Джафаров Ш. З.
курсант 1 курсу ФПФОДР
Дніпропетровського державного
університету внутрішніх справ,
Казначеєв Д. Г.,
науковий керівник, доцент кафедри
тактико-спеціальної підготовки
ФПФППД Дніпропетровського
державного університету внутрішніх
справ, кандидат юридичних наук, доцент

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В СУЧАСНИХ УМОВАХ: ВІТЧИЗНЯНИЙ ТА ЗАРУБІЖНИЙ ДОСВІД

Ми живемо в епоху інформаційного суспільства, коли комп'ютери і телекомунікаційні системи охоплюють всі сфери життєдіяльності людини і держави. Але людство, поставивши собі на службу телекомунікації і глобальні комп'ютерні мережі, не передбачало, які можливості для зловживання створюють ці технології. Сьогодні жертвами злочинців, що орудують у віртуальному просторі, можуть стати не лише люди, але і цілі держави. При цьому безпека тисяч користувачів може виявитися залежна від декількох злочинців. Кількість злочинів, що здійснюються в кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж, і, по оцінках Інтерполу, темпи зростання злочинності, наприклад, в глобальній мережі Інтернет, є найшвидшими на планеті [1].

Небезпека кіберзлочинності як для всього світу, так і для України визнають і вітчизняні правоохоронні органи, як найбільш актуальну проблему. Так, на наш погляд, кіберзлочинність (злочинність у сфері високих технологій) в даний час є однією з найбільш серйозних погроз національній безпеці України в інформаційній сфері.

Враховуючи значущість та гостроту проблем, що виникають у сфері боротьби із вказаним типом злочинності, окремі питання застосування заходів кримінально-правового характеру з метою протидії кіберзлочинності неодноразово були предметом наукових досліджень як теоретичного, так і прикладного характеру. [2]

Під *кіберзлочинністю* розуміється сукупність злочинів, що здійснюються в кіберпросторі з допомогою або за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Відповідно, кіберзлочин – це винне протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні

суспільно небезпечні діяння, здійснені з допомогою або за допомогою комп'ютерів, комп'ютерних мереж і програм, а також з допомогою або за допомогою інших пристроїв доступу до модельованого за допомогою комп'ютера інформаційного простору [3].

Серед дослідників досі не існує єдиної точки зору щодо визначення «кіберзлочинності» чи «комп'ютерного злочину» або злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Так, на погляд одних вчених, до комп'ютерної злочинності відносяться всі протизаконні дії, за яких електронне опрацювання інформації є знаряддям їх вчинення і (чи) засобом [4, с. 14], або всі протизаконні діяння, предметом і засобом здійснення яких є процедури й методи, а також процес комп'ютерного опрацювання даних [5, с. 72]. Пропонується і таке визначення комп'ютерних злочинів: «усі протизаконні дії, при яких електронне опрацювання інформації було засобом їх вчинення або їх об'єктом» [6, с. 65]. Іноді до комп'ютерних злочинів зараховують «злочини, пов'язані з втручанням у роботу комп'ютерів, і злочини, що використовують комп'ютери як необхідні технічні засоби» [7, с. 11]. А.Н. Караханьян під комп'ютерними злочинами розуміє протизаконні дії, об'єктом або знаряддям вчинення яких є ЕОМ [8, с. 243]. В.О. Голубєв вважає, що основна класифікуючи ознака належності злочинів до розряду комп'ютерних – це «використання засобів комп'ютерної техніки» [9, с. 39-40]. В. Лісовий визначає цю ознаку інакше – «електронна обробка інформації» – незалежно від того, на якій стадії злочину вона застосовувалася [10, с. 87]. Пропонується і таке визначення комп'ютерної злочинності, як порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних [11, с. 387].

З метою боротьби зі злочинними проявами у мережі Інтернет 23 листопада 2001 року у Будапешті Радою Європи була прийнята Конвенція про кіберзлочинність[12]. З того часу конференції з проблем інтернет-безпеки у Будапешті стали регулярними і с кожним разом все більше країн не тільки Європи, а й усього світу приймають у них участь.

Наступним кроком стало прийняття «Директиви про атаки проти інформаційних систем». Директива базується на правилах, що діяли з 2005 року (Council Framework Decision 2005/222/JHA). Зберігаючи ряд діючих положень, вона вводить нові види злочинів, такі як використання інструментів для великомасштабних атак, нові обставини, що обтяжують відповідальність та більш суворі санкції, які є необхідними для більш ефективної боротьби проти масштабних атак на інформаційні системи. Крім цього, Директива покращує міжнародне співробітництво між судовими органами та поліцією держав-членів та зобов'язує збирати статистичну інформацію про кібератаки і централізовано направляти її у компетентні органи. Протягом двох років з моменту опублікування Директиви у Офіційному віснику ЄС, державичлени мають впровадити її положення у національні законодавства.

Таким чином, під загрозу кримінальної відповідальності підпадають програмісти (Electronic Frontier Foundation (EFF)), які розробляють інструментарій для тестування вразливості інформаційних систем до кібератак.

На думку членів EFF Європарламент повинен прописати у Директиві мету використання такого інструментарію, а не просто факт його «володіння, використання виробництва чи розповсюдження» [13]. Ст 52

Як зазначає Є. Зозуля ефективна боротьба проти транснаціональної комп'ютерної злочинності та кібертероризму вимагає тісного, швидкого, ефективного й функціонального міжнародного співробітництва усіх державних структур (і щонайперше правоохоронних органів) у розслідуванні такого роду злочинів [14].

