Другий напрям – це приватні цивільні кіберполігони. Основними завданнями таких кіберполігонів (*на прикладі рішення компанії Forward Defense м. Абу-Дабі, ОАЕ*) є: організація та проведення навчальних кібердій наступального та оборонного характеру в реальному масштабі часу з можливостями їх *3D* моделювання; моделювання кібермісій та навчання дій перед проведенням кібероперації; динамічне створення різноманітних мережних комунікацій для відпрацювання дій.

Третій напрям – це національні кіберполігони військового призначення. На прикладі кіберполігону *National Cyber Range* (*м. Орландо, шт. Флорида, США*) збройних сил США встановлено, що основним його призначенням є побудова масштабованої моделі Інтернету для проведення військових кіберігор. Також полігон використовується для створення антивірусних засобів захисту й відпрацювання технологій протидії явищам кібертероризму.

Четвертим напрямом є міжнаціональні кіберполігони. Основним завданням міжнаціональних кіберполігонів (*на прикладі кіберполігону НАТО м. Таллінн, Естонія*) є підготовка експертів під час міжнародних кібернавчань та тренінгів у сфері безпеки інформаційно-комунікаційних систем. Можливості кіберполігону дозволяють моделювати кіберсередовище й відпрацьовувати в ньому випробування рішень та інструментарію у сфері захисту інформаційних технологій.

Узагальнивши та систематизувавши передовий досвід до основних завдань, які покладаються на кіберполігон, можна стверджувати, що як навчальне середовище з метою підготовки персоналу для боротьби з кіберзлочинністю він може використовуватися за такими основними напрямами:

для практичного відпрацювання методик із запобігання, виявлення, припинення та розкриття кіберзлочинів;

відпрацювання методик підвищення інформованості громадян про безпеку в кіберпросторі;

для практичної апробації спеціалізованого програмного забезпечення, призначеного для вирішення спеціальних завдань тощо.

У доповіді розкрито структуру типового кіберполігону, який може бути використаний для вирішення описаних вище та інших додаткових завдань. Показано його склад та можливості, розкрито перспективи створення такого кіберполігону у вищих навчальних закладах України.

Література:

1. Грищук Р. В. Основи кібернетичної безпеки : монографія / Ю. Г. Даник, Р. В. Грищук ; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.
2. Конвенція про кіберзлочинність // Верховна Рада України. – 2005. [Електронний ресурс]. – Режим доступу до ресурсу : http://zakon2.rada.gov.ua/laws /show/994_575. – Назва з екрану.
3. Стратегія кібербезпеки України : Указ Президента України від 15 березня 2016 року № 96/2016 [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/962016-19836. – Назва з екрану.
4. Самчишин О. В. Проект кібернетичного полігону для підготовки висококваліфікованих фахівців у галузі інформаційної безпеки держави / О. В. Самчишин, В. В. Умінський // Сучасний захист інформації. – К. : ДУІКТ, 2012. – № 2. – С. 65–71.

Пріоритетні напрямки діяльності кіберполіції у сфері протидії кіберзлочинності в Україні

Косаревська О.В.
кандидат педагогічних наук., доцент
доцент кафедри кібербезпеки та
інформаційного забезпечення ОДУВС

В сучасних умовах поглиблення процесу інформатизації та впровадження сучасних інформаційних технологій в економіці, управлінні, кредитно-банківській діяльності, стрімкий розвиток інформаційно-телекомунікаційних технологій на основі використання глобальної інформаційної мережі «інтернет» та спрощення доступу до неї широкого кола користувачів через персональні комп’ютери обумовили зростання злочинних проявів в системі інформаційних відносин та інформаційної безпеки.

