Запорожець Анастасія Костянтинівна,
курсант 2-го курсу навчально-наукового інституту № 1 Національної академії внутрішніх справ
Науковий керівник: доцент кафедри кримінології та кримінально-виконавчого права Національної академії внутрішніх справ, кандидат юридичних наук **Миронюк Тетяна Василівна**

НАПРЯМИ ВДОСКОНАЛЕННЯ ЗАХОДІВ ЗАПОБІГАННЯ ЗЛОЧИНАМ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ УКРАЇНИ

Програмне забезпечення, що в умовах стрімкого технологічного розвитку постійно удосконалюється відповідно до вимог сучасності, є тим об'єктом інтелектуальної власності, який зазнає найбільшого впливу від правопорушень, що, в свою чергу, обумовлені суттєвою різницею між витратами інтелектуальних ресурсів на створення комп'ютерних програм та витратами на їх незаконне копіювання та розповсюдження.

Як свідчить статистика, в останні роки українці дедалі частіше купують товари онлайн, щодня працюють із банківськими рахунками на персональному комп'ютері, здійснюють платежі через сучасні технологічні пристрої, як то планшети чи смартфони. Зрозуміло, чому такі інтернет-послуги набувають стрімкого поширення, адже це зручно та набагато швидше, аніж вистоювати черги та заповнювати численні папірці в банківських установах. Утім, зростання популярності систем онлайн-банкінгу спонукає кібершахраїв вигадувати та втілювати в життя все витонченіші способи крадіжок фінансової інформації, а потім грошей із електронних рахунків користувачів [1].

Американським Альянсом виробників програмного забезпечення (BSA), який входить до Міжнародного альянсу інтелектуальної власності (IIPA) було констатовано, що у 2003 р. в Україні рівень злочинів пов'язаних з незаконним відтворенням та розповсюдженням комп'ютерних програм і баз даних становив 91 % (на кожному з досліджених 100 комп'ютерів на 91 було виявлено піратське програмне забезпечення). Надалі спостерігалося певне зменшення цього рівня (у 2007 р. – 83 %), але починаючи з 2008 р. спостерігається поступове зростання рівня комп'ютерного піратства, у 2011 р. він сягнув 86 %, у 2017 р. – 90 %, а у 2018 – 94 %. Такі негативні тенденції свідчать про те, що перед правоохоронними

органами постають нові завдання щодо визначення стратегічних напрямів їх діяльності, пошуку нових підходів до боротьби з комп'ютерним піратством, які б відповідали реаліям та враховували тенденції розвитку суспільства й держави.

Динаміка злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку збільшується з кожним роком: 2010 – 190, 2011 – 131, 2012 – 138, 2013 – 595, 2014 – 443, 2015 – 598, 2016 – 818. А статистика засуджених осіб за вчинення злочинів у цій сфері наразі така: 2010 – 69, 2011 – 56, 2012 – 80, 2013 – 49, 2014 – 37, 2015 – 31, 2016 – 24, 2017 – 25 [2].

Кіберзлочини можна класифікувати на два види: традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету (шахрайство з використанням ЕОМ, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації і т.д.), та нові злочини, що стали можливі завдяки новітнім комп'ютерним технологіям (злочини передбачені Розділом XVI Кримінального кодексу України). Найчастіше з використанням комп'ютера та Інтернету вчиняються такі традиційні злочини: порушення авторського права і суміжних прав (ст. 176); шахрайство (ст. 190); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення (ст. 200); ухилення від сплати податків, зборів (обов'язкових платежів) (ст. 212); ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231) [3; 4].

Сьогодні в Україні про кіберзлочинність зазначають такі нормативно-правові акти: Конвенція про Кіберзлочинність, Закон України «Про ратифікацію Конвенції про кіберзлочинність», Кримінальний Кодекс України. Специфіка даного виду злочинності полягає у тому, що готування та скоєння злочину здійснюється, практично не відходячи від «робочого місця», злочини є доступними; оскільки комп'ютерна техніка постійно дешевшає; злочини можна скоювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксувати та вилучити криміналістично значущу інформацію при виконанні слідчих дій для використання її в якості речового доказу. Усе це, безумовно, є перевагами для кіберзлочинців.

