1. Бахин В.П. Криминалистика. Проблемы и мнения (1962-2002) / В.П. Бахин. – Киев, 2002. – 268 с.

2. Белкин Р.С. Курс криминалистики : учеб. пособие для вузов / Р.С. Белкин. – 3-е изд., доп. – М. : Юнити-дана; Закон и право, 2001. – 837 с.

3. Веліканов С.В. Класифікація слідчих ситуацій у криміналістичній методиці : автореф. дисс. … канд. юрид. наук : спец. 12.00.09 «Кримінальний процес, криміналістика та судова експертиза» / С.В. Веліканов. – Х. : Національна юрид. академія України, 2002. – 19 с.

4. Волчецкая Т.С. Криминалистическая ситуалогия : монография / Т. С. Волчецкая ; под ред. проф. Н. П. Яблокова. – Калининград, 1997. – 248 с.

5. Коновалова В.Е. Версия: концепция и функции в судопроизводстве / В.Е. Коновалова. – Харьков : Консум, 2000. – 176 с.

6. Тіщенко В.В. Теоретичні і практичні основи методики розслідування злочинів : монографія / В.В. Тіщенко ; Одеська національна юридична академія. – О. : Фенікс, 2007. – 260 с.

7. Шевчук В.М. Слідча ситуація: поняття, структура, види та їх значення для оптимізації розслідування злочинів // Юридичний науковий електронний журнал. – № 1. – 2014. – С. 139–143.

Махницький Олександр Васильович
ст. викладач кафедри

Косиченко Олександр Олександрович
к.т.н., доц., доцент кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ: ВІТЧИЗНЯНИЙ І ЗАРУБІЖНИЙ ДОСВІД ТА НАПРЯМКИ ДІЯЛЬНОСТІ

Технічні інновації можна використовувати для соціального блага, але так само легко для мерзенних цілей. Цей вислів більш притаманний кіберзлочинності, ніж, можливо, будь-який інший області злочинності. І кіберзлочинці також стають більш агресивними. Ось чому Європол і його партнерські організації ведуть боротьбу з ними на всіх фронтах.

Кіберзлочинність – це пріоритет EMPACT (європейська міждисциплінарна платформа проти кримінальних загроз) для циклу політики з 2013 по 2018 рік: мета полягає в боротьбі з кіберзлочинами, що здійснюються організованими злочинними групами, і які приносять великий прибуток від таких дій, як шахрайство онлайн і платіжних карт, кіберзлочинності, які завдають серйозної шкоди їх жертвам таких як сексуальна експлуатація дітей і кібератаки, які зачіпають критичну інфраструктуру і інформаційні системи в ЄС.

Згідно самої останньою оцінкою загрози організованої злочинності в Інтернеті (INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA), кіберзлочинність стає більш агресивною і конфронтаційної. Це можна побачити в різних формах кіберзлочинності, включаючи злочини, пов'язані з високими технологіями, порушення даних і сексуальні вимагання.

Кіберзлочинність – це зростаюча проблема для країн, таких як держави-

члени ЄС, в більшості з яких розвинена інтернет-інфраструктура, і платіжні системи знаходяться в режимі онлайн.

Але це не тільки фінансові дані, але дані в цілому, тобто ключова мета для кіберзлочинців. Кількість і частота порушень даних ростуть, і це, в свою чергу, призводить до більшої кількості випадків шахрайства і вимагання.

Є величезний вибір можливостей, які кіберзлочинці намагалися використовувати. До таких злочинів належать:

- використовуючи ботнет-мережі пристроїв, заражених шкідливими програмами, без їх знань користувачів – для передачі вірусів, які отримують незаконний пульт дистанційного керування пристроями, крадуть паролі і відключають антивірусний захист;
- створення «задніх дверей» на скомпрометованих пристроях, що дозволяють крадіжці грошей і даних або віддалений доступ до пристроїв для створення бот-мереж;
- створення онлайн-форумів для обміну досвідом в області хакерства;
- куленепробивний хостинг і створення антивірусних служб;
- відмивання традиційних і віртуальних валют;
- вчинення інтернет-шахрайства, наприклад, через системи онлайн-платежів, кардинг і соціальну інженерію;
- різні форми сексуальної експлуатації дітей в Інтернеті, в тому числі поширення онлайн-матеріалів.
- онлайн-хостинг операцій, пов'язаних з продажем зброї, помилковими паспортами, контрафактними і клонованими кредитними картками, а також ліками і хакерськими послугами.

