**УДК 65.012.8+004**

**Олександр Володимирович Манжай,**
*кандидат юридичних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ*

# Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів

Під час розслідування сучасних злочинів правоохоронним органам нерідко доводиться стикатися з необхідністю обробки великих об'ємів даних, що безпосередньо пов'язано із впровадженням інформаційних технологій в усі сфери людського життя. Ця ситуація є характерною для більшості країн сучасного світу.

Велика кількість проваджень, які розслідуються або перебувають під процесуальним керівництвом в однієї особи, тільки ускладнюють проблему в арифметичній прогресії. Немаловажним аспектом цієї проблеми є те, що кадровий склад правоохоронних органів не завжди в повній мірі володіє знаннями і навичками для обробки та аналізу великих об'ємів даних. Тому при обробці та аналізі великих даних силами пересічних слідчих та оперативних працівників треба виходити з необхідності використання якомога простіших програмних рішень.

Одним з різновидів даних, з якими доводиться мати справу правоохоронцям є відповіді установ, підприємств, організацій. Найчастіше, коли мова йде про великі об'єми даних, правоохоронні органи мають справу з банківськими транзакціями, файлами протоколів провайдерів та операторів телекомунікацій, відповідями фінансових установ. Їх аналіз є достатньо нетривіальним завданням, але потрібним, оскільки описані документи можуть містити відомості про справжні IP-адреси фігурантів, їх номери телефонів, інформацію про рахунки для сплати комунальних послуг тощо.

Перша проблема, з якою стикаються правоохоронці, пов'язана з тим, що часто інформацію одержують на підставі запиту правоохоронного органу. Запит не є процесуальним документом, що зумовлює необхідність паралельного проведення слідчої (розшукової) дії «тимчасовий доступ до

речей і документів». Якщо цього не зробити, то строк зберігання відомостей може спливти. Тому, серед іншого, важливо постійно підтримувати контакт з виконавцем запиту. Другим проблемним моментом є те, що не завжди легко знайти контактні дані адресата запитуваних відомостей – відповідного підприємства, установи, організації. Крім того, існують певні вимоги, які слід висувати до змісту та форми наданих відомостей.

Так, під час складання запитової частини відповідного документу важливо скласти формулювання таким чином, аби одержати якомога повну інформацію та убезпечити себе від необхідності додаткового надсилання запитів. Наприклад, під час запитування відомостей по Інтернет-гаманцях слід одразу вказати на необхідності надання повних номерів банківських платіжних карток, які використовувались для поповнення / виведення коштів з гаманців. Також слід одразу запитати дані щодо гаманців, на які виводились кошти та про інші гаманці, з яких виводились кошти на такі ж банківські платіжні картки, що і з указаних в запиті гаманців.

Що стосується форми наданих відомостей, то оптимальним є їх одержання у форматі, придатному для аналізу в табличному процесорі. Проте нерідко трапляються випадки, коли відомості надаються у pdf форматі, та навіть у вигляді зображень. Якщо відомості від організації, підприємства, установи надійшли в pdf форматі, то найбільш якісне переведення до форми таблиці можна здійснити за допомогою функції експорту в програмі Adobe Acrobat Reader Pro. Очевидно, це пов'язано з тим, що компанія Adobe Systems є розробником стандарту pdf.

Під час опрацювання даних, наданих підприємствами, установами, організаціями слід звернути увагу на:

- засоби фільтрації табличних процесорів (простий та водночас потужний інструмент, доступний для розуміння пересічному правоохоронцю);

- засоби візуалізації текстової інформації (корисно використовувати для графічного представлення текстових даних та відображення відповідних зв'язків);

- методи логічного опрацювання;

- засоби автоматизації перевірки та вилучення даних.

В останньому пункті мова йде про програми, спеціально розроблені для вирішення нескладних завдань, спрямованих на автоматизацію

обробки даних:

- перевірка великої кількості IP-адрес на предмет їх належності до українського сегменту кіберпростору;

- вилучення номерів карток з файлів, наданих банками;

- побудова хмари ключових слів з файлу великих даних;

- проведення ретроспективного аналізу за авторством.

Так, наприклад, завантаження усього змісту даних з сайту оголошень протиправного характеру дає матеріал для подальшого аналізу. Цілком ймовірною ситуацією є те, що спочатку особа була пересічним користувачем на форумі, задавала питання, повідомляла якусь інформацію про себе, а згодом її діяльність стала більш злочинно-орієнтованою. Надалі це могло сприяти виникненню злочинного угруповання та, навіть, злочинної організації. Здійснюючи ретроспективний аналіз відповідних повідомлень, інколи можна встановити справжні особисті дані особи фігуранта.

Таким чином, елементарні знання та навички у сфері інформаційних технологій значно збільшують можливості розслідування.

*Одержано 24.10.2019*