МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ЛУГАНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ ІМЕНІ Е.О. ДІДОРЕНКА

Протидія злочинам у сфері використання інформаційних технологій

Інтегрований навчально-практичний посібник

За редакцією доктора юридичних наук,
професора М. В. Карчевського

Сєвєродонецьк
2019

УДК 343.346.8:004
К 21

Рецензенти:

Р. Л. Степанюк – професор кафедри криміналістики та судової експертології Харківського державного університету внутрішніх справ, доктор юридичних наук, професор;

Н. А. Савінова – декан факультету морського права та менеджменту Національного університету «Одеська морська академія», доктор юридичних наук, старший науковий співробітник.

Авторський колектив:

М. В. Карчевський, д.ю.н., проф. – розділи 1 (підрозділ 1.1. у співавторстві з В. В. Невгадом, підрозділ 1.6 у співавторстві з В.Є. Комлєвим) та 2 (у співавторстві з Р. А. Усмановим); *В. В. Коваленко*, к.ю.н., доц. – розділи 3 та 5 (у співавторстві з В. І. Чубаєвським), розділ 6 (у співавторстві з О. Ю. Мартишем та О. О. Токаревим); *В. Є. Комлєв* – підрозділ 1.6. (у співавторстві з М. В. Карчевським); *О. Ю. Мартиш* – розділ 6 (у співавторстві з В. В. Коваленком та О. О. Токаревим); *В. В. Невгад* – підрозділ 1.1. (у співавторстві з М. В. Карчевським); *О. О. Токарев* – розділ 6 (у співавторстві з В. В. Коваленком та О. Ю. Мартишем); *Р. А. Усманов* – розділ 2 (у співавторстві з М. В. Карчевським); *В. І. Чубаєвський* – к.політ.н., розділ 5 (у співавторстві з В. В. Коваленком); *М. О. Яковенко*, к.ю.н. – розділ 4.

Рекомендовано вченою радою Луганського державного університету внутрішніх справ імені. Е.О. Дідоренка (протокол № 1 від 31 серпня 2018 року)

К 21 Протидія злочинам у сфері використання інформаційних технологій : інтегрований навчально-практичний посібник / кол. авт. ; за ред. д.ю.н., проф. М. В. Карчевського. – Сєвєродонецьк : РВВ ЛДУВС ім. Е.О. Дідоренка, 2019. – 187 с.
ISBN 978-617-616-086-1

У запропонованому інтегрованому посібнику розкрито питання кримінально-правової кваліфікації та криміналістичного забезпечення досудового розслідування «комп'ютерних» злочинів. Інтегрований посібник – це інформаційний простір, який створено з використанням сучасних технологій навчання та професійного спілкування. Він являє собою цікаву книжку, що складається з текстового матеріалу та доступних за допомогою інтернет інформаційних ресурсів додаткових даних, судової практики, відеокоментарів, презентацій, тестувань, форумів для спілкування.

До складу авторського колективу увійшли представники науки, практики та виробництва.

Посібник розрахований на науковців, викладачів, здобувачів вищої освіти навчальних закладів юридичного профілю, а також практичних працівників правоохоронних органів.

УДК 343.346.8:004

ISBN 978-617-616-086-1

АВТОРСЬКИЙ КОЛЕКТИВ

Карчевський М.В., доктор юридичних наук, професор, перший проректор ЛДУВС ім. Е.О. Дідоренка – розділи 1 (підрозділ 1.1. у співавторстві з В.В. Невгадом, підрозділ 1.6 у співавторстві з В.Є. Комлєвим) та 2 (у співавторстві з Р.А. Усмановим);

Коваленко В.В., кандидат юридичних наук, доцент, професор кафедри кримінально-правових дисциплін ЛДУВС ім. Е.О. Дідоренка – розділи 3 та 5 (у співавторстві з В.І. Чубаєвським); розділ 6 (у співавторстві з О.Ю. Мартишем та О.О. Токаревим);

Комлєв В.Є., заступник директора з якості продукції, представник керівництва з інформаційної безпеки в системі менеджменту ІБ ПрАТ «СНВО «Імпульс» – підрозділ 1.6. (у співавторстві з М.В. Карчевським);

Мартиш О.Ю., начальник відділу протидії кіберзлочинам у Луганській області Донецького управління кіберполіції Департаменту кіберполіції Національної поліції України – розділ 6 (у співавторстві з В.В. Коваленком та О.О. Токаревим);

Невгад В.В., заступник Голови Національної поліції України – начальник Головного слідчого управління – підрозділ 1.1. (у співавторстві з М.В. Карчевським);

Токарев О.О., інспектор відділу протидії кіберзлочинам у Луганській області Донецького управління кіберполіції Департаменту кіберполіції Національної поліції України – розділ 6 (у співавторстві з В.В. Коваленком та О.Ю. Мартишем);

Усманов Р.А., начальник слідчого управління Головного управління Національної поліції в Луганській області – розділ 2 (у співавторстві з М.В. Карчевським);

Чубаєвський В.І., кандидат політічних наук, заступник начальника Департаменту кіберполіції – начальник управління протидії злочинам у сфері інтелектуальної власності та господарської діяльності Департаменту кіберполіції Національної поліції України – розділ 5 (у співавторстві з В.В. Коваленком);

Яковенко М.О., кандидат юридичних наук, доцент кафедри організації правоохоронних та судових органів ЛДУВС ім. Е.О. Дідоренка – розділ 4.

ЧОМУ ПОСІБНИК ВАРТИЙ ВАШОЇ УВАГИ

Проблема протидії злочинам у сфері використання інформаційних технологій є непростою, такою, що динамічно змінюється та потребує постійної уваги. У нашому посібнику зроблено спробу об'єднати найбільш насущні для практиків питання кримінально-правової кваліфікації та криміналістичного забезпечення досудового розслідування «комп'ютерних» злочинів.

Інтегрований посібник уміщує власне книжку, яку Ви тримаєте в руках, та доступні за допомогою інтернет та QR-кодів інформаційні ресурси у вигляді додаткових даних, судової практики, відеокоментарів, презентацій, тестувань, форумів для спілкування. Отже, Вашій увазі пропонуємо не просто текст з актуальних питань юридичної науки та правозастосовної практики, а запрошуємо до інформаційного простору, який створено з використанням сучасних технологій для навчання та професійного спілкування.

Доступ до інтерактивних можливостей посібника

Зичимо цікавої та плідної праці й навчання.

Авторський колектив

ПОДЯКИ

Упровадження нових технологій неможливе без ефективної співпраці великої кількості фахівців, прикладом чого і є цей посібник. Робота над проблематикою протидії злочинам у сфері використання інформаційних технологій об'єднала представників науки, практики та виробництва. Дякую співавторам за цікаву спільну роботу та висловлюю надію на співпрацю й надалі.

Щиро вдячний усім, хто допомагав.

Раїса Іллівна Пащук та Галина Йосипівна Васильєва дещо поліпшили мову викладу тексту. Антон Сергійович Кудінов та Ігор Павлович Коченко зробили все для того, щоб інтерактивна складова посібника працювала дієво. Відеокоментарі стали можливими завдяки Юлії Євгенівні Ковальовій.

Плідною була співпраця з ПАТ «Сєвєродонецьке науково-виробниче об'єднання «Імпульс». Удячний голові наглядової ради Володимирові Васильовичу Єлісєєву за підтримку та змістовне спілкування з питань інформаційної безпеки сучасних промислових автоматизованих систем.

Окрема вдячність професійним колективам слідчого управління Головного управління Національної поліції в Луганській області, відділу протидії кіберзлочинам у Луганській області Донецького управління кіберполіції Департаменту кіберполіції Національної поліції України та Луганського державного університету

внутрішніх справ імені Е.О. Дідоренка. Накопичений шанованими колегами досвід і небайдужість до інновацій дає змогу справді робити корисні речі.

Микола Карчевський

РОЗДІЛ 1. КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

1.1. Загальна характеристика злочинів у сфері використання інформаційних технологій. «Комп'ютерний злочин»

«Кіберзлочинність», «хакери», «комп'ютерний злом», «крадіжка машинного часу» – ці терміни вже перестали бути екзотикою для юристів. На сьогодні комп'ютерні злочини – одна з найдинамічніших груп суспільно небезпечних посягань. Беззаперечним є те, що швидке збільшення показників поширеності таких злочинів, а також постійне зростання їх суспільної небезпеки стало зворотним, негативним

Інформаційний «вибух». Комп'ютеризація. Інформатизація

явищем такого суспільно важливого процесу, як інформатизація. Скажімо, якщо 2000 року «фактів, де комп'ютерна техніка виступала як об'єкт скоєння злочину, зокрема фактів несанкціонованого проникнення до локальних відомчих комп'ютерних мереж та банків зареєстровано не було»[1], а 2001 року відповідно до статистики МВС було зареєстровано п'ять таких злочинів, то вже 2002 року їх було 30, 2007 – 145, 2016 – 818, 2017 – 2514. Тобто за десять останніх років спостерігаємо зростання більше ніж у 15 разів (!).

Водночас наголосимо, що кількісна оцінка цих посягань є окремою науковою проблемою. Вітчизняні та зарубіжні кримінологи зараховують «комп'ютерну» злочинність до гіперлатентних. За різними оцінками, правоохоронцям стає відомо лише про 10 – 20 % таких злочинів.

Очевидні труднощі протидії злочинам у сфері використання комп'ютерної техніки національними правоохоронними органами можна рельєфно представити через порівняння: 1) кількості облікованих кримінальних проваджень (статті 361 – 363-1 КК); 2) вироків відповідної категорії, наявних у Єдиному державному реєстрі судових рішень; 3) рівня проникнення Інтернету в країні (співвідношення щомісячної аудиторії Інтернету до кількості населення)[2]. Якщо 2013 року було обліковано

[1] Аналітичний огляд стану комп'ютерної злочинності та інформаційної безпеки в Україні у 2000 році / Національне бюро Інтерполу в Україні. Київ, 2001. С. 6 (Наводиться за: Гуцалюк М. Координація боротьби з комп'ютерною злочинністю. *Право України*. 2002. № 5. С. 121).

[2] Для аналізу рівня проникнення Інтернету використано результати дослідження Factum Group (Мінченко О. Уже більше половини жителів сіл в Україні користуються інтернетом // Watcher: про маркетинг, піар та комунікації в Інтернеті : сайт. 17.01.2018. URL : http://watcher.com.ua/2018/01/17/vzhe-bilshe-polovyny-zhyteliv-sil-v-ukrayini-korystuyutsya-internetom/ (дата звернення : 01.08.2018))

568 проваджень, суди постановили 58 вироків, а рівень проникнення Інтернету складав 53% дорослого населення, то 2017 року, за умови проникнення Інтернету на рівні 63%, суди постановили 33 вироки (зменшення на 43%), а кількість облікованих проваджень склала 2514 (збільшення на 343%).

Таблиця 1

Статистичні дані щодо протидії злочинам у сфері використання інформаційних технологій

Показник	2013	2014	2015	2016	2017
Абсолютні дані					
Кількість вироків у Єдиному державному реєстрі судових рішень	58	40	39	24	33
Обліковано кримінальних правопорушень	568	418	556	818	2514
Кримінальні правопорушення, у яких особам вручено повідомлення про підозру	245	194	250	455	1256
Проникнення Інтернету (Factum Group)	53	57	58	63	63
Відносні дані (відсотки від базового рівня – 2013 р.)					
Кількість вироків у Єдиному державному реєстрі судових рішень	100	69	67	41	57
Обліковано кримінальних правопорушень	100	74	98	144	443
Кримінальні правопорушення, у яких особам вручено повідомлення про підозру	100	79	102	186	513
Проникнення Інтернету (Factum Group)	100	108	109	119	119

Таблиця 2

Структура облікованих кримінальних правопорушень у сфері використання інформаційних технологій

Кримінальне правопорушення	2013	2014	2015	2016	2017
Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, ст. 361	398	327	413	472	1777
Створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних засобів, а також їх розповсюдження або збут, ст. 361-1	8	8	17	13	32
Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, ст. 361-2	17	9	55	21	54
Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, учинені особою, яка має право доступу до неї, ст. 362	142	69	60	296	643

Таблиця 2 *(продовження)*

Кримінальне правопорушення	**2013**	**2014**	**2015**	**2016**	**2017**
Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється, ст. 363	2	4	9	14	5
Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку, ст. 363-1	1	1	2	2	3
Разом	**568**	**418**	**556**	**818**	**2514**

Різноспрямовані тренди реєстрації кримінальних правопорушень у сфері використання комп'ютерної техніки, розгляду судами кримінальних справ цієї категорії та проникнення Інтернету з усією очевидністю свідчать про те, що на сьогодні практика протидії цим правопорушенням перебуває на етапі формування. Ефективні методи виявлення та розкриття ще належить розробити. Фундаментальне значення для розв'язання такого завдання має зміст ознак розглядуваних складів злочинів. Він визначає специфіку оперативного супроводу розслідування, особливості відповідних слідчих дій і криміналістичних методик.

В Україні кримінальну відповідальність за злочини у сфері використання інформаційних технологій уперше було передбачено 1994 року. Законом України № 218/94-ВР від 20 жовтня 1994 року КК України 1960 року було доповнено ст. 198-1 «Порушення роботи автоматизованих систем». Чинний Кримінальний кодекс передбачає самостійний розділ про ці злочини – розділ XVI КК «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Положення цього розділу неодноразово змінювали та доповнювали (закони №908-IV від 05.06.2003, №2289-IV від 23.12.2004; №721-VII від 16.01.2014, №767-VII від 23.02.2014, № 770-VIII від 10.11.2015).

Родовим об'єктом злочинів, передбачених у розділі XVI КК, є частина інформаційних відносин, які можна визначити як *інформаційні відносини, засобом забезпечення яких є ЕОМ, системи, комп'ютерні мережі та мережі електрозв'язку.* Інакше кажучи, злочини, передбачені цим розділом, посягають на *певну частину* інформаційних відносин – інформаційні відносини, пов'язані із застосуванням спеціальних технічних засобів. У кримінальному законі наведено чотири види таких засобів:

– ЕОМ (комп'ютер) – функціональний пристрій, що складається з одного або декількох взаємопов'язаних центральних процесорів і периферійних пристроїв та може виконувати розрахунки без участі людини[1];

[1] ДСТУ 2938:1994. Системи оброблення інформації. Основні положення. Терміни та визначення [Чинний від 1996-01-01]. Вид. офіц. Київ, 1996. С. 7.

– автоматизована система – організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей і персоналу, який здійснює цю діяльність[1];

– комп'ютерна мережа – сукупність територіально розосереджених систем опрацювання даних, засобів і (або) систем зв'язку та передавання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів[2];

– телекомунікаційна мережа (мережа електрозв'язку) – комплекс технічних засобів телекомунікацій і споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду за допомогою радіо, проводових, оптичних чи інших електромагнітних систем між кінцевим обладнанням[3].

Залежно від цих засобів інформаційні відносини, які є родовим об'єктом досліджуваних злочинів, може бути поділено на чотири види:

1) інформаційні відносини, засобом забезпечення яких є комп'ютери;

2) інформаційні відносини, засобом забезпечення яких є комп'ютерні системи;

3) інформаційні відносини, засобом забезпечення яких є комп'ютерні мережі;

---

[1] ДСТУ 2226:19934. Автоматизовані системи. Терміни та визначення [Чинний від 1994-07-01]. Вид. офіц. Київ, 1994. С. 2.

[2] ДСТУ 2938:1994. Системи оброблення інформації. Основні положення. Терміни та визначення [Чинний від 1996-01-01]. Вид. офіц. Київ, 1996. С. 7.

[3] Про телекомунікації : Закон України від 18.11.2003 № 1280-IV. Дата оновлення: 04.11.2018. URL : http://zakon.rada.gov.ua/laws/show/1280-15 (дата звернення : 01.12.2018)

4) інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку.

Перший вид цих інформаційних відносин – це найпростіша форма застосування комп'ютерної техніки для роботи з інформацією. Суб'єкти таких відносин використовують комп'ютерну техніку для виконання здебільшого нескладних операцій: підготування документів, проведення інженерних розрахунків, організація та робота з базами даних. Зазначимо, що під ЕОМ розуміють не тільки комп'ютери в їх «класичному», можна сказати, звичному вигляді, тобто «системний блок – монітор – клавіатура – принтер», але й інше устаткування, яке містить процесор і може виконувати розрахунки без участі людини.

«Нетипові» ЕОМ. Убудовані системи

Використання комп'ютерних систем належить до більш складних інформаційних відносин. Автоматизовані системи використовують для виконання широкого кола завдань: управління підприємством, технологічного підготування виробництва, контролю й випробування промислової продукції, управління службами життєзабезпечення підприємства тощо.

Третій вид інформаційних відносин, які утворюють досліджуваний родовий об'єкт, пов'язаний з використанням комп'ютерних мереж, що бувають двох видів: локальні, які об'єднують комп'ютери в межах однієї організації, і глобальні, що забезпечують зв'язок між різними організаціями, юридичними та фізичними особами. Найвідомішою й найпоширенішою глобальною

комп'ютерною мережею є Інтернет, що застосовують в основному для таких видів роботи з інформацією: електронна пошта; передавання файлів; віддалений доступ – можливість підключатися до віддаленого комп'ютера й працювати з ним в інтерактивному режимі.

Судова практика. Несанкціоноване втручання в роботу електронного лічильника електроенергії

Інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку, полягають у наданні й отриманні послуг електричного зв'язку, тобто у використанні мереж електрозв'язку для передачі або приймання інформації. Що ж до визначення змісту цих суспільних відносин, то певний інтерес становить питання їх відмежування від інформаційних відносин, засобом забезпечення яких є комп'ютерні мережі. Аналіз чинного законодавства у сфері телекомунікації дає змогу стверджувати, що наявність у законі про кримінальну відповідальність одночасно з терміном «мережа електрозв'язку» іншого – «комп'ютерна мережа» – фактично означає, що під мережею електрозв'язку треба розуміти всі телекомунікаційні мережі, крім комп'ютерних (мережі міського, міжміського та міжнародного телефонного зв'язку, рухомого (мобільного) зв'язку, проводового радіомовлення, ефірного телерадіомовлення тощо). Отже, під інформаційними відносинами, засобом забезпечення яких виступають мережі електрозв'язку, треба розуміти суспільні відносини у сфері використання телекомунікаційних мереж за винятком комп'ютерних мереж.

Злочини у сфері використання інформаційних технологій та «комп'ютерні злочини». З визначенням родового об'єкта злочинів у сфері використання ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку пов'язана ще одна проблема – проблема найменування злочинів, які посягають на цей об'єкт. Закон визначає ці злочини терміном «злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Одночасно з цим терміном як тотожний будемо використовувати термін *«злочини у сфері використання інформаційних технологій».*

Відеокоментар до підрозділу 1.1.

Забезпечення кримінально-правового стимулювання позитивних і мінімізації негативних соціальних наслідків інформатизації передбачає визначення як самостійного об'єкта кримінально-правової охорони системи суспільних відносин, що забезпечують реалізацію інформаційної потреби. Для позначення цієї системи використовують термін «інформаційна безпека», структуру якої складають відносини у сфері формування інформаційного ресурсу, забезпечення доступу до інформації, а також відносини у сфері використання інформаційних технологій. Соціальна значущість відносин інформаційної безпеки, а отже, і доцільність їх кримінально-правової охорони визначаються значимістю тих відносин, у межах яких виникає інформаційна потреба. І собі інформаційна технологія є організованою сукупністю інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість

обробки даних, швидкий пошук інформації, передачу даних, доступ до джерел інформації незалежно від місця їх розташування. Отже, злочини у сфері використання інформаційних технологій як один з видів злочинів у сфері інформаційної безпеки визначимо як *передбачені законодавством про кримінальну відповідальність суспільно небезпечні, винні, здійснювані суб'єктом злочину діяння, які заподіюють шкоду забезпеченим засобами обчислювальної техніки відносинам у сфері реалізації інформаційної потреби (*статті 361 – 363-1 КК).

Водночас із запропонованим поняттям («злочин у сфері використання інформаційних технологій») у кримінально-правовому дискурсі досить активно використовують такі: «комп'ютерний злочин», «кіберзлочин», «інтернет-злочин» тощо. Обсяг цих понять визначається по-різному. Проте найбільш поширеним є віднесення до комп'ютерних злочинів усіх суспільно небезпечних посягань, при здійсненні яких комп'ютери використовують як технічні засоби.

Наведене визначення кіберзлочинів є майже загальновизнаним у зарубіжній науковій літературі, а також досить широко представлено у вітчизняній. Наголосимо, що зарубіжний досвід, безсумнівно, треба вивчати й використовувати. Проте бездумне перенесення західних стандартів регулювання політичних, економічних і соціальних процесів без урахування історичних та національних особливостей не завжди приводить до позитивних результатів. Уважаємо, що у випадку з визначенням комп'ютерних злочинів і використанням цього поняття у вітчизняному кримінально-правовому дискурсі йдеться саме про таку ситуацію.

В описаному вище розумінні будь-який злочин, скоєний з використанням комп'ютерної техніки (шахрайство, шпигунство, незаконне розповсюдження наркотичних засобів тощо), має вважатися комп'ютерним. Хоча

цілком очевидно, що перераховані суспільно небезпечні діяння не є злочинами нового виду. Такі дії попри використання для їх здійснення комп'ютерної техніки є державною зрадою, шпигунством, крадіжкою, шахрайством, незаконним збиранням відомостей, що містять комерційну таємницю тощо. Засіб не змінює суті злочину. Вадою такого підходу є його невідповідність основному принципу структурування національного законодавства про кримінальну відповідальність – систематизації норм кримінального закону на основі класифікації посягань за об'єктом. Визначення нової групи злочинів завжди має проводити на основі ознак, що характеризують об'єкт посягання. Саме тому в межах національного кримінально-правового дискурсу необґрунтованим треба вважати визначення групи злочинів на основі ознак, що характеризують спосіб, знаряддя чи засіб посягання.

Як відомо, виготовлення підроблених грошових купюр за допомогою сучасних пристроїв друку попри зростання суспільної небезпеки не змінило кваліфікацію цих дій: винних притягували й продовжують притягувати до кримінальної відповідальності за статтями про фальшивомонетництво, також як і тих, хто використовував для підробки фототехніку або звичайні олівці, фарби й лезо бритви. Комп'ютерна техніка дає змогу довести до досконалості процес виготовлення підроблених документів: перенесені з оригіналу печатки, підписи, інші реквізити майже ідентичні. Для встановлення підробки потрібно буде проведення висококваліфікованої криміналістичної експертизи, проте це не означає, що такого роду підробки документів вимагають особливої, відмінної від наявної кваліфікації. Висновок може бути тільки один: модифікація знарядь і засобів учинення злочину, використання для цього досягнень науково-

технічного прогресу не змінює тих відносин, на які він посягає, чи не свідчить про появу злочинів нового виду.

Отже, доречне в межах зарубіжного кримінально-правового дискурсу визначення комп'ютерних злочинів має досить обмежену цінність для національного. Поняття «комп'ютерний злочин» і «кіберзлочин» в усталеному розумінні може бути ефективно використано при проведенні кримінологічних, кримінально-процесуальних, криміналістичних досліджень. Що ж стосується національного кримінально-правового дискурсу, то тут їх застосування варто обмежити й використовувати запропоноване поняття «злочин у сфері використання інформаційних технологій».

