Отже, інформаційно-аналітична діяльність є важливою складовою різних сфер сучасного суспільства, включаючи бізнес, науку, та, безперечно, правоохоронні органи. Роль ШІ у вдосконаленні інформаційно-аналітичної діяльності важлива, оскільки він допомагає отримати цінну інформацію з великих обсягів даних та прискорює процес прийняття рішень. Таким чином, впровадження ШІ є необхідним етапом у розвитку інформаційно-аналітичної сфери.

1. Демура М.І. Міжнародний досвід використання алгоритмів штучного інтелекту у кримінальному провадженні. Використання технологій штучного інтелекту у протидії злочинності : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 24 – 28.

2. Лаврик Н.С., Неклеса О.В. Аспекти використання штучного інтелекту під час проведення кримінального аналізу в підрозділах Національної поліції України. Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України. 2022. С. 268-269. URL : http://elar.naiau.kiev. ua/jspui/ handle/123456789/24907.

3. Шаєц Є., Лунгол О. Перспективи використання штучного інтелекту в проведенні кримінального аналізу. Актуальні питання діяльності підрозділів кримінальної поліції: Всеукр. наук.-практ. конф. (м. Кропивницький, 14 квітня 2023 р.). Кропивницький: ДонДУВС, 2023. С. 422–424.

СЕМЧИШИН Володимир
перший заступник начальника
Управління СБУ
в Івано-Франківській області
ЯЦЮК Тарас
аспірант кафедри права та публічного
управління Університету
Короля Данила,
начальник відділу Управління СБУ
в Івано-Франківській області
ТКАЧЕНКО Павло
аспірант кафедри кримінально-
правових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
член Асоціації правників України

КРИМІНАЛЬНА АНАЛІТИКА ЯК СКЛАДОВА КІБЕРБЕЗПЕКИ

Кібербезпека – це сукупність заходів, технологій, практик та процедур, спрямованих на захист комп’ютерних систем, мереж, даних та інформації від несанкціонованого доступу, зміни, руйнування чи розповсюдження. Основна

мета кібербезпеки – забезпечення конфіденційності, цілісності та доступності цифрових ресурсів. Водночас кібербезпека держави – це комплексний підхід та система заходів, спрямованих на захист інформаційних, технологічних та комунікаційних ресурсів країни від кіберзагроз та кібератак. Це важливий аспект національної безпеки, оскільки сучасна держава значною мірою залежить від функціонування своїх інформаційних систем та технологічної інфраструктури. Саме забезпечення захисту інформаційної та кібернетичної безпеки держави покладається на спеціальний підрозділ Служби безпеки України (далі – СБУ). В структурі СБУ ефективно функціонує департамент захисту інтересів держави в сфері інформаційної безпеки, який цілодобово забезпечує кібербезпеку особливо важливих інформаційно-телекомунікаційних мереж держави. Спектр діяльності забезпечення кібербезпеки сьогодні не обмежений виключно на інформаційні платформи, а й охоплює об'єкти критичної інфраструктури, державні інформаційний ресурси, кібервійськові операції, навіть кібердипломатію та міжнародне співробітництво. Зважаючи на вищевикладене, підрозділи забезпечення інформаційної та кібернетичної безпеки держави мають бути цілком забезпечені відповідними методичними та прикладними напрямками, серед яких зокрема аналітичне.

Наразі аналітичне забезпечення відіграє ключову роль в діяльності підрозділів кібербезпеки, однак в більшості своїх, на належному рівні, не надається увага такому напрямку роботи, як кримінальна аналітика. Отже, кримінальна аналітика – це складна та мультидисциплінарна область, яка використовує методи та техніки аналізу даних для виявлення та розкриття злочинів. Ця дисципліна орієнтована на дослідження кримінальної діяльності, злочинних тенденцій, а також на розробку стратегій та заходів для їх запобігання та припинення.

На думку більшості вчених, кримінальна аналітика, за умови отримання правильних завдань та ефективного використання її потенціалу, виступає головною зброєю в арсеналі правоохоронних органів. Збір, аналіз і поширення аналітично опрацьованих даних забезпечують набуття правоохоронними органами знань, необхідних для нейтралізації будь-яких проявів злочинності або запобігання їм. Кримінальна аналітика є результатом аналізу злочинців і даних про злочини, чи то на оперативному, тактичному чи стратегічному рівні [1, с. 27].