Способів вчинення «кіберзлочинів» на сьогодні достатньо: викрадення комп'ютерної інформації, DoS-атаки, дефейс, розповсюдження шкідливих програм (вірусів), кардинґ, фішинґ, стирання програм або даних, розсилка листів (спамів), створення фіктивних інтернет-аукціонів тощо. Першою причиною розвитку кіберзлочинності, як і будь-якого бізнесу, є прибутковість, – вона неймовірно прибуткова. Величезні суми грошей з'являються в кишенях злочинців у результаті окремих великих афер, не говорячи вже про невеликі суми, які йдуть просто потоком. Друга причина росту кіберзлочинності як бізнесу – те, що успіх справи не пов'язаний з більшим ризиком. У реальному світі психологічний аспект злочину припускає наявність деяких коштів стримування. У віртуальному світі злочинці не можуть бачити своїх жертв, будь те окремі люди або цілі організації, які вони вибрали для атаки. Грабувати тих, кого ти не бачиш, до кого не можеш дотягтися рукою, набагато легше [5].

Превентивні заходи вже не допомагають, і з кожним роком шкода збільшується, а злочини стають все більш «вишуканими». Найпоширеніші - це злом баз даних компаній та урядових організацій, виведення з ладу промислових об'єктів. До цього, наприклад, призвела атака вірусу на іранську АЕС у Бушері. Ось, наприклад, одна із найбільш простих схем. Шахраї крадуть зарплатні рахунки співробітників компаній. Потім продають їх на чорному ринку, де розцінки починаються від $ 3,5 за рахунок. Є й інший варіант – залишити ці дані собі й просто перевести гроші з сотень і тисяч банківських карт на свій рахунок. Щорічний збиток лише від такої схеми американські компанії оцінюю в $ 1 млрд.

Українською проблемою є як недостатня кількість державних експертів в області комп'ютерно-технічної експертизи, так і складнощі з введенням в правове поле досліджень фахівців комерційних організацій. Типовий термін проведення комп'ютерно-технічних експертиз становить від півроку і вище через високу завантаженість профільних державних установ. Весь цей час підозрюваний може перебувати в СІЗО.

Проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері.

Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній.

Отже, найкращим способом протидії високотехнологічної злочинності можна вважати реалізацію випереджаючого правового регулювання. Також слід додати, що відсутність єдиної міжнародної нормативної правової бази, істотні відмінності в національних законодавствах країн, об'єднаних ідеєю спільної боротьби з комп'ютерною злочинністю, та відсутність єдиного підходу до визначення понятійного апарату розглянутої сукупності суспільно небезпечних діянь суттєво ускладнюють ефективну протидію використанню комп'ютерних технологій при здійсненні злочинів.

Для удосконалення технічної складової забезпечення безпеки інформаційного простору насамперед потрібно: оновлювати системи безпеки (включаючи антивірус) і операційну систему разом з появою їхніх нових версій; створювати резервні копії даних; не відкривати підозрілі листи, що приходять на поштову скриньку; не скачувати програмне забезпечення з неперевірених або підозрілих джерел; оновити операційні системи і системи безпеки; заблокувати ір-адреси і доменні імена, з яких відбувалося поширення шкідливих файлів; заборонити зберігання паролів в LSA Dump у відкритому вигляді; замінити всі паролі на складні для запобігання брута за словником; поставити блокування спливаючих вікон; застосувати сучасні засоби виявлення вторгнень і пісочницю для аналізу файлів; заборонити виконання наступних завдань: viserion_, rhaegal, drogon.

Список використаних джерел

1. Пашковська Т. Кіберзлочинність в Україні: тенденції, статистика, протидії. URL: http://yur-gazeta.com/publications/actual/kiberzlochinnist-v-ukrayini-tendenciyi-statistika-protidiyi.html.

2. Олійник В. М. Висновок на проект Закону України «Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки» № 9575.

3. Вартилецька І. А. Кримінальне право України: альбом схем / І. А. Вартилецька, В. С. Плугатир ; заг. ред. В. Я. Горбачевський ; Національна академія внутрішніх справ України. – К.: Атіка, 2003. – 207 с.

4. Марків С. І. Кіберзлочинність. Нова кримінальна загроза. URL: http://dspace.tneu.edu.ua/bitstream/316497/21460/1/360-362.pdf

5. Глущенко В. А. Криміналістична характеристика особи порушника авторського та суміжних прав / В. А. Глущенко // Держава і право. – К., 2003. – Вип. 21. – С. 526–529.