Кваліфікуючі ознаки злочинів у сфері використання інформаційних технологій. Загальна характеристика злочинів у сфері використання інформаційних технологій була б неповною без дослідження кваліфікуючих ознак цих посягань. Статті 361–362 та 363-1 КК містять такі спільні кваліфікуючі ознаки:

– учинення злочину повторно;

– учинення злочину за попередньою змовою групою осіб;

– учинення злочину, який заподіяв значну шкоду.

Оскільки в розділі XVI Особливої частини КК не передбачено повторності однорідних злочинів, злочин у сфері використання інформаційних технологій слід уважати вчиненим **повторно** у випадках, коли особа два або більше рази вчинила злочин, який було кваліфіковано за однією статтею зазначеного розділу. До того ж вчинення декількох таких злочинів не охоплювалося єдиним умислом (злочин не був продовжуваним), особа не звільнялася від кримінальної відповідальності за тотожний злочин, не закінчилися строки давності притяг-

нення до кримінальної відповідальності за раніше вчинений злочин або судимість за нього не було погашено чи знято.

Злочин буде вважатися вчиненим **групою осіб за попередньою змовою** за наявності відповідних об'єктивних і суб'єктивних ознак. Його об'єктивна сторона може бути такою:

– діяння вчиняють два або більше виконавці, кожен з яких виконує всі дії, що утворюють об'єктивну сторону складу (наприклад, декілька осіб здійснюють несанкціоноване втручання з окремих терміналів і знищують певну інформацію);

– злочин учиняють два або більше співвиконавці, кожен з яких виконує частину дій, що характеризують об'єктивну сторону (скажімо, одна особа вчиняє несанкціоноване втручання й перекручує комп'ютерну інформацію про користувачів комп'ютерної мережі та паролі їх доступу, а інша знищує комп'ютерну інформацію);

– злочин учиняють дві або більше особи й до того ж лише одна з них виконавець, а інші – підбурювачі, пособники або організатори (наприклад, одна особа забезпечує іншу потрібним устаткуванням, а остання вчиняє розповсюдження шкідливої комп'ютерної програми).

До того ж кожен зі співвиконавців повинен мати всі ознаки суб'єкта, тобто бути фізичною осудною особою та досягти віку кримінальної відповідальності[1]. У разі, коли особа не була поінформована про те, що вчиняє злочин разом з малолітнім або неосудним, її дії слід кваліфікувати за правилами фактичної помилки

[1] Певну специфіку матиме вчинення групою осіб за попередньою змовою злочину, передбаченого ст. 362 КК, адже суб'єкт цього злочину – спеціальний. У цьому випадку слід керуватися правилами кваліфікації співучасті зі спеціальним суб'єктом.

як замах на вчинення злочину групою осіб за попередньою змовою.

До об'єктивних ознак учинення злочину за попередньою змовою групою осіб належить також спільність, що характеризується взаємозумовленістю дій, загальним для всіх співучасників наслідком і наявністю причинового зв'язку між діями співучасників і злочином, який учинив виконавець.

Слайди до підрозділу 1.1.

Певну специфіку має суб'єктивна сторона злочину в разі його вчинення за попередньою змовою групою осіб. Особливості використання сучасних мережевих технологій для спілкування (наявність форумів, чатів тощо) дають змогу мовити про те, що домовленість про спільне вчинення злочину може бути досягнута без особистого знайомства співучасників

Значною шкодою в статтях 361–363-1 КК, якщо вона полягає в заподіянні матеріальних збитків, уважається така шкода, яка в сто і більше разів перевищує НМДГ (примітка до ст. 361 КК). Зазвичай ця шкода полягає в заподіянні *позитивних матеріальних збитків*. У такому разі її потрібно оцінювати з огляду на витрати власника щодо придбання комп'ютерної інформації. Але щодо значної шкоди як кваліфікуючої ознаки злочину у сфері використання інформаційних технологій зауважимо, що іноді вона може виражатися і в *упущеній вигоді*. Це можна пояснити тим, що на сучасному етапі будь-яка діяльність як потрібний елемент містить ін-

формаційне забезпечення. Ефективність діяльності багато в чому залежить від кількості та якості вхідної інформації[1], позаяк перекручення або знищення інформації, що має порівняно невелику ціну, здатне завдати значних матеріальних збитків у вигляді упущеної вигоди. Саме тому видається правильним, крім втрати або зменшення обсягу інформації, якою володіє потерпілий, у розмір матеріальних збитків від «комп'ютерного злочину» вносити також і упущену вигоду, яка може полягати в укладанні невигідних договорів, падінні авторитету, невиконанні умов договорів тощо.

Крім матеріальної шкоди, суспільно небезпечні наслідки при вчиненні комп'ютерного злочину можуть виражатись і в *нематеріальних видах шкоди*, що зумовлено використанням ЕОМ, систем і комп'ютерних мереж для контролю над складними технологічними процесами, об'єктами та керування ними. Це така шкода, як порушення нормальної роботи підприємств, зупинення або порушення складних технологічних процесів, погіршення обороноздатності держави, підрив авторитету державних органів, підприємств, установ або організацій, створення загрози або заподіяння шкоди життю та здоров'ю громадян, порушення безпеки руху транспорту тощо.

Суб'єктивна сторона злочину, який заподіяв істотну шкоду, характеризується змішаною формою вини. У таких злочинах психічне ставлення особи до діяння та першого, обов'язкового, наслідку (втрати, підробки, блокування інформації тощо) виражається в умислі

[1] Семухин И. Ю. Информация – фактор общественного воспроизводства. *Матеріали ІІ звітної науково-практичної конференції професорсько-викладацького та курсантського складу Кримського факультету Університету внутрішніх справ*. Сімферополь : Доля, 2000. С. 105–110.

(прямому або непрямому), а до другого (кваліфікованого) наслідку – істотної шкоди – може бути як умисним, так і необережним. Зауважимо, що в деяких випадках умисне заподіяння істотної шкоди в результаті злочину у сфері використання інформаційних технологій може фактично являти собою інший склад злочину. Скажімо, цілком очевидно, що знищення певної надзвичайно важливої для обороноздатності країни комп'ютерної інформації для ослаблення держави не буде вважатися несанкціонованим утручанням, яке заподіяло істотну шкоду (ч. 2 ст. 361 КК), а є нічим іншим, як диверсією (ст. 113 КК).

Тест до підрозділу 1.1.

1.2. Несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку

Безпосереднім об'єктом цього злочину є право власності на комп'ютерну інформацію – сукупність права та можливості особи: володіти носієм інформації; використовувати інформацію, яка міститься на ньому, для задоволення своєї інформаційної потреби; дає змогу іншим особам використовувати інформацію, яка міститься на його носії, змінювати її, визначати долю носія. Таке визначення безпосереднього об'єкта досить повно відображає механізм заподіяння шкоди суспільним відносинам власності на комп'ютерну інформацію, який

полягає в порушенні, позбавленні або обмеженні реалізації власником інформації повноважень володіння, розпоряджання, користування нею.

Слайди до підрозділу 1.2.

Зауважимо також, що редакція статті дає підстави стверджувати, що крім права власності на комп'ютерну інформацію, вона охороняє й *суспільні відносини надання та отримання послуг електрозв'язку*. До цих суспільних відносин можна вжити термін «альтернативний безпосередній об'єкт злочину». Специфіка чинної редакції ст. 361 КК полягає в тому, що вона забезпечує охорону від злочинних посягань двох різних видів суспільних відносин: власності на комп'ютерну інформацію та надання послуг електрозв'язку. Отже, ст. 361 *охороняє, крім відносин власності на комп'ютерну інформацію, суспільні відносини надання послуг електрозв'язку*. Зміст цих відносин полягає в тому, що оператори й провайдери телекомунікацій забезпечують їхнім споживачам можливість передавання та приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду за допомогою радіо, проводових, оптичних або інших електромагнітних систем[1].

Предметом злочину, передбаченого ст. 361 КК, з огляду на диспозицію є *інформація,* але аналіз об'єкта і

[1] Більш докладно див.: Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 116–118.

форм об'єктивної сторони несанкціонованого втручання дає підстави стверджувати, що до предметів цього злочину належить комп'ютерна інформація та інформація, що передається каналами зв'язку.

Комп'ютерна інформація. Об'єкт і предмет будь-якого злочину є взаємозалежними, взаємозумовленими. Тому аналізуючи ознаки предмета несанкціонованого втручання, треба виходити з викладеної вище характеристики змісту безпосереднього об'єкта як *відносин власності на інформацію*. Загальновизнаним у кримінальному праві є погляд, що предмет злочину характеризується сукупністю трьох ознак: фізичної, економічної та юридичної. Визначаючи інформацію предметом злочину, треба проаналізувати її ознаки.

Фізична ознака. Специфіка комп'ютерної інформації як предмета злочину полягає в неможливості її віднесення ні до матеріальних, ні до нематеріальних предметів. Інформація як нематеріальний предмет включається в систему суспільних відносин за допомогою матеріального носія. Інакше кажучи, фізична ознака комп'ютерної інформації як предмета злочину полягає в її носії, котрий зазвичай розуміється як предмет, річ, властивості якої використовують для передачі, зберігання та обробки інформації. Носіями комп'ютерної інформації є оптичні та жорсткі диски, flash-носії, SD-карти, сигнали в мережах передавання даних тощо.

Інформація як предмет злочину має *економічну ознаку,* ціну, яка зрештою визначається її змістом і заінтересованістю споживача в її одержанні. Цінність інформації буває різною: інформація може бути цінною по суті, оскільки є результатом тривалої роботи значної кількості осіб, а може бути цінною за призначенням, адже її наявність є потрібною умовою для вирішення певного завдання. Цінність інформації як предмета злочину має

одну особливість: її корисні властивості як фактор цінності не зводяться до фізичної цілісності її носія. До прикладу, комп'ютерна інформація може бути знищена або перекручена, а фізичні властивості носія залишаться незмінними. З огляду на сказане до економічної ознаки комп'ютерної інформації слід віднести не тільки наявність ціни, але й також *корисних властивостей*, які дають змогу задовольняти інформаційну потребу. Ці властивості можна описати так:

– цілісність – захищеність від несанкціонованих змін;

– доступність – захищеність від несанкціонованого змісту інформаційних ресурсів;

– конфіденційність – захищеність від несанкціонованого одержання комп'ютерної інформації[1].

Юридична ознака комп'ютерної інформації полягає в тому, що вона має бути *чужою* для винного й мати свого власника.

Отже, з огляду на викладене комп'ютерну інформацію як предмет злочину видається можливим визначити в такий спосіб: *відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника й ціну[2].*

---

[1] Ця сукупність ознак одержала назву критеріїв безпеки інформаційної технології *ITSEC* (Information Technology Security Evaluation Criteria), які було прийнято 1991 р. співтовариством чотирьох європейських держав (Франції, Німеччини, Нідерландів і Великої Британії). Тепер застосовуються для характеристики не тільки технічної захищеності системи, але й ефективності правових механізмів охорони суспільних відносин щодо комп'ютерної інформації.

[2] Більш докладно див.: Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 119–123.

Інформація, що передається каналами зв'язку. Співвідношення категорій «інформація, що передається мережами електрозв'язку» та «комп'ютерна інформація», яка теж належить до предметів незаконного втручання, можна визначити так: якщо комп'ютерна інформація – це відомості, подані у формі, яка дає змогу опрацьовувати їх за допомогою ЕОМ, то інформацією, що передається мережами електрозв'язку, є *відомості, подані у формі, що дає змогу їх приймати або передавати засобами електрозв'язку*. Інформація в цих мережах передається за допомогою сигналів, які є матеріальними носіями передавання інформації.

Об'єктивна сторона. Диспозиція статті 361 КК дає змогу виснувати, що об'єктивна сторона несанкціонованого втручання характеризується такою структурою: **діяння** – несанкціоноване втручання в роботу ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку; **суспільно небезпечні наслідки** – витік, втрата, підробка, блокування інформації, спотворення процесу обробки інформації, порушення встановленого порядку маршрутизації інформації (перелічені наслідки є альтернативними, тобто для наявності складу злочину досить настання хоча б одного з наслідків); **причинний зв'язок** між діянням та наслідками.

З огляду на означену специфіку безпосереднього об'єкта складу злочину, передбаченого ст. 361 КК, є можливим виокремити такі види несанкціонованого втручання, що розрізняються за змістом:

Відеокоментар до підрозділу 1.2.

– несанкціоноване втручання в роботу ЕОМ, автоматизованих систем і комп'ютерних мереж;

– несанкціоноване втручання в роботу мереж електрозв'язку.

Утручання в роботу ЕОМ, систем або комп'ютерних мереж – зміна режиму роботи ЕОМ, системи або комп'ютерної мережі, учинена через вплив на носій комп'ютерної інформації або засоби її автоматизованого опрацювання, з порушенням установленого відповідно до законодавства порядку доступу до інформації, що заподіює шкоду суспільним відносинам власності на комп'ютерну інформацію.

До наслідків несанкціонованого втручання в роботу ЕОМ, систем або комп'ютерних мереж належить: 1) витік; 2) утрата; 3) підробка; 4) блокування комп'ютерної інформації; 5) спотворення процесу обробки комп'ютерної інформації; 6) порушення встановленого порядку маршрутизації комп'ютерної інформації. За змістом ці суспільно небезпечні наслідки є різними формами порушення права власності на комп'ютерну інформацію.

Витік інформації – це результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, які не мають права доступу до неї. Витік є порушенням такого повноваження власника комп'ютерної інформації, як право розпорядження.

Утрата комп'ютерної інформації – це такий вплив на носій комп'ютерної інформації, унаслідок якого вона перестає існувати у формі, що дає змогу опрацьовувати її за допомогою комп'ютерної техніки.

Підробка комп'ютерної інформації, як видається, являє собою порушення такого повноваження власника, як користування, адже через підробку він повністю або частково втрачає можливість реалізовувати свою ін-

формаційну потребу. З огляду на це можна так визначити підробку комп'ютерної інформації: зміна без відома власника змісту відомостей, відображених на носії, що робить інформацію цілком або частково непридатною для задоволення інформаційної потреби особою, яка має право власності на таку інформацію.

Блокування комп'ютерної інформації також є специфічною формою порушення повноваження користування інформацією. Воно являє собою ситуацію, коли комп'ютерна інформація не знищена, не підроблена, але можливість використовувати її відсутня. Можна сформулювати таке визначення: блокування комп'ютерної інформації – відсутність у власника можливості використовувати інформацію для задоволення інформаційної потреби за умови, що її не втрачено та не підроблено.

Спотворення процесу обробки комп'ютерної інформації – отримання під час операцій з комп'ютерною інформацією, які здійснювалися за допомогою технічних чи програмних засобів, результатів, що не відповідають характеристикам технічних засобів або алгоритму комп'ютерної програми.

Порушення встановленого порядку маршрутизації комп'ютерної інформації матиме місце, коли комп'ютерна інформація, що передається за допомогою комп'ютерної мережі конкретному абонентові (абонентам), ним не отримується або доступ до певних мережевих ресурсів здійснюється з порушенням установленого порядку.

Несанкціоноване втручання в роботу мережі електрозв'язку являє собою порушення встановленого режиму роботи мережі, учинене через вплив на засоби або споруди зв'язку, що ставить під загрозу суспільні відносини щодо надання й отримання послуг електрозв'язку.

До наслідків несанкціонованого втручання в роботу мереж електрозв'язку зараховують: 1) витік; 2) утрата; 3) підробка; 4) блокування інформації, що передається каналами зв'язку; 5) порушення встановленого порядку маршрутизації інформації, що передається каналами зв'язку. Специфіка об'єкта й предмета цього посягання визначає й особливості змісту його суспільно небезпечних наслідків.

Отже, *витік* інформації, що передається мережею електрозв'язку, є результатом несанкціонованого втручання в роботу мережі електрозв'язку, унаслідок якого інформація, що передається мережею, стає відомою чи доступною фізичним та/або юридичним особам, які не мають права доступу до неї.

Утрата інформації, що передається мережами електрозв'язку, – це порушення електрозв'язку у вигляді неотримання абонентом мережі інформації, якому вона надсилається.

Підробкою інформації буде такий вплив на носій інформації, що передається мережею електрозв'язку, у результаті якого абонент отримує відомості, які не збігаються з тими, що було йому надіслано.

Блокування інформації, що передається каналами зв'язку, є результатом несанкціонованого втручання в роботу мережі електрозв'язку у вигляді неможливості або значного ускладнення протягом певного часу отримувати чи надсилати інформацію за допомогою цієї мережі.

Порушення порядку маршрутизації інформації в мережі електрозв'язку, як звичайно, матиме місце, коли інформація, що передається за допомогою мережі конкретному абонентові (абонентам), ним не отримується, а також у випадках отримання інформації, що передається в мережі, на кінцеве обладнання, яке не є складо-

вою цієї мережі. Типовими прикладами несанкціонованого втручання в роботу мереж електрозв'язку з настанням таких наслідків є незаконне підключення телефонних апаратів до мереж телефонного зв'язку, а також незаконне підключення телевізійних приймачів до мереж кабельного телебачення[1]. Проте зазначимо, що існують і більш складні види порушення порядку маршрутизації, які пов'язані, зокрема, з маршрутизацією вхідного міжнародного трафіку на телефонні мережі загального користування. У судовій практиці такий вид досліджуваних наслідків траплявся в контексті правової оцінки осіб, які займалися незаконною діяльністю щодо надання послуг IP-телефонії[2].

Під *спотворенням процесу обробки* інформації, що передається каналами електрозв'язку, потрібно розуміти отримання під час роботи технічного засобу

[1] Вироки Новокаховського міського суду Херсонської області в справі 1-266/08 від 13 червня 2008 року та в справі № 1-344/08 від 19 серпня 2008 року; вирок Замостянського районного суду м. Вінниця в справі № 1-249/08 від 27 березня 2008 року (див.: Єдиний державний реєстр судових рішень : сайт. URL : http://www.reyestr.court.gov.ua/). Коментуючи ці вироки, зазначимо, що суди правильно кваліфікують випадки незаконного підключення до мереж кабельного телебачення як несанкціоноване втручання в роботу мереж електрозв'язку – злочин, передбачений ст. 361. До того ж до наслідків подібних посягань обґрунтовано зараховують: витік інформації, оскільки програми мовлення, що транслюються в мережі, отримує особа, яка не має на це прав; порушення порядку маршрутизації, оскільки внаслідок дій порушника змінюється встановлений режим роботи мережі (збільшується кількість кінцевого обладнання), та, у разі фіксації зменшення якості сигналу внаслідок дій порушника, блокування інформації, що передається мережами електрозв'язку.

[2] Вирок Кіровського районного суду м. Кіровоград у справі № 1-43/09 від 22 січня 2009 року // Єдиний державний реєстр судових рішень : сайт. URL : http://www.reyestr.court.gov.ua (дата звернення : 01.12.2018).

зв'язку результатів, що не відповідають його характеристиці. Зазначимо, що підроблення та спотворення процесу обробки інформації в мережі електрозв'язку можуть характеризуватися спільним суспільно небезпечним результатом (заподіянням об'єкту однакової шкоди), проте різним є механізм її заподіяння: підроблення вчиняється через вплив на носій інформації, а спотворення процесу оброблення – через вплив на технічний засіб зв'язку.

Судова практика

Причинний зв'язок як обов'язкова ознака об'єктивної сторони несанкціонованого втручання в роботу ЕОМ, систем, комп'ютерних мереж або мереж електрозв'язку полягає в тому, що діяння (несанкціоноване втручання) спричиняє настання наслідків: воно передує настанню зазначених суспільно небезпечних наслідків, містить у собі реальну можливість наслідків і в конкретному випадку є необхідною умовою, без якої б наслідки не настали.

Несанкціоноване втручання буде закінченим з моменту настання суспільно небезпечних наслідків.

Суб'єкт *несанкціонованого втручання* загальний; ним є фізична осудна особа, яка досягла 16-річного віку.

Суб'єктивна сторона несанкціонованого втручання полягає в тому, що особа: а) усвідомлювала суспільну небезпеку втручання, тобто фактичні та соціальні ознаки діяння, його несанкціонованість; б) передбачала наслідки у вигляді витоку, втрати, підроблення, блоку

вання інформації, спотворення процесу обробки інформації або порушення порядку її маршрутизації; в) бажала або свідомо припускала настання цих наслідків. Тобто суб'єктивна сторона аналізованого складу може виражатись у вигляді як прямого, так і непрямого умислу[1].

Тест до підрозділу 1.2.

1.3. Незаконні дії зі шкідливими програмними або технічними засобами

Безпосередній об'єкт злочину, передбаченого ст. 361-1 КК, складають суспільні відносини власності на комп'ютерну інформацію та відносини надання й отримання послуг електрозв'язку. Зазначимо, що специфіка механізму заподіяння шкоди цим суспільним відносинам у результаті вчинення означеного злочину полягає в тому, що через створення, розповсюдження або збут шкідливих програмних чи технічних засобів створюється реальна загроза порушення суспільних відносин власності на інформацію або відносин надання послуг електрозв'язку.

До *предметів* злочину належать:

– шкідливі програмні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів),

[1] З цього питання див. також: Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження). Київ : Атіка, 2007. С. 190.

автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– шкідливі технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Слайди до підрозділу 1.3.

У дальшому викладі шкідливі програмні й технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, будуть називатися скорочено – *шкідливі програмні й технічні засоби*. Отже, до предметів злочину, передбаченого ст. 361-1 КК, закон відносить програмні й технічні засоби, які: а) є шкідливими та б) призначені для несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Передбачена в законі ознака *шкідливі* характеризує ці програмні й технічні засоби як такі, використання яких заподіює шкоду інформаційним відносинам, засобом забезпечення яких є комп'ютерна техніка чи мережі електрозв'язку, або створює небезпеку її заподіяння. Ознака, «призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», указує на їх спеціальне призначення – несанкціоноване втручання в роботу комп'ютерної техніки чи мереж електрозв'язку. На відміну від будь-яких інших комп'ютерних програм та обладнання шкідливі

програмні й технічні засоби спеціально розробляють для несанкціонованого втручання, тобто порушення режиму роботи ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Тому під *шкідливими програмними засобами*, призначеними для несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, слід розуміти програми (програмні блоки, програмне забезпечення), розроблені спеціально для несанкціонованого втручання в роботу комп'ютерної техніки або мереж електрозв'язку, використання яких спричиняє або створює загрозу заподіяння шкоди інформаційним відносинам.

Додаткові та довідкові дані щодо шкідливого програмного й технічного забезпечення

Технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, – це різного роду пристрої, устаткування, розроблені для несанкціонованого втручання в роботу комп'ютерної техніки або мереж електрозв'язку, використання яких спричиняє або створює загрозу заподіяння шкоди інформаційним відносинам.

Об'єктивна сторона. Злочин, передбачений ч. 1 ст. 361-1 КК, належить до злочинів із *формальним* складом, тобто вважається закінченим з моменту вчинення одного з альтернативних діянь, зазначених у диспозиції. Аналізована норма передбачає такі форми об'єктивної сторони:

1) створення шкідливих програмних або технічних засобів для використання, розповсюдження або збуту;

2) розповсюдження шкідливих програмних або технічних засобів;

3) збут шкідливих програмних або технічних засобів.

Створення шкідливих програмних або технічних засобів являє собою результат діяльності щодо розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу. Наголосимо, що створення буде кримінально караним тільки за наявності відповідної ознаки суб'єктивної сторони – мети використання, розповсюдження або збуту.

