КУРМАН О. В.,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики
(Національний юридичний університет імені Ярослава Мудрого)

УДК 343.98

СПОСОБИ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАНИХ МАШИН (КОМП'ЮТЕРІВ), АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ЧИ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

У статті розглядаються проблемні питання визначення способу вчинення досліджуваного виду злочинів, пропонується класифікація та розкриваються деякі особливості даної криміналістичної категорії.

Ключові слова: *несанкціоноване втручання, спосіб вчинення злочину, автоматизована система, комп'ютерна мережа, шкідливе програмне забезпечення.*

В статье рассматриваются проблемные вопросы определения способа совершения исследуемого вида преступлений, предлагается классификация и раскрываются некоторые особенности данной криминалистической категории.

Ключевые слова: *несанкционированное вмешательство, способ совершения преступления, автоматизированная система, компьютерная сеть, вредоносное программное обеспечение.*

In article considers problematic issues of determination of the method of committing an explored type of crime, proposing the classification and disclosing some features of forensic category.

Key words: *unauthorized intervention, method of committing a crime, automated system, computer network, malicious software.*

Вступ. Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства так чи інакше пов'язані з комп'ютерами, комп'ютерними мережами і комп'ютерною інформацією.

Загальновідоме прислів'я про те, що хто володіє інформацією, той володіє світом, характеризує роль інформації у сучасному суспільстві. На нинішньому етапі розвитку суспільства масштаби злочинних посягань на конфіденційні відомості різко зросли. Інформація про результати чужих прикладних і фундаментальних досліджень дає змогу заощадити власні сили й кошти та зосередити увагу на виробництві й маркетингу. Подальший розвиток науково-технічного прогресу, збільшення потоку патентів і жорстка конкуренція роблять викрадення чужих таємниць особливо прибутковою, а тому дуже перспективною справою. Все більше видів інформації у сучасному суспільстві зберігається в електронному вигляді. В Україні практично всі реєстри та бази даних державних установ та органів влади і управління переведені чи переводяться на електронні носії із розміщенням у локальних мережах чи з доступом до них через Інтернет. Така зручність у збиранні, обробці та використанні інформації створює велику спокусу незаконного отримання конфіденційних відомостей

про конкретну особу, об'єднання громадян, підприємства, установи з метою використання в подальшому в протиправних цілях.

Розвиток методів обробки інформації за допомогою комп'ютерів призвів до застосування цих машин в усіх галузях національної економіки та інших сферах суспільного життя. Значна кількість таких машин об'єднана комп'ютерними мережами, деякі з них набули інтернаціонального характеру.

В усьому світі постійно з'являються повідомлення про кібератаки та несанкціоноване втручання в роботу комп'ютерних мереж. Так, у 2003 році через використання комп'ютерного вірусу Slammer була значно уповільнена робота мережі Інтернет у Північній Америці та Європі, а Південна Корея взагалі на деякий час була відключена від всесвітньої мережі. У квітні 2009 року кіберзлочинці змогли подолати захист комп'ютерних систем Пентагону та викрали інформацію щодо нового багатоцільового винищувача п'ятого покоління F-35 Lightning II. Хакерам вдалося скопіювати декілька терабайт даних, які стосувалися дизайну та електронної системи літака. У вересні 2010 року президент Ірану Махмуд Ахмадінежад заявив, що зловмисники через несанкціоноване проникнення змогли створити локальні проблеми у роботі центрифуг комплексу збагачення урана. У 2017 році світ сколихнули дві масштабні комп'ютерні вірусні атаки. У травні з'явилися повідомлення про втручання в роботу сотні тисяч електронних машин у 150 країнах світу за допомогою вірусу WannaCry. Зокрема, вірус вразив низку комп'ютерних систем німецького залізничного концерну Deutsche Bahn. У Великій Британії були заражені комп'ютерні системи багатьох лікарень. У червні з'явилася нова загроза штатній роботі електронно-обчислювальних машин, автоматизованих систем та та мереж електрозв'язку. Злочинцями був застосований новий шифрувальник файлів Petya.A. Жертвами його застосування стали сотні державних та приватних компаній у всьому світі, у тому числі й в Україні.

Постановка завдання. Сьогодні з'являються нові, раніше невідомі способи вчинення злочинів у сфері використання електронно-обчислюваних машин, систем та комп'ютерних мереж і мереж електрозв'язку, де предметом посягання виступає різного роду інформація, що зумовлює необхідність розроблення ефективних методик виявлення й розслідування цих злочинних деліктів.

Проблемі дослідження злочинів у сфері інформаційних технологій приділялася певна увага у вітчизняній криміналістичній науці [2, 4, 5, 6, 7]. Однак постійне вдосконалення існуючих та поява нових способів вчинення робить цю проблему досить актуальною для України сьогодні.

