Онищенко Ю.М., Гнусов Ю.В.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ІНСТРУМЕНТІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Проблема забезпечення кібербезпеки в Україні пояснюється рядом факторів, зокрема і тим, що національне законодавство потребує суттєвого удосконалення та уніфікації відповідно до міжнародних норм на рівні ООН, Інтерполу, НАТО, Європейського Союзу тощо. Підрозділи кіберполіції Національної поліції України вимагають не тільки доукомплектування кваліфікованими фахівцями, але і відповідного матеріально-технічного забезпечення як сучасною комп'ютерною технікою, так і програмними продуктами, що використовуються у провідних країнах світу для ефективної боротьби з кіберзлочинністю.

У країнах Європи та США під час протидії кіберзлочинності значна увага приділяється не тільки превентивному напрямку діяльності, а й розробці та впровадженню програмних продуктів, що розширюють можливості фахівців правоохоронних органів щодо проведення моніторингу кіберпростору, аналітичного супроводження розслідувань, прогнозування ситуації у тактичному та стратегічному форматі.

Організація інформаційно-аналітичної роботи із застосуванням всіх інноваційних підходів щодо розкриття злочинів, вчинених у кіберпросторі, наразі є чи не вирішальним важелем якщо не для повної детермінації кіберзлочинності, то для ефективної боротьби з нею.

Специфіка розслідування так званих високотехнологічних злочинів, що вчиняються у кіберпросторі, часто пов'язана з обробкою величезних обсягів даних. Під обробкою даних в даному випадку слід розуміти перетворення інформації (сортування, угруповання, збагачення, порівняння тощо) у форми, зручні для роботи; впорядкування зібраних матеріалів шляхом їх систематизації з метою зробити осяжними, компактними, придатними для аналізу, тобто приведення їх до виду, коли фактичні дані починають «говорити».

Виконання вище зазначених завдань стає неможливим без використання спеціалізованого програмного забезпечення інформаційно-аналітичного спрямування. У провідних країнах світу у поліцейській діяльності з протидії кіберзлочинності вже активно застосовуються такі програмні продукти, зокрема аналітичні платформи: IBM I2 (Coplink, Analyst's Notebook, iBase, iBridge тощо), Maltego, Splunk тощо. Ці програмні

інструменти представляють собою візуальні середовища, що дозволяють максимально ефективно використовувати величезні обсяги інформації, накопичені державними службами та підприємствами. Завдяки інтуїтивно зрозумілому інтерфейсу з урахуванням контексту вони дозволяють аналітикам швидко зіставляти, аналізувати і наочно представляти дані з різних джерел, скорочуючи час на пошук важливої інформації в складних даних; надають актуальні й дієві аналітичні засоби, що допомагають виявляти, передбачати, запобігати і припиняти злочинну, терористичну і шахрайську діяльність.

За допомогою спеціалізованого програмного забезпечення аналітичного спрямування правоохоронні органи можуть з високою ефективністю та економією часу виконувати наступні завдання:

- виявляти ключі до розкриття злочинів шляхом упорядкування та надання тактичного, стратегічного доступу і доступу для керівного рівня до великих обсягів даних, які здаються непов'язаними між собою;
- візуалізувати і аналізувати дані на схемах за допомогою відтворення часової послідовності (хронологію подій, що представляють слідчий та оперативний інтерес);
- централізувати кілька сховищ даних в єдиній системі та виявляти приховану цінність в існуючих сховищах інформації;
- використовувати дані спільно з іншими правоохоронними органами (у тому числі зарубіжними, за наявності необхідності міжнародного поліцейського співробітництва) і захищати дані за допомогою таких функцій забезпечення безпеки, як захист за допомогою пароля і шифрування даних;
- здійснювати пошук необхідних даних в потрібному місці в потрібний час - за столом, в машині або з мобільного пристрою;
- швидко систематизувати розрізнені дані в єдиному узгодженому виді;
- визначати ключових осіб, події, зв'язки і закономірності, які не завжди можна виявити іншими засобами;
- у зрозумілому виді представляти структури, ієрархії і способи дій злочинних, терористичних і шахрайських організацій;
- здійснювати обмін складними даними, що дозволяє приймати своєчасні і точні оперативні рішення.

Резюмуючи вище викладене, можна дійти висновку про безумовну перспективність використання правоохоронними органами України спеціалізованого програмного забезпечення аналітичного спрямування, інноваційних методів і засобів інформаційно-пошукової та інформаційно-аналітичної роботи для організації ефективної протидії кіберзлочинності.