Відеокоментар до підрозділу 1.3.

Розповсюдження шкідливих програмних засобів. Специфіка предмета цього злочину визначає особливості його розповсюдження, що полягають у такому: до розповсюдження, у цьому складі, слід відносити не тільки надання оплатного або безоплатного доступу до певних предметів невизначеному колу осіб (традиційне розуміння розповсюдження), але також їх поширення низкою принципово нових способів, зумовлених особливостями предмета. До числа таких способів належать: самовідтворення; «закладання» в програмне забезпечення; розповсюдження з використанням комп'ютерної мережі.

Розповсюдження шкідливих програм способом *самовідтворення* означає, що розробник передбачає можливість шкідливої програми створювати свої копії. Цей спосіб найчастіше застосовують для розповсюдження

«комп'ютерних вірусів». Комп'ютерний вірус – це параметр, який проникає в комп'ютерну програму та порушує функціонування комп'ютера, а також здатен самостійно копіювати комп'ютерні команди або заміняти програмні дані[1]. Найяскравішим прикладом комп'ютерного вірусу є так званий вірус Морріса. У листопаді 1988 року ним було уражено комп'ютерні системи Корнельського (Нью-Йорк), Стендфордського, Прінстонського (Нью-Джерсі), Гарвардського університетів, Центр Массачусетського технологічного інституту; заражено близько 1000 вузлів мережі Arpanet, зокрема серед постраждалих виявилася велика кількість урядових організацій, клінік і приватних компаній. Вірус переповнював пам'ять «зараженого» комп'ютера, чим унеможливлював роботу з інформацією, яка в ньому зберігалась. Збитки, завдані цим вірусом, фахівці оцінили у 98 мільйонів доларів[2].

Спосіб *«закладання» шкідливих програмних засобів* у програмне забезпечення полягає в тому, що особа, яка розповсюджує ці засоби, залучає шкідливу програму до складу використовуваного програмного забезпечення. Один з таких способів розповсюдження шкідливих програм одержав назву «троянський кінь». Суть його полягає в тому, що винний розповсюджує якесь корисне програмне забезпечення, скажімо, текстовий редактор, перекладач або навчальну програму, проте крім корисних

[1] Положение по обеспечению безопасности компьютерных информационных систем в КНР. *Борьба с преступностью за рубежом (по материалам зарубежной печати)* : ежемесячный информационный бюллетень. Москва, 1996. № 9.

[2] Компьютерные террористы: новейшие технологии на службе преступного мира / авт.-сост. Т. И. Ревяко. Минск : Литература, 1997. С. 327.

функцій, програма містить і *приховані*, призначені для порушення права власності на інформацію.

Розповсюдження через *використання комп'ютерних мереж* полягає зазвичай у наданні доступу до шкідливих програм у спосіб їх розміщення на мережевих носіях інформації або в розсиланні електронною поштою копій шкідливих програм. *Для прикладу розповсюдження шкідливих програм через надання доступу розглянемо вирок Кіровського районного суду м. Кіровоград у справі № 1-57/08 від 16 січня 2009 року*[1] *з обвинувачення А. у вчиненні злочину, передбаченого ч. 1 ст. 361-1 КК. У вироку зазначено, що А., користуючись локальною комп'ютерною мережею гуртожитків, діючи умисно, завантажив у власний комп'ютер програмні засоби. Ці засоби пізніше під час експертизи було визнано програмами для віддаленого зчитування паролів або нейтралізації засобів захисту комп'ютерних програм чи інформації, які після встановлення паролів та їх нейтралізації дають можливість доступу до певної комп'ютерної інформації, комп'ютерної програми, комп'ютерної мережі, операційної системи та здійснення непомітно для власника чи законного користувача несанкціонованої передачі інформації сторонній особі.*

Після цього А. надав вільний доступ до свого комп'ютера всім абонентам локальної мережі. Суд правильно кваліфікував дії А. за ч. 1 ст. 361-1 КК як розповсюдження шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу комп'ютерної техніки.

[1] Вирок Кіровського районного суду м. Кіровоград у справі № 1-57/08 від 16 січня 2009 року // Єдиний державний реєстр судових рішень : сайт. URL : http://www.reyestr.court.gov.ua (дата звернення : 01.12.2018).

Зазначимо, що можливими є комбінації названих специфічних способів розповсюдження шкідливих програмних засобів, наприклад, розповсюдження «троянського» програмного забезпечення за допомогою електронної пошти або самовідтворення переданих електронною поштою копій шкідливих програм.

Судова практика

З огляду на викладене можна дати таке визначення розповсюдження шкідливого програмного забезпечення: *оплатне або безоплатне надання копій шкідливих програм або доступу до них невизначеному колу осіб, а також їх «закладання» в програмне забезпечення або розповсюдження за допомогою комп'ютерних мереж чи поширення способом самовідтворення.*

Розповсюдження шкідливих технічних засобів аналогічне простому розповсюдженню матеріальних предметів. Проте й це діяння має певну специфіку. Крім простого передавання таких засобів, можливим є їх установлення в ЕОМ, системи або комп'ютерні мережі, які продаються або передаються на іншій основі, наприклад, здаються в оренду. Отже, розповсюдження шкідливих технічних засобів можна визначити в такий спосіб: *оплатне або безоплатне передавання шкідливого технічного засобу, а також його установлення в ЕОМ, системи або комп'ютерні мережі.*

Збут шкідливих програмних або технічних засобів відрізняється від розповсюдження тим, що він пов'язаний з відчуженням предмета. Зазначимо, якщо при розповсюдженні предмет залишається в особи (шкідливе

програмне забезпечення продовжує міститися на мережевому ресурсі, з якого розповсюджується, повертається шкідливий програмний засіб, що передавався для використання), то в результаті збуту він відчужується, тобто не залишається в особи, яка його збуває. Отже, під збутом шкідливих програмних або технічних засобів слід розуміти *їх оплатне або безоплатне відчуження*. Типовим прикладом збуту шкідливих програм є продаж дисків із записаними шкідливими програмами[1].

Суб'єкт цього злочину загальний; ним є фізична осудна особа, яка досягла 16-річного віку.

Суб'єктивна сторона. Оскільки злочин, передбачений ст. 361-1 КК, належить до злочинів із формальним складом, зміст його суб'єктивної сторони визначається лише психічним ставленням до діяння й полягає в усвідомленні суспільної небезпеки та протиправності створення, розповсюдження або збуту шкідливих програмних і технічних засобів та бажанні вчинення таких дій. Отже, у цій формі умисел може бути тільки прямим, а його специфіка виражається в тому, що свідомість особи обов'язково охоплює розуміння того, що створювані або розповсюджувані засоби *спеціально призначені для несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку.*

Тест до підрозділу 1.3.

[1] Вирок Рівненського міського суду Рівненської області в справі № 1-738/2007 від 25 жовтня 2007 року Єдиний державний реєстр судових рішень : сайт. URL : http://www.reyestr.court.gov.ua (дата звернення : 01.12.2018).

1.4. Кримінально-правова охорона комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК)

Об'єктом злочину виступають суспільні відносини власності на комп'ютерну інформацію з обмеженим доступом.

Предметом злочину є інформація з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства. Тобто інформація, що є предметом злочину, передбаченого ст. 361-2 КК, характеризується такими ознаками:

1) вона належить до інформації з обмеженим доступом;

2) зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

3) створена відповідно до чинного законодавства;

4) захищена відповідно до чинного законодавства.

Слайди до підрозділу 1.4.

До *інформації з обмеженим доступом* згідно зі ст. 30 Закону України «Про інформацію» належить таємна й конфіденційна інформація.

Використання терміна «інформація, яка зберігається (або оброблюється (ст. 362 КК)) в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або на носіях такої інформації» є не зовсім вдалим,

оскільки він є громіздким, а за змістом повністю відповідає більш вдалому терміну «комп'ютерна інформація», що використовувався в попередній редакції розділу XVI КК. Крім того, навряд чи можна визнати доцільним розмежування термінів «інформація, що обробляється...» (ст. 362 КК) та «інформація, що зберігається...» (ст. 361-2 КК), оскільки оброблення інформації в ЕОМ, системі чи комп'ютерній мережі обов'язково передбачає її зберігання, а зберігання передбачає оброблення. Отже, друга виділена нами ознака інформації як предмета злочину, передбаченого ст. 361-2 КК, полягає в тому, що вона є комп'ютерною, тобто подана у формі, яка дає змогу її оброблення або зберігання з використанням комп'ютерної техніки.

WikiLeaks, Джуліан Ассанж, Едвард Сноуден...

Інформація, що є предметом цього злочину, *створена відповідно до чинного законодавства*, тобто розповсюдження або збут інформації, отриманої з порушенням законодавства, не є злочином, передбаченим ст. 361-2 КК.

Згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05 липня 1997 року інформацію з обмеженим доступом мають обробляти із застосуванням *комплексної системи захисту інформації з підтвердженою відповідністю* (ч. 2 ст. 8 Закону). Отже, предметом злочину є інформація, що зберігається в такій системі. Склад злочину, передбачений цією статтею, буде мати

місце тоді, коли незаконно розповсюджується або збувається інформація, що зберігається із застосуванням комплексної системи захисту.

За конструкцією *об'єктивної сторони* злочин, передбачений ст. 361-2 КК, є формальним. Він уважається закінченим з моменту вчинення несанкціонованого збуту або несанкціонованого розповсюдження комп'ютерної інформації з обмеженим доступом.

Судова практика

Збут або розповсюдження інформації буде *несанкціонованим*, коли він вчиняється без дозволу власника цієї інформації.

Розповсюдження комп'ютерної інформації з обмеженим доступом являє собою оплатне або безоплатне надання копій цієї інформації або доступу до неї невизначеному колу осіб. Одним з прикладів цього діяння є незаконне розповсюдження персональних даних. Скажімо, 2003 року в продажу з'явилася база даних абонентів одного з лідерів російського ринку операторів стільникового зв'язку – «Мобільні ТелеСистеми» (МТС). База даних містила такі персональні дані про абонентів компанії, як прізвище, ім'я, по батькові, дата народження, паспортні дані, індивідуальний номер платника податків тощо. До того ж інформація про появу такої бази даних перед тим кілька тижнів розповсюджувалася в Інтернеті[1].

[1] Михеева М. Р. Проблема правовой защиты персональных данных. URL : http://www.crime.vl.ru/doc/stats/stat_93.html (дата звернення : 01.12.2018)

Під *збутом комп'ютерної інформації з обмеженим доступом* треба розуміти її оплатне або безоплатне відчуження.

Суб'єкт злочину – загальний.

Суб'єктивна сторона цього злочину характеризується виною у формі прямого умислу: особа усвідомлює суспільну небезпеку й протиправність збуту або розповсюдження комп'ютерної інформації з обмеженим доступом та бажає вчиняти такі дії. Особа усвідомлює, що комп'ютерна інформація, яку вона збуває або розповсюджує, є інформацією з обмеженим доступом; усвідомлює, що не має права або дозволу власника інформації на вчинення подібних дій.

Тест до підрозділу 1.4.

1.5. Незаконні дії з комп'ютерною інформацією, учинені особою, яка має право доступу до неї

У літературі досить поширеною є така класифікація суб'єктів незаконного втручання: а) особи, які перебувають у трудових відносинах з підприємством, організацією, установою, фірмою чи компанією, у якій учинено злочин (особи, які безпосередньо обслуговують ЕОМ: оператори, програмісти, інженери; персонал, який здійснює технічне обслуговування й ремонт комп'ютерної техніки); користувачі ЕОМ, які мають певну підготовку

та вільний доступ до комп'ютерної системи; адміністративно-керівний персонал (керівники, бухгалтери, економісти); б) особи, які не перебувають у трудових відносинах з підприємством, організацією, установою, фірмою чи компанією, у якій учинено злочин[1]. Як свідчить практика правоохоронних органів, досить часто комп'ютерні злочини вчиняють суб'єкти, які належать саме до першої групи, тобто за посадами або за характером обов'язків безпосередньо пов'язані з доступом до роботи з ЕОМ, системами та комп'ютерними мережами[2]. Саме це й зумовило наявність у КК ст. 362, яка передбачає відповідальність спеціального суб'єкта за незаконні дії з комп'ютерною інформацією.

Об'єктом цього злочину виступають суспільні відносини власності на комп'ютерну інформацію. **Предметом** злочину відповідно до диспозиції є інформація, яку опрацьовують в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігають на носіях такої інформації. Як уже зазначалось, термін, що вживається для характеристики предмета, є не зовсім

[1] Лысов Н. Н. Содержание и значение криминалистической характеристики компьютерных преступлений. *Проблемы криминалистики и методики ее преподавания (тезисы выступлений участников семинара-совещания преподавателей криминалистики)*. Москва, 1994. С. 54; Шилан Н. Н., Кривонос Ю. М., Бирюков Г. М. Компьютерные преступления и проблемы защиты информации : монография. Луганск : РИО ЛИВД, 1999. С. 38.

[2] Компьютерные террористы: новейшие технологии на службе преступного мира / авт.-сост. Т. И. Ревяко. Минск : Литература, 1997. С. 219; The National Information Infrastructure Protection Act of 1996 Legislative Analysis By The Computer Crime and Intellectual Property Section United States Department of Justice. URL : http://www.usdoj.gov/criminal/cybercrime/1030_anal.html (дата звернення : 01.12.2018); Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. та ін. Комп'ютерна злочинність : навчальний посібник. Київ : Атіка, 2002. С. 131.

вдалим: він громіздкий, а за змістом не відрізняється від більш вдалого – «комп'ютерна інформація». Отже, предметом зазначеного злочину є комп'ютерна інформація, ознаки якої розглянуто вище.

Слайди до підрозділу 1.5.

Об'єктивна сторона характеризується наявністю декількох форм:

1) несанкціонована зміна комп'ютерної інформації;

2) несанкціоноване знищення комп'ютерної інформації;

3) несанкціоноване блокування комп'ютерної інформації;

4) несанкціоноване перехоплення комп'ютерної інформації, що призвело до її витоку;

5) несанкціоноване копіювання комп'ютерної інформації, що призвело до її витоку.

Несанкціонована зміна комп'ютерної інформації являє собою порушення права власності на інформацію в спосіб перекручення без відома власника змісту відомостей, відображених на носії, що робить інформацію цілком або частково непридатною для задоволення інформаційної потреби особою, яка має право власності на таку інформацію.

Несанкціоноване знищення комп'ютерної інформації відбувається тоді, коли вона перестає існувати у формі, яка дає змогу її опрацювати за допомогою комп'ютерної техніки.

Несанкціоноване блокування комп'ютерної інформації – позбавлення власника можливості використовувати інформацію для задоволення інформаційної потреби за умови, що її не втрачено та не підроблено.

Якщо три перші форми являють собою прості, звичайні злочини з матеріальним складом і вважаються закінченими з моменту настання зазначених наслідків, то структура двох останніх – несанкціонованого перехоплення та копіювання – ускладнена наявністю віддаленого наслідку – витоку інформації, якому передують такі види порушення права власності на комп'ютерну інформацію, як несанкціоноване копіювання або перехоплення.

Оскільки *витік інформації* за визначенням є результатом дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, які *не мають права доступу до неї*, можна висновувати, що предметом несанкціонованого перехоплення або копіювання є тільки комп'ютерна інформація з обмеженим доступом (таємна або конфіденційна).

Копіювання комп'ютерної інформації – це «відтворення даних зі збереженням вихідної інформації»[1]. Отже, несанкціоноване копіювання можна визначити як відтворення, з перевищенням наданих власником прав доступу, комп'ютерної інформації з обмеженим доступом зі збереженням вихідної інформації. Наприклад, особа має право лише на ознайомлення та внесення змін до певної бази даних, а вона, без дозволу власника, створює її копію.

Перехоплення – це специфічний вид копіювання. Його особливість полягає в способі отримання копії. Відповідно до Конвенції про кіберзлочинність, прийнятої в рамках Ради Європи 23 листопада 2001 року (ратифікована Україною у вересні 2005 року), *несанкціонованим перехопленням* є навмисне перехоплення технічними за-

[1] Першиков В. И., Савинков В. М. Толковый словарь по информатике. Москва : Финансы и статистика, 1991. С. 170.

собами, не маючи права на це, передач комп'ютерних даних, не призначених для публічного користування, які проводяться з комп'ютерної системи, усередині її або на неї, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить у собі такі комп'ютерні дані. Отже, несанкціоноване перехоплення: 1) учиняється за допомогою специфічних технічних засобів; 2) полягає в отриманні копії інформації під час її передавання від одного комп'ютера до іншого або від периферійних приладів до комп'ютера, або способом обробки електромагнітних випромінювань під час роботи ЕОМ, автоматизованих систем або комп'ютерних мереж; 3) особа, яка вчиняє перехоплення, не має права на отримання інформації з обмеженим доступом, що є його предметом. Отже, *несанкціоноване перехоплення* – це отримання, з перевищенням наданих власником прав, копії інформації з обмеженим доступом за допомогою специфічних технічних засобів під час передавання цієї інформації від одного комп'ютера до іншого або від периферійних приладів до комп'ютера, або способом обробки електромагнітних випромінювань під час роботи ЕОМ, автоматизованих систем або комп'ютерних мереж, у яких опрацьовується така інформація.

Суб'єкт злочину, передбаченого ст. 362 КК, спеціальний – особа, яка має право доступу до комп'ютерної інформації. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації.

Суб'єктивна сторона цього злочину характеризу-

Судова практика

ється виною у вигляді прямого або непрямого умислу: особа усвідомлює суспільну небезпеку й протиправність своїх дій і бажає або свідомо допускає настання наслідків. До того ж особа має усвідомлювати, що вчиняє дії, які є перевищенням повноважень, наданих власником інформації[1].

Досить цікавий приклад злочину, що розглядається, описано у вироку Косівського районного суду Івано-Франківської області в справі № 1-56/2007 від 07 червня 2007 року[2] з обвинувачення Б. у вчиненні злочинів, передбачених статтями 364, 366 та 362 КК. Б. працював у філії енергетичної компанії на посаді бухгалтера з реалізації та був особою, яка мала доступ до програми, призначеної для комп'ютерної обробки інформації щодо розрахунків з юридичними особами.

Згідно з договором на постачання ПП «Ф.» сплатило за використану електроенергію 382671,45 грн. Б., зловживаючи службовим становищем, діючи умисно, в інтересах третіх осіб, а саме приватних підприємців Т., Р., Л., В., Д., незаконно занизив показник спожитої електроенергії ПП «Ф.» та коштів, фактично сплачених за неї, у сумі 76008,07 грн, які в програмі розрахунків з юридичними споживачами безпідставно розніс указаним приватним підприємцям, які споживали електроенергію, але не здійснювали плати за неї. Унаслідок цих умисних дій енергетичній компанії заподіяно збитки в сумі 76008,07 грн.

---

[1] Див також: Андрушко П. П. Коментар до розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку» Особливої частини Кримінального кодексу України. *Законодавство України.* 2006. № 1. С. 32–54.

[2] Вирок Косівського районного суду Івано-Франківської області в справі № 1-56/2007 від 07 червня 2007 року // Єдиний державний реєстр судових рішень : сайт. URL : http://www.reyestr.court.gov.ua/ (дата звернення : 01.12.2018).

Суд правильно кваліфікував дії Б., що виразились у зловживанні службовим становищем, тобто умисному, в інтересах третіх осіб, використанні свого службового становища всупереч інтересам служби, що заподіяло тяжкі наслідки як злочин, передбачений ч. 2 ст. 364 КК. Крім цього, правильною є й оцінка дій підсудного за ст. 366 як службового підроблення та за ст. 362 як несанкціонованої зміни комп'ютерної інформації, учиненої особою, яка має доступ до неї. Наголосимо, що в цьому випадку вчинене Б. службове підроблення обов'язково потребувало додаткової кваліфікації за ст. 362, оскільки спосіб, у який учинено службове підроблення, являє собою самостійний злочин (ст. 362), який не охоплюється диспозицією відповідної норми про злочин у сфері службової діяльності.

1.6. Порушення правил експлуатації комп'ютерної техніки чи мереж електрозв'язку, порядку чи правил захисту інформації, яка в них оброблюється

Кримінальну відповідальність за порушення правил експлуатації комп'ютерних засобів оброблення інформації та мереж електрозв'язку, а також за порушення порядку чи правил захисту інформації встановлено в ст. 363 КК «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється». **Об'єкт** злочину, передбаченого цією статтею, складають суспільні відносини, у межах яких забезпечується безпека використання ЕОМ

(комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також дотримання порядку та правил захисту комп'ютерної інформації.

Слайди до підрозділу 1.6.

Диспозиція цієї статті є бланкетною, тобто містить посилання на інші нормативно-правові акти. *Правила експлуатації* ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку являють собою вимоги, що ставлять власники ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку до їх використання або обслуговування цих технічних засобів. Вони зазвичай містяться в окремих підзаконних актах (наказах, дорученнях), що видають власники комп'ютерної техніки або мережі електрозв'язку. Наприклад, правила експлуатації засобів обчислювальної техніки в Міністерстві фінансів України регламентуються Наказом міністра фінансів України № 248 від 01 квітня 2003 року «Про затвердження Положення про роботу із засобами обчислювальної техніки та про доступ до інформаційних ресурсів Міністерства фінансів України». Цим наказом користувачам заборонено розкривати корпуси засобів обчислювальної техніки, уносити зміни до конфігурації або самостійно їх ремонтувати; під'єднання засобу обчислювальної техніки користувача до телекомунікаційної мережі, установлення, оновлення та вилучення програмного забезпечення здійснюють відповідні спеціалісти тощо.

Судова практика

Порядок захисту інформації – це визначені нормативно-правовими актами вимоги щодо створення системи захисту інформації та організації її роботи. *Правила захисту інформації* своєю чергою являють собою вимоги щодо використання системи захисту інформації певного інформаційного ресурсу. Тобто, якщо систему захисту певного інформаційного ресурсу не створено, то й неможливо порушити правила захисту цього ресурсу. Той факт, що систему захисту не створено, може бути визнано, за наявності відповідних нормативно-правових положень, порушенням порядку захисту інформації.

Склад злочину, передбаченого цією статтею, **матеріальний**, отже, його **об'єктивна сторона** характеризується такими ознаками:

1) **діяння** – порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту комп'ютерної інформації;

2) **суспільно небезпечні наслідки** – значна шкода;

3) **причинний зв'язок** між діянням і суспільно небезпечними наслідками.

Аналіз диспозиції дає змогу виснувати, що діяння може виявлятися в трьох альтернативних формах:

– порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– порушення порядку захисту комп'ютерної інформації;

Тест до підрозділів 1.5., 1.6.

– порушення правил захисту комп'ютерної інформації.

Порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – недотримання вимог, що ставить власник ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку до їх використання або обслуговування. Таке порушення може полягати, наприклад, у спробі користувача самостійно встановлювати нове програмне або апаратне забезпечення, підключенні комп'ютерної техніки до електромережі без фільтрів, порушенні порядку вмикання або вимикання засобів комп'ютерної техніки тощо.

Порушення порядку захисту комп'ютерної інформації – недотримання визначених нормативними актами вимог щодо створення системи захисту інформації та організації її роботи. Прикладом такого діяння може бути використання комп'ютерної техніки для роботи з таємною інформацією за відсутності належно сертифікованої системи захисту.

