонної служби України;
Якобчук Ярослав Юрійович,
заступник начальника першого відділу управління інформаційно-аналітичного забезпечення та кримінального аналізу Департаменту оперативно-розшукової діяльності Адміністрації Державної прикордонної служби України

АНАЛІЗ ЧИННИКІВ, ЩО ВПЛИВАЮТЬ НА ЕФЕКТИВНІСТЬ РОЗВІДУВАЛЬНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНОГО УГРУПОВАННЯ ВІЙСЬК В ОПЕРАЦІЇ СИЛ ОБОРОНИ З ВИКОРИСТАННЯМ OSINT ЗА ДОСВІДОМ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Розвідувальне забезпечення є ключовим елементом військових операцій, яке дозволяє вчасно отримувати необхідну інформацію, з метою ухвалення рішень. У сучасних умовах ведення бойових дій значну роль відіграє розвідка з відкритих джерел(OSINT, Open Source Intelligence), у тому числі і під час російсько-української війни.

Технології і методики OSINT дозволяють отримати якнайбільше потрібної інформації у короткий термін та витрачаючи щонайменше ресурсів (існує достатня кількість безкоштовних інструментів OSINT), що є досить важливим в умовах воєнного стану [1].

OSINT є відносно новим напрямком у військовій розвідці України, який став особливо актуальним із розвитком інформаційних технологій.

OSINT базується на використанні публічно доступної інформації, яка міститься в медіа, соціальних мережах, геолокаційних даних та інших джерелах, доступних у відкритому інформаційному просторі. Досвід російсько-української війни продемонстрував важливість і складність застосування OSINT для оперативного угруповання військ [2].

OSINT також дозволяє використовувати інформацію, що міститься у ворожих джерелах, як-от пропагандистські ЗМІ або інформаційні ресурси противника. Однак, для забезпечення ефективності такого роду розвідки необхідно враховувати низку чинників, що впливають на якість отриманої інформації.

Найбільшою проблемою розвідки з відкритих джерел є наявність неперевірених джерел інформації, провокаційних ресурсів та недостовірних даних. Щоб отримати актуальну та якісну інформацію, користувачу необхідно обробити значний обсяг даних з різноманітних джерел і узагальнити їх відповідно до мети і завдань розвідки.

Залежно від завдання щодо обробки інформації, зокрема її аналізу та верифікації в інтересах розвідувального забезпечення операцій угруповань військ (сил), рекомендується застосовувати наявні інформаційні системи, програмні засоби та інтернет-сервіси для виконання цих завдань:

– Дані соціальних мереж (Twitter, Facebook, Telegram, Instagram, Tik-Tok, Youtube, Duolingo);

– Геопросторові дані (зображення зі супутників, геолокаційні метадані);

– Публікації в ЗМІ та блоги;

– Відкриті бази даних (державні реєстри, урядові документи).

Головною перевагою цього виду розвідки є можливість швидкого доступу до великої кількості інформації. Водночас основними умовами раціонального використання такої розвідувальної інформації є:

розроблення та впровадження керівних документів з питань розвідки з відкритих джерел;

визначення основних принципів, порядку планування та підготовки розвідки з відкритих джерел;

визначення основних понять, концепцій та методів збору розвідувальних даних з відкритих джерел;

створення підрозділів розвідки з відкритих джерел та набуття ними спроможностей;

створення структури розвідки з відкритих джерел;

створення системи підготовки фахівців розвідки з відкритих джерел;

створення систем аналізу інформації та єдиного центру її обробки;

скорочення часу проходження інформації від першоджерела до центру обробки та забезпечення належної

якості первинної обробки такої інформації (фото, відео фіксація тощо) [3].

Слід виділити чинники, що впливають на ефективність OSINT в розвідувальному забезпеченні оперативного угруповання військ у операції Сил оборони:

Технологічні ресурси є одним із головних чинників, що впливає на ефективність розвідувального забезпечення з використанням OSINT. Для збору та обробки даних потрібні сучасні системи аналізу великих обсягів інформації, алгоритми штучного інтелекту для обробки зображень та тексту, а також спеціалізовані програмні інструменти для геоаналізу.

Швидкість обробки даних є критичним фактором у військових операціях. Угрупування військ (сил) повинно отримувати розвідувальні дані максимально швидко для прийняття рішень у реальному часі. Запізнення в передачі інформації може призвести до втрати ініціативи та переваги на полі бою.

Верифікація та перевірка даних. Зважаючи на великий обсяг фейкової або хибної інформації у відкритих джерелах, важливим чинником є якість процесів верифікації. Ефективні методи перевірки джерел та крос-аналіз інформації з різних джерел дозволяють зменшити ризики, пов’язані з дезінформацією.

Координація з іншими видами розвідки. Для досягнення максимальної ефективності OSINT має бути інтегрованою з іншими типами розвідки, такими як сигнальна розвідка (SIGINT), технічна розвідка (IMINT) та людська розвідка (HUMINT). Такий синергетичний підхід дозволяє створювати комплексну картину операційної обстановки.

Досвід російсько-української війни показав, що OSINT може бути надзвичайно ефективним інструментом для розвідувального забезпечення в сучасних оборонних операціях. Однак його ефективність залежить від низки факторів, таких як технологічні ресурси, швидкість обробки даних, рівень верифікації інформації та координація з іншими видами розвідки. Розвиток інструментів для збору та аналізу відкритих даних, а також впровадження нових технологій, таких як штучний інтелект, може значно підвищити роль OSINT у майбутніх військових операціях.

Список використаних джерел

1. Ланде Д. В. Правові питання конкурентної розвідки // Інформація і право. 2020. № 2(33). URL: http://ippi.org.ua/lande-dv-pravovi-pitannya-konkurentnoirozvidki-st-51-68.

2. Уфімцева О.С. Використання OSINT в умовах збройної агресії рф проти України.

3. Гаценко С.С., Металіді О.Г., Дудник В.П., Мороз М.В. Підвищення ефективності розвідувального забезпечення операції угруповання військ: методичний підхід.

Фаріон Олег Борисович,
доктор військових наук, професор,
професор кафедри прикордонної
безпеки факультету професійної освіти
та лідерства Національної академії
Державної прикордонної служби
України імені Богдана Хмельницького

РЕКОМЕНДАЦІЇ ПРИКОРДОННОМУ ЗАГОНУ ЩОДО ВИКОРИСТАННЯ ІНСТРУМЕНТАРІЮ OSINT І КРИМІНАЛЬНОГО АНАЛІЗУ ДЛЯ МОНІТОРИНГУ ОБСТАНОВКИ НА УКРАЇНСЬКО-РОСІЙСЬКІЙ ДІЛЯНЦІ ДЕРЖАВНОГО КОРДОНУ

Побудова охорони державного кордону на деокупованій українсько-російській ділянці державного кордону передбачає ведення підрозділами прикордонних загонів спостереження за державним кордоном та суміжною територією для завчасного отримання достовірної інформації про дії противника, його наміри та інші зміни обстановки.

В умовах воєнного стану спостереження за змінами обстановки на державному кордоні та в прикордонних районах із використанням військових методів є проблематичним через постійне вогневе ураження противником із активним використанням ракетно-артилерійських систем, засобів повітряної розвідки та радіоелектронної боротьби, ударних безпілотних систем та авіації. За таких умов виникає необхідність пошуку безпечних способів отримання інформації про дії та наміри противника, серед яких пропонується використання можливостей інструментарію OSINT та кримінального аналізу.

Наявні в прикордонному загоні оперативно-розшукові підрозділи мають досвід використання інструментарію OSINT та кримінального аналізу для отримання інформації про дії

злочинців та скоєні ними злочини на державного кордону. Однак, під час збройної агресії російської федерації в Україні особовий склад цих підрозділів свої зусилля спрямовує здебільшого на ведення наземної розвідки з використанням наявних засобів, зокрема безпілотних авіаційних систем, що є неефективним при застосуванні противником засобів радіоелектронної боротьби. Отже, актуальним тут є використання можливостей OSINT та кримінального аналізу.

За допомогою різних способів проведення OSINT може здійснюватись моніторинг, аналіз та дослідження інформації з мережі «Інтернет». Це дозволить підрозділам прикордонного загону в рамках виконання завдань розвідки отримувати дані про зміни обстановки щодо дій противника. Надалі використання методів кримінального аналізу надасть можливість встановити та перебачити зв'язки між даними про дії противника та іншими потенційно з ними пов'язаними даними з метою їх використання у розробленні рішення начальника прикордонного загону (прикордонного підрозділу) на застосування сил та засобів щодо забезпечення недоторканості державного кордону.

Отже, використання інструментарію OSINT та кримінального аналізу надасть можливість прикордонному загону: ефективно збирати (добувати) та аналізувати дані з відкритих джерел для відстеження динаміки змін обстановки та прогнозу її розвитку; виявляти потенційні загрози на державному кордоні; ідентифікувати дезінформацію, розпізнавати та ефективно протидіяти інформаційно-психологічну впливу противника; використовувати продукти аналізу для підтримки прийняття управлінських рішень з питань забезпечення недоторканості державного кордону тощо.

Купрієнко Дмитро Анатолійович,
начальник відділу забезпечення якості освіти – головний науковий співробітник Національної академії Державної прикордонної служби України імені Богдана Хмельницького, доктор військових наук, професор;
Кіреєва Ольга Сергіївна,
кандидат психологічних наук, доцент, доцент кафедри спеціальних дисциплін (факультет правоохоронної діяльності) Національної академії Державної прикордонної служби України імені Богдана Хмельницького

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ OSINT І ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТАБІЛІЗАЦІЙНИХ ЗАХОДІВ ПРИКОРДОННОГО ЗАГОНУ НА ДЕОКУПОВАНІЙ ТЕРИТОРІЇ ПРИКОРДОННИХ РАЙОНІВ УКРАЇНИ

Після відновлення контролю за деокупованою ділянкою державного кордону підрозділи Сил безпеки і оборони України розпочали проведення заходів, спрямованих на стабілізацію обстановки в прикордонних районах. З цією метою прикордонні загони Державної прикордонної служби України основні зусилля зосереджують на посиленні охорони і захисту визначеної ділянки державного кордону. Крім того, приймають вони участь у виконанні заходів територіальної оборони, припиненні збройних провокацій на державному кордоні, боротьбі з диверсійно-розвідувальними групами противника та тероризмом, виконання завдань військової розвідки тощо.

З огляду на те, що на території України зараз відбуваються воєнні дії, спецслужби країни-агресора можуть використовувати соціальні мережі як для коригування вогню ворога, так і для проведення інформаційної війни. Тому, з початком повномасштабного вторгнення рф, громадян України неодноразово закликали не публікувати в соціальних мережах наслідки обстрілів, не передавати жодну інформацію стосовно розташування стратегічних об’єктів по месенджерах [1].

Для забезпечення ефективності проведення стабілізаційних заходів важливим є застосування передових методів отримання

та аналізу інформації про події, що свідчать про порушення законодавства України, та осіб, причетних до них. Отже, тут пропонується використання можливостей OSINT у поєднанні зі штучним інтелектом.

Основні напрямки використання OSINT слід вважати:

моніторинг соціальних мереж з метою виявлення груп або окремих осіб зацікавлених у дестабілізації обстановки в прикордонних районах;

ідентифікація дезінформації з метою своєчасного виявлення та спростування «фейкової» інформації, що може спровокувати конфлікти або дестабілізувати ситуацію на державному кордоні;

відстеження за допомогою геолокаційних інструментів незвичайної активності поблизу державного кордону, що може свідчити про підготовку до спроби незаконного його перетину;

аналіз відкритих джерел (новин) шляхом моніторингу повідомлень про прикордонні інциденти та виявлення тенденцій щодо змін настроїв населення в прикордонних районах;

використання геопросторових даних для відстеження змін в природному середовищі, що можуть вплинути на безпеку державного кордону (наприклад, незаконну діяльність);

використання інструментарію «Human Intelligence» шляхом створення спеціальних каналів для збору інформації від жителів прикордонних районів про ситуації на державному кордоні; організації онлайн-опитувань для з'ясування думки населення щодо різних аспектів безпеки кордону [2].

Спеціальними інструменти OSINT можуть бути: пошукові системи (наприклад Google Dorks, Shodan, Maltego), соціальні мережі (наприклад, SOCMINT), геопросторові інструменти (наприклад, Google Earth, QGIS) [3].

Постає питання про необхідність розроблення певних алгоритмів, правил, опитувальників щодо збирання, документування та обробки оперативної інформації з використанням інструменти OSINT. Алгоритм (араб. аль-Хорезмі – ім'я середньовічного узбецького математика) – система правил виконання обчислювального процесу, що приводить до розв'язання певного класу задач після скінченного числа операцій [4]:

Разом із інструментами OSINT, доцільно використовувати можливості штучного інтелекту у такій послідовності.

збір та попередня обробка даних з відкритих джерел (наприклад, соціальних мереж, засобів масової інформації, веб-сайтів);

перетворення даних для аналізу шляхом «векторизації» тексту, кодування категоріальних ознак, нормалізації числових даних тощо;

навчання моделей штучного інтелекту, таких як класифікатори або нейронні мережі для виявлення зв'язків між особами та подіями, оцінювання ризиків та прогнозування можливих наслідків [5];

ідентифікація осіб, які причетні до подій, що свідчать про порушення законодавства України;

перевірка (оцінювання точності) та підтвердження достовірності отриманих результатів, а також інтерпретація їх у форму, зручну для подальшого використання;

документування подій, що свідчать про порушення законодавства України;

вдосконалення процедури отримання та аналізу інформації (даних) шляхом впровадження нових методів штучного інтелекту.

Таким чином, використання інструментарію OSINT у поєднанні зі штучним інтелектом надасть можливість прикордонним загонам підвищити результативність стабілізаційних заходів на деокупованій території прикордонних районів України.

Список використаних джерел

1. Кіреєва О. С. Використання методів OSINT в роботі кримінальних аналітиків. *«Актуальні питання використання методів і засобів OSINT у роботі підрозділів захисту національної державності»* : збірник матеріалів круглого столу (м. Київ, 31 травня 2023 року). Київ. НА СБУ, 2023. С. 150-153.

2. Модель OSINT. Відкриті джерела у світі розвідки. URL: http://strateger.net/model_osint_otkritie_istochniki_v_mire_razvedki

3. OSINT Інструменти для розслідування. URL : https://hackyourmom.com/ kibervijna/osint-akademiya/osint-instrumentydlya-rozsliduvannya/HackYourMom

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

5. Кіреєва О. С. Використання кримінальними аналітиками інноваційних технологій для виявлення проявів колабораційної діяльності. *«Успіхи і досягнення у науці (Серія «Право»)»* № 3 (3). 2024. С. 46-58: https://doi.org/10.52058/3041-1254-2024-3(3)-46-58.

Федчак Ігор Андрійович,
кандидат юридичних наук, доцент,
доцент кафедри інформаційного
та аналітичного забезпечення
діяльності правоохоронних органів
Львівського державного університету
внутрішніх справ

РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ В ЗНИЖЕННІ РІВНЯ ЗЛОЧИННОСТІ

Огляд наукових досліджень про кримінальний аналіз як вид діяльності унаочнює зростаючий обсяг знань про зміст аналітичної діяльності та методи проведення кримінального аналізу, проте майже не здійснено досліджень, присвячених з'ясуванню зв'язку між кримінальним аналізом і зниженням рівня злочинності. Проте, недостатність досліджень про взаємозв'язок між кримінальним аналізом і зменшенням злочинності не є наслідком відсутності інтересу до цього питання. На запитання про те, чи кримінальний аналіз безпосередньо зумовлює зменшення злочинності дуже складно відповісти.

Кримінальний аналіз використовується для проведення аналізу стану криміногенної ситуації на окремій території діяльності правоохоронного органу, певній ділянці місцевості, або для аналізу конкретного кримінального провадження чи оперативно-розшукової справи. Така діяльність проводиться з метою інформаційно-аналітичної підтримки розкриття та розслідування злочинної діяльності (дослідження злочинної діяльності; виявлення співучасників, потерпілих; встановлення мотивів і мети; встановлення зв'язків між даними, аналіз діяльності організованої групи (злочинної організації) тощо [1, с. 61]. Також кримінальний аналіз здійснюється для ідентифікації та аналізу закономірностей і тенденцій злочинності, встановлення профілів злочину, підозрюваного та потерпілого, аналізу окремих видів злочинів, оцінки пріоритетів загроз, спричинених діяльністю організованих злочинних угруповань, та скоєних тяжких і особливо тяжких злочинів, аналізу й управління ризиками та для складання прогнозів, виявлення місць підвищеної концентрації кримінальної активності.

Як відомо, дані – це відомості криміногенного характеру та дотичні відомості, аналізуючи які аналітики із використанням спеціалізованого аналітичного програмного забезпечення формулюють аналітичні продукти. За змістом, аналітичні

продукти можуть поділятися на аналітичний звіт, досьє, профіль, аналітичний документ, аналітичне орієнтування [2, с. 437]. Такі аналітичні продукти передаються керівникам, які уповноважені приймати управлінські рішення про застосування сил і засобів (ресурсів), щоб більш ефективно вирішувати ідентифіковані проблеми. Нарешті, керівник (зазвичай оперативного підрозділу або органу досудового розслідування), відповідальний за реалізацію визначених завдань, вивчає аналітичні продукти, проводить ще один рівень аналізу і визначає тактику застосування сил та засобів для нейтралізації проблеми. Отже, незважаючи на те, що продукти кримінального аналізу можуть бути точними та високоякісними, успіх у обмеженні поширення злочинності залежить від обраної тактики дій конкретного керівника.

Таким чином, однозначно відповісти на запитання про те, чи протидіє поширенню злочинності підрозділ кримінального аналізу, неможливо. Так, проведення аналітичних досліджень є важливим і необхідним засобом для керівників саме як інструмент націлювання, оскільки аналітичне дослідження може виявити проблему на ранніх стадіях і сприяти у виборі заходів протидії та тактики їх застосування. Однак роль технологій, аналітичних програм, методів і технік проведення аналітичних досліджень кримінологічних даних і аналітиків у виборі заходів протидії проблемам та їх успішному впровадженні є надзвичайно обмеженою. Таким чином, не можна сказати, чи кримінальний аналіз запобігає, або вирішує різні проблеми злочинності, проте можна говорити лише про те, що це важливий, а в деяких випадках і необхідний компонент організації правоохоронної діяльності.