Протидія кіберзлочинності останнім часом набуває своєї актуальності за рахунок: високих темпів її зростання, корисливої мотивації та транснаціональної спрямованості; перенесення центру тяжіння на скоєння комп’ютерних злочинів з використанням глобальних комп’ютерних мереж; вдосконалення способів скоєння цих злочинів, за рахунок зростання рівня професіоналізму

комп'ютерних злочинців; правової неврегульованості взаємодії суб'єктів правовідносин, що складаються під час використання «інтернет»; недостатньої міжнародної взаємодії між правоохоронними поліцейськими структурами; прорахунків у діяльності суб'єктів забезпечення кібербезпеки України в вирішенні системного кіберзахисту країни.

Огляд сучасної наукової думки та аналіз діяльності підрозділів кіберполіції в структурі кримінальної поліції Національної поліції України, що відбилося у роботах провідних фахівців таких, як: Біленчука Д.П.; Васильєва А.А.; Вєхова В.Б.; Гусєва В.О.; Довженка Л.М.; Катеринчука І.П.; Кобзаревої І.В.; Корміч Б.А.; Користіна О.Є.; Лешукової І.В.; Пархоменка Л.В.; Пашнєва Д.В. та інш., дають підстави наголосити основні пріоритетні напрямки діяльності кіберполіції України у сфері протидії кіберзлочинності.

1. Вдосконалення загально-державного законодавства у сфері закріплення функцій та персоніфікації операторів та Internet-провайдерів телекомунікацій, як суб'єктів інформаційних відносин у сфері протидії кіберзлочинності.

Останнім часом комп'ютерна злочинність і комп'ютерний тероризм набули значної масштабності з огляду загроз національній безпеці в інформаційній сфері, яка складає одну з основ життєдіяльності суспільства, тому особливого значення набуває нейтралізація негативного впливу і подолання суспільно-небезпечних факторів які мають прояви в глобальних комп'ютерних мережах.

Так, згідно ст. 35 Конвенції про кіберзлочинність та доручення Президента України від 3 грудня 2010 р. № 02/78475-01 МВС України було створено контактний пункт з реагування на кіберзлочини у структурі Департаменту боротьби з кіберзлочинністю і торгівлею людьми МВС України. На сьогодні національний контактний пункт здійснює свою діяльність цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення.

Більшість запитів, які надсилаються та надходять каналами національного контактного пункту (НКП), стосуються отримання інформації, яка знаходиться в операторів та провайдерів телекомунікацій про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання, так як ця інформація здебільшого має суто технічний характер та є первинною інформацією при проведенні перевірки за будь-яким фактом учинення адміністративного або кримінального правопорушення.

При цьому в п.7 ст.162 КПК України забороняє розповсюдження інформації, яка знаходиться у операторів та провайдерів телекомунікацій.

Національний контактний пункт (НКП), на базі якого створено та функціонує вказана цілодобова контактна мережа, знаходиться в складі оперативного підрозділу - Управління боротьби з кіберзлочинами (УБК). У випадках, якщо цією мережею надходить запит від оперативного підрозділу іноземної держави, то УБК має право безпосередньо його виконати. Проте, відповідно до чинного законодавства, виконання запитів від органів досудового розслідування не входять до його компетенції.

Неузгодженість окремих норм КПК України та інших держав, а також особливі властивості електронних доказів, як: нестійкість та недовговічність збереження висувають необхідність розробки та нормативного закріплення механізму отримання інформації від операторів та провайдерів телекомунікацій за запитами як національних так і міжнародних правоохоронних органів щодо збирання доказів у справах про кіберзлочини і встановлення місцезнаходження підозрюваних в рамках Конвенції Про кіберзлочинність.

2. Вдосконалення професійної підготовки та підвищення кваліфікації кадрів для підрозділів кіберполіції України.

Фахова підготовка спеціалістів для підрозділів кіберполіції починається з навчання у ВНЗ з особливими умовами навчання, яка передбачає юридичну, тактико-спеціальну, психологічну та інформаційно-технологічну підготовку.

З огляду сучасної педагогічної парадигми у сфері підготовки кадрів для підрозділів кіберполіції пріоритетними напрямками, на наш погляд, слід вважати наступне.