Порушення правил захисту комп'ютерної інформації – недотримання вимог щодо використання системи захисту інформації певного інформаційного ресурсу. Це може бути, до прикладу, неналежне зберігання паролів для доступу до інформації.

Оскільки аналізований склад злочину є матеріальним, він буде вважатися закінченим з моменту настання суспільно небезпечних наслідків – значної шкоди.

Суб'єкт злочину, передбаченого ст. 363 КК, спеціальний – особа, яка відповідає за експлуатацію ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації чи засобу її автоматизованого опрацювання та закріпленими на підставі цього наказу функціональними обов'язками.

Суб'єктивна сторона цього злочину характеризується тим, що діяння може бути вчинене як умисно, так і з необережності, а щодо наслідків завжди має бути необережність. Якщо настання наслідків охоплюється умислом винної особи, то склад злочину, передбачений ст. 363 КК, відсутній. У таких випадках дії винної особи, за наявності відповідних ознак, треба кваліфікувати як умисне пошкодження майна (ст. 194 КК) або як пособництво в несанкціонованому втручанні в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 5 ст. 27, ст. 361 КК), або як несанкціоновані дії з комп'ютерною інформацією, учинені особою, яка має доступ до неї (ст. 362 КК).

Методи забезпечення кібербезпеки різноманітні, а само поняття «кібербезпека» є складовою ширшого поняття «інформаційна безпека». Чим відрізняється інформаційна безпека від кібербезпеки? Інформаційна безпека гарантує, що як фізичні, так і цифрові дані є захищеними від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення, тоді як кібербезпека захищає лише цифрові дані. З огляду на особливості ст. 363 КК України в дальшому використовуватимемо поняття «кібербезпека» та «кіберзахист».

Основні вимоги щодо кібербезпеки інформаційних систем (зокрема інформаційних і керуючих систем у рі-

зних галузях промисловості), які викладено в нормативних документах, є запозиченими із загальних вимог до інформаційної безпеки, зібраних та гармонізованих у серії стандартів ISO/IEC 27000[1].

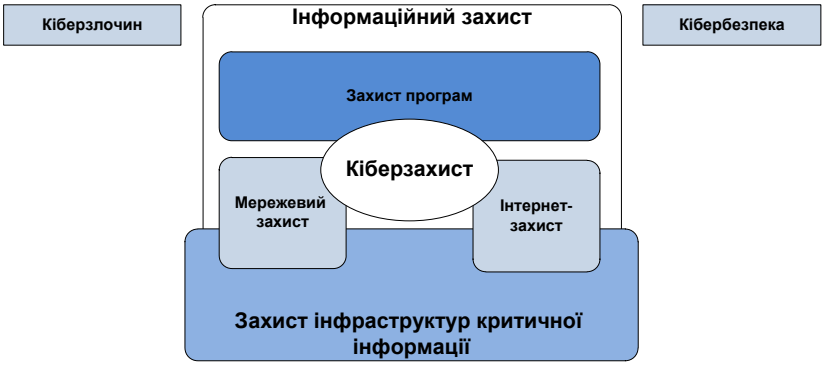

Рис. 1. Зв'язок між кіберзахистом та іншими видами захисту

Залежно від видів інформаційних активів кібербезпека може потерпати від таких основних загроз:

1. Загрози персональним активам. Зазвичай подібні загрози пов'язані з витоком або крадіжкою персональних даних, що може призвести до обмеження доступу до послуг і програм, шахрайства та крадіжки коштів. У найбільш серйозних випадках наслідки можуть коливатися

[1] ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary; ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements; ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls; ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management; ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

від індивідуальних фінансових втрат до загроз національного рівня.

2. Загрози активам підприємств та організацій. Рівень цих загроз може коливатися від труднощів у роботі сайту організації до фізичного знищення критичної інфраструктури.

Приклади:

1) кібератака на іранські підприємства зі збагачення уранового палива в 2009 р., під час якої було виведено з ладу майже 1000 збагачувальних центрифуг (приблизно 20% від загальної кількості). Для проведення атаки використовували зловмисне програмне забезпечення Stuxnet, яке є першим в історії кібератак вірусом, що фізично знищує інфраструктуру, а також першим вірусом, спеціально розробленим задля порушення роботи промислових інформаційних та керуючих систем. Stuxnet використовував уразливості Microsoft Windows для поширення за допомогою USB-flash накопичувачів та вразливості протоколів системи Simatic виробництва Siemens. Він модифікував обмін даними між контролерами та робочими станціями, що спричинило порушення умов роботи центрифуг (збільшення швидкості обертання) та їх пошкодження;

2) кібератака на більше ніж 2000 компаній електроенергетичного та паливного сектору в США та Європі в 2013 р. Для проведення атаки було застосовано зловмисне програмне забезпечення Havex, яке користується вразливістю OPC протоколу, що експлуатують у багатьох галузях промисловості. З огляду на цю вразливість Havex збирав інформацію про пристрої, що функціонують в інформаційних та керуючих системах підприємств. Фізичне пошкодження або знищення обладнання не відбувалось, проте зібрана інформація могла бути використана для підготовки до дальшої атаки;

3) кібератака на західні військові, державні, дослідницькі організації, підприємства оборонної промисловості та виробничі майданчики в 2010 р. Для проведення атаки було застосовано зловмисне програмне забезпечення Blackenergy 2, що початково розробляли для створення ботів (узяття під контроль комп'ютерів користувачів з під'єднанням до мережі Інтернет) і проведення DDoS атак. Вірус поширювався за допомогою документів Word або вкладень PowerPoint, що передавали електронною поштою. Вірус використовував уразливості в людино-машинному інтерфейсі (ЛМІ) систем виробництва Siemens, GE та Advantech для збирання інформації щодо промислових процесів й отримання графічного відображення системи керування через ЛМІ;

4) кібератака на три українські обленерго 23 грудня 2015 року. Це була перша з відомих кібератак, що порушила роботу електророзподільних мереж. При проведенні кібератаки був застосований вірус Blackenergy3, який зловмисники використали для проникнення в корпоративні мережі підприємств, а потім і в мережі керуючих SCADA систем. Вони задіяли функціонал інформаційних та керуючих систем для від'єднання підстанцій від мережі, що призвело до втрати електрозабезпечення більше ніж 225 000 користувачів на шість годин. Зазначимо, що з огляду на зловмисний ПЗ KillDisk, що видаляє операційні системи, а також знищення комутаційних пристроїв способом зміни вбудованого ПЗ процес відновлення роботи систем тривав у деяких випадках майже рік. Причина успішності атаки – необізнаність персоналу з методами соціальної інженерії та порушення базових норм побудови інформаційних мереж. Внутрішня мережа, у якій працювали комп'ютери, що керували роботою підстанцій, мала фізичне під'єднання до зовніш-

ньої мережі Інтернет. У результаті зловмисники отримали доступ до комп'ютерів, використавши проксі-сервери обленерго. Рівень організації атаки був високим, її спрямували одночасно на три обленерго; у заражених комп'ютерах працювали водночас декілька операторів. До того ж була організована DDoS атака на один з колцентрів обленерго;

5) кібератаки на державні установи, банки, медіа та інші компанії в Україні у 2017-2018 рр. Для проведення атаки був використаний вірус-шифрувальник Petya.A, який розповсюджувався способом оновлення для програми M.E.Doc та листів електронною поштою. Вірус шифрував дані на жорсткому диску, безповоротно видаляючи оригінальні файли та виконуючи примусове перезавантаження комп'ютера, після чого формував повідомлення з вимогою викупу. Атака швидко поширилася мережею, зачепивши також США та Європу.

Зауважимо, що всі вказані загрози здійснюють з певною метою: крадіжка інформації, її пошкодження, обмеження доступу для отримання вигоди та/або спричинення збитків. Загрози можуть бути реалізовані лише за наявності вразливостей. Уразливості – це слабкі сторони інформаційних активів або методів контролю, які можуть бути використані під час реалізації загрози. Наприклад, описаної вище кібератаки на обленерго в 2015 р. можна було уникнути через застосування нескладних організаційно-технічних заходів – упровадження на підприємстві політики кібербезпеки та проведення для робітників навчального курсу з правил захисту інформації.

Саме мінімізація можливих уразливостей є головною метою побудови системи інформаційної безпеки (кібербезпеки).

Одним з базових і водночас найбільш ефективних методів побудови системи інформаційної безпеки є залучення в систему менеджменту підприємства заходів згідно з вимогами міжнародного стандарту ISO/IEC 27001 або його національного еквівалента ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги» з дальшим проведенням аудиту та сертифікації системи. На сьогодні сертифікація на відповідність вимогам стандартів серії ISO/IEC 27000 в Україні не є обов'язковою, проте її впроваджують ініціативно на деяких підприємствах, зокрема таких, як ПрАТ «СНВО «Імпульс» з огляду на широке розповсюдження кіберзагроз і необхідність формування системи захисту.

Як зазначено в розділі 1.6 інтегрованого навчально-практичного посібника, якщо система захисту інформації не створена, то порушити правила захисту інформації неможливо. Отже, неможливо оцінити, чи були допущені (навмисно чи ненавмисно) вразливості в системі захисту інформації. До того ж той факт, що систему захисту не створено, може бути порушенням порядку захисту інформації.

При оцінюванні можливих порушень порядку та правил захисту інформації доцільно з'ясувати наступні питання. Загальне питання - «Чи належно впроваджено систему кібербезпеки, тобто чи не порушено порядку захисту інформації?» - конкретизується такими питаннями:

1. Чи впроваджено систему кібербезпеки або її аналог? Упровадження має бути документально підтверджено.

2. Чи визначено перелік норм і вимог, яким має відповідати впроваджена система (бажано документовано)?

Треба чітко знати, відповідно до яких норм побудовано систему.

3. Чи систему належно документовано? Усі впроваджені заходи із забезпечення кібербезпеки має бути підкріплено внутрішніми стандартами, методиками та процедурами, що затвердило керівництво, а також унесеними до системи менеджменту підприємства.

4. Чи відповідають упроваджені заходи галузевим вимогам, які можна віднести до інформаційної безпеки (за їх наявності)? Наприклад, в одному з головних галузевих нормативів атомної енергетики СОУ НАЕК 100:2016 «Інформаційні та керуючі системи, важливі для безпеки атомних станцій. Загальні технічні вимоги» уже наведено вимоги щодо захисту від несанкціонованого доступу, захисту від втручання в роботу ПЗ тощо. Ці вимоги обов'язково має бути враховано в інформаційних та керуючих системах, що функціонують на АЕС.

5. Чи було проведено аудит системи кібербезпеки підприємства (зовнішній або внутрішній)? Якщо так – його результати задокументовано? Чи було знайдено невідповідності, які не виправили за результатами аудиту?

В свою чергу, загальне питання - «Чи дотримано на підприємстві вимог впровадженої системи кібербезпеки, тобто чи не порушено правила захисту інформації?» - конкретизується такими питаннями:

1. Чи відповідають впроваджені заходи внутрішнім нормативним документам підприємства, установленим правилам і процедурам?

2. Чи проведено аналіз головних ризиків і загроз кібербезпеки (або його аналог)? Результати аналізу має бути задокументовано. Аналіз ризиків дає змогу зосередити увагу на найбільш вірогідних та/або найбільш небезпечних загрозах кібербезпеки.

3. Чи впроваджено політику інформаційної безпеки (кібербезпеки)? Чи регулярно її переглядають?

4. Чи визначено посадові функції та обов'язки осіб, які пов'язані з кібербезпекою? Обов'язки має бути чітко визначено та призначено документально.

5. Чи ознайомлено співробітників підприємства зі своїми обов'язками у сфері кібербезпеки під час та після закінчення трудових відносин? Співробітники мають бути належно інформовані та навчені. Навчання, яке сприяє мінімізації одного з основних ризиків/уразливостей кібербезпеки – отримання інформації методом соціальної інженерії, має бути задокументовано.

6. Чи проводять контроль та облік інформаційних активів підприємства (інформація, засоби її обробляння тощо)? Чи розроблено правила роботи з інформаційними активами (використання, передача тощо)? Правила має бути документовано.

7. Чи розроблено політику (стандарт, методику, інструкцію) щодо контролю носіїв інформації? Політику має бути задокументовано.

8. Чи розроблено політику контролю доступу до систем і прикладних програм (обмеження доступу, парольний доступ тощо)? Політику має бути задокументовано.

9. Чи впроваджено на підприємстві систему фізичної безпеки (периметр безпеки, контроль проходження, захист приміщень тощо)? Методи гарантування фізичної безпеки має бути задокументовано.

10. Чи обмежено доступ до критично важливих інформаційних активів, зокрема доступ за допомогою мережі? Доступ має бути обмежено або, якщо обмеження неможливе, має бути забезпечено моніторинг трафіка в мережі за допомогою надійних засобів.

11. Чи організовано резервне копіювання критично важливої інформації?

12. Чи введено обмеження на інсталяцію програмного забезпечення? Інсталяцію має проводити компетентний спеціаліст, ПЗ має входити до затвердженого переліку дозволеного до використання.

13. Чи розроблено програму реагування на інциденти кібербезпеки?

Відповіді на вказані вище запитання допоможуть зрозуміти, чи було допущено порушення правил та/або порядку захисту інформації на підприємстві. Перелік питань не є вичерпним і може бути доповнений відповідно до чинних нормативних документів і найкращих світових практик.

Більш детальну інформацію щодо рекомендованих методів кіберзахисту, а також докладний опис загроз і механізмів кібератаки наведено в ДСТУ ISO/IEC 27032:2016 «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки».

1.7. Масове розповсюдження повідомлень електрозв'язку

Слайди до підрозділу 1.7.

Об'єкт цього злочину складають суспільні відносини щодо забезпечення безвідмовного функціонування комп'ютерної техніки й мереж електрозв'язку як технічних засобів забезпечення відносин власності на інформацію.

Предметом злочину є повідомлення електрозв'язку – відомості, подані у вигляді, що дає змогу їх передавати

за допомогою комп'ютерних мереж або мереж електрозв'язку.

Оскільки склад злочину, передбачений статтею 363-1 КК, є **матеріальним**, то до ознак його об'єктивної сторони належать: 1) **діяння** – масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів; 2) **суспільно небезпечні наслідки** – порушення або припинення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 3) **причинний зв'язок** між діянням і наслідками.

Отже, діяння як ознака об'єктивної сторони цього складу злочину полягає в розповсюдженні повідомлень електрозв'язку, тобто надсиланні певним адресатам копій цих повідомлень, яке, по-перше, є масовим і, по-друге, здійснюється без попередньої згоди адресатів.

Спам може бути корисним. Досвід США

Розповсюдження слід уважати *масовим* тоді, коли одне або кілька повідомлень отримує більше ніж один адресат, адже в диспозиції аналізованої статті йдеться про множинність повідомлень електрозв'язку та їх адресатів. Зазначимо, що поняття «масове» у розгляданій нормі використовується як оцінне, тобто встановлення того, чи було певне розповсюдження повідомлень електрозв'язку масовим залежить від аналізу багатьох обставин конкретного розповсюдження (кількість повідомлень або копій повідомлень, їх розмір; кількість адреса-

тів; час, що було використано для розповсюдження; технічні характеристики обладнання, яке використовувалося для розповсюдження, тощо).

Відсутність попередньої згоди адресатів полягає в тому, що адресат ні в жодній формі (письмово, усно, через використання електронної пошти або в інший спосіб) не давав згоди на надсилання йому повідомлень, що є предметом злочину.

Порушення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку являє собою таку зміну режиму роботи комп'ютерної техніки або мережі електрозв'язку, яка створює загрозу для їх функціонування, тобто погіршення роботи повністю або частково, тимчасове створення перешкод для використання за призначенням.

Припинення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку полягає в тимчасовому або остаточному припиненні функціонування комп'ютерної техніки або мереж електрозв'язку, невиконанні ними завдань щодо зберігання, опрацювання, пересилання чи отримання комп'ютерної інформації або інформації, що передається мережами електрозв'язку.

Судова практика

Суб'єкт цього злочину загальний.

Суб'єктивна сторона характеризується виною у формі прямого умислу стосовно діяння й умисним або необережним ставленням до наслідків. Особа усвідомлює,

що вчиняє масове розповсюдження повідомлень електрозв'язку, і бажає вчиняти такі дії, а також вона бажає або свідомо допускає порушення чи припинення роботи комп'ютерної техніки чи мереж електрозв'язку або легковажно розраховує на ненастання таких наслідків.

Тест до підрозділу 1.7.

Як приклад злочину, передбаченого ст. 363-1 КК, можна навести такий випадок. *Вироком Деснянського районного суду м. Чернігів від 15 квітня 2016 року в справі № 750/2149/16-к було засуджено особу, яка розробила спосіб порушення роботи мереж електрозв'язку через надсилання великої кількості дзвінків та смс-повідомлень, без фактичного звукового й текстового змісту, на абонентські номери будь-якого рухомого (мобільного) зв'язку. Для здійснення таких посягань винна особа створила сайт, з використанням якого здійснювала атаки з великою кількістю запитів, що призводили до відмови в обслуговуванні. Надсилання великої кількості повідомлень електрозв'язку, спрямованих на визначений конкретний абонентський номер рухомого (мобільного) зв'язку будь-якого оператора, протягом нетривалого часу спричиняло порушення або призупинення роботи мереж електрозв'язку у вигляді погіршення роботи й тимчасового створення перешкод для використання за призначенням зазначеного абонентського номера рухомого (мобільного) зв'язку.*

РОЗДІЛ 2. ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Правильна правова оцінка злочину потребує не тільки зіставлення фактичних обставин його вчинення з юридичними ознаками конкретного складу злочину, але й відмежування від інших, суміжних за деякими ознаками, складів злочинів[1]. Визначення критеріїв розмежування комп'ютерних злочинів між собою та ознак, що дають змогу відмежувати ці суспільно небезпечні діяння від інших злочинних посягань, пов'язаних з використанням комп'ютерної техніки, а також детальніше проаналізувати зміст ознак досліджуваних злочинів, що сприятиме їх правильній кваліфікації.

2.1. Розмежування комп'ютерних злочинів

Склади злочинів, передбачені статтями 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем,

[1]Тарарухин С. А. Квалификация преступлений в следственной и судебной практике. Киев : Юринком, 1995. С. 80.

комп'ютерних мереж чи мереж електрозв'язку), 361-1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) та 362 (несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, учинені особою, яка має право доступу до неї) КК України характеризуються однаковим безпосереднім об'єктом. Цей об'єкт складають суспільні відносини, у межах яких реалізується право власності на комп'ютерну інформацію, а також суспільні відносини, пов'язані з наданням та отриманням послуг електрозв'язку (статті 361 та 361-1 КК). Водночас ці склади злочинів розрізняються за ознаками предмета. Предметом злочину, передбаченого ст. 361 КК, є комп'ютерна інформація та інформація, що передається мережами електрозв'язку, а злочину, передбаченого ст. 362 КК, – тільки комп'ютерна інформація. До предмета злочину, передбаченого ст. 361-1 КК, належать шкідливі програмні й технічні засоби. Різною є й конструкція об'єктивної сторони: посягання, передбачені статтями 361 та 362 КК, належать до злочинів з матеріальним складом, а передбачені ч. 1 ст. 361-1 – до злочинів із формальним складом. Розмежовувати ці склади злочинів можна й за ознаками суб'єкта: у складах злочинів, передбачених статтями 361 та 361-1 КК, він загальний, тимчасом як суб'єкт злочину, передбаченого ст. 362 КК, спеціальний – особа, яка має доступ до комп'ютерної інформації.

Проте головною ознакою, що дає змогу відмежувати злочини, передбачені статтями 361 та 362 КК, від злочину, передбаченого ст. 361-1, є, як видається, механізм заподіяння шкоди об'єктові – суспільним відносинам

права власності на комп'ютерну інформацію: якщо статті 361 та 362 КК передбачають відповідальність за певні дії, що призводять до заподіяння шкоди предмету цих відносин, чим зрештою й заподіюється шкода об'єкту, то стаття 361-1 КК передбачає відповідальність за дії, що створюють небезпеку заподіяння шкоди цим суспільним відносинам. З огляду на це зазначимо, що використання під час учинення передбаченого статтями 361 або 362 КК злочину шкідливого програмного або технічного засобу, створеного суб'єктом раніше, потребує додаткової кваліфікації за ст. 361-1 КК як створення шкідливого програмного або технічного засобу для його використання.

Слайди до підрозділу 2.1.

Злочини, передбачені ст. 361-2 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) та ч. 2 ст. 362 КК України, являють собою посягання на суспільні відносини власності на комп'ютерну інформацію з обмеженим доступом і характеризуються тим, що їх предметом може бути тільки така комп'ютерна інформація. Між собою вони розрізняються за конструкцією об'єктивної сторони: перший належить до злочинів із формальним складом, другий – з матеріальним. Різним є й зміст дій суб'єкта. Злочин, передбачений ст. 361-2 КК,

полягає в збуті або розповсюдженні комп'ютерної інформації, а ч. 2 ст. 362 КК передбачено відповідальність за перехоплення або копіювання такої інформації.

Злочин, передбачений ст. 363 КК (порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється), відрізняється від інших посягань, передбачених розділом XVI Особливої частини КК України, майже всіма ознаками складу. Безпосереднім об'єктом більшості складів «комп'ютерних» злочинів є право власності на комп'ютерну інформацію, а злочин, передбачений ст. 363 КК, завдає шкоди відносинам щодо забезпечення встановленого порядку експлуатації комп'ютерної техніки, мереж електрозв'язку, а також порядку та правил захисту інформації. Диспозиція ст. 363 КК є єдиною бланкетною диспозицією в згаданому розділі, тобто тільки в цьому складі злочину діяння полягає в порушенні правил експлуатації комп'ютерної техніки, мереж електрозв'язку або порядку чи правил захисту інформації, передбачених певними нормативно-правовими актами. Спеціальним є й суб'єкт цього злочину – особа, яка відповідає за експлуатацію комп'ютерної техніки або мережі електрозв'язку. Суб'єктивна сторона характеризується змішаною формою вини: щодо порушення правил (діяння) є можливим як умисел, так і необережність, а щодо настання істотної шкоди (наслідків) – тільки необережність. Ознаки складу злочину, передбаченого ст. 363 КК, відсутні, якщо особа умисно порушує правила експлуатації комп'ютерної техніки або порядок чи правила захисту інформації й до настання зазначених наслідків вона ставиться також свідомо. Залежно від обставин справи такі дії можна кваліфікувати як несанкціоновані

дії з комп'ютерною інформацією, учинені особою, яка має право доступу до неї (ст. 362 КК), або пособництво в несанкціонованому втручанні в роботу комп'ютерної техніки чи мереж електрозв'язку (ч. 5 ст. 27 КК, ст. 361 КК).

