Дряпак Олександр Володимирович,
начальник відділу кримінального аналізу
Головного управління Національної
поліції в Полтавській області

ЗАБЕЗПЕЧЕННЯ ОПЕРАЦІЙНОЇ КІБЕРБЕЗПЕКИ ТА КІБЕРГІГІЄНИ КРИМІНАЛЬНОГО АНАЛІТИКА ПІД ЧАС ПРОВЕДЕННЯ ЦИФРОВИХ РОЗСЛІДУВАНЬ

Стрімка цифровізація суспільних процесів та інтеграція новітніх інформаційних технологій у злочинну діяльність докорінно змінили ландшафт досудового розслідування, перемістивши значну частину доказової бази у кіберпростір. За таких умов кримінальний аналіз став базовим елементом моделі Intelligence-Led Policing [1, ch. 3], забезпечуючи ефективне розкриття складних, багатоепізодних та високотехнологічних правопорушень. Проте специфіка аналітичної діяльності, зокрема проведення OSINT-досліджень, моніторинг прихованих сегментів мережі (Dark Web), трекінг криптовалютних транзакцій та аналіз мультимедійного контенту фігурантів пов'язана з постійними та динамічними загрозами для самих кримінальних аналітиків. Робота аналітика у відкритому цифровому середовищі без належного захисту створює критичні ризики його деанонімізації злочинними угрупованнями, цілеспрямованого фішингу та компрометації чи зараження шкідливим програмним забезпеченням службових інформаційних контурів Національної поліції України. Відтак, виникає гостра потреба у переосмисленні та нормативно-методичному закріпленні суворих стандартів операційної кібербезпеки (OPSEC) і повсякденної кібергігієни як невід'ємної складової професійної надійності та безпеки кримінального аналітика.

У сучасних доктринах поліцейської діяльності, керованої аналітикою, зокрема у британській Національній моделі розвідки National Intelligence Model та концепції Intelligence-Led Policing, дотримання операційної безпеки аналітика розглядається як фундаментальна умова захисту інформаційних активів правоохоронних органів. У контексті моделі NIM, яка регламентує стандартизовану оцінку даних (зокрема за системою оцінки джерел та інформації 3x5x2 / 5x5x5) [2; 3, p. 22], будь-яка деанонімізація аналітика перед фігурантами автоматично компрометує весь операційний цикл розслідування та нівелює

цінність отриманих результатів. Оскільки модель NIM трактує аналітика та його робочу станцію як критичний «актив», захист цієї ланки від контррозвідувальних дій з боку організованих злочинних угруповань є першочерговим завданням. Водночас, концепція ILP базується на принципах гарантування безпеки інформації, що вимагає усунення будь-яких ризиків витоку службових масивів Big Data у процесі їх обробки. Таким чином, у межах міжнародних аналітичних стандартів, повсякденна кібергігієна та використання інструментів маскування цифрового сліду є не просто технічними рекомендаціями, а засадничими елементами управління операційними ризиками, що забезпечують безперервність та конфіденційність аналітичного забезпечення досудового розслідування.

Окремим стратегічним вектором кримінального аналізу в Україні є документування та аналітичний супровід розслідувань воєнних злочинів, скоєних військовослужбовцями рф. Робота в цьому напрямі передбачає опрацювання великих масивів неструктурованих даних: від супутникових знімків, матеріалів радіоперехоплень та геолокацій до терабайтів фото- й відеоконтенту в проросійських медіаресурсах. Виконуючи ці завдання, кримінальні аналітики стають пріоритетними мішенями для ворожих спецслужб, військової розвідки та підконтрольних їм висококваліфікованих APT-угруповань, зокрема Sandworm, Fancy Bear тощо [4, розд. 1].

У зв’язку з цим збір доказової бази у ворожому цифровому контурі чи аналіз профілів комбатантів у соціальних мережах має здійснюватися виключно із дзеркально чистих робочих станцій, ізольованих від внутрішніх державних реєстрів. Використання виокремлених фізичних ліній зв’язку, анонімних профілів-фантомів, регулярна ротація криптографічно захищених VPN-тунелів та повне шифрування накопичувачів є критичною операційною необхідністю. Технологічна недбалість у цій сфері загрожує не лише розкриттям особи співробітника, а й проведенням ворогом цілеспрямованих кібератак на критичну інформаційну інфраструктуру Національної поліції України або фізичним відстеженням координат дислокації підрозділів.

У практичній площині реалізація зазначених принципів вимагає категоричної відмови від використання стандартних користувацьких операційних середовищ. Технічним доповненням робочого місця кримінального аналітика має стати розгортання

спеціалізованих ізольованих ОС Whonix / Tails або обов'язкове застосування чистих віртуальних машин VirtualBox / VMware, повністю відсічених від локальної відомчої мережі. Це дозволяє нівелювати ризики фіксації унікальних цифрових відбитків браузерів адміністраторами підконтрольних фігурантам веб-ресурсів під час OSINT-пошуку. Важливим аспектом безпеки є також етап дослідження вилучених у ході слідчих дій цифрових носіїв, оскільки сучасні злочинці дедалі частіше використовують методи комп'ютерної стеганографії для приховування даних чи шкідливого коду всередині звичайних медіаконтейнерів. Будь-яка первинна верифікація мультимедійного контенту, зокрема глибокий аналіз метаданих EXIF за допомогою програмного забезпечення ExifTool чи Exiv2, має здійснюватися виключно всередині локальних ізольованих «пісочниць». Це не лише виключає приховану детонацію експлойтів у внутрішній мережі підрозділу, а й забезпечує належну оцінку автентичності доказів та виявлення ознак цифрового монтажу чи ворожих модифікацій контенту [5, розд. 3].

