підвищувати його. Це ж стосується викладачів і тьюторів (тренерів), які здійснюють підготовку таких фахівців.

Відповідними темпами повинна оновлюватися матеріальна база як підрозділів кіберполіції так і закладів, де здійснюється їх підготовка і перепідготовка. В першу чергу, встигати за швидкими технологічними змінами повинні тренувальні комплекси, які є інструментальною основою системи підготовки. І це повинні бути сучасні високоефективні комплекси типу «Програмно-апаратний симулятор TnS для підготовки фахівців з реагування на кібер-інциденти та загрози», розроблений компанією CyberBit, Ізраіль. Навчально-тренувальний центр з підготовки фахівців для кіберполіції повинен мати сукупність таких інструментальних засобів для відпрацювання практичних навичок різних напрямів дій фахівців в умовах, максимально наближених до реальних. Використання таких засобів передбачає сучасний рівень технічного обладнання тренінгових центрів. Сучасні тренувальні багатофункціональні комплекси такого типу, як і комп'ютерні комплекси для їх функціонування, коштують немалих грошей, але альтернативою є лише суттєвє зниження рівня підготовки фахівців. Не слід також недооцінювати фактор матеріальної мотивації висококваліфікованих фахівців: заробітна платня фахівців поліцейських підрозділів не повинна кардинально (в менший бік) відрізнятися від заробітної плати у комерційних структурах, інакше рано чи пізно неминучий відтік висококваліфікованих кадрів.

І якщо ці фактори не враховувати в навчальному процесі, це матиме негативний вплив на якість підготовки фахівців і, відповідно, на ефективність діяльності підрозділів кіберполіції у протистоянні кіберзлочинності.

Список використаних джерел:

1. Овчинский В. С. Криминология цифрового мира: учеб. М. : Норма ; ИНФРА–М, 2018. 352 с.

УДК 65.012.8 + 004

МИХАЙЛО ЮРІЙОВИЧ БУРДІН
Проректор Харківського національного університету внутрішніх справ,
доктор юридичних наук, професор

ІНСТРУМЕНТАЛЬНІ ЗАСОБИ КРИМІНАЛЬНОГО АНАЛІЗУ В РОЗСЛІДУВАННІ ЗЛОЧИНІВ

В навчальному посібнику, розробленому експертами-аналітиками різних держав в рамках співробітництва з Organization for Security and Co-operation in Europe (OSCE) [1] для , відзначено: «Той факт, що екстремісти, пов'язані з недавніми терористичними актами, включаючи терористів-одинаків, залишалися поза полем зору правоохоронних органів, обумовив

необхідність вироблення попереджувального підходу і всебічного обміну і централізованого аналізу відповідних даних та інформації. Усвідомлення того, що робота за принципом реагування не забезпечить запобігання терористичних актів та раннє виявлення інших серйозних інцидентів, ставить ILP в центр уваги на міжнародній правоохоронній арені.». В цьому реченні у дуже стислому вигляді сформульована необхідність і актуальність якнайшвидшого переходу діяльності правоохоронних органів європейських держав з традиційного принципу реагування на правопорушення на сучасний принцип профілактики і запобігання правопорушенням на основі оперативних даних та інформації – ILP. Передумовою і обгрунтуванням цієї концепції є бурхливий розвиток інформаційних технологій і супроводжуючий його інформаційний вибух. Якщо ще не так давно проблемою в процесі розслідування злочину був пошук і збір даних, то зараз проблемою частіше є виявлення в наявному величезному обсязі різнотипних даних з багатьох джерел корисної інформації у вигляді прихованих або неявних зв'язків типу «об'єкт-об'єкт», «об'єкт-подія», «подія-подія» для формування пропозицій для подальших управлінських рішень або гіпотез щодо розкриття злочину.

Ключовим і самим складним етапом технології ILP є Аналіз, в процесі якого здійснюється систематизація і аналітична обробка зібраних на попередніх етапах даних та інформації [1]. Причому на сучасному етапі кількість інформації, яка підлягає обробці і аналізу, досягає настільки великих обсягів, що людина вручну не в змозі їх опрацювати за реальний час. Тому ефективність виконання цього етапу визначається тими інструментальними засобами, які має в своєму розпорядженні аналітик. В першу чергу, наявністю сучасних програмних інструментальних засобів. В загальному випадку під інструментальними засобами аналітика будемо розуміти програмні системи або модулі і методики і методології опрацювання інформації.

Загальну класифікацію інструментальних засобів кримінального аналізу можна представити наступним чином:

1. Методології і методики аналізу.
2. Загальновикористовувані програмні засоби.
3. Традиційні інформаційно-пошукові системи.
4. Спеціалізовані інформаційно-аналітичні системи і комплекси кримінального аналізу.

До інструментів першої групи можна віднести, зокрема, такі часто використовувані методики як мережний аналіз, ANACAPA, SOCTA. Вони застосовуються як в ручному так і в автоматизованому режимі.

Мережний аналіз це загальна методологія аналізу, яка передбачає використання математичного апарату теорії графів для дослідження і виявлення зв'язків між об'єктами і подіями.