Специфіка складу злочину, передбаченого ст. 363-1 КК (перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку в спосіб масового розповсюдження повідомлень електрозв'язку), полягає передусім в ознаках об'єкта. Як уже зазначалось, ця норма захищає суспільні відносини щодо забезпечення безвідмовного функціонування технічних засобів інформаційної діяльності, тимчасом як більшість інших норм аналізованого розділу (усі, крім ст. 363 КК) забезпечують кримінально-правову охорону відносинам власності на комп'ютерну інформацію, тобто певному виду інформаційної діяльності. Позаяк масове розсилання повідомлень електрозв'язку призводить, скажімо, до блокування комп'ютерної інформації, а функціонування засобів автоматизованого опрацювання інформації не порушено, ознаки складу злочину, передбаченого ст. 363-1 КК, відсутні. За наявності відповідних ознак, такі дії можна кваліфікувати як несанкціоноване втручання (ст. 361 КК), адже шкоду в такій ситуації заподіяно тільки відносинам власності на комп'ютерну інформацію. Водночас, якщо особа здійснила, наприклад, масове розповсюдження комп'ютерної інформації з обмеженим доступом, що внаслідок надмірного перевантаження призвело до порушення роботи комп'ютерної мережі, то має місце ідеальна сукупність злочинів, передбачених статтями 361-2 та 363-1 КК. У цій ситуації шкода заподіюється і відносинам власності на комп'ютерну інформацію з обмеженим доступом, і відносинам щодо забезпечення безвідмовного функціонування технічних засобів інформаційної діяльності.

2.2. Особливості кримінально-правової кваліфікації посягань на власність, учинюваних з використанням комп'ютерної техніки

Слайди до підрозділу 2.2.

Останнім часом кількість повідомлень про вчинення *злочинів проти власності з використанням комп'ютерної техніки* значно збільшилась. Це є природним наслідком процесів інформатизації та комп'ютеризації. Дослідження національної судової практики дає змогу зазначити, що за особливостями кримінально-правової оцінки випадки застосування комп'ютерної техніки для здійснення злочинів проти власності може бути поділено на дві групи: 1) використання комп'ютерної техніки як засобу вчинення злочину проти власності; 2) учинення злочину у сфері використання комп'ютерної техніки (статті 361–363-1 КК) для дальшого вчинення злочину проти власності або приховування його слідів.

Посягання, які слід відносити *до першої групи*, полягають зазвичай у тому, що певну інформаційну систему злочинець використовує для незаконного заволодіння чужою власністю, до того ж ознаки комп'ютерного злочину відсутні. Винний не здійснює незаконного перекручення або знищення комп'ютерної інформації, не завдає іншої шкоди функціонуванню комп'ютерних засобів, можна сказати, використовує їх у штатному режимі. Ознаки комп'ютерного злочину в таких діях відсутні, КК містить спеціальну норму для їх кваліфікації. Частина 3

ст. 190 КК передбачає кримінальну відповідальність за шахрайство, учинене в спосіб незаконних операцій з використанням ЕОМ. Типовим прикладом використання ч. 3 ст. 190 КК для кваліфікації дій, які полягали у використанні комп'ютерної техніки для вчинення шахрайства, за відсутності ознак злочину у сфері використання інформаційних технологій, є вирок Соснівського районного суду м. Черкаси в справі № 1-569/09 від 11 грудня 2009 року[1]. *Засуджений А. для заволодіння грошовими коштами способом обману користувачів мережі Інтернет зареєструвався на інтернет-ресурсі «Aukro.ua» (цей сайт є Інтернет-аукціоном з продажу та купівлі різноманітних товарів) та пропонував до продажу телефони, камери та інші електронні товари. Усі товари виставлялися на лотах за заниженими цінами, щоб привабити якомога більше клієнтів. Покупцеві, після того як він вигравав аукціон, з «Aukro.ua» надходило про це повідомлення, а також указувалися контактний телефон, e-mail та адреса продавця. Коли покупець зв'язувався з А., то останній повідомляв, що він дійсно продає товар, який виставлено на інтернет-аукціоні «Aukro.ua», пропонував перерахувати вартість товару на один з його «web-гаманців» платіжної системи «WebMoney», а після перерахування коштів товар мав бути надісланий покупцеві. Проте після перерахування коштів покупець свого товару так і не отримував. У дальшому А. відкрив платіжну картку «Миттєва» ЧФ ВАТ КБ «ПриватБанк», на яку перераховував гроші, отримані шахрайським способом.*

Зазначимо, що на сьогодні ще одним з видів шахрайства, яке вчиняється з використанням електронно-

[1] Кримінальна справа № 1-569/09 // Архів Соснівського районного суду м. Черкаси.

обчислювальної техніки, є так званий фішинг. Він полягає в тому, що зловмисники масово надсилають електронні листи, у яких від імені якогось відомого банку, інтернет-магазину, фінансової компанії чи під іншим приводом, наприклад, виграшу в лотереї, пропонують адресатам повідомити реквізити своєї пластикової картки, а потім використовують ці реквізити для заволодіння грошима адресатів. Фішинг може полягати й у створенні підроблених сайтів (банківських установ, систем інтернет-платежів для поповнення карткових рахунків або рахунків операторів мобільного зв'язку «без комісії»), рекламі таких сайтів, надсиланні листів із запрошенням відвідати такі сайти та дальшому накопиченні даних, які необережні користувачі залишатимуть на таких ресурсах. Якщо злочинна діяльність обмежується тільки збором певних даних, подібні дії слід кваліфікувати як готування до шахрайства, передбаченого ч. 3 ст. 190.

Більш поширеними є випадки, віднесені нами до *другої групи*. Особливість кримінально-правової оцінки полягає тут у тому, що дії винної особи треба кваліфікувати не тільки як злочин проти власності, але і як «комп'ютерний» злочин. Як приклад такого випадку розглянемо вирок Корольовського районного суду м. Житомир у справі № 1-81/2007 від 05 січня 2007 року[1] з обвинувачення Ц. та Ч. *Серед злочинів, які їм інкримінувались, були посягання, передбачені ч. 2 ст. 361 та ч. 3 ст. 190 КК. Ц. за попередньою змовою із Ч. для заволодіння чужим майном через обман з використанням електронно-обчислювальної техніки та під'єднанням до мережі Інтернет, видавши себе за законного користувача, у примі-*

[1] Кримінальна справа № 1-81/2007 // Архів Корольовського районного суду м. Житомир.

щенні пункту колективного користування послугами Інтернет через підбір випадкових цифр логінів, паролів і трансферів учинили несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем та комп'ютерних мереж для доступу до програмного комплексу віддаленого обслуговування клієнтів сайту, що належав закритому акціонерному товариству комерційний банк (ЗАТ КБ) «ПриватБанк». Унаслідок несанкціонованого втручання зазнала витоку та блокування (зловмисники змінили реквізити доступу до облікового запису клієнта банку) конфіденційна інформація про користувачів автоматизованої системи та інформація про банківський рахунок клієнта банку гр-на Т.

Отримавши доступ до конфіденційного рахунку за кредитною карткою клієнта банку Т., Ц. за попередньою змовою із Ч., продовжуючи свої злочинні дії, за рахунок кредитних коштів ЗАТ КБ «ПриватБанк» учинили через мережу Інтернет шість фінансових операцій із придбання шести електронних ваучерів Закритого акціонерного товариства (ЗАТ) «Київстар GSM» на поповнення рахунку мобільного телефону на загальну суму 1525 грн. Отримавши з автоматизованої системи текстове повідомлення про авторизацію проведених операцій із зазначенням ідентифікаційного коду придбаних ваучерів, Ц. та Ч. через уведення коду ваучерів у свій мобільний телефон з абонентською скретч-карткою для мобільного зв'язку вчинили фінансову операцію та поповнили рахунок своєї скретч-картки на загальну суму 1525 грн, тобто заволоділи чужим майном через обман.

Отже, підсудні, використовуючи комп'ютерну техніку, *незаконно, без відповідного санкціонування, втрутились у діяльність комп'ютерної мережі* (серверу «Приват 24») та *отримали відповідну інформацію щодо*

кількості грошей на рахунках клієнтів банку (витік інформації), через застосування нових паролів *блокували* доступ до інформації про стан відповідних рахунків (ст. 361 КК), після чого *шахрайськими діями заволоділи чужим правом на майно*[1] *– безготівковими грошима* клієнтів ЗАТ КБ «ПриватБанк» (ст. 190 КК).

Наведений та подібні випадки вимагають критично оцінити положення п. 19 постанови Пленуму ВСУ від 06 листопада 2009 року № 10 «Про судову практику в справах про злочини проти власності». У постанові зазначено, що шахрайство, учинене в спосіб незаконних операцій з використанням електронно-обчислювальної техніки, має кваліфікуватися за ч. 3 ст. 190 КК і додаткової кваліфікації не потребує. Означене положення є справедливим тільки тоді, коли використання електронно-обчислювальної техніки не являло собою самостійного злочину у сфері використання комп'ютерної техніки (статті 361, 361-1, 362). Показовим прикладом такого випадку є наведений раніше вирок, пов'язаний із засудженням особи за шахрайські дії, учинені з використанням інформаційної системи інтернет-аукціону «Aukro.ua». Проте, коли шахрайство або інший злочин проти власності пов'язані, наприклад, з незаконним утручанням у роботу комп'ютерної техніки (ст. 361), потрібною є додаткова кваліфікація.

Водночас зауважимо, що використання комп'ютерної техніки при незаконному заволодінні майном не завжди охоплюється складом ч. 3 ст. 190 КК. Наприклад, досить відомим є спосіб незаконного заволодіння чу-

[1] Нижче аргументуємо позицію щодо предмета злочину в посяганнях, пов'язаних з несанкціонованими транзакціями в платіжних системах.

жим майном з використанням засобів автоматизованого опрацювання інформації, який отримав назву «метод салямі». Він використовується в банківських установах і полягає в такій зміні програмного забезпечення фінансового закладу, яка призводить до несанкціонованого перерахування на певний рахунок дуже невеликої кількості грошей при кожній трансакції, пов'язаній з перерахуванням великим сум та значними залишками на відповідних рахунках. Отже, на рахунку, який контролює зловмисник, через деякий час, залежно від кількості операцій на значні суми, накопичується певна сума, яка надалі незаконно привласнюється. Подібні випадки, з позицій відповідальності за злочини проти власності, неправильно кваліфікувати як шахрайство, оскільки наявними є ознаки саме таємного заволодіння чужим майном – крадіжки. Зловмисник бажає якнайдовше залишатися непоміченим, саме тому гроші «знімаються» при операціях на великі суми та з рахунків з великими залишками. У такій ситуації правильною буде кваліфікація вчиненого як крадіжки та несанкціонованого втручання, що призвело до спотворення процесу обробки інформації.

Судова практика. Шахрайство, учинене в спосіб несанкціонованого втручання в роботу автоматизованого пункту обміну електронних грошей та спотворення процесу обробки інформації

Окремої уваги заслуговує питання кваліфікації вчинюваного з використанням комп'ютерної техніки заподіяння майнової шкоди шляхом обману або зловжи-

вання довірою без ознак шахрайства (ст. 192 КК). З вересня до грудня 1999 року в Донецьку (досудове слідство провадилося прокуратурою Донецької області) головний інженер-програміст Центру інформаційних технологій і технічного забезпечення Донецької дирекції Українського державного підприємства електрозв'язку «Укртелеком» розробив комп'ютерну програму, яка давала змогу відшукувати в масиві фіксованої структури телефонні розмови, проведені із заданих номерів телефонів, відбирати їх і стирати інформацію про них у цьому масиві. Винний увійшов у змову з громадянином Пакистану, який навчався в Донецьку та залучав клієнтів. Спільно вони надавали їм за заниженими тарифами послуги міжнародного і міжміського телефонного зв'язку, а інформацію про переговори, які здійснювали клієнти, знищували за допомогою програми, розробленої інженером-програмістом. Унаслідок таких дій підприємству електрозв'язку було заподіяно збитки в розмірі близько 150 тисяч гривень. Кваліфікувати дії головного інженера, якщо б вони були вчинені після набрання чинності змін до КК України, що передбачили нову редакцію розділу XVI Особливої частини КК, потрібно було б за сукупністю злочинів, передбачених ст. 192 КК (заподіяння значної матеріальної шкоди шляхом обману без ознак шахрайства), ст. 361 КК (несанкціоноване втручання в роботу автоматизованої системи обчислення плати за надання послуг міжміського та міжнародного зв'язку, яке спричинило підроблення комп'ютерної інформації) та ст. 361-1 КК (створення з метою використання шкідливої програми, призначеної для несанкціонованого втручання в роботу автоматизованої системи).

Схожий випадок стався влітку 2002 року в Херсоні. Студент одного з вищих навчальних закладів міста вчинив несанкціоноване втручання в роботу комп'ютерної мережі місцевого провайдера інтернет-послуг і перекрутив комп'ютерну інформацію про рахунки клієнтів та сплачений час роботи в мережі Інтернет (створив фіктивний рахунок). Після цього протягом кількох місяців безкоштовно користувався Інтернетом, чим заподіяв матеріальну шкоду провайдерові в розмірі 11000 грн. За чинним КК подібні дії треба кваліфікувати як сукупність злочинів, передбачених статтями 192 і 361 КК.

Подібні випадки у світовій практиці одержали назву «крадіжка машинного часу». Такого роду злочини полягають у тому, що особа неправомірно використовує дороге комп'ютерне устаткування (наприклад суперкомп'ютери) або ресурси комп'ютерних мереж чи передплачених сервісів, абонентом яких вона не є. Найбільш поширеним видом подібних посягань у вітчизняній практиці є отримання доступу до мережі Інтернет за рахунок законних абонентів через використання їхніх логінів і паролів. Видається, що правильною кваліфікацією подібних дій є оцінка їх як сукупності злочинів, передбачених статтями 192 та 361 КК України. Проте відповідальність за злочин, передбачений ст. 192 КК України, настає лише у випадку заподіяння матеріальної шкоди, що перевищує 50 неоподатковуваних мінімумів доходів громадян. Оскільки шкода, що заподіюється внаслідок більшості крадіжок машинного часу, значно менша, подібні дії отримують правову оцінку як блокування комп'ютерної інформації законних користувачів у той час, коли за їх рахунок та під їхніми іменами порушники отримували доступ до інформації (ст. 361), а також якщо

отримання чужих логінів і паролів здійснювалося в спосіб несанкціонованого втручання або особою, яка має доступ до комп'ютерної інформації, відповідно як несанкціоноване втручання, що призвело до витоку комп'ютерної інформації (ст. 361), або як злочин, передбачений ст. 362 КК. У вироку Голованівського районного суду Кіровоградської області в справі № 1-156/08 від 16 вересня 2008 року щодо обвинувачення Р. у вчиненні злочину, передбаченого ч.1 ст. 361 КК України, зазначається таке. *Р., перебуваючи в Голованівському відділенні Гайворонської МДПІ в кабінеті своєї дружини Р-вої при здійсненні нею процедури під'єднання до мережі Інтернет, діючи умисно, незаконно дізнався про інформацію з обмеженим доступом – логін та пароль доступу до мережі Інтернет указаного відділення Гайворонської МДПІ. Після цього протягом п'яти місяців, діючи умисно, незаконно використовуючи логін та пароль доступу до мережі Інтернет Голованівського відділення Гайворонської МДПІ з власного комп'ютера неодноразово здійснював несанкціоноване втручання в роботу комп'ютерної мережі Інтернет, що призвело до блокування інформації Голованівського відділення Гайворонської МДПІ щодо звітності платників податків.*

У висновку експерта зазначалось, що логін і пароль користувача жорстко пов'язані між собою, тобто з допомогою вищевказаного логіна користувач не може підключитися до Інтернету з використанням будь-яких інших паролів. Одночасна робота двох користувачів з однаковими логінами та паролями неможлива. Отже, при виході до Інтернету будь-якої сторонньої особи доступ власникові логіну блокується.

Коментуючи цей вирок, зазначимо також, що Р. здійснив більше 15 підключень з використанням указаних

логіна та пароля, однак суд дав їм правильну оцінку як одиничному продовжуваному злочину, оскільки всі ці факти несанкціонованого втручання охоплювалися єдиним умислом, тож не утворювали повторності злочинів.

Отже, особливістю кримінально-правової кваліфікації злочинів проти власності, які вчиняють з використанням комп'ютерної техніки, слід визнати потребу розв'язання питання про доцільність додаткової кваліфікації дій винної особи за статтями, що передбачають відповідальність за злочини у сфері використання комп'ютерної техніки. Розв'язуючи його, варто керуватися тим, що використання комп'ютерної техніки при вчиненні злочинів проти власності утворює самостійний склад злочину лише тоді, коли заподіяно певну шкоду відповідному об'єкту – відносинам власності на комп'ютерну інформацію, коли певна інформація була незаконно знищена, блокова, модифікована тощо. А в тих випадках, коли певні інформаційні системи використовуються за призначенням (наведений приклад з Інтернет-аукціоном), додаткова кваліфікація не потрібна.

2.3. Кримінально-правова кваліфікація злочинів проти власності, що вчиняються з використанням платіжних карток або їх реквізитів

Посягання на власність, учинені з використанням платіжних карток або їх реквізитів зазвичай представляють собою шахрайство, скоєне в спосіб незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК). Названі посягання становлять

собою ініціювання платежів, що несанкціоновані законними держателями[1] карток, і набувають вигляду оплати товарів і послуг за допомогою платіжних терміналів[2], спеціалізованих інтернет-сайтів або отримання готівкових грошових коштів з банківських автоматів[3]. Зазвичай такі злочинні посягання поділяють на три групи: 1) ті, що вчиняють з використанням справжніх платіжних карток; 2) ті, що вчиняють з використанням підроблених платіжних карток; 3) ті, що вчиняють з використанням реквізитів платіжних карт (без безпосереднього використання самих платіжних карток).

[1] Платіжна картка є власністю емітента й надається ним клієнтові відповідно до умов договору. Тому в аспекті обраної теми автори мовлять не про власників платіжних карток (хоча останні емітенти можуть передавати клієнтам у власність), а про законних і фактичних держателів цих карток. До того ж ст. 1 Закону України «Про платіжні системи та переказ грошей в Україні» від 05 квітня 2001 року містить визначення держателя електронного платіжного засобу – це фізична особа, яка на законних підставах використовує електронний платіжний засіб для ініціювання переказу коштів з відповідного рахунку в банку або здійснює інші операції із застосуванням зазначеного електронного платіжного засобу.

[2] Платіжний термінал – це електронний пристрій, призначений для ініціювання переказу з рахунка, зокрема видачі готівки, отримання довідкової інформації й друкування документа за операцією із застосуванням електронного платіжного засобу.

[3] Банківський автомат самообслуговування (банкомат) – це програмно-технічний комплекс, що надає можливість держателеві спеціального платіжного засобу здійснити самообслуговування за операціями з одержання грошових коштів у готівковій формі, унесення їх для зарахування на відповідні рахунки, одержання інформації щодо стану рахунків, а також виконати інші операції згідно з функціональними можливостями цього комплексу.

До першої групи злочинів належать посягання, для скоєння яких використовуються *викрадені або загублені платіжні картки*, а також злочини, учинювані через недобросовісне використання карток, добровільно переданих їх законними держателями (так зване дружнє шахрайство). Верховний Суд України зазначав, що за своїм юридичним значенням (правовим режимом) та функціональним призначенням платіжні картки як платіжні інструменти – засоби доступу до банківських рахунків – відповідають визначенню поняття «офіційний документ» і є різновидом офіційних документів, а тому за відповідних умов можуть бути предметом злочинів, склади яких передбачено частинами 1, 2 ст. 357 КК України[1]. Отже, якщо зловмисник викрав платіжну карту, здійснивши за її допомогою несанкціоновану транзакцію, його дії слід кваліфікувати за сукупністю злочинів, передбачених статтями 190 та 357 КК.

Відеокоментар до підрозділу 2.3.

Посягання, пов'язані з *використанням підроблених платіжних карток*, означають отримання готівки або оплату товарів чи послуг через ініціювання платежів з карткових рахунків (картрахунків) тих клієнтів банків, платіжні картки яких підробляються[2]. У таких випадках

[1] Постанова Верховного Суду України від 20 червня 2011 року. *Вісник Верховного Суду України.* 2011. № 10 (134). С. 38–41.

[2] Способи підроблення платіжних інструментів детально описано в криміналістичній літературі (див. наприклад: Криміналістична профілактика економічних злочинів : науково-практ. посібник

дії винних осіб потребують додаткової кваліфікації за ст. 200 КК України.

Слайди до підрозділу 2.3.

Злочини, учинювані з *використанням реквізитів платіжних карток*, найчастіше здійснюються в спосіб оплати товарів і послуг в інтернет-магазинах за чужий рахунок. У таких випадках зловмисник ініціює платіж у споіб уведення реквізитів чужої платіжної картки (номер, прізвище та ім'я законного держателя картки, дата закінчення строку її дії тощо) на сайті спеціалізованої платіжної системи або інтернет-магазину. У деяких випадках отримання реквізитів може містити ознаки самостійного складу злочину, передбаченого статтями 361, 361-1, 362 (використання «скімерів», «злам» банківських мереж, інсайдерський виток даних).

Об'єктом шахрайства з використанням платіжних карток або їх реквізитів є суспільні відносини щодо реалізації держателем платіжної картки права власності обумовленого відповідними угодами банківського обслуговування. Предметом є право власності на майно – безготівкові гроші, що фактично представляють собою зобов'язання банка-емітента платіжної картки, відомості про які обліковано на картковому рахунку держателя картки.

/ за ред. д-ра юрид. наук, проф. В. А. Журавля. Харків : Харків юридичний, 2006. С. 110–113; Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування. Київ : Хай-Тек Прес, 2010. С. 337 – 339.).

Особливості об'єктивної сторони цього виду шахрайства полягають у такому. По-перше, надсилаючи несанкціонований законним держателем картки запит на здійснення платежу й використовуючи наявну платіжну систему та установлені в ній правила автоматизованої обробки запитів законних держателів карток, зловмисник обманює банківську установу (банк-емітент) щодо потреби виконання останнім зобов'язань, обумовлених договором, укладеним між банком і законним держателем картки. По-друге, унаслідок цього введення в оману банк-емітент здійснює необґрунтоване списання безготівкових коштів з рахунку законного держателя картки, що призводить до заподіяння останньому збитків у вигляді зменшення кількості безготівкових грошових коштів, урахованих на картрахунку. По-третє, діяння винного у вигляді ініціювання переказу безготівкових грошових коштів і вказані суспільно небезпечні наслідки перебувають у причинному зв'язку.

Судова практика. CashTrapping

Не всі посягання у сфері використання платіжних систем, банкоматів слід кваліфікувати за ч. 3 ст. 190 КК. Наприклад, досить поширеним є заволодіння готівкою, що міститься в банкоматі, за допомогою спеціального пристрою («вилки») або клейкої стрічки. У класифікації фахівців з банківської безпеки випадки отримання грошей, що зберігаються в банкоматах, без ініціаціації несанкціонованого платежу називаються *CashTrapping* (від англ. cash – готівка, trap – пастка, trapping – захоплення). Клю-

човою ознакою таких посягань у контексті кримінально-правової кваліфікації є те, що *несанкціонованої ініціації платежу не відбувається.* Ознаки шахрайства відсутні, а має місце таємне заволодіння чужим майном – крадіжка. Водночас CashTrapping обґрунтовано додатково кваліфікується як несанкціоноване втручання в роботу автоматизованої системи. У процесі роботи банкомат зі встановленим трепінговим пристроєм повертає код помилки в роботі – має місце «несанкціоноване втручання в роботу АС, що призвело до спотворення процесу обробки інформації» (ст. 361 КК).

