кримінального аналізу, але й загалом Національної поліції України з урахуванням етичних принципів, захисту персональних даних та уникнення дискримінаційних упереджень в алгоритмах.

Список використаних джерел

1. Баранов О. О. Визначення терміну «штучний інтелект» / О. О. Баранов // Інформація і право. 2023. № 1. С. 32–49. URL: http://nbuv.gov.ua/UJRN/Infpr_2023_1_5.

2. Стефанчук М. О. Перспективи правового регулювання відносин у сфері використання штучного інтелекту / М. О. Стефанчук, О. А. Музика-Стефанчук, М. М. Стефанчук // Вісник Національної академії правових наук України. 2021. Т. 28, № 1. С. 306–332. URL: http://nbuv.gov.ua/UJRN/vapny_2021_28_1_18.

3. Основи кримінального аналізу: підручник / А. М. Бабенко, О.М. Заєць, В.А, Некрасов, К.Ю. Ісмайлов, Д.О. Пефтієв та ін. / за заг. ред. О.Є. Користіна. Київ, 2020. 296 с.

4. Зачек О. І. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності / О. І. Зачек, Ю. І. Дмитрик, В. В. Сеник // Науковий вісник Львівського державного університету внутрішніх справ. серія юридична. 2023. Вип. 3. С. 148–156. URL: http://nbuv.gov.ua/UJRN/Nvlduvs_2023_3_21.

Лемешко Юрій Олександрович,
начальник Управління кримінального аналізу ГУНП в Харківській області

ПРОБЛЕМНІ ПИТАННЯ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ АНАЛІЗУ АКТИВНОСТІ КОРИСТУВАЧІВ БЕЗ СУДОВОГО САНКЦІОНУВАННЯ

Повномасштабна збройна агресія проти України змінила не лише хід історії, а й формат викликів, із якими щодня зіштовхується система кримінальної юстиції. В умовах воєнного стану на перший план вийшли питання протидії державній зраді, колабораціонізму, інформаційним диверсіям, а також кримінальним правопорушенням, які безпосередньо загрожують національній безпеці. Одночасно з цим значно ускладнилась і сама структура злочинності: ми маємо справу не з одиничними діями, а з скоординованими, часто добре законспірованими мережами – онлайн і офлайн. У цих умовах зростає роль

аналітичної підтримки розслідувань, зокрема через обробку великих обсягів відкритої інформації – OSINT-розвідки. Вміння вчасно ідентифікувати цифровий слід фігуранта, виявити його зв'язки, зафіксувати потенційно деструктивну активність у мережі може мати вирішальне значення у розкритті злочину.

Вирішення оперативно-службових завдань нерідко вимагає від працівників поліції застосування цілого комплексу оперативно-розшукових заходів, проведення слідчих (розшукових) дій, у т.ч. негласних, реалізації заходів забезпечення кримінального провадження. Тому в центрі уваги опиняються спеціалізовані інструменти для кримінального аналізу – системи, які дозволяють не просто збирати дані, а швидко знаходити в них закономірності, зв'язки й потенційні загрози. Переважна більшість описаних дій потребує судового санкціонування, що з одного боку забезпечує дотримання принципу законності у кримінальному судочинстві, а з іншого – суттєво уповільнює хід розслідування.

Водночас існує ціла низка законних способів отримання знеособлених персональних даних, вивчення яких дозволяє ідентифікувати особу правопорушника, визначити місця його перебування, побудувати профіль його активності тощо.

Одним з інструментів, що дозволяє зібрати та проаналізувати знеособлені дані, є застосування advertising intelligence (збирання та аналіз даних з різноманітних рекламних модулів).

Описана категорія даних збирається за згодою користувача різними компаніями через свої електронні сервіси та застосунки з метою подальшого використання для проведення цільової реклами. Наприклад, Google накопичує дані про тип і налаштування браузера й пристрою, операційну систему, мобільну мережу (зокрема, назву та номер телефону оператора) і номер версії додатка, відомості про взаємодію додатків користувача, веб-переглядачів і пристроїв із сервісами Google, зокрема IP-адресу, звіти про аварійне завершення роботи, активність системи й дату, час та URL-адресу напрямку переходу запиту користувача. Якщо особа користується пристроєм Android із додатками Google, він періодично зв'язується із серверами Google, щоб надати інформацію про пристрій і підключення до сервісів Google. Це, зокрема, дані про тип пристрою, назву оператора, звіти про збої, відомості про

встановлені додатки, а також, залежно від налаштувань пристрою Android, інша інформація про те, як особа користуєтеся ним [1].

