Гнусов Ю.В.
кандидат технічних наук, доцент, завідувач кафедри кібербезпеки Харківського національного університету внутрішніх справ,
Онищенко Ю.М.
кандидат наук з державного управління, доцент кафедри кібербезпеки Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ІНСТРУМЕНТІВ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Реалії сьогодення, безпосередньо пов'язані зі стрімким розвитком інформаційно-телекомунікаційних технологій, відкритим, вільним та недостатньо нормативно врегульованим використанням кіберпростору, не тільки розширюють свободу і можливості людей, збагачують суспільство, створюють новий глобальний інтерактивний ринок досліджень, ідей та інновацій, стимулюють відповідальну та ефективну роботу влади, але і створюють загрози для безпеки держави, суспільства та окремих користувачів мережі Інтернет. Питання забезпечення кібербезпеки в Україні, державі з величезним потенціалом у галузі інформаційних технологій, наразі є відкритим, гострим та актуальним.

Проблема забезпечення кібербезпеки в Україні посилюється і тим, що національне законодавство потребує суттєвого удосконалення та уніфікації відповідно до міжнародних норм на рівні ООН, Інтерполу, НАТО, Європейського Союзу тощо; новостворені 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.

Під час протидії кіберзлочинності в країнах Європи та США значна увага приділяється не тільки превентивному напрямку діяльності, а і 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.

Українське законодавство також чітко регламентує повноваження поліції у сфері інформаційно-аналітичного забезпечення, зокрема передбачає, що підрозділи Національної поліції України можуть формувати бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; користуватися базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; здійснювати інформаційно-

пошукову та інформаційно-аналітичну роботу; здійснювати інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями. Також поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень [1].

Необхідно зазначити, що організація інформаційно-аналітичної роботи із застосуванням всіх інноваційних підходів (методів і засобів) 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 вчинюються 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 та інші.

Зазначені програмні інструменти інформаційно-аналітичного спрямування 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 і дієві аналітичні засоби, що допомагають виявляти, передбачати, запобігати і припиняти злочинну, терористичну і шахрайську діяльність [2].

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 і 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 в потрібному місці в потрібний час - за столом, в машині або з мобільного пристрою [3];
- 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;
- економити час за рахунок оперативного впровадження, яке забезпечує швидке зростання продуктивності, завдяки надійним рішенням для візуальної аналітики.

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.

Використані джерела:

1. Про Національну поліцію України: Закон України: [Електронний ресурс] – URL: http://zakon3.rada.gov.ua/laws/show/1556-18 (дата звернення: 22.11.2016).
2. Анализ и визуализация данных для эффективной аналитики [Електронний ресурс] – URL: http://www-03.ibm.com/software/products/ru/analysts-notebook (дата звернення: 22.11.2016).
3. Программное обеспечение для полиции, позволяющее лучше собирать, совместно использовать и анализировать информацию [Електронний ресурс] – URL: http://www-03.ibm.com/software/products/ru/coplink (дата звернення: 22.11.2016).