Філіпенко Тетяна В'ячеславівна
tatkafili@gmail.com
доктор наук з державного управління,
професор,
професор кафедри права та публічного адміністрування
Маріупольського державного університету

НАСЛІДКИ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕОМ, АВТОМАТИЗОВАНИХ СИСТЕМ І КОМП'ЮТЕРНИХ МЕРЕЖ

Розвиток інформаційних технологій надає не тільки унікальні можливості для активного й ефективного розвитку економіки, політики, держави й суспільства, але й стимулює розвиток комп'ютерної злочинності.

Дослідження й аналіз численних випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розподілити на випадкові і навмисні. Навмисні загрози можуть бути виконані шляхом довготривалої масованої атаки несанкціонованими втручаннями або вірусами.

Наслідки, до яких призводить реалізація загроз: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, коректну за формою і змістом, але яка має інше, значення), ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути різною: від невинних жартів до відчутних втрат, що в деяких випадках складають загрозу національній безпеці країни. Попередження наведених наслідків в автоматизованій системі і є основною метою створення системи безпеки інформації. Для створення засобів захисту інформації необхідно визначити природу загроз, форми і шляхи їх можливого вияву і здійснення [1, с. 36].

У юридичній літературі пропонується наступна загальна класифікація можливих наслідків злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж.

1. Порушення функцій: а) тимчасові порушення, котрі призводять до плутанини в графіках роботи, розкладі тих чи інших дій і т.д.; б) недоступність системи для користувачів; в) пошкодження апаратури (деякі практичні спеціалісти вважають, що пошкоджень апаратури, коли це стосується незаконного доступу, не буває); г) пошкодження програмного забезпечення.

2. Втрати значних ресурсів: грошей, речей, обладнання, інформації.

3. Втрата монопольного використання, яка обумовлена тим, що певна інформація цінна для власника лише доти, допоки він є її монопольним володарем.

4. Порушення прав: авторських, суміжних, патентних, винахідницьких і т.д. [2, с. 134-135].

Як зазначають Васильєв А.А. та Пашнєв Д.В., визначити вичерпний перелік можливих наслідків злочину у сфері використання ЕОМ

(комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку надзвичайно важко, оскільки в кожному випадку ці наслідки залежать насамперед від змісту комп'ютерної інформації, яка зазнала шкоди. Характер шкоди в кожному конкретному злочині, як правило, залежить від тих суспільних відносин, які виступають не основним безпосереднім, а додатковим об'єктом. Це можуть бути відносини в різних сферах життєдіяльності людини, пов'язані з використанням ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку. Перешкоджаючи інформаційним відносинам, злочинець завдає або загрожує завдати шкоди тим суспільним відносинам, для інтенсифікації яких застосовуються комп'ютерні технології [3, с. 37].

Слід зазначити, що високі технології відкривають широкі можливості не тільки для всіх громадян, але і для злочинців також. Поряд з розвитком комп'ютеризації відбувається розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки грошових коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем. Крім того, на думку фахівців з питань інформатизації та правового регулювання інформаційних відносин, комп'ютери є знаряддям вчинення таких злочинів як тероризм, шпигунство, шахрайство, крадіжка, дитяча порнографія тощо.

Насторожливим є той факт, що загальна кількість зловживань у сфері комп'ютерних технологій та розмір завданих при цьому збитків неухильно зростають. Це пояснюється декількома факторами:

− високою динамічністю та масовістю впровадження у багатьох сферах людської діяльності різноманітних інформаційних технологій та процесів, що базуються на використанні засобів обчислювальної техніки;

− різким розширенням кола спеціалістів у галузі комп'ютерних технологій, підвищенням їх кваліфікації;

− недосконалістю законодавчої бази у сфері інформаційних відносин та інформаційної безпеки;

− недосконалістю чи відсутністю технічних засобів забезпечення інформаційної безпеки у конкретних інформаційних технологіях;

− низьким ступенем розкриття злочинів.

