Волощенко Андрій Сергійович,
провідний науковий співробітник
Національної академії Служби безпеки
України, кандидат технічних наук,
старший науковий співробітник

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ПРОГРАМНОГО ПРОДУКТУ IBM i2 ANALYST'S NOTEBOOK ДЛЯ АНАЛІТИЧНОЇ ОБРОБКИ ТА ВІЗУАЛІЗАЦІЇ ДАНИХ

Сучасний етап розвитку інформаційного суспільства характеризується стрімким збільшенням обсягів даних, що накопичуються державними органами, підприємствами та організаціями. Інформація надходить із численних джерел: державних реєстрів, інформаційних систем, телекомунікаційних мереж, систем відеоспостереження, банківських операцій, соціальних мереж, відкритих джерел та журналів роботи інформаційних систем. За оцінками фахівців, щоденні обсяги інформації зростають настільки швидко, що їх опрацювання традиційними методами стає практично неможливим.

Особливістю сучасних даних є не лише їхній значний обсяг, а й різноманітність форматів. Поряд зі структурованими базами даних активно використовуються текстові документи, мультимедійні файли, географічні координати, журнали мережевої активності, повідомлення електронної пошти та інші джерела. У результаті аналітик змушений працювати одночасно з десятками інформаційних масивів, між якими необхідно встановити логічні взаємозв'язки. Саме тому останніми роками значного поширення набули технології Big Data та засоби візуальної аналітики [1].

Одним із найпотужніших програмних продуктів цього класу є IBM i2 Analyst's Notebook. Його історія розпочалася ще на початку 1990-х років із розробок компанії i2 Group. Первинною метою створення програмного забезпечення була допомога аналітикам у візуалізації великих обсягів інформації та пошуку прихованих взаємозв'язків між різними об'єктами. Після придбання компанії корпорацією IBM у 2012 році продукт отримав нові можливості інтеграції із серверними платформами, системами управління даними та сучасними засобами

інформаційної безпеки. На сьогодні IBM i2 використовується тисячами організацій у понад 150 країнах світу та підтримує діяльність державних органів, фінансових установ, служб безпеки й комерційних підприємств [2].

Основною перевагою IBM i2 Analyst's Notebook є можливість перетворення великих масивів різнорідної інформації у зрозумілі графічні моделі. На відміну від звичайних електронних таблиць, де взаємозв'язки між записами практично не помітні, система будує діаграми зв'язків, часові лінії, мережеві графи, просторові карти та статистичні залежності. Завдяки цьому аналітик отримує можливість швидко оцінити ситуацію та виявити закономірності, які залишаються непомітними під час традиційного аналізу.

Принцип роботи системи полягає у поданні інформації у вигляді сутностей (осіб, організацій, транспортних засобів, банківських рахунків, телефонних номерів, IP-адрес тощо) та зв'язків між ними. Кожен об'єкт має власний набір атрибутів, а зв'язки можуть характеризувати різні види взаємодії: фінансові перекази, телефонні дзвінки, електронне листування, спільне використання транспортних засобів або участь у певних подіях. У процесі аналізу система автоматично групує інформацію, дозволяючи визначити центральні елементи мережі та ступінь їхнього впливу [3].

Особливу цінність IBM i2 Analyst's Notebook має під час розслідування складних кримінальних правопорушень. Наприклад, під час документування діяльності організованої злочинної групи слідчий може імпортувати до системи інформацію про телефонні з'єднання, банківські операції, результати негласних слідчих (розшукових) дій, дані відеоспостереження та відомості з державних реєстрів. Після автоматичного об'єднання інформації програма формує мережу взаємозв'язків між особами, транспортними засобами, адресами та фінансовими операціями. У результаті можуть бути виявлені координатор злочинної групи, посередники, виконавці та особи, які забезпечують легалізацію доходів, одержаних злочинним шляхом. На малюнку 1 наведено приклад з навчального кейсу з визначення координатора групи за принципом аналізу зв'язків.

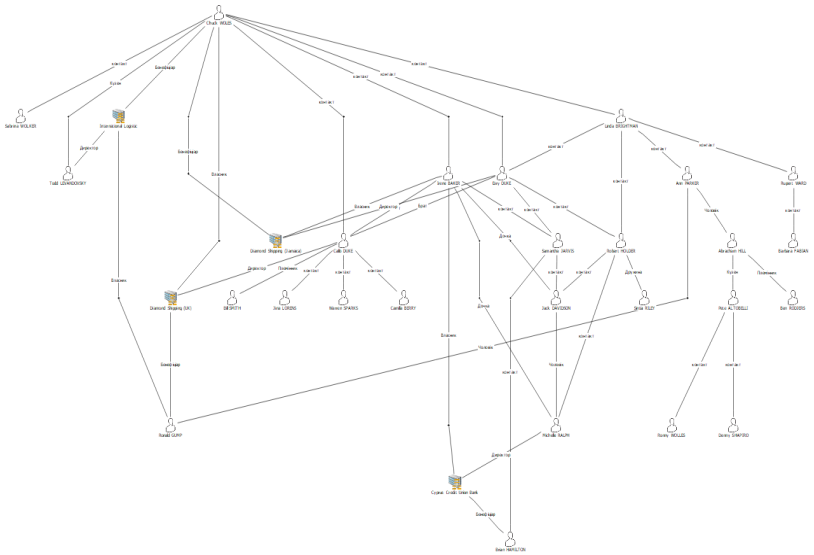

Рис. 1. Ієрархічна схема організації,
створена у IBM i2 Analyst's Notebook

Іншим прикладом є розслідування шахрайства у банківській сфері. Під час аналізу тисяч фінансових транзакцій система дозволяє швидко визначити рахунки, через які проходить найбільша кількість підозрілих переказів, встановити зв'язки між клієнтами банку, компаніями та кінцевими отримувачами коштів. Якщо декілька десятків рахунків використовуються для переведення коштів через одних і тих самих посередників або IP-адреси, IBM i2 автоматично відобразить такі взаємозв'язки у вигляді графічної схеми. Це значно скорочує час аналізу та дозволяє своєчасно заблокувати незаконні фінансові операції.