Аналітик має дані для встановлення «діагнозу» конкретної проблеми злочинності. Вибір відповіді, яка ґрунтується на аналізі, зазвичай проводиться не аналітиком, а оперативними співробітниками або слідчими. Що ще важливіше, реалізація реагування та забезпечення наявності необхідних ресурсів для реагування покладається на керівний склад правоохоронних органів (відповідальних за реагування, у більшості випадків також оперативного складу або слідчих).

Кінцевий продукт кримінального аналізу передається правоохоронному органу, в якому співробітники обирають відповідь, а потім здійснюють нагляд і забезпечують ресурси для реагування (тобто відбір і проведення заходів реагування). Нарешті, результатом реагування в ідеальній ситуації є

зменшення злочинності. Цей ефект, звичайно, потребує ретельного вивчення та строгих методів оцінки, щоб визначити, чи справді реакція поліції, а не інші чинники спричинили зниження злочинності. Таким чином, на питання про те, чи кримінальний аналіз зменшує злочинність, дуже складно відповісти в широкому масштабі чи навіть у більш зосередженому аналізі.

Відповіддю на запитання про те, чи запобігає або чи зменшує кримінальний аналіз стан злочинності, є однозначно ні! Правильним буде формулювати запитання, чи є кримінальний аналіз необхідним компонентом (тобто інструментом діагностики) у правоохоронній діяльності, і відповідь буде однозначно – так! Однак, недостатньо лише «залучити аналітика» або придбати програмне забезпечення. Першим кроком на шляху до позитивного впливу на стан злочинності є вибір однієї із моделей проактивної правоохоронної діяльності, яка найкраще відповідає проблемам громади, а далі слід залучити аналітика, тому що ефективна й дієва «діагностична» здатність є важливим і необхідним компонентом впливу «лікування» на злочинність. Залучення аналітика для того, щоб отримувати інформацію та статистичні дані для конкретного правоохоронного органу та громади без впровадження успішного підходу (моделі) до зменшення злочинності, – недостатньо.

Ключова рекомендація полягає в тому, щоб у дослідженнях ефективності правоохоронної діяльності дослідники приділяли пильнішу увагу саме специфічній ролі кримінального аналізу та аналітиків у реалізації тих чи інших моделей. Виділення кримінального аналізу в експериментальних і прикладних дослідженнях надасть дані науковцям, щоб зробити емпіричні узагальнення стосовно внеску кримінального аналізу в запобігання та протидію злочинності [3, с. 559–560].

Список використаних джерел

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

2. Свиридюк Н., Кардашевський Ю. Розділ 32. Аналітичні продукти. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін., за заг. ред. Користіна О.Є. Київ: «ВАЙТ», 2024. С. 435-442. DOI: https://doi.org/10.36486/978-966-2310-66-5-32

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

Ханькевич Андрій Миколайович,
кандидат юридичних наук, професор,
старший викладач кафедри досудового
розслідування Національного
юридичного університету
імені Ярослава Мудрого

ПРЕДИКТИВНА АНАЛІТИКА В КОНТРРОЗВІДУВАЛЬНІЙ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Стрімкий розвиток цифрових технологій та методів обробки великих даних відкриває принципово нові можливості для підвищення ефективності контррозвідувальної діяльності (далі – КРД). Традиційні підходи до організації роботи Служби безпеки України (далі – СБУ) потребують суттєвого переосмислення з урахуванням викликів сучасності та наявних технологічних можливостей.

За останні роки значно розширились можливості збору та аналізу різноманітних даних, що становлять інтерес у КРД СБУ. Водночас традиційні методи аналітичної роботи вже не здатні у потрібному обсязі забезпечити своєчасну та якісну обробку постійно зростаючих масивів інформації, що актуалізує питання впровадження предиктивної аналітики як сучасного інструментарію прогнозування та виявлення загроз державній безпеці України.

Сьогодні існують різні підходи до визначення поняття предиктивної (прогнозної) аналітики. Як зазначає О. Заєць, це є «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» [1, с. 49].

Метою предиктивної аналітики є здійснення прогнозів щодо майбутніх подій та використання цих прогнозів для покращення процесу ухвалення рішень. При цьому важливо, що такі процедури можуть забезпечити достатній для практики рівень точності прогнозування [1, с. 50].

Аналіз положень Закону України «Про контррозвідувальну діяльність» дозволяє встановити безпосередній зв’язок між законодавчо визначеними завданнями контррозвідувальної діяльності та потенціалом предиктивної аналітики.

Ключовою метою контррозвідувальної діяльності, відповідно до статті 2 Закону, є «попередження, своєчасне

виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють, та причин їх виникнення» [2]. Саме превентивний характер цієї мети зумовлює необхідність використання методів предиктивної аналітики, спрямованих на прогнозування майбутніх подій та загроз.

Серед основних завдань контррозвідувальної діяльності законодавець визначає «добування, аналітичну обробку 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» (ст. 2 Закону) [2], що безпосередньо співвідноситься з можливостями предиктивної аналітики щодо опрацювання великих масивів даних та виявлення прихованих закономірностей.

Важливо зазначити, що зазначений Закон передбачає широкий спектр джерел отримання інформації для контррозвідувальної діяльності, а саме «заяви і повідомлення громадян, осіб, залучених до конфіденційного співробітництва, посадових та службових осіб, громадських організацій, медіа; матеріали органів досудового розслідування та суду; запити, інформації та матеріали спеціальних служб і правоохоронних органів іноземних держав, міжнародних установ і організацій» (ст. 6) [2], що створює значний масив різнорідних даних, ефективне опрацювання яких можливе саме із застосуванням інструментів предиктивної аналітики.

«Комплексне застосування правових, профілактичних та організаційних заходів», визначене як один з основних принципів контррозвідувальної діяльності» (ст. 4 Закону) [2], також потребує використання сучасних аналітичних інструментів для оцінки ефективності та прогнозування результатів таких заходів.

Особливу увагу варто приділити й принципу «адекватності заходів щодо захисту державної безпеки реальним і потенційним загрозам» (ст. 4 Закону України «Про контррозвідувальну діяльність»), оскільки саме предиктивна аналітика надає можливість об’єктивної оцінки потенційних загроз та вибору найбільш адекватних методів реагування через своєчасне виявлення прихованих закономірностей у масивах різнорідних даних.

Практика застосування предиктивної аналітики спеціальними службами низки країн світу демонструє високу ефективність у сфері забезпечення національної безпеки. Зокрема, впровадження аналітичних методів прогнозування в діяльність спеціальних служб дозволило суттєво підвищити результативність превентивних заходів.

У США, Великій Британії, Німеччині, Нідерландах та Китаї розроблені та успішно використовуються спеціальні програмні комплекси, що дозволяють здійснювати прогнозування загроз національній безпеці. Такі системи спираються на аналіз трьох основних змінних: вид загрози, час та місце потенційного інциденту. Важливо, що ці аналітичні інструменти не потребують персональних даних для ефективного функціонування.

Показовим є досвід поліції Німеччини, де система «Precobs» використовує алгоритми та знання про минулі події для прогнозування можливих рецидивів [3, с. 1044]. Система генерує прогнози на основі найактуальніших даних, які можуть використовуватися службами як в оперативних, так і в профілактичних цілях.

Експериментальні дослідження, проведені в США, показали, що алгоритмічні методи прогнозування здатні передбачати загрози з удвічі вищою точністю порівняно з традиційним експертним аналізом. При цьому важливо розуміти, що предиктивна аналітика не замінює традиційних методів роботи спеціальних служб, а посилює їх шляхом застосування передових статистичних моделей та алгоритмів.

У сфері забезпечення національної безпеки досвід провідних держав світу демонструє активне впровадження систем стратегічного моніторингу інформації як різновиду предиктивної аналітики.

Показовим є досвід Німеччини, де застосування системи стратегічного моніторингу регулюється законом G10 [4], законність функціонування якої визнана Європейським судом з прав людини (Case of Weber and Saravia v. Germany, Application № 54934/00, ECHR, 2006) [5]. Система здійснює збір та аналіз інформації для попередження загроз, зокрема: міжнародного тероризму, незаконної зовнішньої торгівлі, міжнародних кібератак на критичну інфраструктуру.

У Великій Британії діє система Tempora (Big brother watch v. The United Kingdom, Applications no. 58170/13, 62322/14, 24960/15, ECHR, 2018), що дозволяє здійснювати аналіз даних

для забезпечення національної безпеки. Подібна система працює і в Швеції, де її функціонування також визнано правомірним (Case of Centrum för rättvisa v. Sweden, Application № 35252/08, ECHR, 2018) [5].

Ключовими особливостями таких систем є:

– автоматизована фільтрація інформації в режимі реального часу;

– застосування складних критеріїв пошуку;

– комплексна аналітична обробка даних;

– чітка регламентація процедур використання отриманої інформації.

Упровадження подібних систем предиктивної аналітики у КРД створює потужний інструментарій для раннього виявлення та запобігання загрозам національній безпеці через автоматизований аналіз значних масивів різнорідної інформації в режимі реального часу.

На основі аналізу практичних аспектів застосування предиктивної аналітики можна виділити ключові напрями її використання у сфері КРД.

Як зазначає А. Фергюсон, основними напрямами застосування є виявлення прихованих зв'язків та мереж (аналіз великих даних дозволяє з високою ймовірністю виявляти структури та зв'язки між особами, що становлять інтерес), комплексний моніторинг активності (системи здатні обробляти візуальні дані, активність в інтернеті, цифрові сліди) та прогнозування загроз через алгоритми машинного навчання [6, с. 272].

За даними компанії Mashable, сьогодні у світовій практиці сформувались два основні підходи до організації систем предиктивної аналітики:

– неперсоніфіковані системи, що працюють виключно зі статистичними даними;

– персоніфіковані системи, що здійснюють комплексний аналіз широкого спектру даних про конкретних осіб [7].

У контексті КРД особливо важливою є здатність таких систем виявляти приховані закономірності та аномалії в поведінці об'єктів спостереження на ранніх стадіях формування загроз, що створює можливості для превентивного реагування.

Важливим елементом предиктивної аналітики є предиктор – фізична або юридична особа, яка призначена для прогнозування можливої майбутньої поведінки. Множина предикторів становить модель предиктивної аналітики, що

дозволяє прогнозувати певні події в майбутньому з визначеним ступенем ймовірності. Безумовним є те, що предиктивну аналітику найефективніше використовувати за наявності широкого спектру максимально повних та очищених пакетів даних. Точність результатів аналізу прямо залежить від обсягу доступних даних з різних сфер [1, с. 51-52].

Отже проведене дослідження дозволяє сформулювати такі висновки щодо ролі та місця предиктивної аналітики в контррозвідувальній діяльності:

1. У сучасних умовах предиктивна аналітика виступає потужним інструментом КРД, що через використання методів статистичного моделювання, машинного навчання та штучного інтелекту забезпечуватиме якісно новий рівень прогнозування та виявлення загроз державній безпеці України. Застосування комплексу аналітичних методів – від поведінкового аналізу до виявлення аномалій та кластерного аналізу, створює можливості для раннього виявлення ознак підготовки ворожих операцій та спроб проникнення у критичну інфраструктуру.

2. Практичний досвід провідних держав світу демонструє, що впровадження систем предиктивної аналітики дозволяє перейти від реактивної до проактивної моделі забезпечення державної безпеки, що підвищить ефективність контррозвідувальних заходів через автоматизацію процесів виявлення загроз та оптимізацію використання наявних ресурсів.

3. Водночас ефективне використання можливостей предиктивної аналітики вимагатиме комплексного підходу до модернізації організаційно-технічної складової КРД, зокрема високого рівню автоматизації процесів та розширення технологічних можливостей моніторингу.

За таких умов впровадження предиктивної аналітики стає не просто технологічною інновацією, а необхідною передумовою забезпечення спроможності контррозвідки ефективно протидіяти сучасним викликам та загрозам національній безпеці України.

Список використаних джерел

1. Заєць О. Prediction Analytics (прогнозна аналітика): визначення, типи моделей і використання. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України* : матеріали науково-практ. конф., м. Київ, 17 листоп. 2023 р. Київ, 2023. С. 49–55. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/6a681285-7ff9-4718-9451-dd907f56ba6f/content.

2. Про контррозвідувальну діяльність : Закон України від 26.12.2002 № 374-IV : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text.

3. Assessing the Generalizability of the Near Repeat Phenomenon / T. J. Youstin et al. *Criminal Justice and Behavior*. 2011. Vol. 38, no. 10. P. 1042–1063. URL: https://doi.org/10.1177/0093854811417551.

4. G 10 - Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses. *Gesetze im Internet*. URL: https://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html.

5. HUDOC - European Court of Human Rights. *HUDOC - European Court of Human Rights*. URL: https://hudoc.echr.coe.int/fre#%7B»sort»:[«kpdate%20Descending»], «itemid»:[«001-76586»]%7D.

6. Ferguson A. G. Chapter: «Blue Data» (Excerpt from «The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement»). *SSRN Electronic Journal*. 2017. URL: https://doi.org/10.2139/ssrn.3959202.

7. China is using AI to predict who will commit crime next. *Mashable*. URL: https://mashable.com/article/china-ai-crime-minority-report?test_uuid=01iI2GpryXngy77uIpA3Y4B&test_variant=b.

Худенко Дмитро Миколайович,
ветеран Національної поліції України,
керівник Департаменту кримінального аналізу у 2021–2023 роках

РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ В РОЗСЛІДУВАННЯХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ДЕ ПРЕДМЕТОМ АБО ЗАСОБОМ ВЧИНЕННЯ Є ШТУЧНИЙ ІНТЕЛЕКТ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ З ПІДГОТОВКИ ФАХІВЦІВ

Глобальна дискусія щодо використання штучного інтелекту вплинула і на сферу кримінального аналізу, де активно почала набирати обертів з 20 років нашого століття. Втім, одною із перших, хто приєднався до неї виявилась ще 2018 року харківська школа кримінального аналізу [1]. Зокрема, Д.Ю. Узловим штучний інтелект було розглянуто, як метод та технологію. Поступово науковим товариством вказано на потребу зміни підходів за допомогою штучного інтелекту [2], його значний технологічний потенціал [3, 4, робились спроби вивчення відповідного закордонного досвіду [5], а сам штучний

інтелект віднесено до інструментарію [6]. Крім того, повідомлено про те, що цю технологію використано для пошуку, збору та аналізу даних, виявлення кримінальних правопорушників у режимі реального часу та ідентифікації потенційних жертв злочинів [7]. За результатами аналізу історіографії можна стверджувати, що штучний інтелект у формі методу, засобу чи шляху вдосконалення увійшов до сфери кримінального аналізу.

Натомість вітчизняні розвідки з кримінального аналізу щодо специфіки розслідувань кримінальних правопорушень, де предметом або засобом вчинення є технологія штучного інтелекту, відсутні. Водночас факти вчинення правопорушень такого роду фіксуються, що сьогодні потребує переосмислення фахової кваліфікації. Адже неякісний або низький рівень підготовки особи, яка проводить кримінальний аналіз, її відсуніть, може призвести до неправильних висновків і неточних оцінок, що ускладнить встановлення істини у кримінальному проваджені та створить ризик із порушення прав людини.

Питання підготовки фахівців із кримінального аналізу досліджували О.В. Корнейко, А.В. Мовчан, Д.І. Овсянюк, А.М. Ханькевич, В.І. Школьніков [8] та інші. Але на сьогодні не висвітлено підготовку таких фахівців з опанування основ технології штучного інтелекту, а також особливостей розкриття та розслідування кримінальних правопорушень, де предметом або засобом вчинення є штучний інтелект.

Метою нашого дослідження є характеристика потреби змін у підготовці фахівців з кримінального аналізу системи з огляду на появу кримінальних правопорушень, де предметом або засобом вчинення є штучний інтелект.

На початку викладення нашого матеріалу обумовимо поняття «штучний інтелект». Під ним пропонується розуміти його законодавчий сенс, а саме, – організовану 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 [9].

Для виявлення тенденцій у злочинній сфері, які пов’язані із штучним інтелектом проаналізовано практику органу досудового розслідування та суду. Так, 23.10.2024 з

використанням Єдиного державного реєстру судових рішень [10] нами зроблено пошук словосполучення «штучний інтелект» у кримінальному судочинстві. Пошуковий запит повернув вибірку у 45 ухвал (38) та вироків (7), з них по одному інформація заборонена для оприлюднення згідно з п. 4 ч. 1 ст. Закону України від 22 грудня 2005 року № 3262-IV «Про доступ до судових рішень». Із 44 судових рішень 30 визнано такими, що не валідні. Наприклад, коли в них мова йшла про обґрунтування характеристики обвинуваченого у частині оцінювання ризиків вчинення повторного кримінального правопорушення та рівня небезпеки особи для суспільства за допомогою автоматизованої системи з штучним інтелектом «Касандра» [11]. Або ж коли декілька судових рішень стосувались однієї справи, то таке рішення визнавалось нами за одне. Або це були скарги на невнесення відомостей до Єдиного реєстру досудових розслідувань [12–13] тощо. І лише 14 судових рішень [14] було піддано подальшому опрацюванню.

Судові рішення для аналізу було представлено у вигляді ухвал, зміст яких говорив про перебування проваджень на етапі досудового розслідування. Досудове розслідування у 78,6 % випадків здійснювали органи Національної поліції України.

За хронологією найбільше таких рішень ухвалено у 2023 та 2024 роках (переважно у шахрайствах), що демонструє зростання активності сторін у судових процесах у згаданий період (*графік*).

Хронологія прийняття судових рішень

Одне із перших судових рішень (прийнято 2021 року) стосувалось шпигунства. За версією Головного управління СБ України у м. Києві та Київській області у кримінальному провадженні, відомості про яке 23.10.2019 року внесені до Єдиного реєстру досудових розслідувань за № 22019101110000179 за ознаками кримінального правопорушення, передбаченого ч. 1 ст. 114 КК України, громадянин Китайської Народної Республіки Чан, який є директором ТОВ «Голден Ег Технолоджі», з початку 2018 року почав проявляти значний інтерес до проектів, у тому числі, з обмеженим доступом, в сфері нанотехнологій, штучного інтелекту, медичної інженерії, теплоенергетики [15].

Найчастіше судові рішення приймалися в судах Києва та Одеси, особливо в Печерському районному суді Києва, що був найбільш активним.

