СЕКЦІЯ 5.
ІНСТРУМЕНТИ, МЕТОДИ ТА АЛГОРИТМИ ЗАСТОСУВАННЯ OSINT У АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ

ІНТЕГРАЦІЯ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ ТА OSINT-ТЕХНОЛОГІЙ У ПРОЦЕСІ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ І ПРОГНОЗУВАННЯ КРИМІНАЛЬНИХ РИЗИКІВ

Балтовський Олексій Анатолійович
доктор технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій, Одеського державного університету внутрішніх справ.
Сіфоров Олександр Іванович
кандидат технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій, Одеського державного університету внутрішніх справ.

У сучасних умовах стрімкої цифрової трансформації суспільства, глобалізації інформаційних потоків, інтенсивного розвитку кіберпростору та зростання рівня залежності державних інституцій, правоохоронних органів, фінансових систем і критичної інфраструктури від інформаційно-комунікаційних технологій особливої актуальності набуває проблема формування ефективних механізмів виявлення, аналізу та прогнозування кіберзагроз і кримінальних ризиків. Кіберпростір перетворився не лише на середовище інформаційної взаємодії, а й на окремий сегмент соціально-технічної реальності, у межах якого виникають нові форми злочинної діяльності, реалізуються складні транснаціональні кримінальні схеми, здійснюється інформаційно-психологічний вплив, координуються деструктивні дії організованих груп та відбувається незаконне використання цифрових ресурсів. Відповідно, сучасна система забезпечення національної безпеки та протидії злочинності потребує якісно нових науково-методологічних підходів, здатних забезпечити інтегроване поєднання

аналітичних, інформаційних, прогностичних та інтелектуальних механізмів обробки даних.

У цьому контексті особливого значення набуває інтеграція методів системного аналізу та технологій OSINT (Open Source Intelligence), які формують міждисциплінарний інструментарій для виявлення латентних загроз, моделювання поведінкових патернів злочинної активності, оцінювання ризиків та підтримки процесів прийняття управлінських рішень у сфері кримінального аналізу й кібербезпеки [1].

З позиції системного аналізу кіберзагроза є складною стохастичною системою, що характеризується невизначеністю, нелінійністю, адаптивністю та високим рівнем латентності. Це обумовлює необхідність використання багатофакторних моделей, методів когнітивного моделювання, сценарного прогнозування, аналізу ризиків, нечіткої логіки, ієрархічного аналізу процесів та математичного моделювання поведінкових моделей. Особливе значення при цьому має концепція ризик-орієнтованого підходу, відповідно до якої ключовим завданням кримінального аналізу стає не лише фіксація вже вчинених правопорушень, а й раннє виявлення потенційних деструктивних тенденцій, індикаторів підготовки злочинної діяльності та факторів ескалації криміногенних процесів.

OSINT-технології у сучасних умовах виступають одним із найефективніших інструментів збору та аналітичної обробки інформації. Їх особливість полягає у використанні відкритих джерел інформації, які, попри публічний характер, можуть містити критично важливі дані для виявлення злочинної активності, встановлення зв'язків між суб'єктами, ідентифікації цифрових слідів та прогнозування поведінки потенційно небезпечних груп або осіб. На відміну від традиційної оперативно-розшукової діяльності, OSINT дозволяє здійснювати безперервний моніторинг інформаційного простору в режимі реального часу, забезпечуючи високий рівень масштабованості та адаптивності аналітичних процедур [1,2].

У контексті кібербезпеки OSINT використовується для виявлення витоків інформації, аналізу діяльності кіберзлочинних угруповань, моніторингу даркнет-середовищ, виявлення фішингових кампаній, збору індикаторів компрометації, аналізу цифрових активів, дослідження мережевої інфраструктури та відстеження деструктивної інформаційної активності. При цьому

ефективність OSINT значною мірою залежить від можливості інтеграції великих масивів даних у єдину аналітичну систему, здатну забезпечити виявлення прихованих закономірностей, аномалій та потенційних ризиків.

