therefore these definitions may well be extended to organizational and administrative as well as administrative and economic functions [2, p.492].

When identifying an official as a subject of a crime, it is necessary to distinguish between official functions and professional responsibilities. In order to bring an official to criminal responsibility for committing a corruption crime, it is necessary to clearly and unambiguously establish which category of officials a person belongs to in connection with the acts committed by him, as holding a certain (specific) position may be related to functions of a representative of power, and organizational-administrative or administrative-economic duties.

REFERENCES

1. Slutskaya T.I. Criminal Liability for Abuse of Power or Official Authority. 2010. p. 232.

2. Resolutions of the Plenum of the Supreme Court of Ukraine in Criminal Cases. 2007. p. 492.

Санакоєв С.Д.
здобувач 1 курсу ННІП ПФПНП Дніпропетровського державного університету внутрішніх справ

Науковий керівник:
Єфімов В.В.
кандидат юридичних наук, доцент, доцент кафедри фінансових та стратегічних розслідувань ННІП ПФПНП Дніпропетровського державного університету внутрішніх справ

СУЧАСНІ ІНСТРУМЕНТИ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ У КРАЇНАХ ЄС: ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ

Використання нових інформаційно-комунікаційних технологій організованими злочинними угрупованнями є ключовим викликом для правоохоронних органів через складність явища, кількість залучених факторів і осіб, а також велику сукупність злочинних технологічних заходів, що використовуються для фінансування та підтримки злочинних і терористичних дій. Використання нових технологій цими групами зміцнює їх можливості для підтримки своєї діяльності (фінансування, відмивання грошей, вербування, планування терористичних атак, шахрайство з використанням особистих даних) та анонімного скоєння злочинів. Більше того, ці організації часто перебувають в авангарді технологічних інновацій для планування, здійснення та приховування своєї злочинної діяльності та доходів від неї, тоді як правоохоронні органи відстають.

Випередження – це пріоритетний напрямок для правоохоронних органів. Їм потрібні ранні та кращі знання та інтелект, щоб діяти на випередження. У цьому контексті фінансований ЄС проект COPKIT [1] розробляє інструментарій

для підтримки методології раннього попередження/раннього реагування, яка дозволить правоохоронним органам випереджати нові технологічні розробки, що використовуються організованою злочинністю.

Рішення COPKIT допомагають пояснити, як розвивається злочинність, виявляють «слабкі сигнали» або тенденції, попереджають про нові ризики (раннє попередження), а також формують основу для надання допомоги особам, які приймають рішення, у розробці ранніх заходів (готовність, пом'якшення, запобігання та інші політики безпеки).

Дослідження та розробка інструментів COPKIT спрямовуються та перевіряються набором відповідних варіантів використання (сценаріїв), запропонованих та контрольованих правоохоронними органами, партнерами проекту.

Спираючись на висновки з різних звітів EUROPOL (SOCTA 2016-2021) [2] та визначення ними пріоритетних областей злочинності на рівні управління ЄС, COPKIT аналізує два варіанти використання:

1) **злочин як послуга / дані як товар:** організовані злочинні групи збирають особисту та професійну інформацію про громадян, співробітників та різні компанії (як на законних підставах, наприклад, шляхом доступу до відкритих даних, так і з використанням незаконних методів, наприклад соціальної інженерії та зламу). Потім спеціалізовані групи збирають, аналізують, обробляють і систематизують цю інформацію, щоб продавати її іншим групам зі злочинними та/або терористичними цілями (вимагання, шахрайство, викрадення тощо).

2) **торгівля вогнепальною зброєю (з використанням нових технологій):** нещодавні терористичні атаки в Європі стимулювали ініціативи боротьби з незаконною торгівлею вогнепальною зброєю відносно невеликим ринком, який під контролем організованих злочинних груп. Незаконний обіг вогнепальної зброї є одним із дев'яти пріоритетів EMPACT, пріоритетних областей злочинності Європолу [3] в рамках політичного циклу ЄС 2017–2021 років.

Цей набір кейсів спрямований на охоплення центральних аспектів підходу «Раннє попередження / Ранні дії», передбаченого COPKIT, та водночас надає конкретні орієнтири для рішень, які будуть досліджені та розроблені в рамках проекту.

У рамках проекту COPKIT були розроблені технології поліцейської діяльності на основі даних для підтримки правоохоронних органів в аналізі, розслідуванні, пом'якшенні наслідків та запобіганні використанню нових інформаційних та комунікаційних технологій організованою злочинністю та терористичними групами.

Набір інструментів COPKIT [4] був розроблений для підтримки методології раннього попередження/раннього реагування, яка допомагає пояснити, як розвивається злочинність, виявляти «слабкі сигнали» або тенденції та надсилати попередження про нові ризики (раннє попередження) та формувати основу для надання допомоги у прийнятті рішень. розробникам для

розробки Early Action (готовності, пом'якшення, запобігання та іншим політикам безпеки).

Всі розроблені інструменти, включаючи їх можливості виявлення та обміну знаннями, були розроблені з урахуванням етичних, юридичних (особливо щодо прав людини та захисту даних) та соціальних аспектів, щоб гарантувати, що ці інструменти є етично прийнятними та соціально бажаними.