Стаття 190 Кримінального кодексу України «Шахрайство» є найпоширенішою в цих рішеннях – вона зустрічається у 9 випадках, тоді як інші статті Кримінального кодексу України, наприклад, де гіпотези норми, пов'язані з крадіжкою чужого майна, прийняттям пропозиції, обіцянки або одержанням неправомірної вигоди службовою особою та інші, з'являються поодиноко.

Технології штучного інтелекту найчастіше у змісті судових рішень представлено зв версією слідства як засоби «підробки голосу чи повідомлення» або «привернення уваги», що вказує на характер використання його зловмисниками, особливо у шахрайських схемах (*таблиця*).

Таблиця

Згадування в судових рішеннях технології штучного інтелекту

Контекст згадування у судовому рішенні технології штучного інтелекту у якості засобу або предмету кримінального правопорушення	**ч. 2 ст. 109 КК**	**ч. 1 ст. 114 КК**	**ч. 4 ст. 185 КК**	**ч. 2 ст. 188-1, ч. 2 ст. 209, ч. 2 ст. 361 КК**	**ст. 190 КК**	**ч. 3 ст. 190, ч. 2 ст. 309 КК**	**ч. 3 ст. 368 КК**	**Всього згадувань**

Контекст згадування у судовому рішенні технології штучного інтелекту у якості засобу або предмету кримінального правопорушення	**ч. 2 ст. 109 КК**	**ч. 1 ст. 114 КК**	**ч. 4 ст. 185 КК**	**ч. 2 ст. 188-1, ч. 2 ст. 209, ч. 2 ст. 361 КК**	**ст. 190 КК**	**ч. 3 ст. 190, ч. 2 ст. 309 КК**	**ч. 3 ст. 368 КК**	**Всього згадувань**
засіб прикриття нелегальної діяльності				1				**1**
засіб підробки голосу або повідомлення	1				4		1	**6**
засіб привернення уваги			1		4	1		**6**
предмет посягання		1						**1**
Всього судових рішень за статтями КК України		**1**	**1**	**1**	**8**	**1**	**1**	**14**

Цілком можливе використання зловмисниками штучного інтелекту у якості засобу підробки голосу чи повідомлення доречно навести такою ілюстрацією: «допитана в якості потерпілого ОСОБА_4, пояснив наступне: 17.07.2023 приблизно о 18:06 мені надійшло повідомлення у соціальній мережі «Viber», від «ЄПідтримки» про те, що я можу отримати грошову допомогу у розмірі 6500 гривень, та разом із цим повідомленням прийшло повідомлення з посиланням на мобільний додаток «ІНФОРМАЦІЯ_2», як пізніше виявилося, що це був не справжній додаток та ввів усі свої данні банківської картки, після чого мені зателефонував «ІНФОРМАЦІЯ_2» із номеру НОМЕР_1, а саме штучний інтелект «Софія», який сказав мені увести 4 цифри у поле, яке з'явилося у мене на екрані телефону, після чого в мене знялися грошові кошти у розмірі 6300 гривень, я намагався зробити знімок екрану переписки, але вона була ними видалена» [16].

Інший випадок стосувався використання інформації про штучний інтелект, як засобу для привернення уваги жертви. Так, «ОСОБА_4 16.03.2023 близько 19 год. 30 хв. за допомогою власного мобільного телефону та інтернет-платформі Playmarket знайшов програму під назвою (посилання ІНФОРМАЦІЯ_2). В описі пояснюється, що програма є штучним інтелектом, який піклується про формалізацію проблем завдань та завантажив

вказану програму. Під час спроби авторизуватися для створення облікового запису його перенаправили на програму за посиланням ІНФОРМАЦІЯ_3 , де він вказав свої дані» [17]. Після цих дій на мобільний телефон жертви надійшло повідомлення про купівлю товару на суму 1497,75 грн з її банківської картки. Потерпілий стверджує, що нічого не купував, сам не здійснював грошові перекази.

Як бачимо, з'явилась та набуває зростання тенденція, коли фіксується використання злочинцями технологій штучного інтелекту, а сама технологія – потенційний предмет шпіонажу. Вбачається, що у перспективі від одного до 5 років зі збереженням поточних умов ми зможемо констатувати збільшення кримінальних правопорушень, де предметом або засобом вчинення є технологія штучного інтелекту. Це можемо розглядати, як виклик для системи підготовки фахівців із кримінального аналізу. Саме тому вкрай необхідне переосмислення підготовки фахівців з кримінального аналізу не тільки з урахуванням знань з використання ними штучного інтелекту, а й щодо делікту, де предметом або засобом вчинення є штучний інтелект, та особливостей їх залучення до розслідування. Одним із таких напрямів підготовки може бути опанування засобів та методів, що виявляють ознаки підробки сутностей, безпосередньо пов'язаних із штучним інтелектом.

Список використаних джерел

1. Узлов Д.Ю. Використання методів і технологій штучного інтелекту в кримінальному аналізі. Застосування інформаційних технологій в діяльності НПУ: матеріали Наук.-практ. семінару, Харків, 21 грудня 2018 р. Х.: Права людини, 2018. С. 17–19.

2. Биков І.О. Інформаційно-аналітичне забезпечення діяльності слідчих та оперативних підрозділів у боротьбі з економічними злочинами. Право і суспільство. 2024. № 1. Т. 2. С. 392–396. DOI: https://doi.org/10.32842/2078-3736/2024.1.2.59.

3. Батраченко Т.С., Розгон О.Г. Використання кримінального аналізу в боротьбі зі злочинністю: сучасні виклики та перспективи. Право і суспільство. 2024. № 7. Т. 2. С. 309–311. DOI: https://doi.org/10.32782/2524-0374/2024-7/75.

4. Макаренко В., Кисельов А. Інтегрування системи штучного інтелекту в кримінальний аналіз. Grail of Science. 2024. № 35. С. 102–106. DOI: https://doi.org/10.36074/grail-of-science.19.01.2024.017.

5. Пядишев В.Г. Перспективи розвитку проактивної діяльності поліції: зарубіжний погляд. Актуальні питання юридичної науки. 2024. № 1. Т. 2. С. 403–412. DOI: https://doi.org/10.32842/2078-3736/2024.1.2.61.

6. Струков В.М. Інструментальні інтелектуальні платформи для кримінального аналізу. Право і безпека. 2021. № 4 (83). С. 64–79. DOI: https://doi.org/10.32631/pb.2021.4.07.

7. Яровий К. Інтеграція штучного інтелекту у правоохоронну діяльність. Юридичний вісник. 2024. № 2. С. 68–76. DOI: https://doi.org/10.32782/yuv.v2.2024.9.

8. Корнейко О.В., Школьніков В.І., Овсянюк Д.І. Використання сучасних інформаційно-аналітичних технологій в діяльності центру кримінальної аналітики Національної академії внутрішніх справ. Інформаційні технології в освіті та практиці: матеріали Всеукр. наук.-практ. конф. (Львів, 18 груд. 2020 р.). Львів, 2020. С. 8-11; Овсянюк Д. І. Удосконалення навичок збору інформації з відкритих джерел (OSINT) в умовах воєнного стану в закладах вищої освіти зі специфічними умовами навчання, які здійснюють підготовку поліцейських. Збірники наукових праць, матеріали конференцій (семінарів, круглих столів). Київ: НАВС, 2024. С. 103–106. URL: https://elar.naiau.kiev.ua/handle/123456789/30594; Корнейко О. В., Худенко Д. М. Підготовка кримінальних аналітиків у Національній академії внутрішніх справ: історія та досвід. Збірники наукових праць, матеріали конференцій (семінарів, круглих столів). Київ: НАВС, 2022. С. 90–93. URL: http://elar.naiau.kiev.ua/jspui/handle/123456789/24808;
Корнейко О. В., Школьніков В. І. Підготовка нової генерації «цифрових оперативників» в Національній академії внутрішніх справ. Інформаційні технології в освіті та практиці: матеріали Всеукр. наук.-практ. конф. (Львів, 17 груд. 2021 р.) / упоряд. Т. В. Магеровська. Львів: ЛьвДУВС, 2021. С. 41–42; Мовчан А. В. Характеристика структури та моделі професійної підготовки фахівців з кримінального аналізу. Законодавче забезпечення діяльності Бюро економічної безпеки України. Київ: НАВС, 2021. С. 183–185; Ханькевич А. М. Оволодіння основами кримінального аналізу як засіб підвищення компетентності оперативних працівників кримінальної поліції. Сучасні проблеми правового, економічного та соціального розвитку держави : тези доп. VIII Міжнар. наук.-практ. конф. (м. Харків, 6 груд. 2019 р.). Харків : ХНУВС, 2019. С. 140–143.

9. Розпорядження Кабінету Міністрів України від 13 квітня 2024 р. № 320-р «Про схвалення Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року». URL: https://zakon.rada.gov.ua/laws/show/320-2024-%D1%80#Text.

10. Єдиний державний реєстр судових рішень України. URL: https://reyestr.court.gov.ua/.

11. Ухвала Ужгородського міськрайонного суду Закарпатської області від 20.07.2021 у справі № 308/7867/21. – URL: https://reyestr.court.gov.ua/Review/98435140.

12. Ухвала Уманського міськрайонного суду Черкаської області від 08.07.2024 № 705/3849/24. URL: https://reyestr.court.gov.ua/Review/120250992.

13. Ухвала Шевченківський районного суду м. Львова від 01.11.2017 у справі № 466/6967/17. URL: https://reyestr.court.gov.ua/Review/70908364.

14. Ухвала Печерського районного суду м. Києва від 21.04.2021 у справі № 757/21307/21-к. URL: https://reyestr.court.gov.ua/Review/96585631; Ухвала Печерського районного суду м. Києва від 01.10.2021 у справі № 757/43441/21-к. URL: https://reyestr.court.gov.ua/ Review/104416403; Ухвала Печерського районного суду м. Києва від 13.12.2022 у справі № 757/35689/22-к. URL: https://reyestr.court.gov.ua/Review/108021992; Ухвала Фастівського міськрайонного суду Київської області від 24.04.2023 у справ № 381/477/23. URL: https://reyestr.court.gov.ua/ Review/110412773; Ухвала Стрийського районного суду Львівської області від 26.07.2023 у справі №463/6244/23. URL: https://reyestr.court.gov.ua/Review/112590868; Ухвала Шевченківського районного суду м. Києва від 06.09.2023 у справі № 638/11185/23. URL: https://reyestr.court.gov.ua/Review/113286919; Ухвала Залізничного районного суду м. Львова від 20.10.2023 у справі № 462/7896/23. URL: https://reyestr.court.gov.ua/ Review/114322319; Ухвала Вінницького міського суду Вінницької області від 11.03.2024 у справі № 127/7820/24. URL: https://reyestr.court.gov.ua/Review/117696764; Ухвала Ленінського районного суду м. Запоріжжя від 21.03.2024 у справі № 334/2256/24. URL: https://reyestr.court.gov.ua/ Review/117862664; Ухвала Дніпровського районного суду м. Києва від 26.03.2024 у справі № 453/500/24. URL: https://reyestr.court.gov.ua/Review/ 117969013; Ухвала Октябрського районного суду м. Полтави від 30.04.2024 у справі № 554/4146/24. URL: https://reyestr.court.gov.ua/

Review/118775517; Ухвала Київського районного суду м. Одеси від 26.08.2024 у справі № 947/17948/24. URL: https://reyestr.court.gov.ua/Review/121194815; Ухвала Приморського районного суду м. Одеси від 10.09.2024 у справі № 522/25297/21. URL: https://reyestr.court.gov.ua/Review/121524211; Ухвала Суворовського районного суду м. Одеси від 16.09.2024 у справі № 523/14956/24. URL: https://reyestr.court.gov.ua/Review/121748039.

15. Ухвала Печерського районного суду м. Києва від 21.04.2021 у справі № 757/21307/21-к. URL: https://reyestr.court.gov.ua/Review/96585631.

16. Ухвала Шевченківського районного суду м. Києва від 06.09.2023 у справі № 638/11185/23. URL: https://reyestr.court.gov.ua/Review/113286919.

17. Ухвала Фастівського міськрайонного суду Київської області від 24.04.2023 у справ № 381/477/23. URL: https://reyestr.court.gov.ua/Review/110412773.

Шаповаленко Євген Володимирович,
кандидат юридичних наук, доцент,
т.в.о. завідувача кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ

ОСОБЛИВОСТІ ВЗАЄМОДІЇ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ З ІНШИМИ ПРАВООХОРОННИМИ ОРГАНАМИ ПІД ЧАС ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ, ПЕРЕДБАЧЕНИМ СТ. 407–409 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ

У Конституції України проголошується: «Захист Вітчизни, незалежності та територіальної цілісності України, шанування її державних символів є обов'язком громадян України. Громадяни відбувають військову службу відповідно до закону». Забезпечення внутрішньої й зовнішньої безпеки України завжди є актуальною проблемою держави. За сучасних умов, коли Україна знаходиться, під час дії правового режиму воєнного стану, це відчутно впливає на стан злочинності в різноманітних сферах життєдіяльності й державності, в тому числі й у Збройних Силах України та інших військових формуваннях, створених відповідно до законодавства.

Посилаючись на статистичні дані Офісу Генерального прокурора, зауважимо, що в період з січня по вересень 2024 року, спостерігаються негативні тенденції проявів злочинності, пов'язані з різноманітними посяганнями на встановлений порядок несення військової служби, що, безперечно, впливає на забезпечення національної безпеки України. Так за статистичними даними:

– ст. 407 КК України (Самовільне залишення військової частини або місця служби), обліковано 34329 кримінальних правопорушень з них лише 3431 особам вручено повідомлення про підозру та 1418 проваджень направлено до суду;

– ст. 408 КК України (Дезертирство), обліковано 18126 кримінальних правопорушень з них лише 507 особам вручено повідомлення про підозру та 175 проваджень направлено до суду;

– ст. 409 КК України (Ухилення від військової служби шляхом самокалічення або іншим способом) обліковано 220 кримінальних правопорушень з них лише 61 особам вручено повідомлення про підозру та 48 проваджень направлено до суду [1].

З метою вдосконалення взаємодії між правоохоронними органами була затверджена міжвідомча Інструкція щодо взаємодії органів прокуратури, Державного бюро розслідувань, Національної поліції України, Служби безпеки України, Військової служби правопорядку у Збройних Силах України під час протидії кримінальним правопорушенням, передбаченим статтями 407–409 Кримінального кодексу України [2].

Зазначена Інструкція зазначає взаємодію між правоохоронними органами держави під час виконання покладених на них завдань щодо протидії ухиленню від військової служби, посилення обороноздатності держави під час дії правового режиму воєнного стану, здійснення спільних заходів із запобігання, виявлення, припинення, розкриття та розслідування кримінальних правопорушень, передбачених статтями 407–409 КК України.

Одна із функцій підрозділів кримінальної поліції Національної поліції України є взаємодія зі структурними підрозділами центрального органу управління поліцією, правоохоронними органами іноземних держав з питань міждержавного та міжнародного розшуку, здійснення розшуку підозрюваних та обвинувачених, безвісти зниклих громадян та ідентифікації невпізнаних трупів.

На підрозділи Національної поліції України та Служби безпеки України покладається здійснення оперативно-розшукової діяльності та досудового розслідування кримінальних правопорушень зазначеної категорії (за дорученням прокурора), реалізація передбачених кримінальним процесуальним законодавством норм, пов'язаних із виконанням доручень слідчого або прокурора, а також участь у спільних заходах щодо розшуку підозрюваних за фактами вчинення ними кримінальних правопорушень, передбачених статтями 407-409 КК України.

Під час здійснення розшукової роботи вищезазначених осіб, передбачається реалізація спільних заходів:

– обмін інформацією, яка може бути використана як джерело доказів, встановлення місцезнаходження військовослужбовців тощо;

– здійснення оперативно-розшукових та інших заходів, спрямованих на встановлення місцезнаходження військовослужбовців, які вчинили кримінальні правопорушення, передбачені статтями 407–409 КК України;

– створення міжвідомчих слідчих груп для забезпечення здійснення досудового розслідування у розумні строки, вжиття заходів щодо встановлення місцезнаходження військовослужбовців, їх затримання та притягнення до кримінальної відповідальності;

– вивчення причин та умов, що сприяють вчиненню кримінальних правопорушень цієї категорії;

– проведення нарад, розроблення й уточнення планів стосовно здійснення розшуку військовослужбовців, які вчинили самовільне залишення військової частини або місця служби, дезертирство, ухилення від військової служби шляхом самокалічення або іншим способом, а також проведення профілактичної роботи з розподілом виконання завдань між правоохоронними органами [2].

Підсумовуючи, варто зазначити, що підрозділи кримінальної поліції Національної поліції України найчастіше виявляють військовослужбовців, які самовільно залишили військову частину, здійснили дезертирство та ухиляються від військової служби шляхом самокалічення або іншим способом. Своєчасна та ретельно налагоджена взаємодія реально може вплинути на хід досудового розслідування через своєчасність повідомлень правоохоронних органів та вжиття заходів щодо розшуку військовослужбовців.

Список використаних джерел

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

2. Про затвердження Інструкції щодо взаємодії органів прокуратури, Державного бюро розслідувань, Національної поліції України, Служби безпеки України, Військової служби правопорядку у Збройних Силах України під час протидії кримінальним правопорушенням, передбаченим статтями 407–409 Кримінального кодексу України: наказ ДБР, ОГП, МВС, МОУ, СБУ України від 03.10.2024 № 375/223/672/657/485.

Шендрик Владислав Володимирович,
доктор юридичних наук, професор,
заступник начальника Інституту
Національного юридичного
університету імені Ярослава Мудрого

ПРЕДИКТИВНА АНАЛІТИКА BIG DATA В ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Сучасні виклики національній безпеці України характеризуються різноманіттям загроз та стрімкою динамікою їх видозмінення. Російська збройна агресія, гібридні впливи, кібератаки та інші деструктивні чинники вимагають від Служби безпеки України (далі – СБ України) впровадження новітніх підходів до організації своєї діяльності. Особливої актуальності набуває потреба переходу від реактивної моделі реагування на загрози до проактивної, що базується на передбаченні та упередженні протиправних дій.

Ефективним інструментом такого переходу є предиктивна аналітика Big Data – сукупність методів інтелектуального аналізу даних, спрямованих на прогнозування майбутніх подій на основі історичних даних. У контексті діяльності СБ України предиктивна аналітика дозволяє виявляти приховані закономірності та взаємозв'язки в масивах різнорідної інформації, формувати прогнозні сценарії розвитку безпекової ситуації.