Не менш ефективно система використовується у сфері кібербезпеки. Під час розслідування комп'ютерного інциденту до IBM i2 можуть бути імпортовані журнали автентифікації користувачів, мережевий трафік, журнали міжмережевих екранів, DNS-запити, інформація про IP-адреси та часові мітки подій. Завдяки цьому аналітик отримує можливість побудувати повний ланцюг розвитку атаки: від первинного проникнення до переміщення мережею, отримання привілеїв та спроб викрадення інформації. Наочне відображення взаємозв'язків між

пристроями, користувачами та серверами значно спрощує пошук джерела компрометації.

Важливе місце в IBM i2 Analyst's Notebook займає часовий аналіз. Його використання дозволяє встановити послідовність подій та виявити причинно-наслідкові залежності. Наприклад, якщо декілька телефонних дзвінків, переказ коштів та переміщення автомобіля відбувалися протягом короткого проміжку часу, система відобразить їх на часовій шкалі. Це допомагає встановити координацію дій між учасниками злочинної діяльності та підтвердити або спростувати окремі слідчі версії.

Ще одним важливим інструментом є геопросторова аналітика. Якщо до системи імпортуються GPS-координати мобільних пристроїв, адреси банкоматів, місця проведення фінансових операцій або координати базових станцій операторів мобільного зв'язку, IBM i2 дозволяє побудувати карту переміщень об'єктів. Наприклад, під час аналізу серії квартирних крадіжок може бути встановлено, що мобільні телефони кількох підозрюваних регулярно реєструвалися поблизу місць вчинення злочинів у схожі проміжки часу. Такі результати дозволяють обґрунтовано формувати подальші напрями оперативної роботи [4].

Візуальна аналітика також значно підвищує ефективність управлінських рішень. Якщо керівнику необхідно швидко оцінити оперативну обстановку, десятки сторінок звітів можна замінити однією інтерактивною діаграмою, яка демонструє основних учасників подій, їхні взаємозв'язки та найбільш критичні елементи мережі. Такий підхід скорочує час підготовки аналітичних матеріалів і полегшує проведення службових нарад та брифінгів.

Серед основних переваг IBM i2 Analyst's Notebook слід виділити можливість інтеграції даних із різних інформаційних систем, автоматичне встановлення взаємозв'язків між об'єктами, підтримку часового, просторового, статистичного та мережевого аналізу, високий рівень наочності представлення результатів, а також можливість спільної роботи декількох аналітиків над єдиною інформаційною моделлю. Усе це суттєво скорочує час проведення аналітичних досліджень і мінімізує ризик пропуску важливих фактів.

Отже, IBM i2 Analyst's Notebook є одним із найбільш функціональних інструментів сучасної візуальної аналітики. Поєднання можливостей інтеграції різнорідних джерел інформації, автоматизованого аналізу зв'язків, часової та геопросторової аналітики дозволяє значно підвищити

ефективність діяльності правоохоронних органів, служб інформаційної та економічної безпеки, фінансових установ і державних організацій. В умовах постійного зростання обсягів даних використання подібних систем стає необхідною складовою сучасної аналітичної діяльності. Подальший розвиток IBM i2 пов'язується з інтеграцією алгоритмів штучного інтелекту, машинного навчання та автоматизованого виявлення аномалій, що дозволить ще більше підвищити якість аналізу та швидкість прийняття обґрунтованих управлінських рішень.

Список використаних джерел

1. Chen H., Chiang R. H. L., Storey V. C. Business Intelligence and Analytics: From Big Data to Big Impact // MIS Quarterly. 2012. Vol. 36, № 4. P. 1165–1188.

2. IBM. IBM i2 Analyst's Notebook Documentation. URL: https://www.ibm.com/docs/en/i2-analysts-notebook

3. Few S. Information Dashboard Design: Displaying Data for At-a-Glance Monitoring. 2nd ed. Burlingame : Analytics Press, 2013. 272 p.

4. Marr B. Big Data: Using SMART Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance. Chichester : John Wiley & Sons, 2015. 256 p.

Гаврилюк Михайло Дмитрович,
начальник відділу кримінального аналізу
Головного управління Національної
поліції у Волинській області

ВИКОРИСТАННЯ В КРИМІНАЛЬНОМУ АНАЛІЗІ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ, ЗОКРЕМА ШТУЧНОГО ІНТЕЛЕКТУ

Стрімкий розвиток цифрових технологій і штучного інтелекту (ШІ) кардинально змінює підходи до забезпечення публічної безпеки та розкриття злочинів в усьому світі. В умовах зростання рівня організованої злочинності, кіберзлочинів і транснаціональних злочинних угруповань традиційні методи кримінального аналізу поступово втрачають ефективність. Саме тому впровадження інноваційних технологій у діяльність правоохоронних органів України є не лише актуальним завданням, а й стратегічним пріоритетом реформування існуючої правоохоронної системи.