Позаслужбова діяльність кримінального аналітика вимагає повного переосмислення особистої цифрової поведінки та формування специфічного стилю життя, заснованого на принципах розумного цифрового аскетизму. Статус працівника аналітичного підрозділу несумісний із публічною активністю у класичних соціальних мережах, де оприлюднення навіть нейтральних побутових фотографій, локацій відпочинку, родинних зв'язків чи відміток друзів дає ворожій розвідці або представникам організованої злочинності готову базу для складання психологічного портрета, шантажу чи виходу на близьке оточення.

Категоричним табу є використання сервісів зворотного пошуку контактів за номерами телефонів на кшталт GetContact тощо. Встановлення таких застосунків на особисті чи службові гаджети призводить до автоматичного витоку всієї телефонної книги у відкриті комерційні бази даних. Як наслідок, робочі номери колег, специфічні відомчі теги або підписи оперативних співробітників стають публічними, що миттєво розкриває внутрішню структуру підрозділу та компрометує конфіденційні контакти. Аналогічно, використання публічних платформ і сайтів знайомств з реальних мобільних пристроїв створює критичний вектор для проведення операцій із соціальної інженерії, де під виглядом звичайного співрозмовника ворожі агенти або

фігуранти розслідувань можуть здійснювати цілеспрямований збір інформації, вивідувати специфіку служби або використовувати вразливості особистого життя для дискредитації підрозділу.

Повсякденна життєдіяльність аналітика поза службою супроводжується безперервним накопиченням латентного цифрового сліду, який за умови його агрегації сторонніми особами може зашкодити інтересам правосуддя. До серйозних факторів ризику належить використання комерційних мобільних застосунків, які у фоновому режимі збирають телеметрію: фітнес-трекерів (типу Strava), які публікують карти постійних маршрутів пробіжок правоохоронця, програм лояльності супермаркетів чи АЗС, що чітко фіксують географію та графік щоденних переміщень, а також служб таксі та доставки їжі. Агрегація цих даних зловмисниками через витоки баз даних або хакерські злами дозволяє з точністю до метра встановити домашню адресу аналітика, час його перебування на робочому місці та межі операційної зони підрозділу. Якщо аналітик веде розслідування щодо високотехнологічних злочинних груп або воєнних злочинів рф, такий побутовий витік дозволяє злочинцям зіставити час аналітичної активності з конкретною фізичною особою. Це тягне за собою ризики фізичного тиску, залякування, або проведення превентивних контрзаходів (знищення доказів, зміна каналів зв'язку), що повністю нівелює результати багатомісячної роботи аналітичного підрозділу та ставить під загрозу життя співробітника.

Проведене дослідження дозволяє констатувати, що в умовах гібридної агресії та стрімкого технологічного розвитку злочинності, операційна кібербезпека та повсякденна кібергігієна кримінального аналітика є базовим критерієм стійкості всієї правоохоронної системи України [6, ст. 2]. Ефективний захист як службового, так і позаслужбового контуру аналітичних підрозділів вимагає негайного переходу від декларативних закликів до побудови чіткої адміністративно-навчальної системи та нормативного закріплення правил «цифрового аскетизму» [7, с. 45].

Разом із технічним навчанням, критично важливим є впровадження жорстких внутрішньовідомчих обмежень щодо позаслужбової поведінки аналітиків, зокрема повного табу на використання комерційних застосунків-ідентифікаторів контактів, мінімізації латентного цифрового сліду від побутових геолокаційних сервісів і відмови від публічних акаунтів у

соцмережах. Додатковим елементом інституційного контролю має стати запровадження регулярних планових кібернавчань [8, розд. 4] і тестів на пильність у вигляді контрольованих фішингових розсилок усередині підрозділів. Тільки такий комплексний підхід, що поєднує інструментальну ізоляцію, жорстку позаслужбову дисципліну та безперервну практичну сертифікацію співробітників, дозволить певною мірою нівелювати ризики деанонімізації правоохоронців, захистити інформаційні контури Національної поліції України від ворожих спецслужб та забезпечити конфіденційність і результативність розслідувань.

Список використаних джерел

1. Ratcliffe J. H. Intelligence-Led Policing. 2nd ed. London : Routledge, 2016. 194 p.
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. *Офіційний вісник України*. 2021. № 68. Ст. 4301.
3. Europol Information Management Strategy 2021–2024: Harnessing Data for a Safer Europe / European Law Enforcement Agency. The Hague : Europol, 2021. 48 p.
4. Організаційно-правові засади протидії кіберзлочинності в Україні : монографія / В. В. Чернєй та ін. Київ : Нац. акад. внутр. справ, 2019. 312 с.
5. Комп'ютерна стеганографія: теорія і практика : навчальний посібник / за ред. Ю. В. Козуба. Харків : ХНУРЕ, 2021. 248 с.
6. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379.
7. Інформаційне забезпечення кримінального аналізу у діяльності Національної поліції України : наук.-практ. рек. / С. С. Чернявський та ін. Київ : НАВС, 2021. 84 с.
8. Кібергігієна у професійній діяльності: правові та організаційні аспекти : підручник / за заг. ред. О. М. Литвинова. Харків : Харків. нац. ун-т внутр. справ, 2023. 296 с.