Предиктивна аналітика – це галузь передової аналітики, яка використовується для прогнозування невідомих майбутніх подій. Предиктивна аналітика використовує багато методів з інтелектуального аналізу даних, статистики, моделювання, машинного навчання та штучного інтелекту для аналізу

поточних даних з метою прогнозування майбутнього. Вона використовує ряд методів інтелектуального аналізу даних, прогнозного моделювання та аналітичних методів, щоб об'єднати управління, інформаційні технології та моделювання процесів, щоб зробити прогнози про майбутнє. Виявлені закономірності можуть бути використані для визначення ризиків і можливостей у майбутньому. Моделі предиктивної аналітики фіксують взаємозв'язки між багатьма факторами для оцінки ризику з певним набором умов для присвоєння балів або ваги [1].

Технологічною основою предиктивної аналітики є Big Data – технології обробки структурованих і неструктурованих даних надвеликих обсягів. Для СБ України, яка в межах визначеної законом компетенції здійснює контррозвідувальну, оперативно-розшукову діяльність та досудове розслідування, застосування інструментів Big Data відкриває принципово нові можливості. Йдеться про автоматизовану обробку значних масивів даних з різних джерел, виявлення прихованих зв'язків між об'єктами оперативної уваги, прогнозування потенційних загроз державній безпеці.

Водночас впровадження технологій предиктивної аналітики Big Data в діяльність СБ України потребує належного нормативно-правового, організаційного та технічного забезпечення. Актуальним залишається пошук балансу між ефективністю аналітичної роботи та захистом прав і свобод громадян.

Впровадження сучасних аналітичних інструментів у діяльність СБ України має ґрунтовну правову основу, закладену в профільному законі, який визначає ключові можливості Служби щодо використання інноваційних технологій аналізу даних.

Аналіз правових засад впровадження предиктивної аналітики в діяльність спецслужби виявляє цікаву особливість: хоча безпосередньо термін «предиктивна аналітика» в законодавстві не згадується, його застосування органічно випливає з покладеного на СБ України обов'язку здійснення інформаційно-аналітичної роботи (п. 1 ч. 1 ст. 24 Закону України «Про Службу безпеки України»). Фундаментальним аспектом виступає законодавче закріплення в системі Центрального управління СБ України окремого інформаційно-аналітичного підрозділу (ч. 1 ст. 10), що з практичної точки зору відкриває широкі можливості для розбудови потужного аналітичного потенціалу спеціальної служби [2]. Інституційне оформлення аналітичної складової

створює організаційне підґрунтя для системного впровадження технологій предиктивної аналітики та обробки великих даних.

Визначальною нормою, яка розкриває сутнісний зміст аналітичної діяльності СБ України, постає законодавчо закріплений обов'язок здійснювати інформаційно-аналітичну роботу в інтересах ефективного проведення органами державної влади внутрішньої і зовнішньої діяльності (п. 1 ч. 1 ст. 24) [2]. Практична реалізація зазначеного обов'язку в сучасних умовах об'єктивно потребує використання передових технологій аналізу даних, здатних забезпечити якісно новий рівень інформаційно-аналітичної підтримки державного управління.

Надзвичайно важливим правовим підґрунтям для розгортання сучасних систем обробки даних виступає закріплене за СБ України право створювати інформаційні системи та вести оперативний облік (п. 12 ч. 1 ст. 25) [2]. Зазначене положення набуває особливої актуальності в контексті необхідності роботи з надвеликими масивами різнорідної інформації при вирішенні завдань забезпечення державної безпеки.

З практичної точки зору вагомим інструментом формування необхідної інформаційної бази для застосування технологій предиктивної аналітики Big Data постає право СБ України одержувати від державних органів, підприємств та організацій дані і відомості, необхідні для забезпечення державної безпеки (п. 3 ч. 1 ст. 25) [2]. При цьому законодавчо визначені межі використання отриманої інформації створюють правові запобіжники від можливих зловживань.

Потужним драйвером розвитку аналітичного потенціалу СБ України виступає законодавчо закріплене право на проведення наукових досліджень і дослідно-конструкторських робіт та впровадження їх результатів у практичну діяльність (п. 15 ч. 1 ст. 24) [2]. Зазначена норма уможливлює не лише використання наявних аналітичних інструментів, але й розробку власних інноваційних рішень, максимально адаптованих під специфічні завдання контррозвідувального захисту державних інтересів.

Принципово важливим при цьому залишається дотримання визначених законом обмежень щодо компетенції СБ України (ст. 2) та забезпечення прав і свобод людини (ст. 5) [2]. Саме баланс між ефективністю аналітичної роботи та дотриманням правових гарантій створює передумови для етичного використання сучасних технологій аналізу Big Data в інтересах державної безпеки.

Аналізуючи законодавчі засади використання можливостей предиктивної аналітики в діяльності СБ України, визначені статтями 24, 25 профільного закону, важливо підкреслити практичний потенціал цієї технології для підвищення ефективності проведення контррозвідувальної та оперативно-розшукової діяльності. Адже саме інформаційно-аналітична робота, згідно із законом про Службу безпеки України є одним з основних обов'язків спецслужби.

У контексті оперативно-розшукової діяльності застосування технологій предиктивної аналітики Big Data набуває особливого значення через її спрямованість на пошук і фіксацію фактичних даних про протиправні діяння та отримання інформації в інтересах безпеки громадян, суспільства і держави (ст. 1 Закону України «Про Оперативно-розшукову діяльність») [4]. При цьому глибинний аналіз великих масивів даних створює принципово нові можливості для виявлення прихованих закономірностей та взаємозв'язків, що можуть вказувати на підготовку протиправних дій.

Ще більш широкі перспективи відкриває впровадження предиктивної аналітики Big Data у сфері контррозвідувальної діяльності, де основним завданням є своєчасне виявлення та запобігання загрозам державній безпеці (ст. 1 Закону України «Про контррозвідувальну діяльність») [5]. Особливо цінним тут стає потенціал прогностичного моделювання для виявлення ознак підготовки розвідувально-підривної діяльності спеціальних служб іноземних держав.

Таким чином, фундаментальною перевагою використання Big Data є можливість переходу від реактивної до проактивної моделі забезпечення державної безпеки. Предиктивна аналітика дозволяє не просто реагувати на загрози, а передбачати їх виникнення на основі комплексного аналізу великих масивів даних.

За дослідженням Business Insider, важливість цього напряму підтверджується зростанням світового ринку предиктивної аналітики до $20,41 млрд у 2022 році через зростаючу потребу в інтелектуальних рішеннях для підвищення ефективності безпекової діяльності. Дослідження Forbes показало, що 86 % організацій, які впровадили предиктивну аналітику, відзначають суттєве підвищення ефективності своєї діяльності [3; 4].

Особливу цінність предиктивна аналітика має для інформаційно-аналітичної роботи СБУ, дозволяючи на основі

аналізу великих даних формувати обґрунтовані прогнози розвитку безпекової ситуації. Як зазначає Ю. Городецький, предиктивна аналітика забезпечує якісно новий рівень інформаційно-аналітичної підтримки прийняття управлінських рішень [7].

Стрімка цифровізація суспільних відносин та експоненціальне зростання обсягів даних, що генеруються в цифровому середовищі, створюють нові можливості для підвищення ефективності діяльності спеціальних служб через впровадження технологій Big Data та предиктивної аналітики. Водночас використання цих інструментів у сфері забезпечення державної безпеки потребує належного правового регулювання, що актуалізує питання вдосконалення відповідної нормативної бази.

Необхідність вдосконалення нормативної бази для ефективного впровадження технологій Big Data у діяльність СБ України зумовлена об'єктивними викликами цифрової епохи, коли стрімкий розвиток інформаційних технологій випереджає наявне правове регулювання.

Першим викликом постає відсутність у чинному законодавстві чітко визначених механізмів регулювання збору та обробки масивів цифрової інформації, хоча загальні норми про інформаційно-аналітичну діяльність СБ України створюють для цього базові передумови. Це породжує правову невизначеність щодо допустимих меж та методів аналізу даних у контексті виконання завдань забезпечення державної безпеки.

Другим важливим аспектом виступає потреба врегулювання питань інтеграції інформаційних масивів різних державних органів та приватних структур. Ефективність предиктивної аналітики Big Data безпосередньо залежить від можливості комплексного аналізу даних з різних джерел, що вимагає створення відповідних правових механізмів міжвідомчого обміну інформацією.

Третім фундаментальним викликом є забезпечення балансу між підвищенням ефективності аналітичної роботи та захистом конституційних прав і свобод громадян. Чинні механізми контролю та нагляду за законністю діяльності спеціальних служб потребують адаптації до специфіки роботи з Big Data.

Окремого законодавчого врегулювання потребують також питання правового статусу та режиму використання Big Data, впровадження стандартів якості аналітичної інформації, правил

транскордонної передачі даних та забезпечення кібербезпеки інформаційних систем.

Таким чином, вдосконалення нормативної бази має створити цілісний правовий механізм використання технологій Big Data при збереженні необхідних гарантій захисту як прав людини, так і інтересів державної безпеки. Це дозволить СБ України ефективно використовувати потенціал сучасних аналітичних інструментів для виявлення та протидії актуальним загрозам.

Список використаних джерел

1. What is Predictive Analytics? Pat Research. URL: https://www.predictiveanalyticstoday.com/what-is-predictive-analytics/#reply-form.

2. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII : станом на 2 серп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text.

3. Бахарєва Я. В. Розвиток предикативної аналітики як пріоритетного напрямку бізнес-аналітики. *Ефективна економіка*. 2018. № 5. URL: http://www.economy.nayka.com.ua/pdf/5_2018/152.pdf.

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

5. Про контррозвідувальну діяльність : Закон України від 26.12.2002 № 374-IV : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text.

6. Predictive Analytics Market Growing at a CAGR of 22.1% During 2017 to 2022 Says a New Research Report at ReportsnReports. *markets.businessinsider.com*. URL: https://markets.businessinsider.com/news/stocks/predictive-analytics-market-growing-at-a-cagr-of-22-1-during-2017-to-2022-says-a-new-research-report-at-reportsnreports-1002265911.

7. Городецький Ю. Д. Предиктивна аналітика та її роль у прийнятті стратегічних рішень у маркетингу. *Journal of Strategic Economic Research*. 2023. № 5. С. 65–72. URL: https://doi.org/10.30857/2786-5398.2023.5.7.

Школьніков Владислав Ігорович,
доктор філософії в галузі права, доцент кафедри кримінології та інформаційних технологій Національної академії внутрішніх справ

АСПЕКТИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ОБРОБКИ Й АНАЛІЗУ РУХУ ГРОШОВИХ КОШТІВ ЗА БАНКІВСЬКИМИ РАХУНКАМИ

Сучасні технології дозволяють правоохоронними органам ефективно ідентифікувати ризики в сфері корупції та тіньової економіки на основі аналізу інформації про рух грошових коштів за банківськими рахунками. Будь-яка інформація в електронній (цифровій) формі може бути неструктурованою та наявною у великих обсягах, що зумовлює необхідність використання спеціалізованих методик обробки та аналізу такої інформації.

Частина 3 статті 62 Закону України «Про банки та банківську діяльність» дозволяє реалізувати практику отримання на підставі запиту компетентного органу відомостей на конкретно визначену дату або за конкретний проміжок часу та стосовно конкретної юридичної або фізичної особи, фізичної особи-підприємця про:

1) наявність рахунків, номери рахунків;
2) інформацію про унікальні ідентифікатори та/або номери емісійних платіжних інструментів;
3) залишок коштів на рахунках;
4) операції списання з рахунків та/або зарахування на рахунки;
5) призначення платежу;
6) ідентифікаційні дані контрагента (для фізичних осіб – прізвище, ім’я та по батькові, ідентифікаційний номер платника податку; для юридичних осіб – повне найменування, ідентифікаційний код у Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань);
7) номер рахунку контрагента;
8) інформацію про унікальні ідентифікатори та/або номери емісійних платіжних інструментів контрагента;
9) єдиний ідентифікатор Національного банку України (код ID НБУ) надавача платіжних послуг контрагента;
10) найменування надавача платіжних послуг контрагента.

Зазвичай у працівника, який на правових підставах отримав виписку за банківським рахунком клієнта, можуть виникати проблеми обробки та аналізу такої інформації з наступних причин:

1) надана інформація не відповідає вимогами, викладеним в додатку до постанови правління Національного банку України від 14.07.2006 року № 267;

2) надана інформація неструктурована;

3) надана інформація у великих обсягах;

4) суми відображені в копійках;

5) не зазначається напрямок руху грошових коштів (дебет або кредит);

6) призначення платежу містить важливі для аналізу дані у неструктурованому вигляді;

7) в одному файлі міститься інформація про різні цільові банківські рахунки щодо яких надсилався запит або здійснювався тимчасовий доступ речей і документів.

Для вирішення вищевказаних проблем необхідно використовувати технології обробки та аналізу інформації. На сьогодні за допомогою програмних продуктів, мов програмування або технологій баз даних можливо ефективно здійснювати обробку та аналіз даних. Для звичайного користувача складність полягатиме в засвоєнні технічних аспектів використання тих або інших програмних продуктів, мов програмування або технологій баз даних.

Працівниками Національної академії внутрішніх справ на постійний основі ведеться розробка спеціалізованого програмного забезпечення, яке може бути використане не тільки в освітньому процесі під час підготовки та перепідготовки кримінальних аналітиків, але і в практичній діяльності правоохоронних органів України [1]. Тому для автоматизації процесів обробки та аналізу руху грошових коштів за банківськими рахунками науковими та науково-педагогічними працівниками Національної академії внутрішніх справ було розроблено спеціалізоване програмного забезпечення “Bankir-v.2.0”, яке має наступні функціональні можливості:

1) автоматизоване створення запитів на отримання банківської інформації на підставі обробки файлу з реєстраційними даними юридичної особи або фізично особи-підприємця;

2) обробка файлів із різноманітною структурою даних про рух грошових коштів за банківським рахунком;

3) автоматизоване визначення напряму руху грошових коштів (дебет або кредет);

4) конвертація валюти за курсом на дату проведення банківської транзакції;

5) конвертація сум, що зазначені у копійках, у гривню;

6) візуалізація взаємозв'язків між контрагентами;

7) автоматизоване визначення ланцюгу виводу грошових коштів з банківських рахунків;

8) автоматизоване визначення ланцюгу вводу грошових активів на банківські рахунки;

9) виокремлення даних із поля про призначення банківської транзакції (прізвище, ім'я, по батькові – для фізичної особи; назву – для юридичної особи; РНОКПП або код ЄДРПОУ; адрес; номерів телефонів; паспортних даних);

10) створення в автоматизованому режимі шаблону протоколу огляду інформації про рух грошових коштів за банківськими рахунками.

Список використаних джерел

1. Школьніков В.І. Автоматизація процесів обробки й аналізу інформації з використанням програмного забезпечення. Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України : зб. тез доп. міжвідом. наук.-практ. конф., 11 серп. 2022, с. 191–192.

2. Школьніков В. І. Види аналітичних технологій та їхня класифікація (досвід Національної поліції України). Вісник Національного технічного університету України «Київський політехнічний інститут». 2023. Вип. 3. С. 110–125. DOI: https://doi.org/10.20535/2308-5053.2023.3(59).295011.

3. Комп'ютерна програма "Встановлення фактів кримінальних правопорушень, вчинених шляхом кредитно-фінансових операцій" / свідоцтво про реєстрацію авторського права на твір № 95245 // Орлов Ю. Ю., Корнейко О. В; Школьніков В. І. Нац. акад. внутр. справ. 2023; Зареєстр. 05.12.2023. URL: https://iprop-ua.com/cr/ztu7vls7.

Комп'ютерна програма "Автоматизоване формування запитів на отримання банківської інформації" / свідоцтво про реєстрацію авторського права на твір № 95250 // Орлов Ю. Ю., Корнейко О. В; Школьніков В. І. Нац. акад. внутр. справ. 2023; Зареєстр. 05.12.2023. URL: https://iprop-ua.com/cr/im3u5za2.

Яровий Кирило Васильович,
кандидат юридичних наук, старший
викладач кафедри кримінології
та інформаційних технологій
Національної академії внутрішніх справ

СТРАТЕГІЇ ПРОТИДІЇ СУЧАСНІЙ КІБЕРЗЛОЧИННОСТІ В МЕРЕЖІ DARKNET

Сучасний розвиток інформаційних технологій, окрім позитивного впливу, зумовлює також появу нових викликів у галузі кібербезпеки. Кіберзлочинність включає різноманітні види правопорушень, що здійснюються у цифровому середовищі з використанням мережевих технологій та методів анонімізації. Зокрема, актуальним залишається питання протидії кіберзлочинності в контексті мережі DarkNet, де тіньові онлайн-ринки та автоматизовані боти значно сприяють ескалації злочинної активності в кіберпросторі. Однак, незважаючи на актуальність досліджень у сфері кіберзлочинності зазначена проблема залишається багатогранною та вимагає комплексного підходу, що поєднує технологічні, організаційні та юридичні аспекти.

Своєю чергою тіньовий або глибинний Інтернет (Deep Web) охоплює значну частину мережі-Інтернет, який не підлягає індексації звичайними пошуковими системами. Окрім цього, глибинний Інтернет складається з веб-ресурсів, доступ до яких обмежується системами автентифікації, що унеможливлює їхній пошук за допомогою загальнодоступних пошукових механізмів. З огляду на вказане, особливу увагу слід приділити області мережі, відомій як DarkNet.

Поняття DarkNet відноситься до спеціалізованої частини Інтернету, яка гарантує анонімність користувачів та захищеність веб-сайтів від відстеження. Децентралізований характер DarkNet охоплює вебсайти, розташовані на серверах із прихованими IP-адресами, що забезпечує мінімальну можливість їх ідентифікації. Відсутність єдиного центру контролю в DarkNet створює умови для поширення нелегальної діяльності,

Зважаючи на погляди окремих дослідників, слід зазначити, що значна частина контенту мережі DarkNet містить легальний контент, однак, інша її сторона асоціюється з незаконною діяльністю, зокрема торгівлі забороненими товарами та послугами, включно торгівлею людьми [1, с. 323]. Важливою проблемою DarkNet є приховування кримінальної діяльності

через закриті форуми, які орієнтовані на експлуатацію потенційних жертв та просування незаконних послуг.