Більш глибоке вивчення питання накопичення даних для таргетованої реклами з мобільних терміналів дозволяє окреслити механізм такого збирання. Мова йде про фіксацію різноманітними мобільними програмами даних користувачів з їх прив'язкою до рекламного ідентифікатора мобільного пристрою. У системах на базі Android такий ідентифікатор називається GAID (Google Advertising ID), а в системах на базі iOS – IDFA (identifier for advertisers).

Очевидно, що набір відповідних даних користувачів із прив'язкою до часу та простору зберігається у володільців відповідних програмних застосунків, які потім ними обмінюються безпосередньо або через проміжних осіб для організації більш ефективної цільової реклами. Наприклад, якщо користувач шукає якийсь товар через застосунок prom.ua, то реклама подібного товару невдовзі з'явиться у встановленому на тому ж пристрої застосунку Viber тощо.

Як можна проаналізувати описані знеособлені рекламні дані?

Перший спосіб полягає в організації власної рекламної компанії через кабінет рекламодавця у відповідних сервісах (рис.).

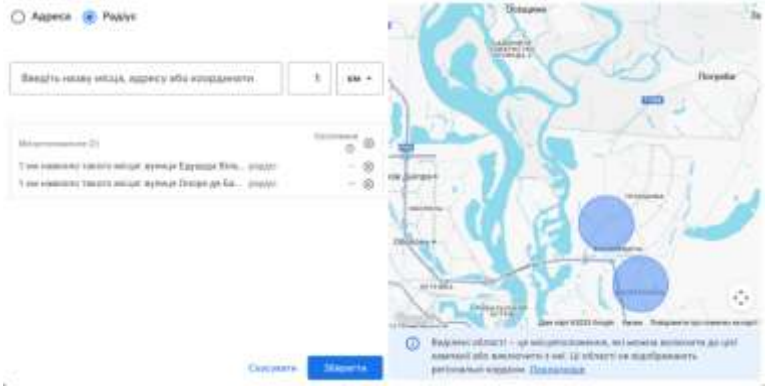

Рис. Налаштування таргетованої реклами в кабінеті Google Ads

У результаті можна відслідковувати появу пристрою на певних ділянках місцевості тощо. Водночас такий підхід дозволяє проводити аналіз у перспективі.

Для того, щоб здійснювати ретроспективний аналіз, існують спеціальні інструменти, як от Tangles від Penlink [2]. Із його використанням можна, наприклад, обрати декілька ділянок місцевості на карті та переглянути, які пристрої були у визначений час у відповідних місцях. Так само можна проводити вивчення ресурсів, які відвідувала особа з певним рекламним ідентифікатором, тощо.

Поліцейські підрозділи в США досить активно використовують подібні інструменти для відслідковування та ідентифікації користувачів [3]. Оскільки використання знеособлених персональних даних не потребує одержання судових рішень, програмне забезпечення, що дає доступ до рекламних даних знайшло широке використання у діяльності спеціальних служб та правоохоронних органів за кордоном.

Як видно з наведеного, головну цінність становлять саме дані користувачів, які можна аналізувати. Якщо розглянути ситуацію в українському вимірі, то відповідні застосунки, від яких можна отримати більшість користувацьких даних для аналізу, такі:

– банківські (Privat24, Ощад, Monobank тощо);
– поштові (Нова пошта, Meest пошта тощо);
– сервіси надання послуг (Bolt, Uklon, Uber тощо);
– сервіси прокату самокатів (Vevi тощо);
– сервіси продажів та партнерських програм (OLX.ua, Prom, Fishka, супермаркети, автозаправні, аптечні тощо).

Для того, щоб в умовах правового режиму воєнного стану більш ефективно попереджувати та розслідувати кримінальні правопорушення, вбачається доцільним внести зміни до чинного законодавства в частині зобов’язання установ, підприємств та організацій передавати відповідні дані користувачів єдиному центру обробки даних, через який правоохоронні органи могли б отримувати відомості для аналізу.

