Василевич В.В., учений секретар вченої ради Національної академії внутрішніх справ, кандидат юридичних наук, професор

НАПРЯМИ РЕАЛІЗАЦІЇ КРИМІНОЛОГІЧНОЇ ПОЛІТИКИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

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 %, а у 2017 р. - 90% [2].

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 свідчить про те, що їх кількість з кожним роком збільшується, зокрема, якщо у 2010 році було зареєстровано 190 таких діянь, то у 2013 - 595, а у 2016 їх уже 818. Разом з тим, статистика засуджених осіб за вчинення злочинів у цій сфері відображає зовсім протилежні тенденції, наразі, якщо у 2010 році було встановлено 69 таких фактів, то у 2013 - 49, а у 2016 лише 24 [3].

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) [4; 5].

Специфіка даного виду злочинності полягає у тому, що готування та вчинення 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.

Однією із основних причин активізації 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 то окремі люди або цілі організації, які вони вибрали для атаки [6].

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.

Українською проблемою є як недостатня кількість державних експертів в сфері 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.

Питанняборотьби з кіберзлочинністю в Україні - це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Потребує удосконалення 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, можуть стати загрозою номер один, змістивши тероризм.

Незважаючи на віртуальність злочинів, збитки вони завдають цілком реальні.

Пріоритетними напрямами реалізації кримінологічної політики в інформаційному просторі, можуть бути удосконалення:

- технічної складової забезпечення безпеки
інформаційного простору, зокрема:оновлення системи безпеки (включаючи антивірус) і операційної системи; блокування ір- адрес і доменних імен, з яких відбувалося поширення шкідливих файлів тощо;

- підготовки фахівців у сфері забезпечення безпеки інформаційного простору для правоохоронних органів:Національної поліції, МВС, СБУ тощо;

- удосконалення нормативно-правового забезпечення безпеки інформаційного простору, зокрема:

а) на реалізацію рішення Ради національної безпеки і оборони України від 27 січня 2016 року та Стратегії кібербезпеки України від 15.03.2016 мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України, зокрема щодо обов'язковості вжиття ними заходів із забезпечення захисту інформації та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту;

б) забезпечити реалізацію положень Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, який набирає чинностічерез шість місяців з дня його опублікування.

в) розроблення поняття й встановлення кримінальної відповідальності за кіберзлочини, зокрема: пеналізація йдиференціація кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку, відповідно до нині чинних норм КК України, тощо.

Список використанихджерел:

1. Пашковська Т. Кіберзлочинність в Україні: тенденції, статистика, протидії. иЯЬ:_____Ьйр://уиг-

gazeta.com/pubHcations/actual/kiberzlochmnist-v-ukrayini-tendenciyi-statistika-protidiyi .html

2. Піщенко Г.І. Сучасні тенденції незаконного відтворення та розповсюдження комп'ютерних програм і баз даних в Україні. 2013. URL:http://mail.lex-line .com.ua/?language=ru&go=fun_article&id= 1369

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

4. 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.

5. Марків С. І. Кіберзлочинність. Нова кримінальна загроза.URL:http://dspace.tneu.edu.ua/bitstream/316497/2l460/1/360-362.pdf

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