На сьогодні в Україні діє низка законів та нормативних документів різних рівнів, що охоплюють питання кібербезпеки держави. Це, зокрема, Закони України «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України», Указ Президента України «Про Національний координаційний центр кібербезпеки» та інші нормативно-правові акти. Крім того, у вересні 2016 року Верховна Рада України прийняла у першому читанні Закон України «Про основні засади забезпечення кібербезпеки України».

Стратегічними документами у цій сфері є Стратегія кібербезпеки України, Стратегія національної безпеки України, а також ратифікована Верховною Радою України «Конвенція про кіберзлочинність». Чинний Кримінальний кодекс України встановлює (відповідно до розділу XVI) відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку».

На сьогодні основним документом, який регулює питання міжнародної співпраці у сфері запобігання та протидії кіберзлочинності є *Конвенція про кіберзлочинність (далі – Конвенція)*, яка була підписана 23 листопада 2001 року в Будапешті. В цій Конвенції сформульовано найбільш загальні та разом із тим визначальні принципи щодо забезпечення заходів боротьби із кіберзлочинами на національному та міжнародному рівнях.

Відповідно до ст. 23 Конвенції, сторони співпрацюють між собою у найширших обсягах шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на ос-

нові єдиного чи взаємного законодавства, і внутрішньодержавного законодавства з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень.

Конвенція виділяє *чотири групи правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем*:

- злочини у сфері незаконного доступу до інформації: нелегальне перехоплення (ст. 3), втручання у дані (ст. 4), втручання у систему (ст. 5), зловживання пристроями (ст. 6);
- злочини, пов'язані з протиправним використанням комп'ютерів: підробка, пов'язана з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8);
- злочини, пов'язані зі змістом, до яких відноситься створення, розповсюдження та зберігання дитячої порнографії (ст. 9);
- злочини, пов'язані з порушенням авторських та суміжних прав (ст. 10)

Відповідно до ст. 15 Конвенції кожна країна, що її ратифікувала, забезпечує, щоб встановлення, імплементація і застосування повноважень і процедур, передбачених Конвенцією, регулювалися умовами і запобіжними заходами, регламентованими внутрішньодержавним правом, які забезпечували б адекватний захист прав і свобод людини.

Система злочинів у сфері кіберзлочинності, запропонована національним законодавством України, охоплює кримінальні правопорушення у сфері: використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем); обігу інформації протиправного характеру із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; господарських відносин та приватної власності, яка включає в себе незаконні фінансові операції та заборонені види господарської діяльності, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж**.**

Так, в чинному Кримінальному кодексі України є *розділ **XVI***, який встановлює відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, до яких віднесено статті 361-363 Кримінального кодексу України.

Державний орган, що відповідає в країні за попередження та розкриття кіберзлочиів є Кіберполіція.

Основні завдання Кіберполіції:

1. Реалізація державної політики у сфері протидії кіберзлочинності.
2. Завчасне інформування населення про появу новітніх кіберзлочинів.
3. Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.
4. Реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів.
5. Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.

6. Участь у міжнародних операціях та співпраця в режимі реального часу. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.

7. Протидія кіберзлочинам: У сфері використання платіжних систем:

• скімінг (шимінг) − незаконне копіювання вмісту треків магнітної смуги (чипів) банківських карток;

• кеш-трепінг − викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки;

• кардінг − незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем;

• несанкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.