Зазначимо, що ч. 3 ст. 190 КК викликає багато зауважень у науковців і практиків. Передусім вони стосуються того, що шахрайство являє злочин, пов'язаний з обманом, тобто повідомленням неправдивих відомостей людині, або зловживанням довірою людини, а отже, «не можна обманути комп'ютер або зловжити його довірою»[1]. Проте при вчиненні такого шахрайства обманюється аж ніяк не комп'ютер, а людина, яка використовує комп'ютер для інтенсифікації діяльності, скажімо, щодо банківських розрахунків. Можна сказати, що має місце опосередкований обман, тобто певні неправдиві відомості повідомляються не безпосередньо людині, а опосередковано, через комп'ютер. Заслуговує на увагу аргументація С. А. Петрова, який критикує положення щодо неможливості застосування норм про відповідальність за шахрайство у випадках, коли воно поєднане з викори-

[1] Музика А. А., Азаров Д. С. Законодавство про кримінальну відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення. Київ : Вид. Паливода А. В., 2005. С. 56-57; Титкова О. И. Уголовно-правовая характеристика мошенничества (по материалам судебной практики Республики Карелия) : дис. … канд. юрид. наук : 12.00.08. Москва, 2004. С. 86.

станням комп'ютерної техніки, уведенням недостовірної інформації або її зміною. «Змінюючи комп'ютерну інформацію, винна особа змінює дійсність, що існує, але особа, яка створила або експлуатує комп'ютерну програму, про це не знає, у результаті чого дійсність не відповідає уявленням цієї особи про неї … можна говорити про обман»[1]. Тому вказана норма «має право на існування», а з огляду на те, що використання комп'ютерної техніки значно підвищує ступінь суспільної небезпеки шахрайства, її використання є доцільним.

2.4. Безготівкові гроші, електронні гроші, криптовалюта

Слайди до підрозділу 2.4

Категорією *«безготівкові гроші»* найчастіше послуговуються в контексті розглянутих перед тим злочинів проти власності, що вчиняються з використанням платіжних карток або їх реквізитів. Фактично вони являють собою зобов'язання банка-емітента платіжної картки, відомості про які обліковано на картковому рахунку держателя картки. У контексті розділу Особливої частини КК «Зло-

[1] Петров С. А. Особенности квалификации хищений, совершенных с использованием компьютерной техники. *Российский следователь.* 2008. № 15. С. 22–24.

чини проти власності» щодо безготівкових грошей найбільш обґрунтовано використовувати термін «право на майно».

Електронні гроші – це «одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі»[1]. Вони з'явилися як реакція ринку банківських послуг на проблеми безпеки використання платіжних карток і як потреба в новому, більш гнучкому, зручному й захищеному платіжному інструменті для оплати товарів та послуг через Інтернет[2]. Цим зумовлюються особливості електронних грошей, які відрізняють їх від безготівкових: електронні гроші не є універсальними, їх приймають лише користувачі відповідних платіжних систем; емісію грошей здійснює тільки НБ, а емісію електронних грошей – банківські установи; унаслідок переказу електронних грошей їхній одержувач набуває право грошової вимоги до того ж суб'єкта, що й платник; електронні гроші існують у межах однієї платіжної системи й не можуть бути переведені в інші платіжні системи в незмінному вигляді[3]. З

[1] Положення про електронні гроші в Україні : постанова Правління Національного банку України від 04.11.2010 № 481. URL : http://zakon.rada.gov.ua/laws/show/z1336-10#n19 (дата звернення : 01.12.2018)

[2] Фінансова грамотність : навч. посібник / за ред. д-ра екон. наук, проф. Т. С. Смовженко. Вид. 2-ге, випр. і доп. Київ, 2013. С. 74.

[3] Більш докладно див.:Шимон С. Електронні гроші: форма грошей чи майнові права вимоги? *Юридична Україна*. 2015. № 9. С. 36–41; Куцевич М., Берзін П. Неправомірний випуск й використання електронних грошей, що вчиняються у системах інтернет-розрахунків (проблеми кримінально-правової кваліфікації). *Вісник Київського*

огляду на означені особливості електронних грошей питання кваліфікації незаконних дій щодо заволодіння ними мають розв'язувати аналогічно з попередньо описаним підходом щодо безготівкових грошей. Зазначимо й те, що КК передбачає відповідальність за підробку документів на переказ чи інших засобів доступу до електронних грошей, а також неправомірний випуск або використання електронних грошей (ст. 200)[1].

Криптовалюта. Криптовалюта, а також усе, що з нею відбувається, стало топовою темою світового суспільно-політичного та медійного дискурсів. Кількість учасників суспільних процесів, безпосередньо пов'язаних з її функціонуванням, постійно збільшується; пропорційним є й зростання задіяного в цій сфері обсягу фінансів. Отже, виникає потреба в правовому регулюванні.

Перспективною для усвідомлення юридичного змісту криптовалюти вбачається систематизація її ознак, які є значущими для правового регулювання. Видається, що найбільш вдалою систематизацією ознак криптовалюти буде традиційна для кримінально-правового регулювання система ознак предмета злочину: фізична, економічна, юридична.

Фізична ознака дає відповідь на запитання: що являє собою криптовалюта з технічного боку? Найбільш вдале визначення технічної сутності криптовалюти запропоновано в одній з перших робіт про криптовалюту, опублікованій під псевдонімом Сатоші Накамото: «We define an electronic coinas a chain of digital signatures. Each owner

національного університету імені Тараса Шевченка. Серія «Юридичні науки». 2013. Вип. 4. С. 13–16.

[1] Коментар до ст. 200, підготовлений О. О. Дудоровим та М. В. Карчевським (Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Хавронюка. Київ : Дакор, 2017. С. 266–279.

transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin»[1]. Електронна монета визначається як послідовність цифрових підписів, що формується під час транзакцій, коли кожний власник передає монету наступному, додаючи до неї свій цифровий підпис, хеш попередньої транзакції та публічний ключ нового власника.

Для цілей правового регулювання досить описати принципову схему роботи системи. Щоб мати можливість здійснювати операції з крипто валютою, особа зазвичай безкоштовно реєструється у відповідній мережі та отримує так званий «електронний гаманець»; у системі Біткоїн його називають також біткоїн-адреса. Для реєстрації в системі не використовують персональні дані, а транзакції здійснюють між деперсоніфікованими «електронними гаманцями». Одна особа може реєструвати невизначену кількість гаманців.

На підставі роботи алгоритму системи «гаманець» отримує позначення з букв і символів, яке криптографічно пов'язане з публічним ключем[2], є ідентифікатором «гаманця» у мережі. Публічний ключ – це відкрита інформація, використовуючи яку інші учасники системи можуть здійснити транзакцію до цього «гаманця», а також переглянути його стан і транзакції, здійснені на нього або з нього. Крім публічного ключа, система генерує цифровий підпис особи, яка реєструє «гаманець»; його ще

[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin project.* URL : https://bitcoin.org/bitcoin.pdf (дата звернення: 16.09.2018).

[2]Наприклад, Bitcoin адреса технічно представляє собою 160-бітний хеш від публічного ключа ECDSA ключової пари (Адрес Bitcoin. Часть I, теория. *Bits.media.* URL : https://bits.media/bitcoin-address-theory/ (дата звернення 19.09.2018)).

називають приватний ключ. Це теж послідовність знаків і цифр, але, на відміну від публічного ключа, доступ до цієї інформації обмежений. Маючи публічний та приватний ключі певного «гаманця», можна здійснити з нього транзакцію криптовалюти.

Хешем називають послідовність цифр, отриману в результаті криптографічного алгоритму. Алгоритм – це хеш-функція. Використовуючи її будь-який текст, набір букв і цифр можна перетворити на послідовність цифр заданої довжини. Зворотний процес перетворення неможливий, але зміна вхідного повідомлення навіть на один символ і повторне використання для нього хеш-функції приведе до обчислення такого хешу, який принципово відрізнятиметься від хешу оригінального повідомлення.

Транзакції можуть мати один або кілька входів та один або кілька виходів. Зазвичай сума виходів є меншою за суму входів, а різниця являє собою комісію (про це згодом). Наприклад, якщо є вхідна транзакція на один біткоїн і треба перевести на певну адресу 0,6 біткоїна, то створюється транзакція з одним входом та двома виходами: 0,6 – переказ, 0,35 – повернення на адресу відправника (для «решти» можна створювати новий «гаманець»), а 0,05 – комісія[1]. У результаті транзакції в системі криптовалюти створюється оригінальний набір даних, що складається з кількості входів, їх хешів, кількості та суми виходів (публічні ключі адресатів), часової мітки, приватного ключа гаманця, з якого проводиться транзакція, та службової інформації.

[1]Докладніше див.: Базанов С. Биткоин за 5 минут: Блок. BitcoinReview. URL : https://medium.com/bitcoin-биткоин-за-5-минут-блок-321984df178c (дата звернення 19.09.2018).

Накопичення даних про транзакцію здійснюється описаним нижче способом. Відомості про транзакції учасників системи об'єднують у певні групи, які називають блоками. Коли блок заповнюється, його хеш обчислюється на основі хешу попереднього блоку та всіх хешів транзакцій цього блоку. У такому вигляді блок закривається, а дані про дальші транзакції накопичуватимуться в наступному блоці. Аргументом обчислення хешу наступного блоку стане хеш цього закритого блоку. Таку технологію зберігання даних називають Blockchain.

Стабільність, захист даних і залучення достатньої для функціонування кількості обчислювальних ресурсів забезпечується організацією криптовалютних систем за принципом пірингової мережі (p2p, peartopear – рівний рівному). Блоки зберігають усі учасники системи, що долучилися до неї як «майнери»; єдиний центр координації мережі відсутній; у вільному доступі представлено інформацію щодо всіх здійснених транзакцій. Програмне забезпечення для функціонування системи криптовалюти є програмою з відкритим кодом, тобто всі зацікавлені мають можливість ознайомитися з алгоритмом роботи системи.

Через потребу здійснення великої кількості обчислень для забезпечення функціонування системи необхідним є постійне залучення обчислювальних потужностей. Тому алгоритм функціонування криптовалюти передбачає винагороду для тих, хто такі потужності надає. Таких осіб називають «майнери». Коли накопичується певна кількість транзакцій для створення чергового блоку, алгоритм системи генерує транзакцію в сумі винагороди за блок (станом на вересень 2018 року в системі Біткоїн це 12, 5 одиниць) і всіх комісій транзакцій блоку. Після цього пропонує всім «майнерам» підібрати такий додаток до змісту блоку (у системі Біткоїн його

називають nonce і це певне число), який дасть змогу отримати хеш блоку із заданою кількістю нулів на початку. Обчислити цей додаток неможливо, завдання ж розв'язується способом перебору можливих варіантів. Складність завдання перебору визначається системою залежно від кількості «майнерів» та швидкості реєстрації в мережі нових транзакцій. Коли один з учасників установив потрібний додаток, він закриває блок, а всі інші «майнери» після перевірки додають цей блок до своїх копій блоків і наступний уже рахуватимуть на підставі створеного.

Такий метод накопичення робить захист інформації щодо транзакцій дуже надійним. Як зазначено в згаданій роботі Сатоші Накамото, для того, щоб додати до системи недостовірні дані, треба змінити вміст блоків у більше ніж половини «майнерів». Зміна інформації одним «майнером» приведе до того, що інші учасники отримають сигнал системи про невідповідність хешів, а об'єктивна інформація буде встановлена автоматично. Навіть якщо комусь удасться отримати контроль над більшою частиною майнерів, такій особі (групі осіб) економічно вигідно буде не змінювати якийсь окремий платіж, а отримувати хоча б половину «легальних» винагород, що система надає «майнерам».

Як результат роботи такої системи маємо ситуацію, коли на кожний конкретний відрізок часу система містить захищену, відкриту для ознайомлення інформацію щодо стану кожного «електронного гаманця», більше того, кожен «гаманець» буде містити оригінальний вміст, оскільки він буде результатом поступового додавання інформації про всі транзакції, що передували цьому часовому моменту. Отже, фізична ознака криптовалюти полягає в тому, що технічно криптовалюта являє собою інформацію про стан певного «електронного

гаманця» цієї системи криптовалюти, яка згенерована за допомогою криптографічних методів на підставі всіх попередніх транзакцій, відповідає фактично здійсненим транзакціям та зберігається в достатньої кількості учасників системи.

Економічну ознаку криптовалюти визначає ціна, яку за неї можуть заплатити зацікавлені особи. Ключова позиція тут полягає в тому, що вартість криптовалюти нічим не забезпечена й визначається ситуативно на підставі попиту та пропозиції; єдиний орган, що встановлює курс до національних валют, відсутній. Проте властивості криптовалюти (захищеність, конфіденційність, децентралізація, майже миттєвий переказ у будь-яку частину світу) забезпечують стабільний попит на неї. Приклади визначення ціни на криптовалюту можна побачити на таких майданчиках, як Bitfinex, Bitstamp, Coinbase. Типовий підхід до визначення ціни криптовалюти полягає в тому, що вона дорівнює ціні останньої за часом біржової операції. Також ціна криптовалюти може обчислюватися як середнє арифметичне операцій, проведених за певний період на одному або кількох майданчиках (наприклад, Bitcoin Liquid Index[1]).

Означена специфіка соціальної ознаки криптовалюти викликає значний комплекс процесуальних запитань. Наприклад, особа вимагає певну суму в Bitcoin. Як установити ознаки предмета злочину? Чи можна розглядати відомості інтернет-джерел щодо курсу Bitcoin як достатній доказ для встановлення економічної ознаки відповідного предмета злочину? На сьогодні чіткої відповіді на поставлені запитання немає. Хоча видається, що це не стане великою проблемою й перші прецеденти розв'язання питання визначення ціни криптовалюти в

[1]Представлений на сайті: https://bravenewcoin.com

межах конкретного провадження отримаємо найближчим часом.

Юридична ознака криптовалюти може бути встановлена на підставі послідовного аналізу передбачених чинним законодавством видів об'єктів цивільних прав. Очевидно, що криптовалюта не може належати до речей. Вона не є грошима та не є електронними грошима. Ще раз зазначимо, що відповідно до Закону України «Про платіжні системи та переказ коштів в Україні» електронні гроші являють собою «одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі». Натомість, як зазначалося раніше, криптовалюта не є грошовим зобов'язанням, її вартість нічим не забезпечена та визначається ситуативно на підставі попиту й пропозиції.

З названих причин криптовалюта не може належати й до майнових прав. Наведений опис фізичної ознаки дає змогу стверджувати, що криптовалюта не належить до результатів інтелектуальної або творчої діяльності.

Криптовалюта є інформацією, даними, які відображені в електронному вигляді[1]. Відповідно до ст. 177 Цивільного кодексу України інформація є об'єктом цивільних прав. Стаття 5 Закону України «Про інформацію» визначає зміст відносин щодо реалізації права на інформацію: «Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Реалізація права на інформацію не повинна порушувати гро-

[1] Відповідно до визначення, що наводиться в законі України «Про інформацію» та Цивільному кодексі України

мадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи й законні інтереси інших громадян, права та інтереси юридичних осіб».

Отже, криптовалюта – це дані в електронному вигляді, що мають ціну та є предметом реалізації права на інформацію.

Проведений аналіз дає можливість відповісти на питання щодо кримінально-правової кваліфікації посягань, пов'язаних з криптовалютою. Зокрема, її вимагання правильно буде кваліфікувати за ст. 189 КК як вимога учинення дій майнового характеру, заволодіння криптовалютою може містити ознаки складу злочину, передбаченого ст. 192 КК. Водночас, якщо особа, скажімо, здійснила «злам» електронної поштової скриньки, знайшла дані щодо реєстрації «електронного гаманця» та, використовуючи їх, ініціювала транзакцію в системі криптовалюти, учинене треба кваліфікувати як несанкціоноване втручання в роботу комп'ютерної мережі, що призвело до підробки інформації (ст. 361 КК). Є підстави розглядати криптовалюту і в контексті таких посягань, як ухилення від сплати податків, незаконне збагачення, неправомірна вигода тощо.

2.5. Відмежування злочинів у сфері використання комп'ютерної техніки від посягань, пов'язаних з інформацією з обмеженим доступом

Відмежування злочинів, передбачених статтями 361 та 362 КК, *від несанкціонованого втручання в роботу Державного реєстру виборців (ст. 158 КК) та незаконного втручання в роботу автоматизованої системи до-*

кументообігу суду (ст. 376-1 КК) слід проводити за правилами розв'язання конкуренції загальних і спеціальних норм. Ст. 376-1 та ст. 158 КК являють собою види спеціальних заборон; загальними для них виступають статті 361 та 362 КК. Тому в разі втручання в роботу названих спеціалізованих автоматизованих систем відповідальність настає тільки за статтею 158 або 376-1 КК.

На окрему увагу заслуговує питання відмежування комп'ютерних злочинів *від злочинів, що полягають у збиранні інформації з обмеженим доступом* (статті 111, 114, 231 та 330 КК України). Ці злочини, якщо їх предметом є відомості, що складають певну таємницю та являють собою комп'ютерну інформацію, збігаються за ознаками об'єктивної сторони з несанкціонованим утручанням, що призвело до витоку інформації (ст. 361), або з несанкціонованим перехопленням чи копіюванням, якщо воно призвело до витоку інформації (ч. 2 ст. 362). Обов'язковою ознакою суб'єктивної сторони зазначених некомп'ютерних злочинів є мета – використання інформації, що є предметом посягання. Тому дії особи, яка використовує, наприклад, інформаційну систему Міністерства оборони України для отримання таємних даних для їх дальшого передавання іноземній державі, слід кваліфікувати тільки за ст. 111 або 114 КК. У разі відсутності такої мети вчинене, за наявності відповідних ознак, треба кваліфікувати як злочин, передбачений статтями 361 або 362 КК України. Зазначимо, що в практиці зарубіжних правоохоронних органів траплялися випадки посягання на закриту комп'ютерну інформацію без мети її використання. Скажімо, у лютому 1998 року громадянин Ізраїлю Ехуд Тенебаум здійснив незаконне втручання в роботу комп'ютерів Міністерства оборони США, де зберігалася закрита інформація. У процесі розслідування було встановлено, що мотив і мета зловмисника не дають змогу кваліфікувати

його дії як шпигунство[1]. Якби ці події відбувалися на території України, то дії ізраїльського громадянина треба було б кваліфікувати як несанкціоноване втручання в роботу електронно-обчислювальних машин, яке призвело до витоку комп'ютерної інформації (ст. 361 КК). Підкреслимо, що можлива й інша ситуація: особа з використанням комп'ютерної техніки вчиняє злочин, передбачений однією з розгляданих статей (111, 114, 231, 330), але крім цього, заподіює певну шкоду відносинам власності на комп'ютерну інформацію, яка перебуває за межами складів названих посягань (наприклад, блокування інформації в спосіб зміни паролів, знищення інформації для приховання слідів тощо). У таких випадках дії винної особи додатково кваліфікуються за статтями 361 або 362 КК.

Досить важливою проблемою є й відмежування злочинів, пов'язаних з розголошенням або передаванням відомостей з обмеженим доступом (статті 111, 114, 132, 145, 168, 182, 232, 328, 330, 381, 387, 422 КК), від несанкціонованого збуту або розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК). У цих випадках потрібно також дотримуватися правил розв'язання конкуренції цілого та частини. Конкретизація відповідних складів тут головно залежить від ознак, що характеризують суб'єкта або особу, якій передаються відомості.

Відмежування злочинів, передбачених статтями 111, 114 та 330 КК (якщо відомості, що складають їх предмет, являють собою комп'ютерну інформацію), від не-

[1] Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers (March 18, 1998) [Electronic resource] // Computer Crime & Intellectual Property Section of United States Department of Justice : site. URL : http://usdoj.gov/criminal/cybercrime/ehudpr.html (дата звернення : 01.12.2018).

санкціонованого збуту або розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК) треба проводити на підставі аналізу ознак, що характеризують особу, якій передається комп'ютерна інформація. Наприклад, якщо комп'ютерна інформація, що становить державну таємницю, передається представникові іноземної організації, наявним є склад злочину, передбачений ст. 111 або ст. 114 КК. Однак, коли така інформація передається іншій особі, дії (за відсутності ознак складу злочину, передбаченого ст. 328 КК) потрібно кваліфікувати за ст. 361-2 КК.

Злочини, передбачені статтями 132, 145, 232, 328, 330, 381, 387 та 422 КК (якщо їх предметом є відповідна комп'ютерна інформація), треба відмежовувати від несанкціонованого збуту або розповсюдження комп'ютерної інформації (ст. 361-2 КК) за ознаками суб'єкта. Усі перелічені некомп'ютерні злочини характеризуються наявністю спеціального суб'єкта, тому розповсюдження або збут комп'ютерної інформації, що є предметом цих злочинів, загальним суб'єктом треба кваліфікувати за ст. 361-2 КК. Крім того, обов'язковою ознакою об'єктивної сторони незаконного розголошення лікарської таємниці (ст. 145 КК) є настання тяжких наслідків, а обов'язковою ознакою об'єктивної сторони розголошення комерційної або банківської таємниці (ст. 232) – настання істотної шкоди, тому розповсюдження комп'ютерної інформації, яка містить лікар-

Слайди до підрозділу 2.5.

ську, банківську або комерційну таємницю, що не привело до названих наслідків, слід кваліфікувати за ст. 361-2 КК.

Відмежування складу злочину, передбаченого ст. 361-2 КК, від розголошення таємниці усиновлення (удочеріння) (ст. 168 КК) та поширення конфіденційної інформації про особу (ст. 182 КК) здійснюється передусім на підставі ознак об'єкта та суб'єктивної сторони. Несанкціоновані розповсюдження або збут комп'ютерної інформації належать до злочинів проти власності на неї, тоді як розголошення таємниці усиновлення та поширення конфіденційної інформації про особу належать до злочинів проти відповідних конституційних прав людини й громадянина. Отже, якщо особа усвідомлює, що вона, до прикладу, розповсюджує конфіденційну інформацію про конкретну особу або конкретну, персонально визначену групу осіб без їх згоди, має місце злочин проти конституційних прав та свобод – порушення недоторканності приватного життя (ст. 182). Але якщо особа не усвідомлює, чиї саме персональні дані вона розповсюджує, скажімо, розміщує на інтернет-сайті електронну базу паспортних даних осіб, які прописані в певному місці, що належить територіальному органу поліції, має місце злочин проти права власності на комп'ютерну інформацію з обмеженим доступом (у цьому випадку проти державної власності на комп'ютерну інформацію), тобто злочин, передбачений ст. 361-2 КК України.

Несанкціоновані дії, що призвели до витоку комп'ютерної інформації (ст. 361 та ч. 2 ст. 362 КК), слід відмежовувати й від порушення *таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються через комп'ютер* (ст. 163 КК Укра-

їни). Незаконне отримання кореспонденції, що передається з використанням засобів електронної пошти, не належить до комп'ютерних злочинів, а являє собою злочин проти особистих прав і свобод людини. Від комп'ютерних злочинів цей склад відрізняється за предметом: предмет комп'ютерних злочинів – комп'ютерна інформація; предмет злочину, передбаченого ст. 163 КК України, – специфічний вид інформації, а саме кореспонденція; а також за об'єктом посягання: право власності на комп'ютерну інформацію та недоторканність приватного життя. Наголосимо, що йдеться тільки про приватну кореспонденцію, тобто про листування між фізичними особами або між фізичною та юридичною особою. Ознайомлення зі змістом листування між юридичними особами слід кваліфікувати, за наявності мети розголошення або іншого використання отриманих відомостей, як умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю (ст. 231), або, за відсутності такої мети й залежно від ознак суб'єкта, як злочин, передбачений статтями 361 або 362 КК.