Сучасний кримінальний аналіз дедалі більше орієнтується на концепцію intelligence-led policing, відповідно до якої ключову роль у діяльності правоохоронних органів відіграє аналітичне забезпечення процесів управління безпекою. У межах цього підходу інформація перетворюється на стратегічний ресурс, а аналітичні системи стають основою для прогнозування кримінальних процесів, визначення пріоритетів оперативної діяльності та розробки превентивних заходів. Інтеграція системного аналізу та OSINT-технологій дозволяє формувати багаторівневі моделі кримінальних ризиків, що враховують як технічні, так і соціально-поведінкові фактори [2,3].

Одним із ключових аспектів інтеграції зазначених підходів є формування системи індикаторів кіберзагроз та кримінальних ризиків. Такі індикатори можуть включати аномальну мережеву активність, зміни у цифровій поведінці користувачів, поширення деструктивного контенту, активізацію закритих онлайн-спільнот, збільшення кількості спроб несанкціонованого доступу, появу інформації про продаж викрадених даних, координацію інформаційних атак та інші ознаки потенційної злочинної діяльності. Використання системного підходу дозволяє інтегрувати ці індикатори у комплексну модель оцінювання ризиків, де кожен параметр розглядається у взаємозв'язку з іншими елементами системи.

Важливу роль у процесі прогнозування кримінальних ризиків відіграють методи машинного навчання та інтелектуального аналізу даних. Застосування алгоритмів класифікації, кластеризації, нейронних мереж, аналізу часових рядів та поведінкової аналітики дозволяє виявляти приховані закономірності у великих масивах інформації та прогнозувати ймовірність реалізації певних загрозових сценаріїв. У поєднанні з OSINT-технологіями це створює можливість автоматизованого моніторингу інформаційного середовища та побудови систем раннього попередження про потенційні кіберінциденти.

Особливої уваги заслуговує використання графових моделей та мережевого аналізу у кримінальному аналізі. Соціальні

мережі, цифрові комунікації та онлайн-платформи формують складні мережеві структури, в межах яких відбувається взаємодія між суб'єктами злочинної діяльності. Аналіз таких структур дозволяє виявляти ключові вузли, канали комунікації, ієрархічні зв'язки та механізми координації деструктивної активності. Використання методів соціометричного аналізу, центральності вузлів, аналізу спільнот та алгоритмів пошуку аномалій сприяє підвищенню ефективності оперативно-аналітичної діяльності правоохоронних органів.

Водночас інтеграція системного аналізу та OSINT-технологій супроводжується низкою викликів та обмежень. Однією з ключових проблем є надмірний обсяг інформації, що генерується у цифровому середовищі. Великі масиви даних характеризуються високим рівнем шуму, неоднорідністю, фрагментарністю та наявністю дезінформаційних елементів. Це обумовлює необхідність розробки ефективних механізмів фільтрації, верифікації та оцінювання достовірності інформації. У цьому аспекті особливого значення набувають методи семантичного аналізу, обробки природної мови, автоматизованого фактчекінгу та виявлення інформаційних маніпуляцій [2].

Іншою важливою проблемою є забезпечення балансу між ефективністю аналітичної діяльності та дотриманням принципів законності, захисту персональних даних і прав людини. Масштабне використання відкритих джерел інформації створює ризики порушення приватності, неправомірного збору персональних даних та надмірного цифрового контролю. У зв'язку з цим виникає необхідність формування чіткої нормативно-правової бази, яка б регламентувала використання OSINT-технологій у діяльності правоохоронних органів, визначала межі допустимого моніторингу та забезпечувала прозорість аналітичних процедур.

Важливим напрямом розвитку є створення інтегрованих інформаційно-аналітичних платформ, здатних об'єднувати дані з різних джерел та забезпечувати комплексне оцінювання ризиків у режимі реального часу. Такі системи повинні базуватися на принципах модульності, масштабованості, адаптивності та кіберстійкості. Інтеграція технологій Big Data, штучного інтелекту, системної динаміки та OSINT-аналітики дозволить сформувати нове покоління аналітичних систем, орієнтованих на проактивне управління безпекою.

