КРИМІНАЛЬНИЙ АНАЛІЗ У ЦИФРОВОМУ СЕРЕДОВИЩІ: СУЧАСНІ ПІДХОДИ ДО ВИЯВЛЕННЯ КІБЕРЗЛОЧИННОСТІ ТА ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ

Сіфоров Олександр Іванович
кандидат технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій, Одеського державного університету внутрішніх справ.
Іванченко Валерія Сергіївна
викладач кафедри кримінального аналізу та інформаційних технологій

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням ролі цифрових технологій у функціонуванні державних інституцій, економічних систем, соціальних комунікацій та безпекового сектору. Цифровізація суспільних процесів, інтеграція інформаційно-комунікаційних технологій у всі сфери життєдіяльності, поширення хмарних платформ, систем штучного інтелекту, великих даних, інтернету речей та кіберфізичних систем формують принципово нове середовище функціонування сучасної держави. Разом із беззаперечними перевагами цифрової трансформації відбувається суттєве ускладнення структури криміногенних загроз, що набувають транснаціонального, латентного, високотехнологічного та адаптивного характеру. Кіберзлочинність у сучасних умовах перестає бути окремим сегментом кримінальної діяльності, поступово трансформуючись у комплексний багаторівневий феномен, який інтегрується у фінансову, соціальну, політичну, інформаційну та безпекову сфери [2].

Формування цифрового середовища як простору взаємодії суб'єктів суспільних відносин спричинило появу нових форм кримінальної активності, що характеризуються високим рівнем анонімності, складністю технічної ідентифікації, використанням розподілених інформаційних інфраструктур та активним застосуванням технологій приховування цифрових слідів. У цих умовах традиційні механізми правоохоронної діяльності виявляються недостатньо ефективними, оскільки орієнтувалися переважно на фізичний простір вчинення правопорушень, лінійні моделі аналізу та реактивний характер прийняття управлінських рішень. Саме тому особливого значення набуває кримінальний аналіз як

інтегрований міждисциплінарний напрям, що поєднує методологію системного аналізу, інструменти інтелектуального аналізу даних, технології OSINT, засоби кіберрозвідки, математичне моделювання ризиків, прогнозування поведінкових сценаріїв та інформаційно-аналітичне забезпечення процесів управління у сфері протидії злочинності.

У сучасному науковому дискурсі кримінальний аналіз дедалі частіше розглядається не лише як окрема функція правоохоронної діяльності, а як стратегічний механізм підтримки управлінських рішень, спрямований на формування доказово обґрунтованої системи реагування на криміногенні процеси. Цифрове середовище значно змінює природу кримінального аналізу, оскільки основним об'єктом дослідження стають інформаційні потоки, цифрові комунікації, поведінкові патерни користувачів, мережеві взаємозв'язки, електронні транзакції, лог-файли, телекомунікаційні метадані, цифрові артефакти та інші структуровані й неструктуровані дані. У таких умовах аналітична діяльність набуває ознак високотехнологічної інтелектуальної системи, яка базується на комплексному застосуванні методів data science, штучного інтелекту, машинного навчання та адаптивного прогнозування ризиків [3].

Кіберзлочинність як складний соціотехнічний феномен характеризується динамічністю, високою швидкістю трансформації та здатністю до самоадаптації. Сучасні кіберзлочинні угруповання активно використовують технології автоматизації атак, шкідливе програмне забезпечення, фішингові механізми, соціальну інженерію, криптовалютні платформи, анонімні мережі, бот-мережі та елементи штучного інтелекту для здійснення деструктивної діяльності. Це суттєво ускладнює процеси виявлення, ідентифікації та прогнозування кіберзагроз. Традиційні підходи до аналізу криміногенної ситуації втрачають ефективність через значний обсяг даних, багатовимірність інформаційних взаємозв'язків та високу швидкість виникнення нових форм кіберризиків.

