bitstream/lib/25207/2/MSNK_2018v2_Pelcher_M-Advantages_and_lack_of_application_72-73.pdf.

4. Штучний інтелект (AI): Що це таке і чому це важливо? URL: https://www.everest.ua/ai-platform/analytics/shtuchnij-intelekt-ai-shho-ce-take-i-chomu-ce-v/.

5. N. Wirth, (2018). Hello marketing, what can artificial intelligence help you with? International Journal of Market Research. 435-438. URL: https://doi.org/10.1177/1470785318776841.

Олейніков Олег Анатолійович,
начальник відділу програмно-технічного забезпечення слідчої та оперативно-розшукової діяльності Управління інформаційних технологій Державного бюро розслідувань

МЕТОДИ ТА ПІДХОДИ ОПРАЦЮВАННЯ ТАБЛИЦЬ З'ЄДНАНЬ АБОНЕНТІВ ЗВ'ЯЗКУ ПІД ЧАС РОЗСЛІДУВАННЯ ТА РОЗКРИТТЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Значна кількість розслідувань пов'язана зі здійсненням тимчасового доступу до даних операторів рухомого (мобільного) зв'язку в частині історичних записів про з'єднання з іншими абонентами, фактів обміну повідомленнями, реєстрації мережі інтернет, використання переадресації дзвінків. В закордонних публікаціях також відомі як CDR (від англ. «*call data records*»). Відомості, отримані в результаті виїмки, можуть бути використані в процесі дослідження події правопорушення, підтверджуючи чи спростовуючи обставини, що підлягають доказуванню. Законодавець визначає загальний порядок здійснення доступу до таких даних, визначаючи їх як охоронювану законом таємницю – інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

Типовий зміст такої інформації складається з табличних записів, що містять відомості про дату та час події, тип з'єднання, цільового абонента та використаного пристрою, другого учасника розмови або використану IP-адресу, інформацію про використану станцію зв'язку.

Сукупність записів надає можливість здійснювати широке коло аналітичних звітів. Типовими задачами є підтвердження

фактів з'єднань, уточнення дати та часу подій, оцінювати переміщення та перебування абонента у періоди, що становлять інтерес для доказування, підтвердження використання певного пристрою.

Окремими напрямками можна виділити опрацювання цих даних з метою встановлення місцезнаходження розшукуваного або виявлення інших епізодів злочинної діяльності, інших співучасників правопорушення.

Методи та підходи до аналізу записів:

Найбільш поширеними є використання табличних процесорів для пошуку окремих записів відповідно критеріїв дати та часу або ідентифікаторів абонентів, що становлять інтерес; формування впорядкованих варіаційних вибірок для виявлення значень, що повторюються частіше (найближче коло спілкування, ділянки місцевості, які відвідуються частіше); виявлення перетинів множин (встановлення переліку спільних співрозмовників, спільного використання пристроїв зв'язку, тощо).

Структура отриманих даних може бути опрацьована з використанням інших статистичних методів, методів аналізу часових рядів або аналізу графів зв'язків. Розширені підходи можуть бути надлишковими для працівників, які безпосередньо залучені до розслідування, але доцільними для формування системних рішень. Також при створенні аналітичних систем чи програмного забезпечення можуть бути використані методи машинного навчання.

Пропонується розділити сценарії опрацювання записів про з'єднання на типові та похідні (розширені, комбіновані).

Типові аналітичні задачі:

Типові аналітичні задачі є інтуїтивно зрозумілими, популярними та покликані відповідати на питання, що перші виникають при дослідженні таких даних. За складність умовно можна виділити задачі:

– щодо одного абонента (перебування у місці злочину, підтвердження використання пристрою, підтвердження з'єднань, що відносяться до обставин вчинення правопорушення);

– порівняння двох абонентів (підтвердження попереднього знайомства співучасників, фактів зв'язків між собою, тривалості знайомства);

– дослідження зв'язків групи абонентів (побудова схем зв'язків, виявлення та оцінки зв'язків осіб, що поєднують співучасників або мають зв'язки з потерпілим).

Основними недоліками типових підходів є абсолютне сприйняття кількісних показників, не врахування особливостей поведінки для кожного з досліджуваних абонентів, обмежена здатність до розширення.

Похідні аналітичні задачі:

Похідні (або розширені) аналітичні задачі можуть полягати у комбінації методів, бути менш очевидними, але мають здатність до виділення закономірностей та фактів, що неможливо досягнути іншим способом або у розумний строк. Умовно можна виділити:

- прикладні статистичні зведення;
- геопросторовий аналіз;
- обернений аналіз співрозмовників;
- зважений аналіз зв'язків;
- застосування алгоритмів машинного навчання.

Здійснення *статистичних зведень* щодо календарних періодів, днів тижня та часу доби з подальшим застосуванням таких зведень до окремої вибірки записів (щодо абонента, станції зв'язку, окремого співрозмовника) дають смогу швидко оцінити характер таких зв'язків. Зв'язки в нічний час або у вихідні дні можуть вказувати на більш особистий характер, тоді як схильність до зв'язків в робочі години – навпаки. Календарні графіки дають змогу оцінити загальні закономірності, що можуть вказувати на зміни у звичній поведінці, повторюваності та періодичності. Певна складність у формуванні зведень виникає через різну «ціну» або «вагу» періодів доби та тижня, зокрема через очікувану різницю у активності вночі або у вихідні дні. Проблема зваженості може бути вирішена нормалізацією даних, що досліджуються, введенням маски ваг відповідно частот кожного з періодів, застосування методів ковзного вікна, тощо.