Значний інтерес у контексті питання відмежування комп'ютерних злочинів від порушення таємниці кореспонденції становить вирок Першотравневого районного суду м. Чернівці в справі № 1-235/2008 від 29 серпня 2008 року за обвинуваченням Д. у вчиненні злочинів, передбачених ч. 2 ст. 361-1, ч. 2 ст. 361 та ч. 1 ст. 163 КК. *Зокрема, Л. установив, що існує категорія шкідливих програмних засобів, які можна створювати через спеціальне налаштування вже створених програм. Однією з таких програм є Ardamax keyloger 2.9. Вона є трояном-кейлогером, яка здійснює електронне шпигунство за користувачем «зараженого» комп'ютера: інформація, що вводиться з клавіатури, знімки екрану, список активних програм і дії користувача з ними зберігаються у файлі на*

диску та періодично відправляються зловмисникові. У мережі Інтернет він відшукав дистрибутив цієї програми й завантажив собі в комп'ютер. Ознайомившись детально з принципом її дії, налаштував цю програму в такий спосіб, щоб уся інформація, яку вона збирала в чужих комп'ютерах, надсилалася на його електронну поштову скриньку. Усвідомлюючи, що створена ним комп'ютерна програма є шкідливою програмою (Trojan-Spy.Win32.Ardamax.n), призначеною для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), Л. вирішив розповсюдити її серед необмеженої кількості користувачів локальної мережі одного з провайдерів послуг мережі Інтернет. За допомогою власного комп'ютера й стандартного програмного забезпечення він навмисно розмістив означену шкідливу комп'ютерну програму на сервері локальної комп'ютерної мережі під назвою Winamp_6.0_New_Edition.exe. Знаючи, що Winamp.exe – це назва популярного програвача комп'ютерної музики та фільмів, він тим самим намагався приховати від користувачів справжнє призначення цієї шкідливої програми й у такий спосіб змусити активізувати її. Ю., один з абонентів локальної мережі, завантажила її та активізувала, помиляючись щодо її дійсного призначення. Після зараження комп'ютера Ю. троянська програма Trojan-Spy.Win32.Ardamax.n стала в автоматичному режимі вести електронний журнал натискання користувача на клавіатуру та робити знімки з робочого столу (монітора), після чого зібрану інформацію періодично відправляла на електронну скриньку Л. У результаті останній незаконно ознайомився з реквізитами авторизації Ю. у комп'ютерній мережі та на сервері електронної пошти, а також зі змістом її листування з друзями та знайомими, яке здійснювалося за допомогою електронної служби миттєвих текстових повідомлень.

У цьому випадку суд правильно оцінив той факт, що серед відомостей, отриманих унаслідок несанкціонованого втручання в роботу комп'ютера Ю., є такі, які становлять таємницю кореспонденції, що передається через комп'ютер, а отже, учинене потребує додаткової кваліфікації за ст. 163 КК. Крім цього, звернемо увагу й на те, що Л., як указано у вироку (для прикладу ми навели лише частину цього документа), здійснив подібні дії, тобто розповсюдження троянської програми та несанкціоноване отримання внаслідок її роботи на комп'ютерах потерпілих відповідних відомостей стосовно ще шести потерпілих. Отже, Л. фактично здійснив кілька розповсюджень шкідливих програм, несанкціонованих утручань і порушень таємниці кореспонденції. Суд, застосовуючи правила кваліфікації при повторності злочинів, дав учиненим діянням правильну правову оцінку – як злочинам, учиненим повторно.

Важливим питанням у визначенні критеріїв відмежування комп'ютерних злочинів від суміжних є формулювання ознак, які дають змогу розмежувати несанкціоноване втручання, що спричинило втрату або підробку комп'ютерної інформації (ст. 361 КК) або несанкціоновану зміну чи знищення комп'ютерної інформації, учинену особою, яка мала право доступу до неї (ст. 362 КК), і злочини, передбачені ст. 357 КК «Викрадення, присвоєння, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження», ст. 358 КК «Підроблення документів, печаток, штампів та бланків, їх збут, використання підроблених документів» та ст. 366 КК «Службове підроблення». Оскільки документ є одним з видів інформації, подібність зазначених складів полягає в тому, що статті 357, 358, 366 та ст. 361 і 362 КК

передбачають відповідальність за знищення або перекручення інформації. Видається можливим сформулювати таке правило: у тих випадках, коли документ, що є предметом злочинів, передбачених статтями 357, 358 або 366, являє собою комп'ютерну інформацію та є електронним, дії особи щодо його підроблення або знищення потребують, залежно від ознак суб'єкта, додаткової кваліфікації за статтями 361 або 362 КК. Таке правило пояснюється тим, що в означених випадках спосіб підробки або знищення документа представляє собою самостійний склад злочину. Передусім в цих випадках ідеться про електронні документи, до яких згідно із Законом України «Про електронні документи та електронний документообіг» від 22 травня 2003 року належать документи, інформація в яких зафіксована у вигляді електронних даних, охоплюючи обов'язкові реквізити документа (ст. 5 Закону).

Зазначимо також, що деякі способи вчинення комп'ютерних злочинів потребують додаткової кваліфікації. Скажімо, використання для несанкціонованого втручання (ст. 361 КК) або несанкціонованого перехоплення чи копіювання (ст. 362) спеціальних технічних засобів негласного отримання інформації потребує додаткової кваліфікації за ст. 359 КК як незаконне використання спеціальних технічних засобів негласного отримання інформації. Якщо ж несанкціоноване втручання в роботу комп'ютерної мережі або мережі електрозв'язку вчиняється в спосіб умисного пошкодження кабельної,

Тест
до розділу 2

радіорелейної, повітряної лінії зв'язку, проводового мовлення або споруд чи обладнання, які входять до їх складу, і це, крім наслідків, передбачених у ст. 361 КК, призводить до тимчасового припинення зв'язку, учинене належить кваліфікувати за сукупністю злочинів, передбачених статтями 361 та 360 КК «Умисне пошкодження ліній зв'язку».

Ми розглянули аж ніяк не всі можливі випадки відмежування досліджуваних злочинів від суміжних. Сучасний, без перебільшення, вибуховий розвиток інформаційних технологій разом з рівнем їх проникнення в суспільне життя, що постійно зростає, розширенням сфери застосування комп'ютерної техніки призвели до ситуації, коли майже будь-який злочин може бути вчинено з використанням комп'ютерної техніки. Скажімо, останнім часом спостерігається певна тенденція використання комп'ютерної мережі для розповсюдження матеріалів із закликами до насильницького захоплення державної влади (ч. 2 ст. 109 КК) або умисних дій, спрямованих на розпалювання расової ворожнечі та ненависті (ст. 161 КК). В окремих випадках норми КК містять спеціальну вказівку щодо можливості вчинення певного посягання з використанням комп'ютерної техніки (наприклад, ч. 2 ст. 301 КК). Проте використання комп'ютерної техніки ще не дає змогу твердити про те, що скоєно злочин у сфері використання ІТ і потрібною є кваліфікація вчиненого за статтями 361 – 363-1 КК. Основним критерієм відмежування цих злочинів від суміжних, пов'язаних з використанням комп'ютерної техніки тільки як знаряддя або засобу, є об'єкт посягання. Можна сказати, що особливістю кримінально-правової кваліфікації злочинів, учинюваних з використанням комп'ютерної техніки, слід визнати потребу вирішення питання про доцільність додаткової кваліфікації дій

винної особи за статтями, що передбачають відповідальність за злочини у сфері використання комп'ютерної техніки. З'ясовуючи це питання, треба керуватися тим, що використання комп'ютерної техніки при вчиненні інших злочинів утворює самостійний склад злочину лише тоді, коли заподіяно певну шкоду відповідному об'єкту – відносинам власності на комп'ютерну інформацію, коли певна інформація була незаконно знищена, блокована, модифікована тощо. У тих випадках, коли певні інформаційні системи використовуються за призначенням та їх функціонування не порушується, додаткова кваліфікація не потрібна.

Підсумовуючи кримінально-правовий аналіз злочинів у сфері використання комп'ютерної техніки, варто звернути увагу на те, що даючи первинну кримінально-правову оцінку діям підозрюваних осіб під час кримінального провадження, слідчі мають з підвищеною увагою встановлювати обставини, що свідчать про суспільну небезпеку посягання (заподіяна шкода, порушення роботи підприємства або організації тощо), а також розглядати можливість застосування положень КК про малозначність діяння (ч. 2 ст. 11 КК).

РОЗДІЛ 3. КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

3.1. Способи вчинення злочинів у сфері використання інформаційних технологій

У структурі елементів криміналістичної характеристики злочинів одне з ключових місць належить способам готування, учинення та приховування слідів злочину.

Як показує вивчення слідчої та судової практики, усе ширшого застосування набувають операції, що вчиняються з використанням платіжних карток у мережі Інтернет (сервіси Приват 24, Ощад 24 тощо), що обумовлює виникнення нових, ще не досить досліджених, способів злочинного збагачення – злочинів, учинених у сфері функціонування електронних розрахунків з використанням конфіденційних даних про реквізити справжніх платіжних карток. Способи вчинення таких злочинів може бути умовно поділено на дві групи:

а) способи отримання конфіденційних даних про реквізити справжніх платіжних карток;

б) способи використання отриманих реквізитів для вчинення шахрайства у сфері функціонування електронних розрахунків.

Найпоширенішими способами отримання конфіденційних даних про реквізити справжніх платіжних карток та їх власників є:

1) *незаконне використання спеціальних технічних засобів (СТЗ), призначених (розроблених, пристосованих, запрограмованих) для негласного отримання конфіденційної інформації про реквізити платіжних карток та їх власників.* Для України найбільш характерними з них є ті, що пристосовані з побутової апаратури – скімери (спеціальні сканери, міні-комп'ютери). Це пристрої зі зчитувальною магнітною голівкою, підсилювачем, перетворювачем, пам'яттю та перехідником для під'єднання до комп'ютера, які злочинці таємно встановлюють на банкомат, камуфлюючи їх під технологічні елементи його корпусу, а в дальшому також негласно вилучають[1]. Скімінгові пристрої мають такі блоки:

а) спеціальна клавіатура із сенсорними клавішами, яка накладається на стандартну управляючу клавіатуру банкомата. Вона не дає змогу натискати на клавіші «рідної» клавіатури й управляти роботою банкомата. Кнопки накладеної клавіатури встановлено в такий спосіб, щоб ПІН-код, який набирає власник платіжної картки, передавався до блоку управління СТЗ (таким зазвичай виступає портативний комп'ютер);

[1] Див.: Каблуков А. О. Деякі аспекти протидії злочинам, що здійснюються у сфері використання пластикових карток. *Використання сучасних інформаційних технологій у діяльності ОВС* : матеріали Всеукраїнського наук.-практ. семінару (м. Дніпропетровськ, ДДУВС, 23 листопада 2007 р.). Дніпропетровськ : Дніпропетровський державний університет внутрішніх справ, 2008. С. 18.

б) рамка, що кріпиться до технологічної щілини зчитувального пристрою банкомата для електромагнітного перехоплення (сканування) електронних реквізитів з магнітної смуги платіжної картки. З використанням подібного пристрою злочинцеві вдається скопіювати лише інформацію, що міститься на магнітній смузі платіжної картки, проте він не може дізнатися її ПІН-код. Саме тому рамку, що кріпиться до технологічної щілини зчитувального пристрою банкомата зазвичай використовують у комплексі зі звичайною цифровою міні відеокамерою (або ж у комплексі зі спеціальною клавіатурою із сенсорними клавішами, яку накладають на стандартну управляючу клавіатуру банкомата, про яку згадано вище). Відеокамеру встановлюють так, щоб зафіксувати ПІН-код, який уводить утримувач з клавіатури банкомата. Оскільки в деяких банкоматах установлено зовнішні камери автоматизованих охоронних систем, вона, як звичайно, не привертає увагу клієнтів;

в) мініатюрний блок управління клавіатурою, сканером і пристроєм для запису перехопленої інформації на флеш-картку у вигляді міні-ЕОМ.

2) *злам клієнтської бази Інтернет-магазину*. Цей спосіб полягає в інтелектуальному зламі програмного захисту бази даних електронних магазинів, що містять усю конфіденційну інформацію про клієнтів (утримувачів) і реквізити їхніх платіжних карток. Він здійснюється з використанням програм-зломщиків, які дають змогу злочинцям нейтралізувати (блокувати, модифікувати тощо) програмні засоби захисту від несанкціонованого доступу до електронних реквізитів платіжних карток;

3) *емпіричне вираховування правильних реквізитів платіжних карток*. Для вчинення зазначених дій злочинці зазвичай використовують програми генерації та пі-

дбору електронних ідентифікаційних реквізитів платіжних карток, які працюють за принципом простого перебору або підбору невідомих цифр по криптоалгоритмам[1] (наприклад, код-граббери[2], генератори паролів[3]). До того ж чим більше відомих злочинцеві цифр зі вказаних реквізитів буде введено в програму, тим швидше вона (програма) видасть правильний варіант;

4) *фішинг* (англ. phishing) – password harvesting fishing (збір паролів) – спосіб злочинних дій, здійснюваний з використанням спамерських розсилок або вірусів потенційним жертвам для отримання з мережі відомостей, що надають доступ до банківських рахунків (паролі, PIN-коди та іншу особисту інформацію) та застогсовуються в дальшому для розкрадання грошових коштів з електронних рахунків[4].

---

[1] Програма генерації ідентифікаційних пар та інших цифрових ідентифікаційних реквізитів платіжних карток.

[2] Код-граббер – програми для ЕОМ, що автоматично підбирають невідомі цифри в номері карти або номер карти з його складових, що стали відомими шахраям (Див.: Вехов В. Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов : монография. Волгоград : ВА МВД России, 2005. С. 274).

[3] Генератори паролів – комп'ютерні програми, що перебирають ідентифікаційні пари конфіденційних реквізитів для визначення правильної, або визначають невідомий реквізит з відомого способом певного обчислення (Див.: Вехов В. Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов : монография. Волгоград : ВА МВД России, 2005. С. 273).

[4] Докладніше про це див.: Коваленко В. В., Анапольська А. І. Розслідування шахрайств та пов'язаних з ними злочинів, учинених у сфері функціонування електронних розрахунків : монографія / МВС України, ЛДУВС ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2013. С. 33.

5) *фармінг* – спосіб злочинних дій, при якому клієнт уже не запрошується, а прямує на фальшивий сайт автоматично, коли власник рахунку намагається увійти на офіційний сайт банку[1];

6) *вішинг* – технологія Інтернет-шахрайства, різновид фішинга, яка полягає у використанні war diallers (модемів, що керуються комп'ютером, які автоматично набирають один або декілька телефонних номерів і встановлюють зв'язок з абонентами) і можливостей Інтернет-телефонії для крадіжки особистих конфіденційних даних[2];

7) *використання кейлогерів* (з англ. Keylogger – реєстратор натиснень клавіш) – програмного забезпечення й апаратних засобів, основним призначенням яких є прихований моніторинг натиснень клавіш на ЕОМ і ведення журналу цих натиснень[3] тощо.

Судова практика

Залежно від напрямів використання незаконно отриманих конфіденційних даних про реквізити справжніх платіжних карток способи вчинення злочинів у сфері функціонування електронних розрахунків може бути класифіковано так:

[1] Див.: Хафизова Л. С. Фишинг – новый вид финансового мошенничества в сети Интернет. *Закон и право.* 2007. № 9. С. 67.

[2] Див.: Хафизова Л. С. Фишинг – новый вид финансового мошенничества в сети Интернет. *Закон и право.* 2007. № 9. С. 67–68.

[3] Див.: Скалозуб Л. П., Василинчук В. І., Лебідь С. А., Дяченко Т. В. та ін. Збірник методичних рекомендацій з викриття та документування злочинів у сфері інтелектуальної власності та високих технологій. Київ : 2009. С. 49.

1) *модифікація даних у комп'ютерній системі банку, що обслуговує картковий рахунок.* Цей спосіб зазвичай використовує співробітник організації-емітента (або колишній співробітник, якому відомі коди й паролі доступу до системи обслуговування електронних рахунків), який пов'язаний з обслуговуванням карткових рахунків утримувачів платіжних карток. Маючи доступ до комп'ютерної системи обліку клієнтів або операційної роботи за картковими рахунками, злочинець таємно вносить в електронні документи несанкціоновані зміни, що впливають на результати розрахунків і, відповідно, на баланс конкретного електронного рахунку.

Це може бути вчинено в спосіб:

а) навмисного створення уяви про банківську помилку в системі управління базами даних. При цьому способі злочинець незаконно втручається в діяльність комп'ютерної системи управління базами даних, що містять інформацію про стан рахунків, та під виглядом банківської помилки навмисно зменшує дані витягу з конкретного карткового рахунку, що в дальшому надає можливість шахраям звернутися в банк з вимогою повернути «зниклі» грошові кошти на певний рахунок[1];

б) несанкціонованого встановлення на рахунок платіжної картки кредитного ліміту. Цей спосіб може застосувати тільки співробітник організації-емітента, який пов'язаний з обслуговуванням картрахунків. Він полягає в тому, що злочинець входить у змову з утримувачем карти для того, аби в несанкціонований спосіб заволодіти грошовими коштами, які належать емітентові. Маючи доступ до комп'ютерної системи обліку клієнтів або

[1] Див.: Вехов В. Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов : монография. Волгоград : ВА МВД России, 2005. С. 108.

операційної роботи за картрахунком, злочинець таємно вносить у відповідні електронні документи несанкціоновані зміни, які впливають на кінцеві результати обчислень розрахунків за картрахунком[1];

в) несанкціонованого встановлення в системі спеціального статусу рахунку, що дає змогу в певних межах знімати з картки грошові кошти. Зазначений спосіб полягає в тому, що шахраї у двох або декількох банках відкривають безліч спеціальних карткових рахунків, розрахунки по яких можуть здійснюватися за допомогою банківських карток однієї або декількох платіжних систем. На одну з таких карт (її рахунок) злочинці кладуть деяку суму грошей. Зазвичай банки, що емітують кредитні й дебетові карти, для залучення клієнтів допускають деяку суму перевитрат коштів при проведенні платіжно-розрахункових операцій у тому випадку, якщо картрахунок не закривається. Інакше кажучи, надається відтермінування за понадлімітним платежем на певну суму, наперед обумовлену в договорі на обслуговування карти. Цією технологічною особливістю й користуються злочинці. Вони повністю з допустимою перевитратою знімають грошові кошти з указаного рахунку й переводять цю суму на другий картковий рахунок, з якого й собі всі кошти також знімають з перевитратою й перекладають на третій. Це повторюється багато разів доти, доки грошова сума не досягне розміру, який влаштовує шахраїв. Після чого гроші оперативно знімають готівкою через вуличний банкомат[2];

[1] Див.: Гамза В. А., Ткачук И. Б. Безопасность коммерческого банка : учебно-практическое пособие. Москва : Изд. Шумилова И. И., 2000. С. 101.

[2] Див.: Вехов В. Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов : монография. Волгоград : ВА МВД России, 2005. С.92.

г) використання реквізитів паралельної картки – двійника. Цей спосіб заснований на використанні злочинцями «генератора паролів» (шкідливої програми для ЕОМ). Знаючи номер дійсної карти, злочинці за допомогою «генератора» обчислюють з неї ПІН-код і відповідний йому номер карти. Отже, у злочинців фактично з'являється фантомна платіжна картка, яка повністю відповідає всім технічним та ідентифікаційним вимогам справжньої, з тією лише відмінністю, що її номер і ПІН-код не зареєстровані жодним емітентом. Учинити злочин з використанням таких реквізитів платіжної картки можна лише розплатившись карткою в мережі Інтернет[1].

2) *створення й використання «фірм-одноденок».* Цей спосіб полягає в тому, що члени організованих груп (ОГ), які спеціалізуються на вчиненні злочинів, що нами розглядаються, легально реєструють магазин (підприємство сфери послуг), який на договірній основі входить на правах мерчанта[2] в платіжну систему. Основною метою створення таких підприємств є несанкціоноване заволодіння грошовими коштами через упровадження в платіжну систему первинних розрахункових документів, складених з використанням незаконно одержаних конфіденційних даних про реквізити платіжних карток та їх утримувачів. Залежно від кількості реквізитів, що є

[1] Див.: Организованная преступность и частные инвестиции : Учеб. пособ. / под ред. В. И. Попова, А. С. Овчинского. Москва, 1998. С. 364–365.

[2] Мерчант – підприємство торгівлі або сфери послуг – фізична або юридична особа, яка згідно з підписаною нею угодою з емітентом або еквайєром несе зобов'язання щодо прийняття документів, складених з використанням платіжно-розрахункових карт як оплати за надані товари (послуги) (Див.: Вехов В. Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов : монография. Волгоград : ВА МВД России, 2005. С. 79–80).

в розпорядженні шахраїв, цей спосіб може бути поділено на дві групи:

а) за наявності декількох десятків реквізитів створюване підприємство реєструють на підставну особу або з використанням викрадених документів (шахраї одержують потрібний комплект реєстраційних документів і ставлять підприємство на облік у податковій інспекції).

Протиправна діяльність створеного в такий спосіб підприємства полягає у виконанні максимально можливої кількості трансакцій з використанням реквізитів платіжних карток. Насправді таке підприємство реально нічим не торгує й ніяких послуг не надає. При цьому в обслуговуючий банк надсилаються запити авторизацій[1] на проведення операцій з використанням незаконно отриманих реквізитів справжніх платіжних карток і на інкасацію[2] виставляються відповідні комплекти документів, на підставі яких на рахунок магазину зараховуються грошові кошти;

б) за наявності великої бази даних, що містить декілька десятків тисяч реквізитів платіжних карток (зазвичай така база даних постійно поповнюється за рахунок

[1] Авторизація – процедура отримання дозволу на проведення операції із застосуванням платіжної картки (Див.: Про затвердження Положення про порядок емісії платіжних карток і здійснення операцій з їх застосуванням : постанова Правління Національного банку України від 19 квітня 2005 року № 137 зі змінами, унесеними Постановою правління Національного банку України від 04 січня 2008 року № 2. *Офіційний вісник України*. 2008. № 6. Ст. 159).

[2] Інкасація – збирання та доставка коштів до каси установи банку (Див.: Про затвердження змін до Інструкції з організації перевезення валютних цінностей та інкасації коштів в установах банків України : постанова Правління Національного банку України від 15.12.2004 № 644. *Офіційний вісник України*. 2005. № 3. Ст. 255).

добре налагодженого каналу отримання конфіденційних даних про реквізити платіжних карток), для несанкціонованого заволодіння грошовими коштами використовується підприємство торгівлі або сфери послуг, що реально функціонує, яке може мати свій Інтернет-магазин. Діяльність таких підприємств розрахована на тривалий термін. Тактика, обрана злочинцями в подібних випадках, полягає у вчиненні незаконних трансакцій на незначні суми (зазвичай, 50-100 грн), які чергуються з проведенням дійсних трансакцій. Подібні дії дають можливість злочинцям тривалий час бути непоміченими. Так продовжується до того моменту, поки рівень chargeback (відмов від платежів) не стане свідчити про можливий факт шахрайства з боку співробітників конкретного мерчанта.

3.2. Обстановка незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж

У криміналістичній літературі під обстановкою злочину прийнято розуміти систему різного роду об'єктів, явищ, процесів, які взаємодіють між собою та характеризують умови місця й часу, матеріальні, природно-кліматичні, виробничо-побутові та інші умови навколишнього середовища, особливості поведінки учасників протиправної події та інші обставини об'єктивної реальності, що склалися в момент злочину і впливають на спосіб, умови та інші обставини його вчинення[1].