У контексті цифрового середовища особливого значення набуває системний підхід до організації кримінального аналізу. Системний аналіз дозволяє розглядати кіберзлочинність як складну адаптивну систему, що складається з великої кількості взаємопов'язаних елементів, між якими існують нелінійні зв'язки, зворотні інформаційні потоки та механізми самоорганізації. Застосування принципів системності, ієрархічності, цілісності, багаторівневого моделювання та адаптивного управління забезпечує

можливість комплексного дослідження кіберзагроз, виявлення прихованих закономірностей та формування ефективних управлінських рішень у сфері забезпечення інформаційної безпеки [1].

Важливою особливістю сучасного кримінального аналізу є інтеграція технологій інтелектуального аналізу даних у процес обробки криміналістично значущої інформації. Інтелектуальний аналіз даних дозволяє автоматизувати процес виявлення аномалій, класифікації поведінкових моделей, прогнозування ризиків та встановлення прихованих взаємозв'язків між суб'єктами кримінальної діяльності. Алгоритми машинного навчання, нейронні мережі, кластеризація, дерева рішень, байєсівські моделі, методи асоціативних правил та інші інструменти data mining суттєво розширюють можливості правоохоронних органів у сфері виявлення складних кіберзлочинних схем [4].

Особливу роль у сучасному кримінальному аналізі відіграють технології OSINT, які забезпечують отримання, структуризацію та інтерпретацію інформації з відкритих джерел. В умовах цифровізації значна частина криміналістично важливої інформації міститься у соціальних мережах, форумах, відкритих реєстрах, месенджерах, вебресурсах, телекомунікаційних сервісах та інших елементах цифрового простору. Використання OSINT-технологій дозволяє здійснювати моніторинг інформаційного середовища, аналізувати поведінкові характеристики суб'єктів, встановлювати комунікаційні зв'язки, прогнозувати потенційні ризики та формувати аналітичні профілі об'єктів дослідження. У поєднанні з методами системного аналізу та інтелектуального моделювання OSINT перетворюється на потужний інструмент інформаційно-аналітичного забезпечення управлінської діяльності.

Суттєвого значення у процесі кримінального аналізу набувають питання обробки великих даних. Сучасні інформаційно-аналітичні системи правоохоронних органів функціонують в умовах надзвичайно великих обсягів інформації, що надходить із різноманітних джерел у реальному масштабі часу. Технології Big Data забезпечують можливість інтеграції, агрегації, фільтрації та аналітичної обробки інформаційних потоків із подальшим формуванням прогнозних моделей ризиків. Аналіз великих даних дозволяє виявляти приховані закономірності злочинної діяльності, встановлювати часові та просторові взаємозв'язки між подіями, формувати ризик-орієнтовані профілі та визначати критичні вузли кіберзлочинної активності [3].

Важливим напрямом розвитку кримінального аналізу у цифровому середовищі є використання технологій штучного інтелекту для автоматизації процесів підтримки прийняття управлінських рішень. Системи штучного інтелекту забезпечують можливість адаптивного аналізу інформації, прогнозування сценаріїв розвитку криміногенної ситуації, моделювання ризиків та формування рекомендацій для суб'єктів управління. Використання інтелектуальних аналітичних платформ дозволяє значно скоротити час обробки інформації, підвищити точність прогнозування та забезпечити своєчасне реагування на кіберзагрози.

У сучасних умовах підтримка прийняття управлінських рішень у сфері протидії кіберзлочинності повинна базуватися на ризик-орієнтованому підході. Такий підхід передбачає оцінювання ймовірності виникнення загроз, визначення потенційних наслідків реалізації ризиків та формування пріоритетів управлінського реагування. Системи кримінального аналізу повинні забезпечувати не лише фіксацію фактів протиправної діяльності, а й прогнозування можливих сценаріїв розвитку подій, виявлення тенденцій та формування стратегічних рішень щодо нейтралізації загроз.