Українське законодавство не містить обмежень на використання програмного забезпечення та технічних засобів, які надають користувачам повну анонімність під час доступу до мережі DarkNet. Окрім того, існують технічні труднощі у блокуванні функціонування таких програмних продуктів і рішень. Дослідження можливостей ідентифікації осіб у мережах Інтернет та DarkNet є ключовим аспектом, що підкреслює необхідність розробки ефективних стратегій для протидії сучасній кіберзлочинності.

Доступ до мережі DarkNet можливий тільки за допомогою спеціалізованого програмного забезпечення, найпоширенішим з яких є браузер TOR (The Onion Router). TOR є спеціально налаштованим браузером, який дозволяє користувачам отримувати доступ до веб-сервісів способами, що ускладнюють або унеможливлюють їх відстеження.

TOR можуть користуватися особи для доступу до різноманітних ресурсів, до яких раніше було обмежено доступ [2, с. 98]. Варто зазначити, що не весь контент містить заборонений або аморальний характер, оскільки багато користувачів використовують зазначену технологію виключно для збереження анонімності в мережі-Інтернет.

Браузер TOR забезпечує захист даних за допомогою багаторівневого шифрування, яке передбачає передачу трафіку через три незалежні сервери, розташовані у різних частинах світу. Такий метод шифрування значно ускладнює можливість спостереження за діями користувача в мережі-Інтернет [3, с. 1087].

Водночас користувачі, залучені до незаконних операцій, таких як розповсюдження дитячої порнографії, торгівля наркотичними речовинами, людьми чи зброєю можуть бути виявлені правоохоронними органами, що застосовують спеціалізовані методи моніторингу для виявлення кіберзлочинців.

Зростання статистичних показників кіберзлочинності підкреслює необхідність посилення заходів кібербезпеки. DarkNet залишається одним із ключових осередків кіберзлочинної діяльності, що потребує розробки ефективних стратегій протидії та впровадження сучасних технологій моніторингу й контролю для зменшення ризиків у кіберпросторі.

Стратегічно важливим завданням державної політики України є розвиток державної системи стратегічного

планування, створення інтегрованої системи моніторингу, аналізу, прогнозування та прийняття рішень у сфері національної безпеки та оборони [4]. Зазначене включає забезпечення ефективної координації та злагодженого функціонування єдиної мережі ситуаційних центрів ключових державних органів у секторі безпеки та оборони, що сприятиме підвищенню рівня захищеності країни від сучасних загроз.

Між тим, дослідження сучасних стратегій протидії кіберзлочинності у DarkNet є вкрай актуальним і передбачає аналіз інноваційних методів відстеження анонімних дій, розробку нових технологій для моніторингу та оцінки ризиків, а також вироблення ефективних підходів до ідентифікації злочинних угруповань та припинення їх діяльності.

Враховуючи вищевикладене, необхідно зробити наступні висновки, що для ефективної протидії викликам у мережі-Інтернет необхідні не лише сучасні технічні заходи правоохоронних органів, а й удосконалення законодавства та міжнародне співробітництво. Важливо також підвищувати обізнаність користувачів щодо безпечного користування мережею DarkNet та можливих наслідків її порушення. Крім цього, слід досягти балансу між заходами безпеки та приватністю, забезпечити оперативне реагування на злочини та уникати порушень прав користувачів мережі DarkNet.

Список використаних джерел

1. Okhrimenko, Ivan M; Okhrimenko, Svitlana S; Yarovyi, Kyrylo V; Melnykov, Illia M; Kudinov, Vadym A; Marchenko, Olga G; Bordiyan, Yaroslav I. (2024) Motivational orientations of students towards internet dependent behavior and measures for its prevention Polski merkuriusz lekarski: organ Polskiego Towarzystwa Lekarskiego. 52 (3), 319-325. doi: 10.36740/Merkur202403108.

2. Ткачук Т. Ю. Тіньовий Інтернет: співвідношення можливостей і загроз. Інтернет речей: проблеми правового регулювання та впровадження : матеріали наук.-практ. конф., 24 жовт. 2017 р. Київ : Політехніка, 2017. С. 94–100.

3. Ahmed Ghappour, Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, 69 Stan. L. Rev. 1075, 1083 (2017); Restatement (Third) of the Foreign Relations Law of the United States § 432(2) (дата звернення 30.10.2024).

4. Про рішення Ради національної безпеки і оборони України від 26.05.2015 р. № 287/2015 «Про Стратегію національної безпеки України». URL: https://zakon.rada.gov.ua/laws/show/287/2015.

Богаченко Валерія Василівна,
курсант навчально-наукового інституту № 1
Національної академії внутрішніх справ;
Марков Михайло Миколайович,
кандидат юридичних наук, доцент, професор
кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ

КРИМІНАЛЬНИЙ АНАЛІЗ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Проблема впровадження сучасних методів роботи у діяльність правоохоронних органів України є надактуальною. Результативність діяльності у боротьбі зі злочинністю безпосередньо залежить від якісного, своєчасного і достатнього інформаційно-аналітичного забезпечення цієї діяльності. Сучасний рівень злочинності, вимагає від правоохоронних органів здійснення своєчасного, оперативного та достовірного аналізу діяльності організованих груп та злочинних організацій [1, с. 61].

У країнах Європейського Союзу, США та інших розвинених країнах світу, розуміючи потребу в здійснення кримінального аналізу, у боротьбі зі злочинністю використовують модель Intelligence-Led Policing (ILP – поліцейська діяльність, керована аналітикою), яка полягає в аналізі відомостей, здобутих шляхом специфічної поліцейської діяльності у сфері збирання інформації, а отримана оперативно-аналітична інформація є підставою для проведення операцій/розслідувань, а не навпаки.

Кримінальний аналіз можна визначити як діяльність аналітиків - працівників правоохоронних органів, що полягає у перевірці, оцінці та інтерпретації інформації про протиправні, кримінально карані діяння окремих осіб та груп, яка отримана в ході проведення оперативно-розшукової діяльності або під час досудового розслідування, а також у встановленні суттєвих зв’язків між вищевказаною інформацією з метою їх подальшого використання для визначення тактичних та стратегічних напрямків протидії та запобіганню злочинності.

В аналітичній роботі правоохоронних органів і служб використовується: оперативний аналіз; тактичний аналіз;

стратегічний аналіз; аналіз даних з відкритих джерел (OSINT); аналіз даних з багатьох джерел

(Multi-Source Analysis).

На сьогодні у підрозділах кримінального аналізу найбільш часто використовують оперативний кримінальний аналіз, який призначений для забезпечення оперативно-розшукових підрозділів необхідною інформацією в рамках роботи щодо оперативно-розшукових справ.

Оперативний кримінальний аналіз може здійснюватися у трьох формах:

1. аналіз, що супроводжує оперативно-розшукову діяльність (наявна інформація, що стосується справи, упорядковується, нова інформація відповідно співвідноситься та оцінюється, у поточному порядку формулюються гіпотези, які підтримуються доказами чи висновками або за їх допомогою спростовуються);

2. аналіз, який ведеться для підтримки оперативно-розшукової діяльності (аналітик бере на себе аналітичні завдання, представляє результати аналізу, займається пошуком інформації з власних баз тощо);

3. аналіз, що ініціює оперативно-розшукову діяльність.

Для проведення аналізу застосовуються сучасні аналітичні інструменти, відповідне програмне забезпечення, а також наявні інформаційні ресурси. Найбільш поширеним інструментом, що сьогодні використовується у повсякденній роботі органів Національної поліції, є Microsoft Office (Word та Excel), та лише в деяких департаментах застосовується аналітичне програмне забезпечення, зокрема IBM i2 Analyst's Notebook,Maltego, E-Gis maps, ArcGIS, тощо.

Пріоритетним напрямом діяльності інформаційно-аналітичних підрозділів Національної поліції України є вжиття комплексу заходів, спрямованих на успішну реалізацію та впровадження нових методів кримінального аналізу, що дасть можливість активно використовувати сучасні аналітичні технології для створення передумов ефективного виконання оперативними і слідчими підрозділами своїх завдань, підвищить ефективність документування та розкриття злочинів, що вчиняються за складними схемами, потребують обробки великих масивів даних [2, с. 150].

Також, важливо усвідомити, що кримінальний аналіз не збігається з кримінологічним дослідженням. Працівники кримінального аналізу працюють у динамічному середовищі з

постійно змінюючимся набором даних, що надходять щодня. Їх завдання – створювати інформацію, яка стане корисною для поліцейських дій. Навички, необхідні для аналізу та інтерпретації цих даних, можуть відрізнятися від стандартних методів кримінологічного дослідження.

Кримінальний аналіз є сучасним та важливим в діяльності Національної поліції України, що сприяє підвищенню ефективності правоохоронної діяльності. У результаті проведеного дослідження було виявлено, що застосування сучасних методів кримінального аналізу дозволяє значно покращити процеси розслідування злочинів, попередження кримінальних проявів та оптимізації використання ресурсів. Використання кримінального аналізу сприяє більш точному і швидкому виявленню злочинних схем та зв'язків між злочинцями, що значно скорочує час на розкриття злочинів. Завдяки аналізу кримінальних тенденцій та закономірностей поведінки злочинців, поліція має можливість розробляти ефективні стратегії профілактики та своєчасно реагувати на потенційні загрози [3, с. 399]. Кримінальний аналіз дозволяє більш раціонально розподіляти ресурси, зокрема людські та матеріальні, зосереджуючи їх на найбільш критичних напрямках діяльності. У цілому, аналітичні дані сприяють більш ефективній координації між різними підрозділами поліції та іншими правоохоронними органами, що підвищує загальну ефективність боротьби зі злочинністю. Загалом, впровадження та розвиток кримінального аналізу в діяльності Національної поліції України є необхідним кроком на шляху до створення сучасної, ефективної та прозорої правоохоронної системи та інтеграцію новітніх технологій для ще більш ефективного протидії злочинності.

Список використаних джерел

1. Гнусов Ю. В., Калякін С. В. Кримінальний аналіз у роботі підрозділів Національної поліції України. 2019. URL: https://search.app/fHaKyzC4xeHUDhN17.

2. Крутоголов А. В., Базаренко І. О., науковий керівник Кисельов А. О. Методи кримінального аналізу. Дніпровський державний університет внутрішніх справ. 2024. URL: https://search.app/dfPRkJCZzMfBbkz27.

3. Корнієнко М. В. Кримінальний аналіз у діяльності Національної поліції України. Одеський державний університет внутрішніх справ. 2024. URL: https://search.app/FtjDPVY2p8bsXH2x7.

Горобець Тетяна Мирославівна,
курсант навчально-наукового інституту № 1
Національної академії внутрішніх справ
Науковий керівник:
кандидат юридичних наук, доцент, професор
кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ
Марков М. М.

ВИКОРИСТАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ДЛЯ ПРОТИДІЇ ЗЛОЧИННОСТІ

Використання кримінального аналізу в розслідуванні злочинів є надзвичайно актуальним і важливим у сучасному правоохоронному середовищі. Кримінальний аналіз надає можливість систематично збирати, аналізувати та оцінювати інформацію, що стосується злочинів. Він дозволяє виявляти та аналізувати тенденції злочинів, встановлювати зв'язки між різними подіями та суб'єктами, а також забезпечує можливість прогнозування можливих ризиків та небезпек.

Взагалі, кримінальний аналіз становить собою дії, спрямовані на ідентифікацію і точне визначення взаємозв'язків між відомостями, які стосуються подій злочинного характеру, осіб, пов'язаних з ними та даними, що походять з різних джерел, і в подальшому їх використання слідчими органами, прокуратурою та судами. В цьому контексті недослідженим є питання визнання допустимості фактичних даних здобутих шляхом кримінального аналізу в кримінальному процесі України [1].

Кримінальний аналіз включає в себе систематичний аналіз доказів, отриманих в процесі слідства, з метою виявлення співвідношень та встановлення схеми подій. Він здійснюється шляхом використання різних методів аналізу, таких як логічне мислення, індуктивне та дедуктивне мислення, статистичний аналіз. У процесі кримінального аналізу важливо враховувати не лише прямі докази, а й вказівки, свідчення та інші обставини, що можуть мати значення для справи. Це дозволяє створити повну та достовірну картину подій та виявити можливі зв'язки, між різними аспектами кримінального провадження. Його ціль полягає у встановленні взаємозв'язків між фактами, подіями, суб'єктами та об'єктами злочинної діяльності з метою оптимізації управління правоохоронними органами на різних рівнях – від державного до територіального.

Визначають такі види кримінального аналізу:

Операційний (оперативний) кримінальний аналіз – це інформаційно-аналітична діяльність за конкретними кримінальними провадженнями стосовно інформації, що становить інтерес для кримінальної поліції або органів досудового розслідування поліції, осіб, об'єктів, організованих груп чи злочинних організацій, щодо ознак та інших відомостей, які їх характеризують і в подальшому сприятимуть розслідуванню правопорушень.

Тактичний кримінальний аналіз – аналіз злочинності та злочинів на конкретній території за невеликий проміжок часу, за певним видом злочину чи протиправної діяльності певної групи з метою напрацювання тактичних заходів із затримання злочинців, виявлення ризиків і попередження конкретних правопорушень.

Стратегічний кримінальний аналіз – ідентифікація та оцінювання кримінальних загроз особі, суспільству, державі, метою яких є визначення вразливості правоохоронної системи або середовища, та формування управлінських рішень щодо запобігання вчиненню кримінальних правопорушень і протидії злочинності (виявлення тенденцій, закономірностей, прогнозування розвитку встановлених загроз за великий період часу). Проводиться з метою підготовки стратегічних управлінських рішень та визначення ризиків розвитку криміногенної ситуації [2, ст. 29–31].

На базі використання різнопланових відомостей, кримінальний аналіз дозволяє встановлювати індивідуальну або групову приналежність різних об'єктів оперативної уваги підрозділів кримінальної поліції; досліджувати їх властивості та стан, результати і співвідношення різних факторів, що можуть на них певним чином впливати; прогнозувати подальший хід кримінальних подій; виявляти приховані взаємозв'язки між об'єктами тощо. Безсумнівно, вирішення поставлених перед оперативними підрозділами кримінальної поліції завдань багато в чому визначається ефективністю діяльності спеціалізованих підрозділів Управління кримінального аналізу, створеного у 2017 році.

Кримінальний аналіз дозволяє:

1) виявляти фактичні дані, що можуть бути доказами у кримінальному провадженні;

2) самостійно слідчому і прокурору виявляти факт вчинення кримінального правопорушення, вносити відомості до Єдиного реєстру досудових розслідувань та розпочинати розслідування;

3) отримати інформацію в рамках досудового розслідування кримінального провадження, яка матиме орієнтуюче значення [3].

Під час аналітичного процесу оцінюють інформацію щодо злочинця, перебіг подій, знарядь учинення злочину, часу й місця його вчинення тощо. Обіг цієї інформації відбувається між оперативними працівниками та слідчими й полягає не тільки в наданні або отриманні інформації, а й в активному її здобуванні.

Обробка великих обсягів інформації може бути здійснена лише за допомогою інтелектуальних технологій, щоб звільнити слідчого або оперативного працівника від тягаря та допомогти йому вжити відповідних заходів і прийняти процесуальні рішення. У сучасних умовах неможливо розкрити резонансні, тяжкі та особливо тяжкі кримінальні правопорушення без залучення кримінальних аналітиків та належної аналітичної оперативно-розшукової роботи під час розслідування та кримінального провадження.

Під час розслідування злочинів, кримінальний аналіз включає в себе докладне дослідження місця події, збір фізичних слідів, проведення експертизи, аналіз медичних документів, психологічні профілі підозрюваних, інтерв'ю з свідками та інші методи аналізу доказів. Цей процес допомагає правоохоронним органам встановити обставини злочину, визначити можливі мотиви та ідентифікувати винних осіб.

Майстерність у користуванні інтернет-ресурсами та базами даних вимагає спеціальних знань, навичок та умінь. Це підкреслює необхідність постійної самоосвіти аналітиків, їхнього постійного підвищення кваліфікації і участі в відповідних навчальних заходах та тренінгах. Дотримання аналітиками алгоритму та врахування особливостей процесу дослідження дозволить підвищити результативність аналітичної роботи. Для подальшого розвитку та впровадження кримінального аналізу в правоохоронну практику України доцільно вживати наступні заходи:

– забезпечити стале та стабільне фінансування;

– постійно підвищувати кваліфікацію кримінальних аналітиків;

– проводити постійну розробку нових та модернізацію наявних технічних засобів, впроваджувати інноваційні технології;

– розширювати сферу застосування кримінального аналізу як позитивного чинника у протидії злочинності та розширювати його географію застосування.

У висновку варто зазначити, що кримінальний аналіз є невід'ємною складовою правоохоронної діяльності, яка відіграє важливу роль у розкритті злочинів та забезпеченні справедливості, захисту прав та інтересів громадян. Ця аналітична діяльність дозволяє правоохоронним органам систематично та методично збирати, аналізувати та інтерпретувати важливі докази, необхідні для встановлення фактів злочину та визначення винних осіб. Використання різних методів та технік аналізу дозволяє правоохоронцям отримати повну та об'єктивну картину подій, що сприяє успішному завершенню кримінальних проваджень [4].

Список використаних джерел

1. Ханькевич А.М. 2018 р. «Використання кримінального аналізу в діяльності підрозділів кримінальної поліції» chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://univd.edu.ua/general/publishing/konf/30_11_2018/pdf/95.pdf.

2. ЛЬВДУВС Федчак І.А. Навчальний посібник «Основи кримінального аналізу» chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/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.

3. Школьніков В.І. , Калиновський О.В. «Використання результатів кримінального аналізу в кримінальному процесі України» 2017 р chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://elar.naiau.kiev.ua/server/api/core/bitstreams/73653c8a-e65c-4de4-ad76-ae2f326e7dbc/content.

4. Білоус Д.М., Діденко Д.О., Копилов О.В., «Використання кримінального аналізу в розслідуванні злочинів проти життя та здоров'я особи» №07/2024 https://archive.liga.science/index.php/conference-proceedings/issue/view/inter-05.07.2024.

Гриб Аліна Сергіївна,
курсант навчально-наукового інституту № 1
Національної академії внутрішніх справ
Науковий керівник:
кандидат юридичних наук, доцент, професор
кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ
Марков М. М.