Діяльність аналітиків з підготовки аналітичних продуктів передбачає дослідження інформації та даних, отриманих з різноманітних джерел за визначеним алгоритмом, який характерний для усіх рівнів аналітичних досліджень. Цей алгоритм називають аналітичним процесом, і він складається з таких етапів: формування аналітичного завдання, збирання відомостей, їх оцінювання, накопичення та збереження (упорядкування), інтеграція та візуалізація для проведення аналізу, підготовка висновку, оцінка висновку, поширення (доведення продукту аналітики замовникові).

Під час проведення аналітичного процесу для отримання аналітичного продукту можуть застосовуватись різні методи: аналіз взаємозв'язків, аналіз злочинних мереж, аналіз телефонних з'єднань, аналіз подій, аналіз дій, аналіз обігу (руху), аналіз фінансових транзакцій, порівняльний аналіз справ, аналіз злочинних моделей (серій), картографування криміногенної інформації (ГІС), статистичний аналіз злочинів, SWOT аналіз, аналіз ризиків, PEST аналіз; SOCTA, OSINT, аналіз злочинних моделей, аналіз тенденцій тощо. Результати аналітичного дослідження виражаються у вигляді письмових аналітичних звітів, досьє на фізичну або юридичну особу, об'єкт (предмет), організовану групу чи злочинну організацію, подію, профілів, аналітичних орієнтувань та інших аналітичних документів (довідки, інформаційні зведення, аналітичні огляди) [1, с. 27].

До принципів кримінально-аналітичної діяльності варто віднести: законність, функціональна спеціалізація, розумна достатність, взаємодія, професійна компетентність, об'єктивність, сумісність форм і методів, цілеспрямованість, незалежність, системність та безперервність. Водночас за видами кримінального аналізу виділяють операційний, тактичний та стратегічний. Безумовно кожний з напрямків – це частка інформаційно-аналітичної діяльності.

Операційний кримінальний аналіз – це інформаційно-аналітична діяльність за конкретними кримінальними провадженнями або оперативними справами стосовно інформації, що становить інтерес для підрозділів кібербезпеки щодо ознак та інших відомостей, які характеризують осіб, об'єктів, організованих груп чи злочинних організацій, що в подальшому сприятиме розслідуванню правопорушень. У процесі операційного кримінального аналізу здійснюється встановлення тенденцій злочинності, з'ясовуються місця концентрації вчинення злочинів, визначається профіль підозрюваного та потерпілого. До цих дій вдаються з метою підготовки управлінських рішень щодо розподілу сил та засобів і проведення операційного аналізу.

Тактичний кримінальний аналіз – це 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 – це 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 [1, с. 30].

Технології кримінального аналізу передбачають впровадження моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing» (ILP), як моделі, яка спрямована на підтримку, супровід інституційного управління та рішень посадових осіб на основі процесу аналізу інформації і даних. Основні складові розвитку моделі ILP є такими: нормативно-правова база для врегулювання; інформаційні ресурси; система наповнення інформаційних ресурсів; система оцінювання джерел та достовірності інформації; спеціальне програмне забезпечення; інтегрування спеціалізованого програмного забезпечення з інформаційними ресурсами та іншими джерелами інформації; тренінги для аналітиків практичних підрозділів; стандартизовані форми аналітичних продуктів.

Разом з цим, варто підкреслити, що кримінальний аналітик повинен співпрацювати з оперативними підрозділами в рамках оперативно-розшукової діяльності та виконувати покладені на нього завдання. Швидко та оперативно знайдена інформація дасть змогу та можливості швидко розслідувати кримінальне провадження, спираючись на отриману інформацію.

Отже, зважаючи на вищевикладене можливо визначити, що кримінальна аналітика є невід'ємною складовою кібербезпеки. Шляхом аналізу кіберзлочинів, їхньої характеристики та особливостей, а також ідентифікації злочинців та прогнозування їхньої діяльності, оперативні підрозділи в змозі ефективно захищати інформаційно-телекомунікаційні системи та державні інформаційні ресурси. Вдосконалення стратегій та політик кібербезпеки на основі аналітичних даних допоможе побудувати більш безпечне цифрове майбутнє.

---

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