Особливого значення набуває інтеграція кримінального аналізу у структуру інформаційно-аналітичних систем правоохоронних органів. Сучасні аналітичні платформи повинні забезпечувати міжвідомчу взаємодію, обмін інформацією, синхронізацію баз даних, підтримку колективного аналізу та формування єдиного інформаційного простору безпеки. В умовах цифрового середовища ефективність управлінських рішень значною мірою залежить від швидкості отримання достовірної інформації, рівня інтеграції інформаційних ресурсів та здатності системи здійснювати адаптивне реагування на динамічні загрози [1].

У контексті сучасних безпекових викликів особливого значення набувають питання кіберстійкості інформаційно-аналітичних систем. Зростання кількості кібератак на державні інформаційні ресурси, критичну інфраструктуру та правоохоронні системи актуалізує необхідність формування комплексної системи кіберзахисту. Кримінальний аналіз у цифровому середовищі повинен враховувати не лише кримінологічні аспекти кіберзлочинності, а й технічні характеристики інформаційних систем, архітектуру мережевих взаємодій, особливості функціонування цифрової інфраструктури та механізми забезпечення кібербезпеки.

Одним із перспективних напрямів розвитку кримінального аналізу є застосування технологій предиктивної аналітики. Предиктивні моделі дозволяють прогнозувати ймовірність виникнення кіберінцидентів на основі аналізу історичних даних, поведінкових характеристик та поточних інформаційних потоків. Використання алгоритмів прогнозування забезпечує можливість переходу від реактивної моделі правоохоронної діяльності до проактивної системи управління безпекою, орієнтованої на попередження загроз.

Не менш важливим аспектом є етичний та правовий вимір використання цифрових технологій у кримінальному аналізі. Активне застосування систем штучного інтелекту, автоматизованого моніторингу, біометричних технологій та масового аналізу даних потребує забезпечення балансу між безпекою та дотриманням прав людини. У сучасних умовах формування інформаційно-аналітичних систем повинно здійснюватися з урахуванням принципів законності, пропорційності, прозорості, відповідальності та захисту персональних даних.

Сучасний кримінальний аналіз поступово трансформується у складну інтегровану систему підтримки управлінських рішень, що функціонує на основі цифрових технологій, алгоритмів штучного інтелекту та міждисциплінарних методологій. Ефективність протидії кіберзлочинності значною мірою залежить від здатності правоохоронних органів здійснювати комплексний аналіз інформації, прогнозувати ризики, адаптуватися до динамічних загроз та забезпечувати високий рівень координації управлінських процесів [2].

Таким чином, кримінальний аналіз у цифровому середовищі виступає одним із ключових елементів сучасної системи забезпечення безпеки держави. Його розвиток безпосередньо пов'язаний із впровадженням інноваційних інформаційних технологій, інтеграцією системного аналізу, штучного інтелекту, OSINT, Big Data та методів інтелектуального прогнозування. Удосконалення інформаційно-аналітичного забезпечення правоохоронної діяльності створює передумови для формування проактивної моделі протидії кіберзлочинності, підвищення ефективності управлінських рішень та забезпечення належного рівня кібербезпеки в умовах цифрової трансформації суспільства [3].

Список використаних джерел:

1. Балтовський О.А., Ісмайлов К.Ю., Сіфоров О.І., Форос Г.В., Заєць О.М. Теорія систем і системний аналіз: навч. посібник. Одеський держ. унів-т внутр. справ, 2020. 156 с.

2. Гончарук О. М. Зародження та еволюція формування кримінального аналізу в світовій парадигмі правоохоронної діяльності. Південноукраїнський правничий часопис. 1. 2023 р. С. 130-137

3. 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. 5

4. Балтовський О.А., Форос Г.В., Пядишев В.Г., Сіфоров О.І. Системи підтримки прийняття рішень: навчальний посібник. Одеса: РВВ ОДУВС. 2022. 176 с.