ОСНОВИ ВЗАЄМОДІЇ МІЖ КРИМІНАЛЬНИМ АНАЛІЗОМ І ПІДРОЗДІЛАМИ, ЯКІ ЗДІЙСНЮЮТЬ ОПЕРАТИВНО-РОЗШУКОВУ ДІЯЛЬНІСТЬ

Актуальність теми полягає в тому, що сучасні виклики злочинності, включаючи організовану та транснаціональну злочинність, тероризм і кіберзлочини, вимагають вдосконалення методів правоохоронної діяльності. У зв'язку з цим кримінальний аналіз стає важливим інструментом для оптимізації оперативно-розшукових заходів.

Ефективна взаємодія між кримінальними аналітиками і оперативними підрозділами дозволяє підвищити точність прогнозування злочинів, покращити збір і обробку інформації та прийняття рішень на основі аналітичних даних. Така співпраця сприяє більш ефективній профілактиці та розкриттю злочинів, а також знижує ризики прийняття необґрунтованих рішень.

Кримінальний аналіз є важливим інструментом у роботі правоохоронних органів, що дозволяє зібрати, обробити та систематизувати великий обсяг інформації, пов'язаної зі злочинністю. Аналітичні дані використовуються для виявлення закономірностей і тенденції у поведінці злочинців, прогнозування їхніх майбутніх дій та визначення потенційних загроз. Таким чином, кримінальний аналіз сприяє глибшому розумінню природи злочинів та механізмів їх вчинення.

Сучасний розвиток технологій дозволяє аналітикам використовувати широкий спектр інструментів для аналізу інформації, таких як штучний інтелект, великі дані, геоінформаційні системи та інші сучасні технології. Завдяки цьому правоохоронні органи можуть отримати більш точні прогнози, що є важливим для ефективного розслідування і профілактики злочинів.

Кримінальний аналіз – це інтелектуально-аналітична діяльність співробітників правоохоронних органів, яка включає перевірку, оцінку та інтерпретацію інформації, встановлення

зв'язків між отриманими під час розслідування даними, що мають значення для кримінального провадження. Ці результати використовуються правоохоронними органами та судом, а також служать основою для подальшого проведення оперативного та стратегічного аналізу [1].

Оперативно-розшукова діяльність є одним із головних інструментів розслідування злочинів і виявлення осіб, причетних до протиправної діяльності. Вона полягає в організації та проведенні спеціальних заходів, спрямованих на попередження, виявлення, припинення та розслідування злочинів. Підрозділи, які здійснюють оперативно-розшукову діяльність, виконують безпосередню роботу з отримання та збору інформації про злочинців і їхні дії.

Завдяки безпосередньому доступу до оперативної інформації ці підрозділи можуть виявляти підозрюваних, відстежувати їхні зв'язки, виявляти злочинні угруповання, а також здійснювати розшукові заходи. Оперативна інформація, що збирається, є важливим джерелом для кримінального аналізу, оскільки дозволяє отримати детальнішу картину про злочинну діяльність.

Згідно зі статтею 2 Закону України «Про оперативно-розшукову діяльність», оперативно-розшукова діяльність - це система гласних і негласних пошукових та контррозвідувальних заходів, що здійснюється із застосуванням оперативних та оперативно-технічних засобів. Згідно зі статтею 5 цього ж закону, оперативні підрозділи Національної поліції – зокрема підрозділи кримінальної та спеціальної поліції – мають право на здійснення оперативно-розшукової діяльності [2].

Певною мірою визначення кримінального аналізу перегукується з поняттям оперативно-розшукового прогнозування організованої злочинності в аналітичній розвідці. Зокрема, О. Ю. Бусол трактує це як науковий метод дослідження, який здійснюють аналітики оперативних підрозділів, і який включає збір, аналіз, оцінку та обробку оперативно-розшукової інформації. Це робиться з метою визначення напрямків і форм діяльності та прогнозування наслідків дій організованих злочинних угруповань або їхніх окремих членів, що забезпечує керівництво оперативних підрозділів можливістю ухвалення оптимальних оперативно-тактичних і стратегічних рішень [3].

Використання кримінального аналізу в системі МВС і Національної поліції, зокрема для аналізу оперативної

обстановки та протидії злочинності (стратегічний кримінальний аналіз), має тривалу історію. Основою цього є моніторинг оперативної обстановки, що включає аналіз, прогнозування та планування заходів для стабілізації ситуації [4, с. 237].

Ефективна взаємодія між кримінальним аналізом і оперативно-розшуковими підрозділами є необхідною для забезпечення результативної боротьби зі злочинністю. Основою цієї взаємодії є обмін інформацією та використання аналітичних даних для планування і проведення оперативно-розшукових заходів.

Завдяки даним кримінального аналізу, оперативні підрозділи можуть точніше визначати потенційні цілі та ризики, а також краще планувати свої дії. Аналітики, зі свого боку, отримують від оперативників інформацію, яка дозволяє їм вдосконалювати методи аналізу та прогнозування. Одним із найважливіших елементів цієї взаємодії є співпраця на етапі збору даних. Оперативні підрозділи можуть надавати аналітикам ключову інформацію, отриману в процесі слідчих дій або розслідувань, що допомагає аналітикам створювати більш точні моделі і прогнози. Також аналітики можуть вказувати оперативникам на нові напрями розслідування, які могли бути упущені.

Сучасний кримінальний аналіз ґрунтується на якісно організованому інформаційно-аналітичному забезпеченні (ІАЗ) Національної поліції України. ІАЗ функціонує як окрема система з чіткими цілями розвитку, структурними зв'язками між підсистемами і є частиною системи управління поліцією [5, с. 68].

У процесі кримінального аналізу збирається, оцінюється та опрацьовується оперативно-розшукова інформація з метою виявлення закономірностей, що допомагають розслідувати злочини, використовуючи комп'ютерні програми. Правові підстави ІАЗ базуються на нормативних актах МВС, які регулюють порядок здійснення оперативно-розшукових заходів і забезпечують достовірність та ефективність інформації для досудового слідства [6, с. 149].

Сучасний кримінальний аналіз базується на добре організованій системі збору, оцінки та опрацювання інформації. ІАЗ не просто є допоміжним елементом, а самостійною системою з чіткими цілями та структурними зв'язками, яка інтегрована в загальну систему управління поліцією. Це дозволяє аналізувати оперативну обстановку і виявляти

закономірності в злочинній діяльності для своєчасної реакції та розслідувань.

Ключову роль у цьому процесі відіграють нормативні акти МВС, які регулюють порядок здійснення оперативно-розшукових заходів та гарантують достовірність і законність отриманої інформації. Використання комп'ютерних програм для аналізу даних робить процес більш ефективним, забезпечуючи високий рівень інформаційної підтримки під час досудового слідства та в кримінальному судочинстві.

Взаємодія між кримінальним аналізом і підрозділами, що здійснюють оперативно-розшукову діяльність, є критично важливою для ефективної боротьби зі злочинністю в сучасних умовах. Синергія між аналітичними даними та оперативною роботою дозволяє не лише швидше виявляти злочинців, а й ефективніше планувати дії з їхнього затримання і профілактики правопорушень. Без належної взаємодії між цими двома напрямами діяльності правоохоронні органи ризикують втратити важливі можливості для швидкого й ефективного реагування на злочини, що може призвести до зниження загального рівня безпеки в суспільстві. Завдяки стратегічному аналізу та інформаційно-аналітичному забезпеченню, поліція може не лише оперативно реагувати на поточні загрози, але й прогнозувати злочинну діяльність, що сприяє прийняттю оптимальних рішень у протидії злочинності. Використання сучасних технологій та правових механізмів забезпечує вірогідність і результативність зібраної інформації, що підвищує ефективність кримінального судочинства.

Список використаних джерел

1. Половніков В.В. Характеристика кримінального аналізу з урахуванням практики його використання в оперативно-розшуковій діяльності Державної прикордонної служби України., Питання боротьби зі злочинністю : зб. наук. пр. / редкол.: В.І. Борисов та ін. Харків : Право, 2020. Вип. 39. 28–40 с.

2. Про оперативно-розшукову діяльність : Закон України, Відомості Верховної Ради України (ВВР), 1992, № 22, ст. 303.

3. Бусол О. Ю. Підрозділи аналітичної розвідки як спеціальний суб'єкт оперативно-розшукового прогнозування. Юрид. часоп. Нац. акад. внутр. справ. 2011. №2(2). С. 106–115.

4. Шинкаренко І. Р. Проблеми запровадження кримінального аналізу в діяльність підрозділів кримінальної поліції: теоретико історичне підґрунтя. Науковий вісник

Дніпропетровського державного університету внутрішніх справ, 2017. № 1. С. 233–242.

5. Шендрик В. В. Аналіз організації інформаційно-аналітичного забезпечення діяльності Національної поліції України. Науковий вісник Харківського національного університету внутрішніх справ, 2017. №3 (78) С. 66–73.

6. Пеньков С. В. Інформаційно-аналітичне забезпечення діяльності оперативних підрозділів Міністерства внутрішніх справ України: нормативно-правове регулювання. Національний юридичний журнал: теорія і практика. 2015. №4/2 (14). Ч. 2. С. 146–151.

Долгий Дмитро Максимович,
здобувач вищої освіти Національного
юридичного університету
імені Ярослава Мудрого
Науковий керівник:
кандидат юридичних наук, професор,
старший викладач кафедри досудового
розслідування Національного
юридичного університету
імені Ярослава Мудрого
Ханькевич А. М.

РОЛЬ АНАЛІТИЧНОЇ РОЗВІДКИ В РОЗСЛІДУВАННІ КОРУПЦІЙНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

У сучасному суспільстві одним із ключових інструментів для боротьби зі складними соціально-економічними проблемами є аналітична розвідка.

Поняття «аналітична розвідка» визначається як системний аналіз та інтерпретація великого обсягу даних з метою отримання цінної інформації та розкриття взаємозв'язків та закономірностей [1]. Корупційне кримінальне правопорушення – це вчинене осудною особою, у віці з якого настає кримінальна відповідальність, діяння, що включає використання службовими особами своїх прав або посадових можливостей з метою особистого збагачення, та за яке законом встановлено кримінальну, дисциплінарну та/або цивільно-правову відповідальність [2].

Актуальність теми визначається декількома ключовими факторами: постійна загроза корупції; потреба в ефективних інструментах боротьби з корупційними кримінальними

правопорушеннями; потреба в інноваційних підходах і поширення використання аналітичної розвідки.

Наразі корупція є серйозною загрозою для правопорядку та стабільності, а виявляння та розкриття кримінальних правопорушень є надзвичайно важливим для забезпечення сталого розвитку держави. Саме в цьому контексті аналітична розвідка є ключовим інструментом, який допомагає розкрити складні корупційні схеми та сприяє ефективній роботі слідчих підрозділів. Розглянемо сфери її застосування на конкретних прикладах, таких як аналіз грошових потоків та моніторинг телефонного трафіку.

Аналіз грошових потоків – це використання аналітичної розвідки для аналізу фінансових транзакцій та переказів, який дозволяє швидко виявити незвичайні та підозрілі операції, що можуть вказувати на отримання неправомірної вигоди. Наприклад, детальний аналіз банківських виписок може викрити підозрілі перекази грошей на рахунки осіб, причетних до корупційних схем, або допомогти встановити невідповідність фактичних доходів задекларованим.

Моніторинг телефонного трафіку – це використання аналітичних програм для аналізу мобільних та електронних комунікацій, що дає змогу виявити факти спілкування між посадовими особами та бізнесменами щодо отримання неправомірної вигоди. Викриття корупційних схем, у яких задіяно багато посадових осіб та інших фігурантів, неможливо уявити без аналізу телефонного трафіку, що ще раз підкреслює важливість аналітичної розвідки у контексті розкриття корупційних кримінальних правопорушень.

До переваг аналітичних інструментів відносяться їх ефективність та об’єктивність. Вони дозволяють швидко обробляти великі обсяги даних та виключають вплив суб’єктивних чинників у процесі розслідування, забезпечуючи об’єктивність та неупередженість. Тому застосування аналітичної розвідки у виявленні кримінальних правопорушень є необхідним етапом у боротьбі з корупцією та забезпеченні правопорядку в суспільстві.

Розвиток аналітичної розвідки є необхідною умовою для ефективної боротьби з корупцією, оскільки корупційні схеми та методи їх приховування постійно вдосконалюються. Наразі актуальним напрямом розвитку є інтеграція штучного інтелекту (далі – ШІ) та машинного навчання (далі – МН) в інструменти аналітичної розвідки.

Використання ШІ та МН має дві основні переваги: автоматизація процесів аналізу та розширення його можливостей. Автоматизація процесів аналізу дає змогу зменшити витрату часу та підвищити точність розслідувань. Так, алгоритми ШІ можуть автоматично сортувати та класифікувати великі обсяги даних, такі як фінансові звіти, електронні листи та інші. Також системи ШІ можуть безперервно обробляти дані у реальному часі та сповіщати слідчих про виявлення підозрілої активності, що в свою чергу дозволить своєчасно реагувати на потенційні загрози. Розширення можливостей аналізу за допомогою ШІ полягає у поглибленому аналізі даних, що дозволить виявляти приховані закономірності та зв'язки, які важко або неможливо знайти класичними методами. Такий підхід виключає вплив людського фактору, коли людина могла помилитися у класифікації та сортуванні інформації для її подальшого аналізу. Інтеграція зазначених технологій також дозволить звільнити слідчих, і вони зможуть розслідувати інші кримінальні правопорушення.

Аналізуючи роль аналітичної розвідки у розслідуванні корупційних кримінальних правопорушень, ми бачимо її критичну важливість для забезпечення ефективності діяльності слідчих та подальшого викриття корупційних схем. Аналітична розвідка є незамінним інструментом у боротьбі з корупцією. Використання ШІ та МН дозволяє автоматизувати процеси сортування та класифікації даних, моніторингу та виявлення аномалій у фінансових транзакціях, а також аналізу телефонного трафіку для виявлення зв'язків між учасниками корупційних схем, що не тільки знижує витрати часу та ресурсів, але й підвищує точність та ефективність розслідувань.

Таким чином, розвиток аналітичної розвідки є важливим кроком на шляху до зміцнення правопорядку та довіри суспільства до правоохоронних органів. Інвестиції у ці технології та їх інтеграція у правоохоронну діяльність сприятимуть підвищенню прозорості, об'єктивності та оперативності розслідувань, забезпечуючи більш ефективну боротьбу з корупцією та захист інтересів суспільства.

Список використаних джерел

1. Мовчан А. В. Поняття та сутність аналітичної розвідки як особливої форми інформаційно-аналітичної роботи в ОРД. Науковий вісник. 2012. Т. 3, № 58. С. 443–450. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/2167/1/Мовчан.pdf

2. Дубас В. М. Поняття та види корупційних кримінальних правопорушень в кримінальному законодавстві України. Юридичний науковий електронний журнал. 2023. № 6. С. 64–68. URL: http://lsej.org.ua/6_2023/13.pdf.

Кравчук Артур Максимович,
слухач магістратури навчально-наукового інституту № 1 Національної академії внутрішніх справ
Науковий керівник:
кандидат юридичних наук, старший викладач кафедри кримінології та інформаційних технологій Національної академії внутрішніх справ
Яровий К. В.

ВПЛИВ ДЕЗІНФОРМАЦІЇ НА ГРОМАДСЬКУ ДУМКУ ПІД ЧАС ВІЙНИ

Сучасний інформаційний простір відіграє ключову роль у розвитку та взаємодії суспільства. Проте з поширенням Інтернету і соціальних мереж він стає складнішим і вразливішим до маніпуляцій. Особливо це актуально в умовах воєнного стану, коли зловживання інформацією може загрожувати національній безпеці. Протидія дезінформації в мережі-Інтернеті є пріоритетним завданням, адже швидкість поширення інформації дозволяє легко впливати на громадську думку і формувати негативне сприйняття подій.

Незважаючи на те, що теоретичні та практичні аспекти пов'язані з питаннями протидії дезінформації були предметом досліджень у роботах І. Гирича, Б. Гуменюка, Л. Масенка, В. Огнев'юка, В. Огризка, О. Палія,В. Піскун, П. Полянського, К. Ярового та інших, зазначена проблематика залишається актуальною та потребує подальших досліджень. Тому деякі аспекти вимагають більш детального аналізу.

На законодавчому рівні дезінформація визначається як створення та розповсюдження відомостей, що можуть викликати паніку серед населення або вводити в оману [1].

Дезінформація, як свідомо неправдива або маніпулятивна інформація, має дві ключові ознаки. По-перше, вона поширюється для отримання фінансової вигоди або з метою дезорієнтації суспільства. По-друге, вона може загрожувати суспільним інтересам, зокрема демократичним процесам, політичним рішенням і безпеці, зокрема у сфері охорони здоров'я та довкілля. Соціальні мережі, новинні сайти та блоги є основними каналами її розповсюдження, що створює плутанину і негативно впливає на громадську думку [2, с. 57].

Слід зауважити, що термін «дезінформація», особливо в умовах війни, має два ключові визначення: широке та вузьке. У широкому розумінні дезінформація – це навмисно викривлена або неправдива інформація, що містить елементи брехні та наклепу. У вузькому значенні під дезінформацію слід розуміти, особливий вид інформаційно-психологічного впливу, що полягає в модифікації вихідних даних з метою створення спотвореного сприйняття фактів у отримувача [3, с. 352–353]. Зазначене може призвести до рішень або дій, вигідних джерелу дезінформації. Основною характеристикою дезінформації є навмисний намір її створення, що відрізняє її від недостовірної інформації.

З початком повномасштабного вторгнення кількість неправдивої інформації значно зросла, перетворившись на інструмент психологічного впливу на населення. Російські медіа активно використовують дезінформацію для дискредитації України, підриву довіри до її державних інститутів та зниження міжнародної підтримки.

Враховуючи вищевикладене, можна зробити висновок, що дезінформація є суттєвою загрозою для суспільства під час війни, адже її вплив на громадську думку може бути руйнівним. Проте, завдяки зусиллям держави, медіа та суспільства, можливо зменшити цей негативний вплив. Важливо пам’ятати, що в умовах інформаційної війни кожен із нас має відповідальність за інформацію, яку ми споживаємо, поширюємо та вважаємо правдою.

На нашу думку, для ефективної протидії дезінформації під час війни необхідно підвищити медіаграмотність населення через освітні кампанії та створити національні платформи для поширення достовірної інформації. Також важливо забезпечити співпрацю з незалежними медіа, міжнародними організаціями та залучити громадськість до виявлення і спростування фейків.