2.1. В рамках навчально-виховного процесу ВУЗів зі специфічними умовами навчання підготовки майбутніх фахівців базової спеціалізації: «Боротьба з кіберзлочинністю», «Комп'ютерна безпека» надзвичайно важливим постає удосконалення первинного загально-освітнього рівня комп'ютерної грамотності навчаємих за рахунок:

- спеціалізованої інформаційно-технічної підготовки;
- підвищення рівня професійної компетенції науково-педагогічного складу;
- впровадження сучасних комп'ютерних технологій у навчання;

- створення практико-орієнтованого середовища, за рахунок інноваційних виробничих технологій «соціального партнерства» та «модернізації професійно-технічного навчання».

2.2. В рамках перепідготовки для підрозділів кіберполіції доцільним, на наш погляд, буде ознайомлення з сучасними експертно-криміналістичними дослідженнями у сфері боротьби з кіберзлочинністю по збору, фіксації, аналізу і звітності доказів, отриманих за допомогою інформаційних технологій.

Наприклад:

- проведення комп'ютерно-цифрової експертизи, за рахунок експертно-криміналістичного програмного забезпечення, яке використовується практичними працівниками оперативних та слідчих підрозділів Національної поліції України;

- оцінки рівня кібербезпеки в Україні (автор Кудімов В.А.), за рахунок числової характеристики комплексного показника кібербезпеки держави;

- аналізу соціальних мереж – прогноз формування зв'язків між «акторами» та «співтовариствами», що дозволяють прогнозувати ступінь інформаційно-психологічних впливів та інформаційно-психологічного керування. (Автори: Мелешко Є.В., Строк Ф.В., Новіков Д.А.).

3. Активізація міжнародної взаємодії між правоохоронними поліцейськими структурами у сфері протидії кіберзлочинності.

В рамках європейської Конвенції про взаємодопомогу у кримінальних справах між державами учасницями Європейського Союзу необхідними, на наш погляд, постають наступні завдання:

- проведення уніфікації національного кримінального та кримінального процесуального законодавств щодо протидії кіберзлочинам, з метою усунення норм подвійного права;

- розробка на міжнародному рівні та імплементації в національні законодавства держав учасниць міжнародної правоохоронної співпраці процесуальних стандартів в розслідуванні злочинів в глобальних інформаційних мережах, з метою вирішення проблем оперативного-отримання із закордону вилученої або збереженої, на час надання правової допомоги, комп'ютерної інформації в документальному вигляді для використання її у якості доказів;

- вдосконалення протоколів офіційної правової допомоги для ефективного розслідування злочинів і вирішення проблем оперативного отримання із закордону вилученої або збереженої, на час надання правової допомоги, комп'ютерної інформації в документальному вигляді для використання її в якості доказів;

- організація забезпечення обміну адресами операторів та провайдерів інформаційних мереж (постачальників).

На підставі вищезазначеного ми дійшли наступних узагальнень.

До основних заходів попередження кіберзлочинності та шляхів удосконалення діяльності підрозділів кіберполіції України слід віднести:

Правові заходи:

1) удосконалення чинного законодавства у сфері боротьби з комп'ютерними злочинами в глобальних інформаційних мережах;

2) нормативно-правове урегулювання процесуально-кримінальних процедур по міжнародній взаємодії правоохоронних структур в сфері отримання інформації від операторів та провайдерів телекомунікацій.

Організаційно-технологічні заходи:

1) забезпечення підрозділів кіберполіції необхідним спеціалізованим програмним та апаратним забезпеченням у сфері виконання оперативно-розшукових завдань з протидії кіберзлочинності;

2) укріплення матеріально-технічної бази ВНЗ з особливими умовами навчання по створенню профільних навчальних класів з сучасним інформаційним забезпеченням та лабораторій кримінального аналізу.