Результати дослідження. У Кримінальному кодексі передбачена відповідальність (ст. 361) за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.

Обов'язковим елементом злочинного механізму даного виду злочинів є «несанкціоноване втручання в роботу». На жаль, законодавство України не дає однозначного визначення цієї категорії. У Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» наводиться така дефініція як «несанкціоновані дії щодо інформації в системі», до яких відносяться такі, що провадяться з порушенням порядку доступу до цієї інформації, встановленого відповідно до законодавства. Згідно зі ст. 1 зазначеного Закону доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі. Порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації. Обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Виходячи з аналізу наведених категорій, можна зробити висновок, що несанкціоноване втручання в роботу – це порушення користувачем умов та правил отримання і обробки ін-

формації. Такі умови та правила отримання і обробки інформації встановлюються володільцем інформації. Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством. Згідно зі ст.ст. 5 та 6 Закону власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом. Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу. Закон України «Про телекомунікації» у п. 3 ст. 9 зобов'язує операторів і провайдерів телекомунікацій (електрозв'язку) вживати відповідно до законодавства технічні та організаційні заходи із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами.

Таким чином, вести мову про незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку можна за сукупності умов: 1) володільцем інформації повинні бути визначені умови та правила отримання і обробки інформації; 2) власник (розпорядник) електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи оператор (провайдер) мереж електрозв'язку повинні розробити та впровадити заходи захисту інформації в системі; 3) власник (розпорядник) комп'ютерів, систем та оператор (провайдер) мереж повинні розробити правила роботи системи; 4) між власником (оператором, провайдером) системи та володільцем інформації повинен бути укладений договір щодо захисту інформації в системі; 5) злочинець виконав хоча б одну із операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання інформації.

Способи несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку можуть бути класифіковані за різними підставами.

1. За місцем знаходження (локалізацією) злочинців існує внутрішнє та зовнішнє втручання.

Внутрішнім доступом вважається несанкціоноване втручання до мережі або системи, яке здійснюється з комп'ютерів, під'єднаних до однієї локальної або корпоративної мережі. Цей вид несанкціонованого доступу виконати легше, адже брандмауери, які повинні захищати дані у мережі, налаштовані на «атаку ззовні» і, здебільшого, не відстежують нелегітимні дії всередині мережі. Крім того, більшість таких мереж будується на принципах довіри стосовно інших локальних пристроїв, а робота зловмисника всередині мережі є, як правило, легальною. До зовнішнього несанкціонованого доступу належить дистанційний доступ, який здійснюється з комп'ютера, що не належить до мережі, на яку спрямовано посягання [8, с. 55].

2. За кількістю злочинців несанкціоноване втручання може бути одноосібне та групове.

3. За ступенем участі злочинця – особисте активне втручання, програмне (опосередкована участь) та комбіноване.

До першого виду належать ситуації, коли особа безпосередньо за допомогою клавіатури або іншого пристрою вводу даних надає команди до комп'ютера. Для цього може застосовуватися вільний доступ сторонньої особи до службового комп'ютера, власна електронно-обчислювальна машина зловмисника або таємне проникнення до приміщення, де встановлені комп'ютерно-технічні засоби. Після отримання фізичного доступу до необхідного комп'ютера проникнення до системи (мережі) здійснюється за допомогою чужих паролів та логінів. Для цього попередньо обстежують робочі місця з метою виявлення паперових нотатків з необхідними даними або вивчають на комп'ютері певні реєстрі, де фіксуються набрані раніше паролі, які, як правило, ніхто із співробітників установ, організацій не видаляє.

Іншим варіантом отримання пароля для наступного незаконного проникнення в систему (мережу) є так званий «соціальний інженеринг». При цьому інформація отримується в процесі спілкування (телефонного або через повідомлення на телефон чи електронну

почту). Злочинець представляється системним адміністратором, співробітником комп'ютерної фірми, що обслуговує систему, іншим колегою та запитує у співрозмовника пароль для доступу [1, с. 309].

Як різновид – це фізичне підключення до мережі шляхом під'єднання на комутуючих шафах або дротових лініях. Даний спосіб можна порівняти з роботою двох паралельних телефонних апаратів, підключених до одного абонентського номеру: якщо один телефон знаходиться в активному режимі (ведеться розмова з абонентом) та на другому апараті піднімається слухавка, то коли розмова на першому закінчена, вона може бути продовжена на другому апараті.

Програмне (опосередковане) втручання має на увазі використання різного роду програмних засобів, де злочинець тільки ініціює роботу спеціальних комп'ютерних програм, а все інше програма виконує сама. На відміну від описаного вище способу, в даному випадку добір пароля для доступу здійснює спеціально розроблена програма, наприклад, Password Cracker, Office Key, Accent Office Password Recovery та інші, яких сьогодні велика кількість.