Тому існує потреба осмислення комп'ютерної злочинності як соціального явища та напрацювання відповідних методик боротьби з нею, в тому числі виявлення і розслідування злочинів, що вчиняються з використанням комп'ютерних технологій.

Ефективна система боротьби з комп'ютерними злочинами передбачає створення законодавчого забезпечення такої боротьби, розробку захищених інформаційних технологій та засобів захисту з метою модернізації існуючих інформаційних технологій.

Зміни в суспільних відносинах у результаті інформаційних процесів знайшли своє відбиття в нормативних актах Ради Європи, резолюціях,

конвенціях, рекомендаціях і директивах Європарламенту і Євросоюзу. Процеси інформатизації відображаються в правовому просторі, нормативних та етичних нормах суб'єктів інформаційних відносин усіх розвинених країн світу.

За даними спеціалістів, станом на листопад 2019 року в світі до Інтернету під'єднані 4,1 млрд людей. Найвищий рівень підключення в Європі (82,5%), а найнижчий – в Африці (28,2%). Україна входить до першої десятки країн Європи за кількістю інтернет-користувачів. За даними Gemius, станом на червень 2019 року в Україні є 24,8 млн користувачів Інтернету. Згідно даних щорічного дослідження «Kantar Україна» у 2019 році 74% населення України користується Інтернетом, 85% з них – кожного дня [4].

Україна, інтегруючись у світове співтовариство, за роки незалежності здійснила стрибок у єдиний світовий інформаційний простір у багатьох сферах суспільного життя. Наприклад, створення єдиної загальнодержавної системи електронних платежів під егідою Національного банку України є певним досягненням держави, сприяє укріпленню її суверенітету, економічній безпеці, здатності краще протистояти загальносвітовим і регіональним потрясінням. Зараз важко уявити перспективну сферу суспільної діяльності, в якій би не використовувалися сучасні комп'ютери, локальні і глобальні комп'ютерні мережі, програмні комплекси від найпростіших до найвищого рівня складності [5, с. 25].

При цьому надзвичайну стурбованість у спеціалістів викликає загрозливий розрив між рівнем втілення інформаційних комп'ютерних технологій і рівнем засобів їх правового, організаційно-технологічного захисту.

На 73-й сесії Генеральної асамблеї ООН генеральний секретар Антоніу Гуттереш оцінив щорічні збитки від кіберзлочинності у світі в розмірі 1,5 трлн доларів. На жаль, прогнози експертів з кібербезпеки невтішні. В майбутньому кількість злочинів та збитків від кібератак зростатиме, адже правопорушники йдуть щонайменше на крок попереду механізмів, які мають державні органи та приватні особи щодо запобігання і розкриття таких злочинів [6].

Якщо порівнювати традиційні злочини і комп'ютерні, то останні відрізняються, перш за все, феноменом розповсюдження у часі та просторі, місцем та суб'єктом посягання. Інакше кажучи, щоб вкрасти гроші, немає потреби проникати в сховище банку, перетинати кордони, долати системи охорони і сигналізації. Досить мати комп'ютер, вихідну інформацію стосовно доступу та захисту електронних систем банку, набір хакерських програм і досвід такої роботи.

Інший важливий аспект комп'ютерних злочинів – це феномен безликості інформації. Такі традиційні ознаки криміналістичної експертизи, як почерк, відбитки пальців та ін. – в електронних імпульсах комп'ютера безликі.

Ще одна специфіка комп'ютерних злочинів – феномен інструментарію комп'ютерних посягань. На відміну від традиційних способів злочину (зброя,

ніж і т.д.) інструментарій комп'ютерних злочинів – різноманітні програмні засоби комп'ютерних втручань.

На увагу заслуговує техніко-технологічний спосіб скоєння злочину. Суть його – злочинне порушення функціонування інформаційних систем, обумовлене впливом на їх вразливі компоненти. І, хоча цей вид злочину суттєво відрізняється від традиційних терористичних злочинів, наслідки за своєю трагічністю можуть бути подібними до великих техногенних катастроф.