1. Збір даних:

- *GENDSCRAP – інструмент збору даних у даркнет.* Спеціалізовані сканери, що можуть працювати в Clear Web і Dark Web (особливо в TOR). Це дозволяє реалізувати точний знімок домену з політикою сканування, визначеною користувачем. Знімок зберігає всі дані з веб-сайту у вигляді текстів або зображень та інших мультимедійних об’єктів.

2. Вилучення інформації:

- *CKNER* – розпізнавання іменованих об’єктів. Інструмент розроблений Австрійським технологічним інститутом (AIT). Служба, що об’єднує кілька найсучасніших засобів розпізнавання, кожен із яких має стандартні та специфічні для домену моделі, які зосереджені на текстових даних, отриманих через сканування маркетплейсів даркнету, що пропонують зброю та наркотики, зосереджено на коротких, злочинних письмових текстах;

- *CKRELEXT* – вилучення зв’язків (інструмент розроблений Австрійським технологічним інститутом (AIT). Сервіс REST для розпізнавання зв'язків між сутностями (наркотики, зброя, імена користувачів, місцезнаходження тощо). Він аналізує текст (наприклад, один або кілька абзаців тексту, взятого з реклами ринку даркнет) як вхідні дані й створює іменований графік об’єктів. Компонент залежить від сутностей, розпізнаних CKNER;

- *MOREC (Moment Recognizer)* – інструмент розроблений IBM Ireland (IBM). Сервіс REST для виділення важливих моментів утворює багатосторонню бесіду, наприклад дискусійні форуми в контексті Dark Net Markets. Вхідні дані для служби — це серія текстових повідомлень, якими обмінюються користувачі системи, повертаючи важливі моменти як події у форматі JSON.

3. Збагачення знань:

- *GP* – розбиття графів: виявлення спільнот і моделей взаємовідносин. (розробка Thales SIX GTS). Виконує виявлення груп подібних вузлів у мережі взаємодій, таких як мережі відносин між людьми, блоги, облікові записи криптовалюти тощо. Він може виявляти конкретні структури злочинної (прихованої) мережі, відмінні від тих, які зазвичай спостерігаються в аналізі соціальних мереж.

- *CF* – пошук підключення (розробка Legind Technologies (LTA). Шукає зв’язки в графах об’єктів (наприклад, не обмежуючись «особами» чи ідентичностями, але також неоднорідними) з невизначеними посиланнями. Може використовуватися в онлайнових (включаючи Dark Net) дослідженнях для пошуку зв’язків між різними елементами цифрових ідентифікаційних даних (наприклад, іменами користувачів, гаманцями криптовалюти, тощо), у зв’язку з внутрішніми розвідувальними базами, якщо є (і якщо можливе об’єднання

графіків).

4. Оцінка:

- CTSAE (контекстуальна оцінка та оцінка загроз і ситуацій) розроблений Thales Nederland (TNL). Оцінка контекстної загрози та ситуації. Підхід до класифікації ймовірнісної оцінки, що включає машинне навчання та попередні знання предметної області. Застосування для оцінки реклами на ринку Dark Net відповідно до різних концепцій, таких як серйозність і пріоритет для розслідування з використанням визначення та пріоритетів LEA;

- SA – оцінка ситуації (розробка Legind Technologies (LTA). Спрямований на автоматизований моніторинг та оцінку реклами в Dark Net, а також подібних даних, оцінку ризиків, загроз, характеристик та аномалій в рекламі, узагальнення цих даних шляхом продажу товарів, постачальників тощо та представлення результатів на всеосяжній інформаційній панелі.

5. Візуалізація:

- *HMI – людино-машинний інтерфейс* (розробка Thales Nederland (TNL). Візуалізація для стратегічних та оперативних аналітиків, що дозволяє використовувати методологію раннього попередження/ранніх дій (наприклад, використання стратегічних ідей в операційному аналізі і навпаки). Підтримує візуалізацію різних типів даних (анотовані тексти, графіки відносин і просторові тимчасові дані). Включає функції спільного доступу та контролю доступу, а також елементи, що підтримують етичні, юридичні аспекти та аспекти конфіденційності.

Ці та інші інструменти, розроблені європейськими фахівцями, сприяють впровадженню методології раннього попередження/раннього реагування, зокрема підрозділами кримінального аналізу та аналітичних підрозділів Департаменту стратегічних розслідувань Національної поліції України, випереджаючи нові технологічні розробки, що використовуються організованою злочинністю, та ефективно протидіяти їй у середньостроковій перспективі в рамках реалізації Стратегії боротьби з організованою злочинністю [5].

Список використаних джерел:

1. COPKIT : [офіційна сторінка]. Електронний ресурс : https://copkit.eu/

2. Europol IOCTA [офіційна сторінка]. Електронний ресурс : https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

3. EU Policy Cycle – EMPACT : [офіційна сторінка]. Електронний ресурс : https://www.europol.europa.eu/crime-areas-and-statistics/empact

4. COPKIT tools: [офіційна сторінка]. Електронний ресурс : https://copkit.eu/copkit-tools/

5. Про схвалення Стратегії боротьби з організованою злочинністю / Розпорядження кабінету Міністрів України від 16.09.2020 № 1126-р. Електронний ресурс : https://zakon.rada.gov.ua/laws/show/1126-2020-