Криміналістичні заходи:

1) підвищення наукового потенціалу вищих навчальних закладів системи МВС України та практичних підрозділів Національної поліції України в сфері розробки сучасних методик розслідування кіберзлочинів та проведення експертиз по фіксації «електронних слідів», удосконалення теоретико-методологічних засад категорійного апарату в сфері кіберзлочинності.

Література:

1. Конвенція Ради Європи про кіберзлочинність: від 21.11.2001 [електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.

2. Указ «Про введення в дію рішення Ради національної безпеки та оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» http://zakon2.rada.gov.ua/laws/show/96/2016.

3. Кіберзлочинність у всіх його проявах:види, наслідки та способи боротьби [Електронний ресурс] http://gurt.org.ua/articles/34602/.

4. Кримінальний процесуальний кодекс України//Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88. Редакція від 03.08.2017 р. [Електронний ресурс] http://zakon5.rada.gov.ua/laws/show/4651-17.

5. Наказ Національної поліції України від 10.11.2015 № 85 «Про затвердження Положення про Департамент кіберполіції Національної поліції України».

Деякі аспекти міжнародного співробітництва правоохоронних органів у сфері боротьби з кіберзлочинністю

Косаревська О.В.
кандидат педагогічних наук, доцент,
доцент кафедри кібербезпеки
та інформаційного забезпечення ОДУВС
Шутило С.В.
слухач 2 курсу магістратури
факультету №4 ОДУВС

Сучасні інформаційні технології є новим засобом масової комунікації оскільки вони охоплюють практично всі сфери людської діяльності. Слід відзначити, що технічне удосконалення телекомунікаційних систем глобального зв'язку і спрощення доступу до використання інформаційних технологій веде до трансформації злочинності, яка для реалізації протиправних намірів переміщується у кіберпростір.

Сама мережа інтернет створює існування кіберзлочинності ознаками якої є: висока латентність, за рахунок можливості здійснювати протиправні дії швидко, безконтактно з жертвою, на великій відстані і багаторазово.

Беручи до уваги той факт, що з кожним днем кіберзлочинність зростає та розповсюджується і жодна держава сьогодні вже не спроможна самостійно протистояти цій небезпеці, з'явилася наявна необхідність активізації міжнародного співробітництва у цій сфері.

Огляд сучасної наукової думки, стосовно проблеми міжнародної взаємодії правоохоронних органів у сфері протидії кіберзлочинності, що відбилося у роботах: Бондаренка О.О., Бутузова В.М., Гвоздецької В.В., Глобенко Г.І., Гусева В.О., Лешукової І.В., Літвінова М.Ю та інш., доводить актуальність цієї проблеми, яку, на наш погляд, слід розглядати в наступних аспектах.

1. Оскільки, сьогодні як на міжнародному, так і на національному рівні відсутнє універсальне визначення «кіберзлочинності» чи «комп'ютерного злочину», вкрай необхідним є узгодження термінологічного апарату визначення міжнародної кіберзлочинності, що дозволить більш точно визначити її межі, а також правильно кваліфікувати дії винних осіб.

2. Окремі недоліки в системі міжнародного законодавства стосовно захисту глобальних інформаційних мереж від кібератак відбуваються за рахунок існуючої неузгодженості національних та міжнародних правових актів, стосовно закріплення єдиного правового механізму міжнародної взаємодії правоохоронних органів у забезпеченні трансграничного доступу до інформації щодо суб'єктів транснаціональної кіберзлочинності та комп'ютерного тероризму.

3. Також слід наголосити на відсутність єдиних стандартів та сталих методик по фіксуванню і тимчасовому зберіганню виявлених електронних доказів під час проведення оперативно-розшукових і розвідувальних заходів, що проводяться міжнародними поліцейськими структурами.

Одним із важливих підходів щодо боротьби з кіберзлочинністю у транснаціональному аспекті і розвитку міжнародної співпраці, було створення та спроби стандартизації відповідної нормативно-правової бази, що на теперішній час активно застосовується в багатьох країнах.