Серед іншого, пропонуємо внести зміни до Закону України «Про захист персональних даних», якими офіційно визначити поняття «контролер персональних даних» як суб’єкт,

що визначає мету та способи обробки даних, у тому числі знеособлених даних. Контролери, які використовують такі дані для таргетингу реклами, повинні бути зобов'язані передавати зведену інформацію органу державної влади в порядку, затвердженому Кабінетом Міністрів України. Така передача не повинна вимагати згоди фізичних осіб, якщо ідентифікація суб'єкта неможлива. Закон «Про рекламу» має містити положення, що зобов'язують рекламодавців, агенції та цифрові платформи надавати державі знеособлені дані про аудиторію для проведення рекламних кампаній. Уповноважений орган має бути наділений повноваженнями перевіряти дотримання цієї вимоги та застосовувати відповідні санкції у разі порушення.

Водночас, Закон України «Про інформацію» має бути доповнений положеннями про визнання анонімних даних окремим видом інформації. Хоча вони не дозволяють ідентифікувати особу, їх можна використовувати для аналізу поведінкових моделей. Держава повинна мати право доступу до таких не конфіденційних даних для забезпечення прозорості цифрових процесів, протидії дезінформації та моніторингу рекламної діяльності.

Крім того, пропонуємо розглянути можливість внесення змін до Закону України «Про електронні комунікації», оскільки рекламні дані часто передаються через телекомунікаційну інфраструктуру. Необхідно визначити поняття знеособлених телекомунікаційних даних, а також зобов'язати провайдерів електронних комунікаційних послуг надавати державним органам узагальнену інформацію про користувачів, яка використовується для реклами. Крім того, необхідно встановити зобов'язання щодо прозорої обробки таких даних та їх правового захисту.

Прийняття вказаних змін дозволить отримати важливу для правоохоронних органів та спеціальних служб інформацію без надмірної витрати коштів, які в іншому випадку необхідно сплачувати стороннім особам – володільцям та розпорядникам рекламних даних.

Список використаних джерел

1. Політика конфіденційності Google. URL: https://policies.google.com/privacy?hl=uk.

2. Transforming Investigations with Digital Intelligence and Evidence Analysis. URL: https://www.penlink.com/why-penlink/.

3. Texas state police expands surveillance with PenLink's controversial technology raising privacy concerns. URL: https://www.business-humanrights.org/ru/свежие-новости/texas-state-police-expands-surveillance-with-penlinks-controversial-technology-raising-privacy-concerns/.

Овсянюк Дмитро Іванович,
начальник аналітичного відділу (Центр кримінальної аналітики) Національної академії внутрішніх справ

ОРГАНІЗАЦІЯ АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ У СФЕРІ ПРОТИДІЇ НАРКОЗЛОЧИННОСТІ

Актуальність протидії наркозлочинності зумовлена її системними загрозами для сталого розвитку держави, громадського здоров'я, безпеки та правопорядку. Міжнародний незаконний обіг наркотиків є високоприбутковим кримінальним бізнесом, який переважно контролюється організованими злочинними групами. Ці групи відзначаються гнучкістю, адаптивністю до заходів протидії та значними фінансовими ресурсами, що спрямовуються на технічне оснащення та підтримання корупційних зв'язків. Торгівля наркотиками визнана однією з найсерйозніших загроз безпеці, з якою стикається Європейський Союз, і, за оцінками, становить близько однієї п'ятої світових злочинних доходів [1].

Ефективне розв'язання цієї проблеми вимагає розробки та впровадження стратегій, що базуються на найкращих практиках та наукових дослідженнях, оптимізують використання ресурсів правоохоронних органів і зменшують шкоду від незаконного обігу наркотиків. Це підкреслює необхідність застосування структурованих підходів, де ключову роль відіграє кримінальний аналіз.

Ключовим аспектом успішної та ефективної організації аналітичної діяльності та її основою є глибоке розуміння та осмислене дотримання аналітиком етапів динамічного розвідувального циклу, який є фундаментом кримінального аналізу [2]. Застосування цього циклу може підняти протидію наркозлочинності на якісно новий рівень, дозволяючи