Список використаних джерел

1. Деякі питання адаптації законодавства України до законодавства Європейського Союзу: Постанова Кабінету Міністрів України від 15.10.2004 р. № 1365// Офіційний вісник України від 05.11.2004. 2004р., № 42, с. 35, ст. 2763.

2. Почепцов Г. Г. Смисли і війна. Україна і росія в інформаційні та смисловій війні. Київ, 2016. 151 с.

3. Яровий К. В. Актуальні проблеми управління інформаційною безпекою держави: зб. матер. Всеукр. наук.-практ. конференції. Київ : Нац. акад. СБУ, 2023. 618 с.

Кузнєцова Валерія Юріївна,
курсант навчально-наукового інституту № 1
Національної академії внутрішніх справ
Науковий керівник:
кандидат юридичних наук, доцент, професор
кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ
Марков М. М.

АКТУАЛЬНІСТЬ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ

Світ давно не стоїть на місці – це слова, які знають всі люди нашої планети. Кожного дня зростає науковий прогрес, з невідомості з'являються великі генії тієї чи іншої сфери і відповідно активно розвиваються сучасні технології, які поступово замінюють всі застарілі і вкоріненні предмети, техніку та й, загалом, спосіб життя. Сучасні технології спрямовані на покращення, полегшення та удосконалення життя суспільства, що згодом може привести до здійснення роботи, яку на даний час вважають доволі клопіткою, всього в декілька натискань умовної кнопки.

Відносно нещодавно сучасний технічний прогрес дійшов і до системи правоохоронних органів. Електронні бази даних замість гори паперів, які так легко втратити; контрольно-пропускний пункт, який здійснюється за допомогою індивідуальних карток, щоб унеможливити вільний прохід незнайомців – це лише маленькі кроки до значного полегшення роботи працівників правоохоронних органів. На наш погляд, застосування штучного інтелекту також неабияк вплине на правоохоронну діяльність, тому сьогодні перед нами постає питання – наскільки важливий штучний інтелект в кримінальному аналізі та чи є сенс інтегрувати його в правоохоронну діяльність.

У загальному випадку штучний інтелект – це галузь науки, яка займається розробкою програм та алгоритмів, які дозволяють комп'ютерам виконувати завдання, що раніше вимагали людського інтелекту. Відтак штучний інтелект може бути використаний для покращення ефективності роботи правоохоронних органів та забезпечення публічної безпеки. Наприклад, використання штучного інтелекту може допомогти правоохоронним органам відстежувати правопорушників та злочинні групи, визначати їх місцезнаходження, аналізувати

відео- та аудіозаписи, шукати співвідношення між різними злочинами та правопорушниками тощо. За допомогою аналізу мовної інформації комп'ютерна програма може виявляти ключові слова та зв'язки між повідомленнями, що дає можливість виявити можливі загрози та, безпосередньо, самих правопорушників; за допомогою програм розпізнавання облич можна ідентифікувати осіб, правопорушення яких були зафіксовані засобами фото та відеоспостереження [1, с. 149].

Системи штучного інтелекту (ШІ) можуть аналізувати великі набори даних, включаючи відеоматеріали, текстові дані, соціальні мережі та інші джерела. Алгоритми машинного навчання дозволяють автоматично виявляти закономірності, що можуть служити індикаторами можливих злочинів або незаконних дій. Це значно спрощує роботу правоохоронних органів у виявленні та аналізі потенційно небезпечних ситуацій. Застосування ШІ в кримінальному аналізі також дозволяє створювати моделі, які враховують не тільки видимі фактори, але й складні зв'язки між різними параметрами, що підвищує точність передбачення та ускладнює обхід захисних стратегій злочинців. Такий підхід вирішує завдання попередження та протидії злочинності на новому рівні, дозволяючи оперативно реагувати на зміни у кримінальній ситуації та запобігати можливим загрозам [2, с. 103].

Як зазначає Кисельов А.О, тактично правильне здійснення кримінального аналізу здатне мінімізувати витрати часу працівників оперативних та слідчих підрозділів Національної поліції на вирішення поставлених перед ними завдань та, відповідно, підвищити якість їх діяльності з попередження та протидії злочинності [2, с.03].

З вищезазначеного можна впевнено сказати, що застосування штучного інтелекту в кримінальному аналізі допоможе правоохоронцям діяти швидше та ефективніше. Через недостатню кількість працівників у Національній поліції, на одного слідчого припадає чимало кримінальних проваджень, що просто фізично унеможливлює їх розкриття, тому що брак часу та людський фактор відіграють свою роль.

Застосування систем штучного інтелекту у кримінальному аналізі дозволяє створити прогностичні моделі для передбачення потенційних злочинів. На основі аналізу історичних даних та інших факторів, системи можуть надавати оцінки ймовірності вчинення злочинів у конкретних районах чи контекстах. Це не лише полегшує роботу правоохоронних

органів у виявленні можливих загроз, але й дозволяє вчасно вживати заходів для запобігання злочинам [2, с. 103].

Інтеграція системи штучного інтелекту в кримінальний аналіз сприятиме покращенню обміну інформацією між різними правоохоронними органами. Системи можуть автоматично аналізувати та інтегрувати дані з різних джерел, що допоможе утворювати комплексні картини кримінальної ситуації та сприяти спільним діям для боротьби з злочинністю. Це сприятиме підвищенню ефективності розслідувань та оперативності в прийнятті стратегічних рішень. Забезпечуючи швидкий та автоматизований обмін інформацією між різними суб'єктами правоохоронної системи, інтеграція штучного інтелекту у кримінальний аналіз створює базу для ефективного реагування на кризові ситуації та формування єдиної стратегії боротьби зі злочинністю. Це важливий крок у напрямку створення сприятливого середовища для взаємодії правоохоронних структур та досягнення спільних цілей щодо забезпечення громадської безпеки [2, с. 104].

Україна активно працює над розвитком інноваційного сектора, підтримкою підприємництва та стартапів, впровадженням цифрових технологій у сфери освіти, охорони здоров'я, енергетики та інших галузей діяльності. Метою цих зусиль є створення конкурентоспроможної, інноваційної та цифрової економіки в Україні, яка дозволить підвищити якість життя населення та забезпечити сталий розвиток країни в цілому [1, с. 153].

Інтеграція штучного інтелекту (ШІ) в кримінальний аналіз дозволяє створювати інтелектуальні системи безпеки, які можуть автоматично реагувати на підозрілі дії та події. Це забезпечить вдосконалення систем виявлення та запобігання злочинам. Інтелектуальні системи безпеки, побудовані на базі ШІ, можуть аналізувати реальний час інформації з різних джерел, включаючи відеоспостереження, датчики, та соціальні мережі. Здатність системи виявляти непередбачені аномалії та підозрілі взаємодії може слугувати важливим інструментом у запобіганні та виявленні потенційно небезпечних ситуацій [2, с. 104].

Додатково, інтеграція ШІ дозволяє автоматизувати взаємодію між системами безпеки та правоохоронними органами, що прискорює реакцію на події та оптимізує використання ресурсів. Такі системи можуть ефективно ідентифікувати потенційні загрози та надавати рекомендації для прийняття стратегічних рішень. Це забезпечить високий рівень

безпеки та допоможе у створенні превентивних заходів для зменшення ймовірності вчинення злочинів, сприяючи таким чином створенню безпечного та захищеного суспільства [2, с. 104–105].

Розвиток та вдосконалення інтегрованих систем штучного інтелекту в кримінальний аналіз залишається актуальним напрямком подальших досліджень. Важливо досліджувати нові алгоритми, методи обробки даних, а також вдосконалювати аспекти етики та захисту приватності. Розробка та впровадження більш продуктивних методів аналізу великих обсягів даних, зокрема врахування взаємодії різних видів інтелектуальних систем, може значно підвищити точність та ефективність кримінального аналізу [2, с. 105].

Підсумовуючи, можна впевнено стверджувати, що застосування штучного інтелекту в кримінальному аналізі неабияк полегшило б роботу правоохоронних органів. Також це було б доволі ефективно в сфері аналізу даних, тому що не завжди людське око може знайти якісь деталі, невеличкі збіги, які в результаті стануть вагомими доказами. Тобто штучний інтелект аналізуючи відео, аудіо та інші дані набагато швидше знайде співвідношення між кримінальними правопорушеннями, ніж звичайна людина. Також штучний інтелект може створювати певну систему безпеки, яка буде завчасно моніторити інформацію і виявляти порушення.

Саме тому, ми вважаємо, що штучний інтелект в кримінальному аналізі буде відігравати важливу роль і зробить діяльність правоохоронних органів більш ефективною і удосконаленою.

Список використаних джерел

1. Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична: збірник наукових праць / головний редактор Ю. Назар. Львів: ЛьвДУВС, 2023. Вип. 3. 208 с.

2. Макаренко В.І., Кисельов А.О. Інтегрування системи штучного інтелекту в кримінальний аналіз. Міжнародний науковий журнал «Грааль науки». 2024. Вип. 35. URL: https://www.researchgate.net/publication/378350904_INTEGRUVANNA_SISTEMI_STUCNOGO_INTELEKTU_V_KRIMINALNIJ_ANALIZ

Михайлицька Карина Сергіївна,
курсант навчально-наукового інституту № 1
Національної академії внутрішніх справ
Науковий керівник:
кандидат юридичних наук, доцент, професор
кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ
Марков М. М.

ПРОВЕДЕННЯ АНАЛІЗУ ОПЕРАТИВНИХ ДАНИХ ПРАВООХОРОННИМИ ОРГАНАМИ В УМОВАХ ВОЄННОГО СТАНУ

Військова агресія рф і запровадження воєнного стану в Україні суттєво вплинули на всі сфери нашого життя. Скоєні злочини на території нашої держави, є надзвичайно масштабними, і їх фіксування та розслідування потребують дослідження чималого обсягу подій та ретельного збирання значного масиву доказів. Сучасний кримінальний аналіз використовує широкий спектр інструментів, від баз даних та алгоритмів машинного навчання до технологій штучного інтелекту, що дозволяє обробляти великі обсяги інформації та визначати закономірності та тенденції у кримінальних правопорушеннях.

Незважаючи на фактичне використання результатів аналітичної роботи як в оперативно-розшуковій діяльності, так і в кримінальному процесі, та її велике значення у розкритті тяжких та особливо тяжких злочинів, на сьогодні на законодавчому рівні цей термін не визначено, що спричиняє розбіжності у ході оцінки сторонами кримінального провадження правомірності процесуальних рішень, прийнятих за результатами аналітичної обробки масивів технічної інформації та належності здобутих доказів в результаті цієї роботи [1, с. 98].

Кримінальний аналіз становить собою дії, спрямовані на ідентифікацію і точне визначення взаємозв'язків між відомостями, які стосуються подій злочинного характеру, осіб, пов'язаних з ними та даними, що походять з різних джерел, і в подальшому їх використання слідчими органами, прокуратурою та судами. Основу кримінального аналізу складають поняття, які визначають його як процес збору, обробки та інтерпретації даних про злочинну діяльність. Це включає вивчення злочинних інцидентів, злочинців, жертв злочинів та соціально-економічного контексту, у якому ці злочини відбуваються [2, с. 9].

Загальна мета кримінального аналізу полягає у напрацюванні нових напрямів в оперативно-розшуковій діяльності та досудовому розслідуванні кримінальних проваджень, зокрема для:

1. якісного планування окремих оперативно-розшукових заходів та слідчих (гласних та негласних) дій;

2. аналітичного супроводження оперативно-розшукової діяльності та досудового розслідування;

3. аналізу стану та ефективності досудового розслідування, оперативно-розшукової та превентивної діяльності у протидії злочинності;

4. оброблення великого обсягу інформації, що унеможливлює відстеження та пов'язування фактів без застосування спеціальних аналітичних методів;

5. аналізу складної і розгалуженої структури зв'язків об'єктів оперативно-розшукової справи або кримінального провадження;

6. виявлення ризиків, тенденцій майбутнього розвитку злочинності та, у подальшому, її запобігання;

7. вирішення більш масштабних довгострокових проблем і цілей, для виявлення крупних фігур злочинного світу, прогнозування зростання видів злочинної діяльності і встановлення пріоритетів діяльності правоохоронних органів [2, с. 8].

Розповсюдженим прикладом застосування аналітики є довідки, які оперативні працівники надають прокурорам та суддям для оцінювання матеріалів оперативно-розшукової діяльності, щодо наявності підстав для погодження проведення оперативно-розшукового заходу, або слідчим у відповідь на доручення для аргументації прокурору та слідчому-судді необхідності проведення окремих слідчих дій. У таких довідках результати аналізу раніше отриманого масиву інформації, проведеного за допомогою різних аналітичних інструментів, фактично перетворюються в аналітичний висновок, в якому обов'язково є посилання на джерела досліджуваної інформації та логічне пояснення досліджуваних обставин, які на розсуд аналітиків обумовлюють необхідність проведення інших оперативно-розшукового заходу, слідчих дій або дають відповіді на питання, які підлягають перевірці під час здійснення оперативно-розшукової діяльності або розслідуванні кримінального правопорушення [2, с. 9–11].

Результатом аналітичної роботи є висновок та рекомендації, які створюються в електронному або письмовому

вигляді, з обов'язковим зазначенням використаних аналітичних інструментів, баз даних, ухвал слідчого-судді, судді апеляційного суду, дозволів прокурора або слідчого, якщо досліджувана інформація отримана в результаті проведення оперативно-розшукових заходів, слідчих (розшукових) та інших процесуальних дій [2, с. 13].

На практиці результати аналізу матеріалів проведення слідчих (розшукових) дій, зафіксованих у протоколах та їх додатках, з'являються у кримінальному провадженні як відповідь оперативного підрозділу на доручення слідчого щодо здійснення аналітичного відпрацювання інформації, що міститься на певному носії інформації, наприклад CD-R диску, одержаному в результаті проведення тимчасового доступу до речей і документів оператора стільникового зв'язку, або флешці з відеоматеріалами, отриманими у результаті обшуку домоволодіння [3, с. 13].

Відповідно до пункту 3 частини 2 статті 40 КПК слідчий уповноважений доручати проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій відповідним оперативним підрозділам шляхом винесення процесуального документа – доручення, а оперативний підрозділ відповідно до статті 41 КПК зобов'язаний їх виконувати. При цьому у главах 20 та 21 КПК України наданий вичерпний перелік слідчих (розшукових) дій та негласних слідчих (розшукових) дій. Щодо переліку слідчих (розшукових) дій, негласних слідчих (розшукових) дій, то в науці кримінального процесу існують різні доктринальні підходи, а такий термін як аналітичне відпрацювання матеріалів є заходом забезпечення оперативного та кримінального провадження, нормативно не визначений як в Законі України «Про оперативно-розшукову діяльність» , так і в КПК України [1, с. 40].

Слід при цьому зазначити, що виконання працівниками оперативних підрозділів доручень слідчого, а також обмін між ними оперативно-розшуковою чи процесуальною інформацією є відповідними формами їх взаємодії, що виникає в процесі їх правовідносин. Особливо цінним аналітичний висновок є на початковому етапі досудового розслідування, у тому числі й кримінальних проваджень щодо терористичних актів та інших тяжких злочинів, що в умовах воєнного стану є надзвичайно актуальним [4, с. 9].

Разом з тим без використання аналітичного відпрацювання великого масиву технічних даних слідчі,

прокурори та слідчі-судді не в змозі отримати скомпоновану, зручну для сприйняття інформацію, відокремлену від залишку, що не має значення у кримінальному провадженні. У зв'язку з тим, що у главі 20 КПК України відсутні такі види слідчих (розшукових) дій як аналітичне відпрацювання матеріалів, виконання вказаних доручень слідчих та складання відповідного протоколу не є можливим. При цьому слід враховувати, що залучення працівників оперативних підрозділів в якості спеціалістів може не відповідати загальним правилам залучення спеціаліста, оскільки останні можуть бути суб'єктом доказування у кримінальному провадженні (у випадку надання доручень в порядку ст. 40-41 КПК України) [5, с. 100]. Крім того, вони перебувають у службовій залежності від сторони обвинувачення (слідчий прокурор може надавати обов'язкові для виконання письмові доручення) [4, с. 12–14].

Зокрема, за допомогою OSINT-аналізу були отримані першочергові відомості для ідентифікації громадянина однієї з інших держав у військових формуваннях рф, що діють на території України. Також, вдалося встановити підрозділ, де іноземець проходив службу та встановлено причетність до воєнних злочинів аналогічного спрямування. 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 [3, с. 100].

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. 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 процесуальний кодекс України від 13.04.2012 No4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.
2. Василинчук В.І, Погорецький М.М., Тіхонов С.В. Аналітичний висновок у оперативно-розшуковій діяльності та кримінальному процесі. URL: https:/visnyk_krim_sud_1-2_23_231013_avt_2-8-18.pdf.
3. Петров В.А. Нові вектори роботи кримінального аналізу в умовах воєнного стану: матеріали міжвідомчої науково-практичної конференції (17 листопада 2023 р.), Київ, НАВС 2023. ст. 98–-100.
4. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.
5. Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: затв. наказом МВС від 07.07.2017 № 575 URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text.

Михайлюк Іванна Олександрівна,
курсант навчально-наукового інституту № 1
Національної академії внутрішніх справ
Науковий керівник:
кандидат юридичних наук, доцент, доцент
кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ
Шевчук О. Ю.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ GOOGLE FORMS ДЛЯ ОПИТУВАННЯ НАСЕЛЕННЯ ЩОДО ЗРОСТАННЯ РІВНЯ ЗЛОЧИННОСТІ ПІД ЧАС ВОЄННОГО СТАНУ

Google Forms– це хмарний сервіс від провідної IT-корпорації, призначений для отримання зворотного зв’язку. Можливості, які він пропонує, знайшли своє застосування і в процесі збору інформації щодо злочинності під час воєнного стану.

За його допомогою можна створювати онлайн-опитування щодо кількості вчинених кримінальних правопорушень в межах певної територіальної одиниці, чи була особа потерпілою від такого кримінального правопорушення тощо [1, с. 16–23].

Основними рисами, які характеризують Google Forms як зручний додаток для проведення подібних опитувань є:

1. Безкоштовний доступ. Google Forms є безкоштовним додатком. Це дуже вагома перевага, оскільки створення і підтримка продуктів такого класу й якості вимагає від компаній-розробників значних ресурсів.

