тактику реагування та розслідування, значно спростити щоденні завдання. В результаті, процес прийняття рішень стає більш ефективним і виваженим.

УДК 65.012.8 + 004

СЕРГІЙ МИКОЛАЙОВИЧ БОРТНИК
Перший проректор Харківського національного університету внутрішніх справ, доктор юридичних наук, полковник поліції

ПРОБЛЕМИ ПІДГОТОВКИ КАДРІВ ДЛЯ ПІДРОЗДІЛІВ КІБЕРПОЛІЦІЇ УКРАЇНИ

Характерним і незворотним трендом епохи третьої і четвертої промислових революцій є стрімкий перехід матеріальних відносин у віртуальну сферу. Одним з негативних наслідків цього в цілому позитивного процесу є віртуалізація все більшої частки кримінальних правопорушень. Серед фахівців існує думка, що вже в найближчі 10 років зникнуть всі види злочинів, крім кіберзлочинів [1]. І це не популістська заява, а цілком обгрунтоване передбачення, засноване, в першу чергу, на таких двох факторах: а) можливість дистанційного отримання великих коштів незаконним шляхом, і б) відносна безпека і анонімність для виконавця.

Як проміжний етап реагування правоохоронних структур цивілізованого світу на цей виклик є створення підрозділів кіберполіції. В подальшому префікс кібер- можна буде відкинути, оскільки більшість підрозділів поліції будуть займатися профілактикою і розкриттям розгалужених різновидів кіберзлочинів.

Правоохоронці по всьому світу всерйоз готуються до появи підпільних синдикатів, що спеціалізуються на замовних високотехнологічних вбивствах, замаскованих під технічні інциденти різного роду. Беручи до уваги обсяг ринку замовних вбивств в Сполучених Штатах, що становить близько 2 млрд. дол. на рік, фахівці ФБР очікують появу такого мережевого синдикату, а швидше за все не одного, а декількох, в найближчі один-два роки. Враховуючі той факт, що така думка була висловлена 2 роки тому, є підстави вважати, що такий синдикат (синдикати) на поточний момент вже існують.

Головним інструментом подібних синдикатів можуть стати не хакерські програми самі по собі, а штучний інтелект.

Враховуючі вищезазначені обставини, не підлягає сумніву, що для виконання таких злочинів будуть а) залучені висококваліфіковані фахівці в галузі ІТ технологій і інтелектуальної обробки великих масивів даних з відповідно високим матеріальним заохоченням, б) залучене потужне високотехнологічне технічне і програмне забезпечення [1].

З цього незворотно випливає логічний висновок, що кваліфікація фахівців кіберполіції повинна бути як мінімум не гіршою ніж кіберзлочинців. Ситуація ускладнюється тим, що бурхливо розвивається як програмне так і технічне забезпечення комп'ютерів і комп'ютерних мереж, тобто змінюються їх можливості і, відповідно, правила їх застосування, що вимагає від фахівців

у цій сфері постійно вивчати і засвоювати нові інструментальні засоби для того, щоб не тільки підтримувати свій кваліфікаційний рівень, а й 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,