Також одним із видів програмного забезпечення, що використовують злочинці, є шкідливі «комп'ютерні віруси». Залежно від середовища існування розрізняють такі типи вірусів. Файлові віруси - проникають у файли, що виконуються (exe, com, bat), у системні файли, файли драйверів (sys, drv, vxd), файли бібліотек (DLL), а також у ряд інших типів файлів. Після вкорінення файлові віруси починають розмножуватися під час кожного запуску файла. Завантажувальні віруси - заражають завантажувальний сектор диска (Boot сектор) або сектор, що містить програму системного завантажувача вінчестера (Master Boot Record). Такий вірус заміщає собою програму в завантажувальному секторі, внаслідок цього потрапляє до оперативної пам'яті й перехоплює керування відразу під час завантаження операційної системи. Файлово завантажувальні віруси можуть проникати як у файли, так і в завантажувальні сектори. До таких вірусів належать, зокрема, стелс-віруси і найнебезпечніші екземпляри поліморфних вірусів. Макровіруси проникають у файли документів (пакет Microsoft Office) й інші файли, підготовлені в додатках, що мають свою мову макрокоманд. Формально ці віруси є файловими, але заражають вони не файли, що виконуються, а файли даних. Небезпека макровірусів не стільки в їхній руйнівній дії, скільки в поширеності документів, підготовлених у популярних системах Word і Excel. Мережні віруси поширюються по комп'ютерній мережі. Особливість цих вірусів полягає в тому, що вони заражають тільки оперативну пам'ять комп'ютерів і не записуються на носії інформації. У зв'яку з існуванням різних способів зараження використовують терміни «резидентний» і «нерезидентний» вірус. Резидентні віруси потрапляють до оперативної пам'яті комп'ютера і можуть постійно виявляти свою активність аж до вимикання або перезавантаження комп'ютера. Нерезидентні віруси, навпаки, до пам'яті не потрапляють і активні лише протягом часу, пов'язаного з виконанням певних завдань [3].

При комбінованому втручанні злочинець виконує фізичні дії з підключення до мережі або встановлення спеціального технічного пристрою (наприклад, на банкомат) з наступним запуском програмного продукту, що виконує прописані злочинцем алгоритми роботи.

Висновки. В контексті останніх подій у світі у сфері інформаційних технологій проблема боротьби із кіберзлочинністю видається досить актуальною для України. Дослідження такого елемента криміналістичної характеристики як спосіб вчинення несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку має велике значення для вдосконалення існуючих та створення нових мікрометодик розслідування злочинів у сфері інформаційних технологій та кібербезпеки. Знання типових ознак цієї криміналістичної категорії дає слідчому можливість правильно кваліфікувати протиправне діяння, висувати версії щодо причетних осіб, визначати напрями розслідування.

Список використаних джерел:

1. Гаврилин Ю.В. Расследование преступлений против личности и собственности: [учебное пособие] / Ю.В. Гаврилин. – М. : «Ось-89», 2006. – 384 с.

2. Керівництво з розслідування злочинів: [науково-практичний посібник] / [В.Ю. Шепітько, В.О. Коновалова, В.А. Журавель та ін.] ; за ред. В.Ю. Шепітька. – Х. : «Одіссей», 2009. – 960 с.

3. Комп'ютерні віруси, їх класифікація та типи / Л.І. Пачесюк [Електронний ресурс]. – Режим доступу: http://urok-informatiku.ru/komp-yuterni-virusi-yih-klasifikatsiya-ta-tipi/

4. Мотлях О.І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореферат дис. ... канд. юрид. наук: спец. 12.00.09 Кримінальний процес та криміналістика. Судова експертиза / О.І. Мотлях. – Київ : Б. в., 2005. – 20 с.

5. Паламарчук Л.П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : автореферат дис. ... канд. юрид. наук: спец. 12.00.09 Кримінальний процес та криміналістика. Судова експертиза / Л.П. Паламарчук. – Київ : Б. в., 2005. – 18 с.

6. Пашнєв Д.В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : автореферат дис. ... канд. юрид. наук: спец. 12.00.09 Кримінальний процес та криміналістика. Судова експертиза / Д.В. Пашнєв – Харків, 2007 – 20 с.

7. Преступления в сфере использования компьютерной техники: квалификация, расследование и противодействие: [монография] / И.Р. Шинкаренко, В.О. Голубев, Н.В. Карчевський, И.Ф. Хараберюш. – Донецк: РВВ ЛДУВС, 2007. – 267 с.

8. Скалозуб Л.П. Збірник методичних рекомендацій з викриття та документування злочинів у сфері інтелектуальної власності та високих технологій / Л.П. Скалозуб, В.І. Василинчук, С.А. Лебідь та ін. – К. : КНУВС, 2009. – 188 с.