У сфері електронної комерції та господарської діяльності:

• фішинг − виманювання у користувачів Інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти, тощо;

• онлайн-шахрайство − заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

У сфері інтелектуальної власності:

• піратство − незаконне розповсюдження інтелектуальної власності в Інтернеті;

• кардшарінг − надання незаконного доступу до перегляду супутникового та кабельного TV;

У сфері інформаційної безпеки:

• соціальна інженерія − технологія управління людьми в Інтернет просторі;

• мальвер (англ. *malware*) − створення та розповсюдження вірусів і шкідливого програмного забезпечення;

• протиправний контент − контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;

• рефайлінг − незаконна підміна телефонного трафіку.

Поширеність і суспільна небезпечність кіберзлочинів останніми роками набула загрозливих масштабів, що диктує необхідність формування адекватної відповіді з боку держави. Вивчення зарубіжного досвіду протидії кіберзлочинності в окремо взятих країнах і надбань міжнародної спільноти, удосконалення механізму міжнародної взаємодії є важливим, адже більшість кіберзлочинів мають транснаціональний характер. З огляду на сучасну ситуацію в державі та світі, Україна має постійно вдосконалювати методи боротьби з кіберзлочинністю, удосконалюючи чинне законодавство, у т. ч. в галузі адміністративного права, враховуючи надбання окремих зарубіжних держав, міжнародної спільноти загалом, спрямовані на забезпечення кібербезпеки країни;

З врахуванням наявних проблем діяльності судових та правоохоронних органів у сфері боротьби з кіберзлочинністю, вирішення чи подолання цих проблем має бути насамперед спрямоване на:

• гармонізацію міжнародного та вітчизняного та законодавства у сфері кіберзлочинності, внесенням відповідних змін у кримінальне процесуальне законодавство України, зокрема щодо врахування особливостей оцінки судом електронних доказів, як таких, що найчастіше фігурують у кримінальних провадженнях з розслідування кіберзлочинів;

- подальшу розробку окремих криміналістичних методи розслідування кіберзлочинів, з врахуванням останніх тенденцій щодо типових способів вчинення даного виду злочинів;
- забезпечення належної фахової підготовки правоохоронців та суддів, до обов'язків яких належить розслідування кіберзлочинів та розгляд судових справ щодо них.

1. Кримінальний кодекс України від 05.04.2001 №2341-ІІІ. Режим доступу: http://zakon2.rada.gov.ua/laws/show/2341-14/card6#Public;
2. Конвенція про кіберзлочинність // Відомості Верховної Ради України. – 2006. - № 5- 6. – Ст. 71. Режим доступу: http://zakon5.rada.gov.ua/ laws/show/994_575;
3. INTERNET ORGANISED CRIME THREAT ASSESSMENT/ europol.europa.eu// Режим доступу: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment;
4. EU POLICY CYCLE – EMPACT/ europol.europa.eu // Режим доступу: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact

Мельковський Олександр Вікторович
к.ю.н., доцент кафедри
кримінального права та правосуддя
Запорізького національного університету

ДЕЯКІ ПИТАННЯ ЩОДО ВИКОРИСТАННЯ ПОНЯТТЯ ВНУТРІШНЬОЇ БЕЗПЕКИ У СИСТЕМІ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

На даний час в юридичній науці немає достатньої чіткості у дефініціях „безпека" – „внутрішня безпека". У зв'язку з появою наукових досліджень, присвячених забезпеченню національної безпеки та безпеки окремих сфер життєдіяльності суспільства, опинилася розмитою суттєва та змістова грань між поняттями „національна безпека", „суспільна безпека", „сили забезпечення безпеки".

Зволікання у науковому висвітленні цих проблем негативним чином діє на правоохоронну практику, перешкоджає чіткості нормативно-правового закріплення повноважень, функцій державних структур та органів місцевого самоврядування в охоронній сфері, правовому регулюванні форм та засобів їх діяльності із забезпечення прав та законних інтересів особистості, суспільства та держави.

Нормативний зміст поняття „безпеки" у вітчизняному законодавстві не визначено, але досить чітко сформульовано устатті 1 Закону України „Про основи національної безпеки України" [1]. Так, поняття „національна безпека" визначено як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, охорони дитинства, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, соціальної політики та пенсійного забезпечення, житлово-