2. Висока якість розробки. Сервіс створювався спеціалістами найвищого класу. Це забезпечує стабільну роботу, мінімальну кількість помилок, які швидко виправляються, стійкість до злому, відповідність сучасним веб-стандартам, коректне відображення в різних браузерах тощо.

3. Регулярне оновлення. Даний сервіс регулярно оновлюється. Це хороша ознака, яка свідчить, що розробники розвивають та удосконалюють його.

4. Відсутність реклами. На цьому ресурсі відсутня реклама, що є надзвичайно вагомою перевагою для будь-якого інтернет-ресурсу. Варте уваги, що розробники повністю відключають рекламу для користувачів.

5. Безпечність. Google Forms є одним із найбільш безпечних сайтів Інтернету, ймовірність вірусної активності і наявності небажаного програмного коду на ньому зведені до мінімуму. Користування цим сервісом гарантовано не завдає шкоди комп'ютеру чи іншому пристрою, який буде використовуватися для виходу в Інтернет.

6. Адаптивний дизайн. Перевагою є адаптивний дизайн, який забезпечує коректне відображання електронних форм на мобільних пристроях. Завдяки цьому для роботи з формами свідки та потерпілі можуть використовувати власні мобільні телефони.

7. Простота та зручність користування. Відзначено простоту та зручність роботи з даним сервісом. Його інтерфейс інтуїтивно зрозумілий: за кілька років використання електронних форм не було жодного випадку, щоб користувач потребував додаткових інструкцій або пояснень щодо роботи з ними [2, с. 83–87].

На мою думку, вказані особливості переконливо доводять, що Google Forms має суттєві переваги перед будь-якими іншими сервісами зворотного зв'язку.

Окремо сліз зазначити, що оформлення анкет в електронному вигляді виглядає коректно та професійно. Для того, щоб подібним чином оформити паперові анкети,

знадобилися б залучити спеціалістів з лав правоохоронних органів.

Google Forms і Microsoft Forms пропонують стандартні шаблони оформлення, також можна надати створюваній формі унікального дизайну, завантаживши власне зображення. У Google Forms зовсім нещодавно з'явилися додаткові можливості оформлення окремих елементів форми [3, с. 20–29].

Окрім того в електронних формах наявні можливості, яких у паперовому варіанті не може бути в принципі, наприклад, збільшення або зменшення розмірів шрифту.

Значною перевагою електронних форм є те, що результати анкетування в них опрацьовуються автоматично, аналізуються, виводяться в наочному вигляді.

Електронні форми зберігаються в хмарному сховищі, а також постійно доступні, до них можна звернутися у будь-який момент.

Також слід відзначити, що відмова від паперових анкет та перехід до електронних форм корисна з точки зору екології, є однією з складових охорони природи [4].

Окремо варто приділити увагу питанню поширення електронних форм серед респондентів. Посилання на форму можна відправити на адресу електронної пошти респондента або залишити на загальнодоступному інтернет-ресурсі. Приємним бонусом від Google Forms є можливість отримати короткі URL форми.

Те, що поширення форми не потребує особистого контакту з респондентами, дозволяє тримати зв'язок з потерпілими та свідками в усіх куточках держави.

Перешкодою для використання електронних форм може стати відсутність вільного та постійного доступу до Інтернету як от під час масових відключень електроенергії внаслідок ворожих обстрілів [5].

Отже, у ході дослідження було з'ясовано, що спільними рисами сервісу Google Forms є безкоштовність, висока якість розробки, регулярне оновлення, відсутність реклами, безпечність, адаптивний дизайн, простота та зручність користування. Вказані особливості підтверджують доцільність використання цього сервіса у кримінально-аналітичній діяльності. З'ясовано, що даний сервіс доцільно використовувати для проведення онлайн-опитувань, щодо вчинених кримінальних правопорушень. Це дозволяє додати в процес збору відповідної інформації швидкості та мобільності.

Список використаних джерел

1. Вакалюк Т. А. Зарубіжний досвід розвитку хмаро орієнтованого навчального середовища вищого навчального закладу. *Наукові записки. Випуск 11. Серія: Проблеми методики фізико-математичної і технологічної освіти. Частина 2. Кропивницький: РВВ КДПУ ім. В. Винниченка,* 2017. С. 16–23. URL: http://eprints.zu.edu.ua/25122/1/фахова_стаття_Вакалюк_КДПУ.pdf /.

2. Вакалюк Т. А. Підходи до використання хмарних технологій у навчальному процесі вищої школи у вітчизняній науковій літературі. *Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми // Зб. наук. пр.* Випуск 48. Київ-Вінниця: ФОП Тарнашинський О. В., 2017. С. 83–87. URL: http://eprints.zu.edu.ua/25124/1/стаття_Вакалюк.pdf.

3. Морзе Н. В., Кузьмінська О. Г. Педагогічні аспекти використання хмарних обчислень. *Інформаційні технології в освіті:* зб. наук. пр. №9, Херсон, 2011. С. 20–29. URL: http://nbuv.gov.ua/UJRN/itvo_2011_9_4.

4. Akshat Sharma. *6 ways Quizzes in Google Forms are getting smarter. Education. Google Official Blog.* 10.05.2018. URL: https://blog.google/topics/education/6-ways-quizzes-google-formsare-getting-smarter/.

5. Miguel Guhlin. *Forms Smackdown: Google vs Microsoft.* 25.01.2017. URL: https://blog.tcea.org/forms-smackdown/

Соломко Денис Клайдович,
аспірант Національної академії Служби безпеки України

ОСОБЛИВОСТІ АНАЛІТИЧНОЇ РОЗВІДКИ В УМОВАХ ВОЄННОГО СТАНУ

Військова агресія російської федерації проти нашої держави завдала значної шкоди українській економіці та її об’єктам. Удари ракетами та безпілотними літальними апаратами, підривна діяльність ворожих іноземних спецслужб, розвиток кіберзлочинності й інші загрози становлять значний ризик для країни та суттєво підвищують уразливість об’єктів інфраструктури, що мають важливе значення для функціонування суспільства та безпеки населення.

Наявність у ворога широкого спектра можливостей отримання з метою реалізації своїх агресивних цілей в Україні

відомостей про ресурсне забезпечення, необхідне для забезпечення відсічі збройної агресії російської федерації, а також про об'єкти критичної інфраструктури, обумовлює необхідність забезпечення захисту стратегічно важливих об'єктів оборонного комплексу, енергетики, транспорту, зв'язку, а також важливих об'єктів інших галузей господарства.

Одним із першочергових інструментів протидії вказаним небезпекам є аналітична розвідка, як один із основних напрямів інформаційно-аналітичного забезпечення правоохоронної діяльності, заснований на органічній єдності усіх форм інформаційно-аналітичної роботи, що застосовується, насамперед, у випадках, коли традиційні засоби й методи не можуть бути застосовані, є небезпечними або потребують значних зусиль чи витрат для їх реалізації [1].

Проблемам розробки та впровадження аналітичної розвідки у практичну діяльність правоохоронних органів приділяли увагу у своїх працях вітчизняні науковці: А.В. Мовчан, Г. М. Артюшин, Н. М. Блавацька, Б. Й. Міщенко.

Вимоги сьогодення зі створення сприятливих умов забезпечення захисту державних інтересів обумовлюють необхідність концептуальної розробки та запровадження аналітичної розвідки в правоохоронній сфері, що дасть змогу встановити інформаційно-аналітичні можливості протидії загрозам в сучасному суспільстві, а також адекватність напрямів реалізації системного аналізу в аналітичній роботі ступеню національної безпеки.

Вдосконалення реалізації інформаційно-аналітичної діяльності, у тому числі й аналітичної розвідки, дозволяють побачити розвиток позитивних процесів, дають можливість стратегічно осмислити всі аспекти діяльності управлінських структур в державній сфері, зокрема, і в правоохоронній діяльності, керованої аналітичною розвідкою, а також своєчасно блокувати несприятливі тенденції [2].

Зокрема, відповідними органами державної влади, на основі даних аналітичної розвідки та в межах компетенції здійснюється здобування, аналітична обробка та надання визначеним споживачам у встановленому Законом України «Про розвідку» та нормативно-правовими актами Президента України інформації стосовно виявлених загроз, забезпечується аналіз стану і тенденцій поширення протиправної діяльності, причин і умов, що впливають на її виникнення, проводиться постійний моніторинг розвитку безпекової обстановки на

окупованих територіях України, в суміжних та інших державах на предмет виявлення протиправних намірів, ризиків авіаційній безпеці, джерел фінансування російської терористичної діяльності, направленої проти України, загроз для населення від негативних інформаційно-психологічних впливів [3].

Одним із інструментів аналітичної розвідки в системі інформаційно-аналітичної роботи також є налагодження щоденного інформаційного обміну між Службою безпеки України, Національною поліцією України, Державною прикордонною службою України, Службою зовнішньої розвідки України, ГУР Міністерства оборони України, Збройними силами України та Державною службою України з надзвичайних ситуацій. Так, з метою забезпечення захисту даних та своєчасного обміну інформацією про реальні і потенційні загрози у кіберпросторі, а також недопущення використання кіберпростору в протиправних цілях, між суб'єктами правоохоронної діяльності та іншими державними органами створюються технологічні можливості для автоматичного виявлення кіберінцидентів та кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем, а також на окремих об'єктах критичної інфраструктури, для подальшого їх блокування. Зокрема, на базі одного із департаментів СБУ відкрито Ситуаційний центр забезпечення кібернетичної безпеки, яким здійснюється протидія російським хакерським кібератакам, спрямованим на системи та об'єкти критичної інфраструктури нашої країни, урядові та банківські установи. Ключові можливості Центру полягають у системі виявлення та реагування на кіберінциденти, що дозволяють попереджати кібератаки, встановлювати їх походження, аналізувати для вдосконалення протидії [4].

В рамках вдосконалення аналітичної діяльності правоохоронними органами здійснюються заходи із вдосконалення навичок використання спеціальних аналітичних інструментів (Power BI, IBM i2 Analyst's Notebook, ArcGIS, Google Map, різноманітні електронні таблиці та інші спеціальні програми) з обробки інформації та перетворення її у форму, прийнятну для розуміння та використання, підготовки оперативних співробітників на курсах підготовки, перепідготовки, підвищення кваліфікації у навчальних закладах інших суб'єктів правоохоронної діяльності, участі у засіданнях круглих столів, використання у практичній діяльності концепції, методології і технології добування відомостей Open source intelligence (OSINT) та інших, для пошуку

інформації, її обліку, аналізу та аналітико-синтетичної обробки первинної інформації [5].

Не зважаючи на фактичне використання результатів аналітичної роботи в правоохоронній діяльності, на сьогодні на законодавчому рівні цей термін не визначено, що спричиняє розбіжності у ході оцінки результатів аналітичної обробки масивів технічних даних та належності здобутих в результаті цієї роботи відомостей, що підтверджують певні припущення. Розповсюдженим прикладом застосування аналітики є довідки, складені оперативними працівниками, у яких викладаються результати аналізу раніше отриманого масиву інформації, проведеного за допомогою різних аналітичних інструментів, фактично перетворюються у аналітичний висновок, в якому обов'язково є посилання на джерела досліджуємої інформації та логічне пояснення досліджуємих обставин, які на розсуд аналітиків обумовлюють необхідність проведення відповідних заходів [6].

Таким чином, в умовах воєнного стану та з врахуванням необхідності відбудови України у повоєнний період, а також поступової інтеграції України в євроатлантичний економічний, політичний та безпековий простір все більше актуалізується необхідність удосконалення аналітичної розвідки у призмі виявлення, оцінювання, прогнозування соціальних процесів, подій, заходів на основі відомостей, одержуваних як з відкритих джерел, так і здобутих у ході спеціальних (агентурних, оперативно-технічних) заходів.

Для вирішення зазначених завдань необхідне запровадження інноваційних технологій, методів аналізу інформації, інформаційної взаємодії, прогнозування розвитку ситуацій у сфері національної безпеки, зокрема використання додаткових людських і фінансових ресурсів для здійснення спеціальними службами інформаційно-аналітичної діяльності.

Список використаних джерел

1. Мовчан А.В. Поняття та сутність аналітичної розвідки як особливої форми інформаційно-аналітичної роботи в ОРД. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор М.М. Цимбалюк*. – Львів: ЛьвДУВС, 2012. – Вип. 3. С. 443–448.

2. Кардашевський Ю.Р. Витоки аналітичної розвідки. *Науковий вісник Ужгородського національного університету. Серія: Право. Том 3 № 82* (2024). С. 72–78. URL: https: //visnyk-pravo.uzhnu.edu.ua/article/view/304938/296708.

3. Про розвідку : Закон України від 17.09.2020 № 912-IX : станом на 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text.

4. В Україні з'явився Ситуаційний центр, що відбиватиме кібератаки: веб сайт. URL: https://www.ukrinform.ua/rubric-technology/2389847-v-ukraini-zavivsa-situacijnij-centr-so-vidbivatime-kiberataki.html.

5. Корнейко О.В., Худенко Д.М. Підготовка кримінальних аналітиків у національній академії внутрішніх справ: історія та досвід. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України [Текст] : 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. 90–-93.

6. Тіхонов С. В., Василинчук В. І. Аналітична робота у боротьбі з кримінальними правопорушеннями: шляхи удосконалення. *Актуальні питання удосконалення загальнодержавної системи боротьби з тероризмом в умовах функціонування режиму воєнного стану : зб. Матер. Круглого столу (м. Київ, 31 серпня 2022 року).* – Київ: НА СБУ, 2022. С. 127–131.

Ткачук Маргарита Геннадіївна,
слухач магістратури навчально-наукового інституту № 1 Національної академії внутрішніх справ
Науковий керівник:
кандидат юридичних наук, старший викладач кафедри кримінології та інформаційних технологій Національної академії внутрішніх справ
Яровий К. В.

КІБЕРЗЛОЧИННІСТЬ ТА ЇЇ ВПЛИВ НА ПРАВООХОРОННУ ДІЯЛЬНІСТЬ УКРАЇНИ

Проблематика кіберзлочинності в Україні є особливо актуальною з огляду на її стрімкий розвиток та зростання впливу на правоохоронну діяльність. Сучасні кібератаки та загрози комп'ютерного тероризму визнані одними з ключових чинників, що становлять реальну та потенційну загрозу національній безпеці та суспільній стабільності держави.

Протягом останніх років проблема кіберзлочинності стала вкрай важливою на державному рівні, адже її вплив на правоохоронну систему відчутно зріс.

Серед найуразливіших об'єктів, які найчастіше стають мішенями для кібератак, є критична інфраструктура країни, що включає енергетичні системи, транспортну інфраструктуру та банківський сектор. Інтенсивність та частота кібератак на ці об'єкти підкреслюють необхідність посилення захисту й адаптації правоохоронної системи до сучасних викликів у сфері кібербезпеки. Така ситуація вимагає не лише активного впровадження новітніх методів протидії кіберзагрозам, а й тісної міжвідомчої співпраці та міжнародної взаємодії.

Кіберзлочинність, що вперше згадується в літературі 1960-х років, визначається як порушення прав у сфері автоматизованих систем обробки даних. Зазначене поняття охоплює всі види злочинів у сфері інформаційних технологій включаючи злочини, вчинені у кіберпросторі з використанням комп'ютерних систем, мереж або інших засобів доступу [1, с. 98].

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

На нашу думку, протидія кіберзлочинності потребує спільних зусиль державного і приватного секторів, вдосконалення міжнародного та національного законодавства, а також створення ефективного інституційного механізму. Дослідники поділяють кіберзлочини на два типи: нові, зумовлені сучасними технологіями, та традиційні, вчинені за допомогою комп'ютерів і Інтернету. Водночас другий тип чітко не визначений, а державна статистика щодо нього відсутня.

З метою розгляду та порівняння кіберзлочинності в правоохоронній діяльності України, варто звернутися до статистичних даних Офісу Генерального прокурора за 2022 рік, органами правопорядку зареєстровано 3415 кримінальних правопорушень у сфері інформаційних технологій, у 2021 році – 3187 кримінальних правопорушень та у 2020 році – 2498, що свідчить про суттєве зростання вчинення кримінальних правопорушень у сфері інформаційних технологій [3].

Вважаємо за доцільне також звернути увагу на офіційну сторінку Кіберполіції у Facebook, де відображено результати розслідувань кримінальних проваджень за 2023 рік, а саме:

– виявлено понад 3600 кіберзлочинів;

– за оперативного супроводу кіберполіції оголошено підозру понад 1700 особам за вчинення понад 3700 злочинів, що на 59 % перевищує аналогічний показник у 2022 році:

– направлено до суду матеріали щодо 42 організованих злочинних груп, у тому числі 7 злочинних організацій, що на 83% перевищує аналогічний показник у 2022 році;

– проведено 18 міжнародних спецопераций спільно з правоохоронцями з Грузії, Швейцарії, Чехії, Ізраїлю, Норвегії, Нідерландів, Франції, Німеччини та США;

– за оперативного супроводу кіберполіції направлено до суду обвинувальні акти щодо вчинення понад 4000 злочинів [6].

Підсумовуючи, можна зазначити, що розвиток правоохоронної системи України сприяє швидшому розкриттю кіберзлочинів. Водночас ефективність протидії кіберзагрозам вимагає постійного контролю, підвищення правової грамотності населення, удосконалення законодавства та регулярного навчання фахівців. Кібербезпека є пріоритетом державної політики, що потребує узгоджених дій між державою, суспільством і міжнародною спільнотою.

Список використаних джерел

1. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

2. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/term/39984.

3. Офіційний сайт Офісу Генерального прокурора. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата зведення: 30.10.2024).

4. Офіційна сторінка Кіберполіції України в Facebook URL: https://www.facebook.com/cyberpoliceua/videos/722135096772255.

Наукове видання

АКТУАЛЬНІ ПИТАННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КРИМІНАЛЬНОГО АНАЛІЗУ В ПРАВООХОРОННІЙ СИСТЕМІ УКРАЇНИ

Матеріали
міжвідомчої науково-практичної конференції
(Київ, 1 листопада 2024 року)

Відповідальний упрядник – *Дмитро ОВСЯНЮК*

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 19.12.2024. Формат 60x84/16. Папір офсетний.
Обл.-вид. арк. 11,5. Ум. друк. арк. 10,69.
Тираж 20 прим.