ANACAPA представляє собою методику розслідування злочинів і аналізу оперативної інформації, яка була розроблена в 1960-ті роки, після вбивства президента Кенеді. Методику названо на честь острова на західному

узбережжі Америки. Спочатку методика представляла собою систему структурування, візуалізації та аналізу інформації у паперовому виконанні. В подальшому фірмою Anacapa Sciences Inc. (США) були розроблені програмні продукти, які реалізують дану методику. Anacapa Sciences Inc. стояла у витоків розробки спеціальних аналітичних методик для сфери безпеки і ще на початку 1970-тих років почала проведення навчальних курсів з підготовки фахівців-аналітиків. На даний момент Anacapa Sciences Inc. пропонує наступні 4 базових курси:

1) аналіз інформації в ході проведення розслідувань Criminal Intelligence Analysis (CIA);

2) аналітичні методи розслідування Analytical Investigation Methods (AIM);

3) аналіз фінансових махінацій Financial Manipulation Analysis (FMA);

4) поглиблений аналіз з використанням комп'ютерних технологій Computer-Aided Analysis (CAA).

SOCTA (SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT) є методикою з оцінки ризиків щодо тяжких злочинів та організованої злочинності. SOCTA – ключовий стратегічно-аналітичний документ, присвячений боротьбі зі злочинністю, розроблений Європолом. Останній документ SOCTA опублікований Європолом у 2017 році – SOCTA 2017. Він готувався на протязі 2015-2017 років. В ході його підготовки був проведений безпрецедентний за масштабами аналіз серйозної і організованої злочинності, за результатами якого розроблені відповідні рекомендації.

До інструментів другої групи можна віднести комп’ютерні програми і системи загального призначення та проблемно-орієнтовані, які з успіхом використовуються для розв’язання задач кримінального аналізу з відносно невеликим обсягом даних. До числа таких інструментів можна віднести Microsoft Excel, MatCAD, MatLAB, StatGraph, Statistica та ін. Можливість ефективного застосування цих інструментів значною мірою визначається наявністю відповідних методик їх застосування для розв’язання конкретних задач кримінального аналізу, кваліфікацією і практичним досвідом фахівців. До інструментальних засобів цієї групи можна також віднести гео-інформаційні системи (ГІС), призначені для візуалізації об’єктів і подій на географічній мапі. Без застосування ГІС на сучасному етапі неможливо уявити аналітичну роботу як у правоохоронній так і у цивільній сфері. Вони є базовим інструментом візуалізації даних.

Типовими прикладами традиційних інформаційно-пошукових систем можна вважати Ліга-Закон і Google. Принципом роботи таких систем є опрацювання пошукового запиту, сформованого за певним шаблоном. Результатом роботи є перелік даних або документів, які відповідають пошуковому запиту. До систем такого типу належить і відомча інформаційно-пошукова система «Інформаційний портал Національної поліції України». Головною метою систем даного типу є пошук інформації. Вони, як правило, не мають інструментів аналітичної обробки великих і надвеликих обсягів інформації.

Найбільш ефективними інструментами кримінальних аналітиків є спеціалізовані інформаційно-аналітичні системи і комплекси кримінального аналізу. Системи цього класу мають потужний набір інструментів аналітика, які дозволяють проводити глибокий всебічний аналіз великих обсягів різнотипних даних і формувати гіпотези щодо аналізуємих подій і об'єктів. Найбільш відомими системами даного класу є I2, Palantir, HOLMS2, RICAS, Maltego.

Список використаних джерел:

1. Vol. 13 OSCE Guidebook Intelligence-Led Policing, TNTD/SPMU Publication Series Vol. 13, Vienna, June 2017.

УДК 343.9:159.9.075

ЛЕОНІД ВОЛОДИМИРОВИЧ МОГІЛЕВСЬКИЙ
Проректор Харківського національного університету внутрішніх справ,
доктор юридичних наук, професор

АРГУМЕНТАЦІЯ ЄДИНОГО ПІДХОДУ АРХІТЕКТУРИ БАЗ ДАНИХ ПРАВООХОРОННИХ АГЕНЦІЙ УКРАЇНИ

Згідно Рішення Колегії МВС України від 05.11.2018 р. № 18КМ, а також Наказу МВС України від 11.12.2018 р. № 1004 в МВС України з метою інтеграції інформаційних ресурсів МВС в національну систему електронної взаємодії державних інформаційних ресурсів в МВС розробляється і впроваджується Єдина Інформаційна Система органів внутрішніх справ України. В Концепції і Програмі реалізації цієї Концепції передбачено створення єдиної програмно-технічної платформи для інформаційної взаємодії всіх відомчих структур МВС України. Крім того, цими документами передбачено реалізація механізму міжвідомчої взаємодії ЄІС з інформаційними ресурсами інших відомств.

В рішенні колегії МВС України від 05.11.2018 р. № 18КМ також зазначено, що «існує нагальна потреба в забезпеченні автоматизованого доступу центральних органів виконавчої влади, у межах повноважень, до електронних інформаційних ресурсів МВС та ЦОВВ і в агрегації даних» оскільки МВС постійно здійснює активну інформаційну взаємодію з такими відомствами як Служба безпеки України, Національне антикорупційне бюро України, Генеральна прокуратура України, Міністерство юстиції, Національний банк України тощо. На поточний момент така взаємодія здійснюється «…за принципом формування запиту та відповіді безпосередньо користувачем, тоді як доцільно забезпечити автоматизований доступ у межах повноважень і агрегацію даних». Такий же принцип реалізований у взаємодії муж окремими відомствами всередині МВС оскільки інформаційні ресурси відомств як правило мають характер закритих корпоративних розподілених систем, які побудовані незалежно одне від