Стан інформаційно-телекомунікаційних систем і рівень їх захисту є одним із найважливіших факторів, що впливає на інформаційну безпеку держави. Економічні збитки від комп'ютерних злочинів сьогодні стоять на одному рівні з перевагами, здобутими від впровадження електронно-обчислювальних машин у практику, а соціальні та моральні втрати взагалі не підлягають оцінці [7, с. 34].

Отже, швидкий розвиток процесів автоматизації, проникнення комп'ютерів в усі сфери сучасного життя спричинили, крім безсумнівних переваг, появу цілого ряду специфічних проблем, однією з яких є забезпечення ефективного захисту інформації та засобів її обробки. Поширення інформаційних технологій надає можливості для нових та раніше невідомих правопорушень, а також для вчинення традиційних злочинів нетрадиційними засобами.

Література

1. Голубєв В.О., Юрченко О.М. Злочини у сфері комп'ютерної інформації: способи скоєння та засоби захисту / Під ред. д.ю.н. Снігерьова О.П. та д.т.н. Вертузаєва М.С. Запоріжжя: ВЦ «Павел», 1998. 246 с.

2. Батурин Ю.М. Проблемы компьютерного права. М.: Юрид. лит., 1991. 272 с.

3. Васильєв А.А., Пашнєв Д.В. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Вісник Кримінологічної асоціації України*. 2013. № 5. С. 34-42

4. Історія Інтернету від Arpanet до сьогодні. URL: https://ucloud.ua/istoriya-internetu-vid-arpanet-do-sogodni/

5. Філіпенко Т.В., Калайда В.В. Інформаційна безпека: науково-практичний посібник. Донецьк: ДЮІ ЛДУВС, 2007. 168 с.

6. Нікулеску Д. Кібербезпека: вразливі моменти. *Юридична газета Онлайн*. 14.05.2019. URL: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html

7. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: Монографія. Запоріжжя: ГУ «ЗІДМУ», 2003. 250 с.

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ЮРИДИЧНИЙ ІНСТИТУТ

НАУКОВО-ПРАКТИЧНИЙ СЕМІНАР

03 квітня 2020 р., м. Кривий Ріг

«Інформаційна безпека в діяльності поліції»

Матеріали семінару

м. Кривий Ріг
2020

УДК 34:004.056.5

Рекомендовано до друку
Вченою радою Донецького
юридичного інституту
МВС України
29 квітня 2020 р., протокол № 8

Інформаційна безпека в діяльності поліції: матеріали науково-практичного семінару (м. Кривий Ріг, 03 квітня 2020 року). – Кривий Ріг: Донецький юридичний інститут МВС України, 2020 – с.100

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова оргкомітету

НАЗИМКО Єгор Сергійович – *т.в.о. ректора Донецького юридичного інституту МВС України, доктор юридичних наук, старший науковий співробітник, капітан поліції*

Заступник голови організаційного комітету

ЧЕРВІНЧУК Андрій Васильович *– начальник відділу організації наукової роботи Донецького юридичного інституту МВС України, кандидат юридичних наук*

Відповідальний секретар організаційного комітету

ТУЛІНОВ Валентин Сергійович – *завідувач кафедри спеціальної техніки та інформаційних технологій Донецького юридичного інституту МВС України, кандидат юридичних наук*

Секретар організаційного комітету

ПАВЛИШ Тетяна Григорівна – *доцент кафедри спеціальної техніки та інформаційних технологій Донецького юридичного інституту МВС України, кандидат педагогічних наук*

Члени оргкомітету:

УТКІНА Галина Анатоліївна *– доцент кафедри спеціальної техніки та інформаційних технологій Донецького юридичного інституту МВС України, кандидат економічних наук, доцент*

ТРОФІМЕНКО Єлизавета Сергіївна – *викладач кафедри спеціальної техніки та інформаційних технологій Донецького юридичного інституту МВС України*

Збірник матеріалів є підсумком роботи науково-практичного семінару «Інформаційна безпека в діяльності поліції».

Для ад'юнктів, аспірантів, курсантів, студентів, слухачів закладів вищої освіти, а також усіх, хто цікавиться проблемами, розглянутими під час семінару.

ЗМІСТ