Зважаючи на загальну концепцію формування окремого запису, яка також полягає у фіксації розташування базової станції зв'язку, це відкриває окремий напрямок *геопросторового аналізу*. Встановлення відвідування абонентом місця вчинення злочину за весь період перевірки не може бути досягнуто класичними методами, оскільки потребує порівнянь всіх зафіксованих ділянок перебування з місцем злочину. Невизначеність дати орієнтовного відвідування створює значні обтяження у вигляді збільшення кількості записів, що потребують перевірки, а також знання місцевості щодо якої здійснюється перевірка. Окрему складність додає невизначеність

відстані обслуговування базових станцій розташованих в різних умовах (рельєфу, щільності покриття, навантаження мережі). Системно задачі геопросторового аналізу можуть бути вирішені застосуванням алгоритмів пошуку спільних сусідів (KNN), оптимізації порівнянь вибірок (апроксимація, використання дерев пошуку), використанням моделей передбачення відстані обслуговування (PathLoss алгоритм, обернено-пропорційна функція, інші методи, що використовуються при побудові мереж). Застосування вирівнювання вибірки та інтерполяції ділянки перебування абонентів дозволяє виявляти можливі зустрічі співучасників злочину, визначення ділянок та їх тривалості, при цьому забезпечивши повну автоматизацію.

Обернений аналіз співрозмовників полягає у здійсненні тимчасового доступу до записів, де абонент, що становить інтерес значився співрозмовником. Зворотня таблиця надає можливість застосувати вже існуючі методи для визначення осіб з кола оточення підозрюваного, які також перебували у ділянках, що становлять інтерес для розслідування. Такий підхід спрощує забір даних та не потребує здійснення запитів щодо всієї множини співрозмовників.

Однією з проблем релевантної візуалізації схем зв'язків або оцінки ступеню зв'язку двох абонентів є орієнтація на кількісні показники з'єднань. Переважно абоненти мають різні вподобання щодо способів зв'язку та різну активність. Використання *зваженої оцінки зв'язків* для кожного окремого абонента дозволяє правильно оцінити його роль у схемі зв'язків або надати більш наближену оцінку щодо ступеню зв'язку з іншим абонентом.

Іншим напрямком автоматизації є застосування алгоритмів *машинного навчання*. Зокрема, алгоритми класифікації (RF, LGBM, XGBoost) та алгоритми кластеризації (DBSCAN, HDBSCAN, HC, KNN, Radius-based KNN) дозволяють визначати групу базових станцій, що обслуговують ділянку з подальшим уточненням місцезнаходження через перекриття ділянок обслуговування; виявлення дійсного кола зв'язків шляхом відсіювання кластеру «дрібних» співрозмовників.

Перспективи розвитку напрямку аналітики з'єднань:

Зважаючи на зростаючу складність аналітичних задач, збільшення використання VoIP телефонії, що схиляє до більшої роботи в напрямку геопросторового аналізу, виникає потреба у створенні повторюваних алгоритмів, які забезпечать необхідний рівень абстракції кінцевого користувача (слідчого,

оперуповноваженого), без необхідності розуміння внутрішньої логіки.

Також значна кількість задач потребує впровадження підходів автоматизації у прийнятті рішень (визначенні переліку дійсного кола зв'язків, припущень щодо наявності зустрічей, формування груп базових станцій, що обслуговують окрему географічну ділянку). Це може бути забезпечено впровадженням комплексних моделей здатних до внесення змін, налаштувань та навчання на тренувальних вибірках.

Популяризація використання сучасних підходів може бути забезпечена наданням кінцевим користувачам ефективних та зрозумілих програмних додатків та проведенням достатньої просвітницької роботи щодо сценаріїв та орієнтовних результатів використання таких інструментів.

Системне впровадження запропонованих методів дозволить значно збільшити ефективність використання даних отриманих в результаті тимчасового доступу до відомостей операторів рухомого (мобільного) зв'язку, скоротити витрати часу аналітиків, здобути додаткові відомості, що сприятимуть розслідуванню.

Паламарчук Іван Васильович,
кандидат юридичних наук, головний спеціаліст Департаменту правового забезпечення Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів (АРМА)

ПЕРЕДУМОВИ ПІДГОТОВКИ АНАЛІТИКІВ ДЛЯ ВИКОНАННЯ ЗАВДАНЬ З ВИЯВЛЕННЯ ТА РОЗШУКУ АКТИВІВ

Невід'ємною складовою державного механізму формування та реалізації як внутрішньої так і зовнішньої політики держави є складові загального механізму держави, зокрема, якими є органи державної влади та їх службові і посадові особи.

Відомо, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1].

Тому догматичним є той факт, що інтерес держави, який спрямований на забезпечення економічного добробуту України –