– блокування сайтів із забороненою інформацією.

2. Зміцнення потенціалу спеціальних органів, які протидіють кіберзлочинності, оснащення їх сучасними програмно-технічними засобами.

3. Координація діяльності підрозділів різних правоохоронних відомств.

4. Широке інформування населення про заходи безпеки в кіберпросторі.

5. Тісне міжнародне співробітництво із закордонними правоохоронними органами, використання можливостей Євроюсту та Європолу.

1. Николай Коваль, руководитель команды реагирования на компьютерные инциденты CyS-CERT [Електронний ресурс]. – Режим доступу: http://internetua.com/k-kakim-priemam-kiberprestupnikov-nuzgno-gotovitsya-ukraincam-v-2017-m

2. [Електронний ресурс]. – Режим доступу: http://ema.com.ua/fraud-digest-5-01-2017/

3. [Електронний ресурс]. – Режим доступу: https://www.nomoreransom.org/

4. [Електронний ресурс]. – Режим доступу: cybercrime.gov.ua

Кононець Віта Петрівна
ст. викладач кафедри адміністративного права,
процесу та адміністративної діяльності,
кандидат юридичних наук

Карпенко Андрій Віталійович
курсант факультету підготовки фацівців
для підрозділів поліції превентивної діяльності

*(Дніпропетровський державний
університет внутрішніх справ)*

ЩОДО ЗАРУБІЖНОГО ДОСВІДУ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Актуальність обраної теми полягає в тому, що стрімкий розвиток інформаційного суспільства охоплює практично усі сфери життя людини – від науки до державного управління. Інформатизація стає основною ознакою переходу цивілізованого світу до нового простору. Зростає роль та місце захисту інформації поряд із захистом прав та свобод людини та громадянина, особливо якщо ця інформація має обмежений доступ.

Становлення нового інформаційного суспільства в Україні має певну низку проблем як технічного, так і нормативно-правового характеру. В першу чергу це обумовлено тим, що швидкий розвиток інформатизації супроводжується злочинним зловживанням таких технологій. Тому питання кіберзлочинності в Україні є досить актуальним та потребує наукового дослідження [1, с. 67].

Аспекти становлення, розвитку та здійснення протидії кіберзлочинності розглядалися такими науковцями: М. О. Будаков, В. М. Бутузов, М. М. Галамб, Р. А. Калюжний, В. В. Коваленко, Я. Ю. Кондратьєв, Б. А. Кормич, Ю. Є. Максименко, А. І. Марущак, Г. В. Новицький та іноземними фахівцями А. Роберт, К. Осакв, Т. Блентан, Д. Банісар.

Однак дослідження цієї галузі потребує постійного удосконалення, адже

інформатизація не стоїть на місці, а українське законодавство має низку прогалин у цьому питанні та потребує модернізації та реформування, а також запозичення зарубіжного досвіду протидії кіберзлочинності [2, с. 5–6].

Становлення інформаційного суспільства має як позитивні, так і негативні наслідки. Серед позитивних – прискорення інформаційного розвитку дає змогу швидко отримувати та обмінюватися інформацією, а серед негативних – не уся інформація має загальний доступ, тим самим є об'єктом для злочинних посягань.

Одним із підходів до боротьби з кіберзлочинністю є стандартизація нормативно-правової бази. На міжнародній арені Радою Європи 23 листопада 2001 року було прийнято Конвенцію про кіберзлочинність, яка стала фундаментом у боротьбі з кіберзлочинністю на міжнародному рівні, а також сприяла співпраці держав у даному напрямку, оскільки Конвенція є відкритою для підписання. Для багатьох країн світу боротьба з мережевою злочинністю (кіберзлочинністю), що стрімко розвивається завдяки впровадженню в економічні процеси сучасних технологій, є досить болючим питанням [4, с. 89].

Основними проблемами викриття, протидії та розслідування "транскордонних" злочинів є територіальність та проміжок часу, впродовж якого може зберігатися інформація. Поліції дуже складно окреслити територію здійснення злочину та місцезнаходження злочинця. Такі злочини можна назвати "анонімними". При розслідуванні даного роду злочинів найбільш важливим є співпраця з іншими країнами, адже глобальний простір Інтернету не має меж, а процесуальний порядок запитів на отримання інформації міждержавних відомств тривалий. За цей час "викрадення", розповсюдження інформації, що має закритий доступ, може спричинити негативні наслідки.

Для покращення співпраці Конвенцією передбачено створення сторонами на національному рівні органу для здійснення контактів цілодобово з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така допомога включає в себе сприяння або, якщо це дозволяється внутрішньодержавним законодавством і практикою, пряме: a) надання технічних порад; b) збереження даних відповідно до статей 29 («Термінове збереження комп'ютерних даних, які зберігаються») і 30 («Термінове розкриття збережених даних про рух інформації»); c) збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних (ст. 35) [4].

Багатьма нормативно-правовими актами встановлено, що кіберзлочинність є небезпечною для держав. Вона може негативно вплинути не тільки на національну безпеку однієї держави, а й всього світу. З аналізу роботи поліції різних країн можна дійти висновку, що діяльність країн у сфері кіберзлочинності забезпечується створенням спеціальних підрозділів для боротьби з нею. До речі, в України теж існує подібне, наприклад Комісія Нотаріальної палати України з питань запобігання та протидії кіберзлочинності, а також підрозділи Національної поліції України.

Серед основних функцій створених підрозділів є такі: моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення; здійснення оперативно-розшукових та розвідувальних заходів з метою фіксування протиправної діяльності кіберзлочинців; розкриття кіберзлочинів; профілактика та нагляд за телекомунікаційними послугами; експертне дослідження доказів на електронних носіях та ін. [4, с. 245].

Для виявлення кіберзлочинців використовуються програми, які здатні перехоплювати так звані віруси. В більшості випадків для оперативно-розшукових заходів залучаються справжні хакери.

Крім того, в останні роки у різних регіонах світу було застосовано низку індивідуальних підходів для боротьби з кіберзлочинністю. Так, у 2015 році Співдружністю націй було розроблено типовий закон про комп'ютерні та пов'язані з комп'ютерами злочини, метою якого є удосконалення членів Співдружності в галузі боротьби з кіберзлочинністю і поглиблення міжнародної співпраці.

Отже, Україна потребує нормативно-правового удосконалення на шляху боротьби з кіберзлочинністю. У своїй діяльності з питань кіберзлочинності українському законодавцю слід брати досвід у канадських та європейських відомствах, також скоординувати зусилля з міжнародними правоохоронними органами, для вирішення транскордонних злочинів. Скоординовані зусилля зорієнтують нашу державу у вірному векторі руху щодо забезпечення та реалізації заходів боротьби з кіберзлочинністю.

1. Бойченко О. В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : монографія / О. В. Бойченко. – Сімферополь, 2011. – 288 с.

2. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. / В. С. Сідак, В. Ю. Артемов. – К. : КНТ, 2009. – 160 с.

3. Конвенція [Ради Європи] про кіберзлочинність від 23 листоп. 2001 р. ; ратифікована Україною 7 верес. 2005 р. // Офіційний вісник України. – 2007. – № 65. – Ст. 2535.

4. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, від 28 січ. 2003 р. ; ратифікований Україною 21 серп. 2006 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_687.

5. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін. – К. : Скіф, 2012. – 728 с.