Верховною радою України створено спеціальні організаційні структури з питань організаційно-правового забезпечення боротьби з кіберзлочинністю, а саме: Урядову комісію з питань інформаційно-аналітичного забезпечення органів виконавчої влади, Міжвідомчий комітет з проблем захисту прав на об'єкти інтелектуальної власності, Міжвідомчу робочу групу з розроблення та узгодження Концепції легалізації програмних продуктів та боротьби з їх нелегальним використанням. Як зазначає С. Каланча, проблема превентивних можливостей глобальних інформаційних мереж, у тому числі Інтернет, та використання їх для боротьби зі злочинами, причому не тільки зі специфічними комп'ютерними, а й іншими видами злочинів, особливо транснаціональними і організованими, сьогодні майже не освоєна кримінологією [15].

Таким чином, можна зробити висновок про те, що національний рівень кіберзлочинності невпинно зростає, для зниження рівня його розвитку потрібна розробка суттєвих заходів, починаючи з прийняття адекватного законодавства та закінчуючи рішенням суто технологічних питань. Головне ж завдання полягає в тому, щоб на міжнародному рівні, наприклад, в рамках ООН, розробити комплексну програму, що включатиме в себе всі можливі форми та методи боротьби з електронним шпіонажем – юридичні, програмні, технологічні, організаційні, економічні, політичні і т. д. Ці дії матимуть успіх лише в тому випадку, якщо будуть спиратися на систему постійного моніторингу кіберпростору на загальнопланетарному та національному рівнях.

Список використаних джерел:

1. Номоконов В.А. Глобализация информационных процессов и преступность / В.А. Номоконов // Інформаційні технології та безпека: зб. наук. праць. – Вип. 1. – К., 2002. – С. 95–103
2. Гусаров С.М. Розслідування кіберзлочинів органами внутрішніх справ України: наукове та кадрове забезпечення / Актуальні питання розслідування кіберзлочинів // Матеріали Міжнародної науково-практичної конференції. м. Харків., 2013. - С.14-15.
3. Олійник В.М. Кіберзлочинність як умова порушення громадської безпеки України // Актуальні питання розслідування кіберзлочинів // Матеріали Міжнародної науково-практичної конференції. м. Харків., 2013. - С. 19-20.
4. Калюжный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект): автореф. дис. … д-ра юрид. наук: спец. 12.00.02

«Государственное право и управление; административное право; финансовое право» / Р.А. Калюжный – К., 1992. – 47 с.
5. Азаров Д. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації / Д. Азаров // Право України. – 2000. – № 12. – С. 69–73.
6. Комп'ютерна злочинність : [навч. посіб.] / П.Д.Біленчук, Б.В. Романюк, В.С. Цимбалюк [та ін.]. – К.: Атіка, 2002. – 240 с.
7. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. – М.: Юрид. лит., 1991. – 157 с.
8. Правовая информатика и кибернетика: учебник / [Г.А.Атанесян, О.А.Гаврилов, Дёри П. и др.] ; под ред. Н.С. Полевого. – М.: Юрид. лит., 1993. – 528 с.
9. Голубєв В.О. Правові проблеми захисту інформаційних технологій / В.О. Голубєв // Вісник Запорізького юридичного інституту. – 1997. – № 2. – С. 35–40.
10. Лісовий В. «Комп'ютерні» злочини: питання кваліфікації / В. Лісовий // Право України. – 2002. – № 2. – С. 86–88.
11. Дашян М.С. Право информационных магистралей / М.С. Дашян. – М. : Волтерс Клувер, 2007. – 288 с.
12. Convention on Cybercrime : Budapest, 23.11.2001 [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/ Treaty/en/Treaties/Html/185.htm.
13. EFF требует защитить права программистов [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/ 420736.php. – 28.02.2012.
14. Европейский центр по борьбе с киберпреступностью демонстрирует свои первые результаты // Europa. Новости с европейским акцентом [Електронний ресурс]. – Режим доступу: http://euroua.com/europe/eu/1762.
15. Каланча С.Г. Кіберзлочинність: шляхи попередження та протидії / С.Г. Каланча // Наше право. – 2012. – № 3, ч. 2. – С. 213–217.

Єна І. В.
доцент кафедри кримінально права та правосуддя юридичного факультету Запорізького національного університету,кандидат юридичних наук

ОКРЕМІ ПИТАННЯ УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ СТРАТЕГІЇ УКРАЇНИ ЩОДО ПІДВИЩЕННЯ БЕЗПЕКИ КІБЕРПРОСТОРУ

Сьогодні Україна, як і світ в цілому, живе в той час, коли всі громадяни держави, підприємства, установи, організації, незалежно від того великі вони чи маленькі, яка їх форма власності, є незахищеними перед атаками кіберзлочинців.

Сучасні традиційні заходи безпеки є неефективними, оскільки ландшафт загроз занадто розвинутий і дуже швидко розширюється, про що свідчить світова статистика. Так, наприклад, дослідження проведене у 2016 році в Канаді показало, що понад 50 % кібератак на канадські кампанії були успішними, і їх кількість, у порівнянні з минулим роком збільшилась на 17 % [1], а в управлінні