У контексті сучасних гібридних загроз кіберпростір дедалі більше використовується як інструмент інформаційно-психологічного впливу, координації деструктивної діяльності та реалізації транснаціональних кримінальних схем. Це обумовлює необхідність міжвідомчої та міжнародної інтеграції у сфері обміну аналітичною інформацією, координації кібербезпекових заходів та формування спільних стандартів кримінального аналізу. Особливого значення набуває співпраця між правоохоронними органами, науковими установами, освітніми закладами та приватним сектором, оскільки лише комплексний міждисциплінарний підхід здатний забезпечити ефективну протидію сучасним кіберзагрозам [3].

Таким чином, інтеграція методів системного аналізу та OSINT-технологій є одним із ключових напрямів розвитку сучасного кримінального аналізу та систем забезпечення кібербезпеки. Поєднання системної методології, інтелектуального аналізу даних, відкритої розвідки та прогнозних моделей створює передумови для переходу від реактивної моделі протидії злочинності до проактивної системи управління ризиками. Використання таких підходів дозволяє не лише підвищити ефективність виявлення кіберзагроз, а й забезпечити стратегічне прогнозування криміногенних процесів, мінімізувати рівень невизначеності та підвищити адаптивність правоохоронних систем до нових викликів цифрової епохи [3].

Перспективи подальших наукових досліджень у зазначеному напрямі пов'язані з удосконаленням моделей когнітивного аналізу кіберзагроз, розвитком систем ситуаційної обізнаності, впровадженням технологій explainable AI у кримінальному аналізі, розробкою інтелектуальних систем підтримки прийняття рішень та формуванням цифрових екосистем безпеки, орієнтованих на інтеграцію аналітичних, прогностичних і превентивних механізмів управління ризиками. У сучасних умовах саме синергія системного аналізу, OSINT-технологій та інтелектуальних інформаційних систем здатна забезпечити належний рівень стійкості держави, суспільства та правоохоронної системи до складних багатовекторних кіберзагроз і кримінальних викликів XXI століття.

Список використаних джерел:

1. Ісмайлов К.Ю., Балтовський О.А., Сіфоров О.І. Основні підходи щодо вирішення завдання оптимального календарного планування з використанням спеціалізованих алгоритмів.

Електронне наукове видання «Порівняльно аналітичне право». 2019. №2. С. 98 - 101.

2. Гіренко О. В., Гіренко О. О., Кулик Н. С. Методологія системного аналізу та прогнозування ризиків // Вісник Київського національного торговельно-економічного університету. Серія «Економіка і управління». 2021. № 2. С. 12-20.

3. Гіренко О. В., Гіренко О. О., Кулик Н. С. Методи прогнозування ризиків у системному аналізі // Вісник Київського національного торговельно-економічного університету. Серія «Менеджмент». 2022. № 1. С. 23-30.

ПРАКТИЧНІ ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИКОРИСТАННЯ OSINT У КРИМІНАЛЬНОМУ АНАЛІЗІ

Зеленчук Володимир Васильович
начальник ВКА ГУНП
в Івано-Франківській області
Куций Роман Володимирович
кандидат юридичних наук
заступник начальника ВКА ГУНП
в Івано-Франківській області
Черній Андрій Ігорович
старший інспектор з ОД ВКА ГУНП
в Івано-Франківській області

Актуальність дослідження. У сучасних умовах особливої актуальності набуває розвиток цифрових технологій та зростання кількості високотехнологічних загроз, що в свою чергу виникає необхідність в удосконаленні традиційних підходів до отримання й аналізу інформації. Інструменти OSINT (Open Source Intelligence) відіграють ключову роль, як засіб оперативного отримання, перевірки та систематизації відомостей із відкритих джерел що розміщенні на інтернет платформах. Запровадження підходів, заснованих на моделі Intelligence-led Policing, сприяє перетворенню розрізнених цифрових даних на структурований аналітичний продукт, який може бути використаний у процесі документування та розслідування кримінальних правопорушень. Це, у