[1] Криминалистика : учебник / отв. ред. Н. П. Яблоков. 2-е изд., перераб. и доп. Москва : Юристъ, 2001. С. 22.

Додатковими факторами обстановки незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж можуть бути: наявність і стан засобів захисту комп'ютерної техніки (організаційних, технічних, програмних); стан дисципліни на об'єкті; вимогливість з боку керівників до дотримання норм і правил інформаційної безпеки й експлуатації ЕОМ тощо.

Для обстановки, за якої можливе вчинення комп'ютерного злочину, характерне таке: невисокий техніко-організаційний рівень господарської діяльності, низький контроль за інформаційною безпекою, відсутність системи захисту інформації, атмосфера байдужості до випадків порушення вимог інформаційної безпеки тощо.

З'ясування особливостей обстановки, що склалась, дає змогу швидше визначити, на що саме слід звернути особливу увагу при огляді місця події, вивченні комп'ютерного обладнання й документів, виклику й допиті конкретних свідків і вирішенні питань про потребу вилучення певних документів тощо.

Особливістю незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж є те, що ***місце*** безпосереднього вчинення протиправного діяння (місце, де виконувалися дії об'єктивної сторони складу злочину) і місце настання шкідливих наслідків (місце, де настав результат протиправного діяння) можуть не збігатись. Це трапляється майже в кожному випадку опосередкованого (віддаленого) доступу до комп'ютерної інформації. При безпосередньому ж доступі місце вчинення протиправного діяння й місце настання шкідливих наслідків збігаються. Такий злочин часто вчиняють працівники підприємства чи організації, закладу чи фірми. Саме тому

найбільш розповсюдженими місцями вчинення таких злочинів є: адміністративні та службові приміщення різного типу суб'єктів господарювання; власні та орендовані житлові приміщення; приміщення комунальної власності або ж споріднені з ними, котрі на правах власності чи оренди можуть використовуватися під комп'ютерні клуби, Інтернет-кафе тощо[1].

Транснаціональний характер незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж часто обумовлює й те, що зазначені злочини можуть учинятися в одній країні, а негативні наслідки наставати в іншій. Якщо неправомірний доступ здійснюється одночасно з декількох комп'ютерів, то кількість місць учинення злочину відповідає кількості задіяних при цьому комп'ютерів[2].

Місцем, де в результаті вчинення комп'ютерного злочину настав злочинний результат, є підприємства, організації, заклади різних форм власності, що мають інформацію на машинному носії, в електронно-обчислювальній машині, системі ЕОМ або їх мережі. До них належать ті, у яких використовуються високі технології тощо. Значна кількість банків, пенсійних фондів часто стикаються з проблемою захисту персональних даних вкладників. Гострою є й проблема захисту відомостей, що зберігаються в паспортно-візовій службі про реєстрацію за місцем проживання окремих категорій громадян.

[1] Див.: Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09. Київ, 2005. С. 64.

[2] Див.: Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации : учебное пособие / под ред. проф. Н. Г. Шурухнова. Москва : ЮИ МВД РФ, Книжный мир, 2001. С. 29.

Підприємствами, закладами, організаціями (різних форм власності), де такі злочини вчиняють особи, які в них працюють, є:

1. Підприємства, організації, заклади, фірми, компанії, в управлінській діяльності яких беруть участь люди, які мають стосунок до програмного забезпечення й баз даних автоматизованих інформаційних систем, що надає їм можливість учиняти незаконні дії.

2. Підприємства, організації, заклади, фірми, компанії, що мають високі темпи розвитку, за якими не встигають управлінські функції. У деяких випадках самі керівники достеменно не знають, з чого почати, до яких організаційно-управлінських заходів треба вдатись, аби унеможливити незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж.

3. Підприємства, організації, заклади, фірми, компанії, які згортають свою діяльність. Їх ресурси також обмежені, що створює передумови для протиправних дій.

4. Підприємства, організації, заклади, фірми, компанії, створені із залученням іноземного капіталу, які підтримують стійкі ділові стосунки з ближнім і дальнім зарубіжжям.

5. Підприємства, організації, заклади, фірми, компанії, де через різні обставини панує ненормальний морально-психологічний клімат (наприклад, через образу осіб, які перебувають на нижчому щаблі соціальної драбини; щодо власного принизливого становища порівняно з іншими (оплата праці, надання пільг).

Незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж зазвичай здійснюється: 1) у службових приміщеннях підприємства (організації), де встановлено комп'ютер або група комп'ютерів (у випадку безпосереднього доступу до комп'ютерної інформації); 2) у житлових приміщеннях, приміщеннях інших

підприємств або організацій, раніше орендованих приміщеннях, спеціально обладнаних автомобілях тощо.

3.3. Сліди вчинення злочинів у сфері використання інформаційних технологій

Слідами вчинення досліджуваних злочинів можуть бути будь-які рукописні записи, роздруківки, що свідчать про підготовку й учинення злочину. Матеріальні сліди можуть залишатися й на самій обчислювальній техніці (сліди пальців рук, мікрочастинки на клавіатурі, дисководах, принтері тощо[1]), а також на магнітних носіях і CD-дисках. Крім того, слідами є результати роботи антивірусних і тестових програм. Ці сліди можуть бути виявлені при вивченні комп'ютерного устаткування, робочих записів програмістів, протоколів роботи антивірусних програм, а також програмного забезпечення. Для виявлення таких слідів треба залучати фахівця.

Труднощі встановлення слідової картини щодо такої категорії злочинів пояснюється тим, що зовні факт учинення розкрадання та його прояв у навколишньому

[1] Характеристику зазначених слідів детально розглянуто в науковій літературі. Див.: Колесниченко А. Н. Криминалистическая характеристика преступлений : учеб. пособие. Харьков : Юрид. институт, 1985. 92 с.; Ларичев В. Д. Выявление преступлений, совершаемых в сфере экономики при переходе к рыночным отношениям : метод. рекомендации. Москва : НИИ МВД РФ, 1993. 56 с.; Реуцький А. В. Методика розслідування злочинів у сфері виготовлення та обігу платіжних карток : автореф. дис. … канд. юрид. наук : 12.00.09. Харків, 2009. 21 с.; Белкин Р. С. Курс криминалистики : в 3-х т. Москва : Юристь, 1997. Т. 3. Криминалистические средства, приемы и рекомендации. 480 с.

середовищі ледве помітні або непомітні зовсім, носять інформаційний характер (є змінами в комп'ютерній інформації (знищення, модифікація, копіювання, блокування)). У цьому випадку йдеться про електронні цифрові сліди – відомості (повідомлення, дані), зафіксовані на матеріальному носії та об'єктивно представлені у вигляді відображення інформації тимчасового й ідентифікаційного характеру в автоматизованих інформаційних системах, що утворюється за допомогою електромагнітної взаємодії, пов'язаної з подією злочину[1].

Сліди можуть залишатися й при опосередкованому доступі через комп'ютерні мережі, наприклад, через Інтернет. Вони виникають тому, що система, через яку здійснюється доступ, має інформацію, яку вона запитує в особи, що намагається з'єднатися з іншим комп'ютером. Система визначає електронну адресу, програмне забезпечення і його версію. Крім того, при доступі в мережу зазвичай запитується адреса електронної пошти, реальне ім'я та інші дані[2]. Цю інформацію запитує системний адміністратор (провайдер) для контролю звернень на його сервер, і це також дає змогу ідентифікувати особу, яка проникає в мережу.

Слідами, що вказують на сторонній доступ до інформації, можуть бути: перейменування каталогів і файлів;

[1] Див.: Коваленко В. В., Анапольська А. І. Розслідування шахрайств та пов'язаних з ними злочинів, учинених у сфері функціонування електронних розрахунків : монографія / МВС України, ЛДУВС ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2013. С. 63.

[2] Див.: Коваленко В. В., Анапольська А. І. Розслідування шахрайств та пов'язаних з ними злочинів, учинених у сфері функціонування електронних розрахунків : монографія / МВС України, ЛДУВС ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2013. С. 47.

зміни розмірів і вмісту файлів; зміни стандартних реквізитів файлів, дати й часу їх створення; поява нових каталогів, файлів тощо.

Перелічене може свідчити про зміни в заданій структурі файлової системи, а також про зміни вмісту файлів. Крім того, на незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж можуть вказувати зміни в раніше заданій конфігурації комп'ютера, зокрема: зміни картинки й кольору екрана при вмиканні; зміна порядку взаємодії з периферійним обладнанням (принтером, модемом тощо); поява нових і знищення попередніх мережевих приладів тощо.

На незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж можуть указувати й незвичні прояви в роботі ЕОМ – уповільнене або неправильне завантаження операційної системи; уповільнена реакція машини на введення з клавіатури; уповільнена робота машини з дисковими накопичувачами під час записування й зчитування інформації; неадекватна реакція ЕОМ на команди користувача; поява на екрані нестандартних символів, знаків тощо[1].

Установити механізм учинення протиправної дії, як один з варіантів, можна за умови сприяння персоналу, який працює з комп'ютерними системами в установі, де стався злочин, та й то не завжди. Здебільшого може йтися не про матеріальні, а про ідеальні сліди відображення. Адміністрація володіє інформацією про всіх працівників структури, системи допуску, контролю та персонального складу, допущеного до роботи з комп'ютер-

[1] Див.: Самойлов С. В. Співвідношення Інтернет-шахрайств та комп'ютерних злочинів. *Забезпечення законності в діяльності органів дізнання та досудового слідства* : матеріали І наук.-практ. конф., (Луганськ 25 березня 2011 року). Луганськ, 2011. С. 83–88.

ними мережами. Вона також оперує даними про нештатні ситуації у функціонуванні обчислювальної техніки й технологічних управлінських процесах, що зрештою допоможе спрямувати слідчого на правильний шлях у досудовому розслідуванні.

Ідеальні сліди може бути класифіковано в такий спосіб:

1) за характером формування слідів пам'яті осіб, які безпосередньо сприймали подію злочину або брали в ній участь (підозрюваний, потерпілий, свідок); опосередковано сприймали подію злочину (поняті, спеціалісти); не мали стосунку до події злочину та його сприйняття, проте володіють іншою інформацією, що має значення для кримінального провадження (фахівці, відомчі інспектори, працівники служби безпеки та інші);

2) за процесуальним положенням особи, яка надає інформацію – одержана від потерпілого (фізичної особи, представника юридичної особи), свідка (учасники затримання; поняті; представники контролюючих органів; провайдери; співробітники торгівельного чи сервісного підприємства; очевидці протиправної діяльності підозрюваного, які працюють з ним на одному підприємстві, але в інших відділах, володіють відомостями про діяльність злочинців, їхній спосіб життя, коло спілкування, епізоди злочинної діяльності); фахівця, підозрюваного, іншої особи;

3) залежно від обставин, що підлягають доказуванню – про подію злочину; про об'єкти злочинного посягання (конфіденційна інформація тощо); про спосіб учинення злочину; про знаряддя злочину або засоби для їх виготовлення; про місце настання суспільно небезпечних наслідків і безпосереднього вчинення злочинних діянь; про дату, час та інші обставини злочину за кожним епізодом; про кількість епізодів злочинної діяль-

ності й роль кожного із співучасників за кожним епізодом; про характер і розмір збитку (з чого він складається); про обставини, що сприяли підготовці, учиненню та прихованню злочину; про винуватість певних осіб у вчиненні злочинів[1].

3.4. Особа злочинця

Як свідчить слідча та судова практика, в «електронну» злочинність утягнуто широке коло осіб – від висококваліфікованих фахівців до дилетантів. Злочинці можуть бути зайняті в різних сферах діяльності та мати різний рівень підготовки. Але найчастіше злочин здійснюють особи, які мають досить високу кваліфікацію, особливо, коли йдеться про незаконний доступ до комп'ютерної інформації в системі ЕОМ або мережі ЕОМ, оскільки вчинення зазначених дій вимагає складних технологічних й інформаційних заходів. Тому чим складніший і «хитріший» спосіб неправомірного доступу, тим вужче коло вірогідних злочинців.

Усіх їх можна розділити на дві великі групи:

1. Особи, які мають з потерпілим трудові або інші ділові стосунки.
2. Особи, не зв'язані діловими стосунками з потерпілим[2].

До першої групи належать співробітники, які зловживають службовим становищем. Це різного роду клерки,

[1] Див.: Суворова Л. А. Идеальные следы в криминалистике. Москва : Юрлитинформ, 2006. С. 11.

[2] Див.: Голубев 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. С. 45.

працівники служби безпеки, працівники контролюючих служб, інженерно-технічний персонал. Потенційну загрозу складають і представники інших організацій, які здійснюють сервісне обслуговування й ремонт систем.

До другої групи належать особи, які мають вагомі знання у сфері комп'ютерних технологій, і здебільшого керуються корисливими мотивами. До цієї ж групи належать також і спеціалісти-професіонали, які сприймають засоби безпеки комп'ютерних систем як виклик своєму професіоналізму.

Більшість комп'ютерних злочинів учиняються умисно. Розробники програм і спеціалісти служб безпеки майже до нуля звели можливість випадкового або необережного спричинення шкоди інтересам користувачів комп'ютерної техніки[1].

Мотивами вчинення комп'ютерних злочинів зазвичай є корисливі мотиви, політичні мотиви (тероризм, політичні акції), дослідницька цікавість, хуліганські мотиви та бешкетництво, помста.

Здебільшого вік зловмисників на момент учинення злочину коливається від 20 до 40 років. У п'ять разів частіше злочини у сфері використання комп'ютерних технологій учиняють чоловіки. Більшість суб'єктів таких злочинів мають вищу або незакінчену вищу технічну освіту, а також іншу вищу або незакінчену вищу освіту. Але останнім часом постійно збільшується серед них і частка жінок. Це пов'язане з професійною орієнтацією деяких спеціальностей і посад, обладнаних автоматизованими комп'ютерними робочими місцями, орієнтованими на жінок (секретар, бухгалтер, економіст, менеджер, касир, контролер тощо).

[1] Див.: Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. та ін Комп'ютерна злочинність : навчальний посібник. Київ : Атіка, 2002. С. 123.

Професійна спрямованість таких злочинців характеризується тим, що найчастіше вони:

– мають спеціальну підготовку в галузі автоматизованої комп'ютерної обробки інформації;

– є співробітниками державних закладів і організацій, які використовують комп'ютерні системи й інформаційні технології у своїй повсякденній діяльності;

– мають безпосередній стосунок до експлуатації засобів комп'ютерної техніки[1].

Не є винятком учинення таких злочинів співробітниками організацій, які займають відповідальні посади. Сучасні керівники зазвичай спеціалісти високого рівня, володіють достатньою комп'ютерною підготовкою й професійними знаннями, мають доступ до широкого кола інформації та можуть віддавати розпорядження, але безпосередньо не відповідати за роботу комп'ютерної системи.

[1] Див.: Глазырин Ф. В. Изучение личности обвиняемого и тактика следственных действий. Свердловск : СЮИ, 1973. С. 18.

РОЗДІЛ 4. ОСОБЛИВОСТІ ПОЧАТКОВОГО ЕТАПУ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕОМ (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Слайди до розділу 4

Відповідно до статті 214 КПК України слідчий, прокурор невідкладно, але не пізніше 24 годин після подання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про злочин, зобов'язаний унести відповідні відомості до Єдиного реєстру досудових розслідувань і розпочати розслідування (далі – ЄРДР)[1].

Джерелом інформації про вчинення кримінальних правопорушень у сфері використання електронно-об-

[1] Кримінальний процесуальний Кодекс України від 13 квітня 2012 року № 4651-VI. URL : http://zakon3.rada.gov.ua/laws/show/4651-17 (дата звернення : 17.03.2018).

числювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є:

– повідомлення фізичних або юридичних осіб та самостійно виявлені слідчим або іншою службовою особою органів Національної поліції з будь-якого джерела обставини кримінальних правопорушень;

– повідомлення представників влади, громадськості або окремих громадян, які затримали підозрювану особу при вчиненні кримінального правопорушення;

– повідомлення про вчинення кримінального правопорушення, опубліковані в засобах масової інформації;

– інформація, що надійшла засобами телефонного зв'язку, телеграфом або іншими засобами зв'язку про вчинення кримінального правопорушення[1];

– матеріали оперативно-розшукової справи щодо осіб, стосовно яких є дані про участь у підготовці до вчинення кримінального правопорушення[2] у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Відеокоментар до розділу 4

[1] Про затвердження Інструкції про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події : наказ МВС України від 06.11.2015 № 1177.

[2] Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07 липня 2017 року № 575.

У кримінальних провадженнях наведеної категорії найтиповішими слідчими ситуаціями є:

– власник або користувач комп'ютерної мережі (бази даних) власними силами виявили факт незаконного проникнення й інших протиправних дій, знайшли винну особу й заявили про це в правоохоронні органи;

– власник або користувач комп'ютерної мережі (бази даних, інформаційної системи) виявили факт незаконного проникнення й інших протиправних дій, але не змогли встановити винної особи й заявили про це в правоохоронні органи;

– дані про порушення цілісності (конфіденційності) інформації в інформаційній системі, а також про винну особу стали загальновідомими чи безпосередньо виявлені правоохоронними органами (наприклад, під час проведення оперативно-розшукових заходів у межах оперативного супроводження або щодо осіб, які готуються учинити злочин)[1].

До того ж слід ураховувати й інші слідчі ситуації, коли злочинця затримали на місці вчинення злочину, наприклад, у момент несанкціонованого копіювання конфіденційної інформації або при викраденні машинних носіїв з такою інформацією, передачі їх третім особам тощо. За таких умов проводиться низка заходів, спрямованих на розкриття злочину по «гарячих слідах» (в інтересах попередження втрати чи знищення доказів злочину досудове розслідування розпочинається невідкладно)[2].

Уповноваженим органом, який безпосередньо бере

[1] Яблоков Н. П. Криминалистика : учебное пособие. Москва : Юристъ, 1999. С. 621.

[2] Європіна І. В. Особливості порушення кримінальних справ про комп'ютерні злочини. *Адвокат*. 2011. № 3 (126). С. 35.

участь у виявленні та документуванні злочинів, учинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, є Департамент кіберполіції Національної поліції України. Ці підрозділи належать до міжрегіональних територіальних органів Національної поліції України, що входять до структури кримінальної поліції та проводять роботу щодо формування й забезпечення реалізації державної політики з попередження та протидії злочинам і правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також іншим злочинам та правопорушенням, учиненим з їх використанням. Зокрема:

– злочинам і правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– злочинам і правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем; обігу інформації протиправного характеру з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; економіки, яка включає в себе фінансові та торгові трансакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж, а також протидія забороненим видам господарської діяльності у цій сфері; надання телекомунікаційних послуг; а також шахрайствам і легалізації (відмиванню) доходів, одержаних від зазначених вище злочинів).

Оптимальна програма роботи з виявлення комп'ютерних злочинів охоплює такі заходи: 1) огляд місця події з обов'язковим дослідженням електронно-обчислювальних машин, сервера мережі ЕОМ, машинних носіїв інформації й комп'ютерної інформації; 2) опитування персоналу потерпілої організації (особливо фахівців, які мають стосунок до комп'ютерної техніки); 3) попереднє вивчення й дослідження документів і предметів (програмно-технічних засобів); 4) надання доручень фахівцям щодо проведення в потрібних випадках документальних перевірок; 5) якщо є підозра про конкретного суб'єкта, то в деяких випадках можливе отримання пояснення в нього, а також в інших осіб[1].

Специфіка виявлення несанкціонованого втручання в роботу ЕОМ полягає в застосуванні спеціальних технічних засобів, програмно-технологічних прийомів огляду й фіксації інформації, у використанні спеціальних інженерних рішень, обов'язковому залученні фахівця оперативно-технічного підрозділу, тісній узаємодії з операторами зв'язку й провайдерами.

Фактичні дані про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можна визначити як достовірні відомості, отримані уповноваженим підрозділом правоохоронного органу у визначеному правовими актами порядку, про зміст та характер змін, пов'язаних з подіями злочинів у цій сфері як у фізичному (сліди, залишені на предметах та у свідомості людини), так і в електронному середовищі (інформаційні сліди), на підставі яких можна дійти висновку

[1] Козак Н. С., Цимбал П. В., Данкович Н. О. Криміналістичні аспекти виявлення комп'ютерних злочинів. *Науковий вісник Національного університету ДПС України (економіка, право).* 2010. № 4 (51). С. 255.

про наявність або відсутність у цих діяннях ознак конкретного складу злочину.

У дальшому провадиться процес, пов'язаний з документуванням злочину, який має свою специфіку, а саме:

– документування злочинів є передбаченою законом діяльністю уповноваженої особи щодо пізнання подій певного виду злочинів як у фізичному (сліди, залишені на предметах та у свідомості людини), так і в електронному середовищі (інформаційні сліди);

– метою документування є забезпечення використання виявлених фактичних даних про злочини певного виду в інтересах кримінального судочинства в спосіб їх документального закріплення й посвідчення;

– предмет документування – фактичні дані, на підставі яких у визначеному законом порядку уповноважені органи встановлюють наявність або відсутність суспільно небезпечного діяння, передбаченого XVI розділом КК України, винність особи (групи осіб), яка його вчинила, та інші обставини, що мають значення для правильного вирішення провадження;

– у документі відображаються (посвідчуються, фіксуються) як власне фактичні дані, так і дії, прийоми та програмно-технічні засоби, які дали змогу їх виявити, спостерігати та зафіксувати;

– документуванням досягається сприйняття та розуміння відповідними особами фактів і обставин в електронному середовищі, які вони потім можуть посвідчити;

– документуванням забезпечується створення умов для послідовного накопичення інформації до того часу, поки будуть установлені всі обставини, що входять до предмета доказування, і досягнуті встановлені межі доказування; забезпечення умов збереження інформації

для багаторазового використання в інтересах кримінального судочинства;

– для проведення документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку на якісно високому рівні й досягнення позитивних результатів, а також для відповідних комп'ютерно-технічних досліджень потрібне використання наукових, технічних та інших спеціальних знань, специфічних програмно-технічних засобів і методів[1].

Перед вирішенням питання про реєстрацію кримінального правопорушення треба встановити:

– сліди злочину;

– місце неправомірного проникнення в комп'ютерну мережу (зсередини потерпілої організації чи ззовні);

–способи здійснення неправомірного доступу (подолання програмних засобів захисту, вилучення засобів комп'ютерної техніки, маніпуляції з даними, керуючими командами та інформацією, використання шкідливих програмних чи технічних засобів);

– засоби, що використовувалися при вчиненні злочину (технічні, програмні, інші);

– способи подолання інформаційного захисту (підбір ключів і паролів, крадіжка паролів, вимкнення засобів доступу тощо)[2].

У сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і

[1] Середа Г. П. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Інформаційна безпека людини, суспільства, держави.* 2011. № 2 (6). С. 110.

[2] Європіна І. В. Особливості порушення кримінальних справ про комп'ютерні злочини. *Адвокат*. 2011. № 3 (126). С. 35.

мереж електрозв'язку виокремлюють два типи слідів злочинів: традиційні (сліди-відображення, які розглядає трасологія, сліди-речовини, сліди-предмети) та нетрадиційні – інформаційні (певні зміни в електронному середовищі, пов'язані з подією злочину)[1].

Інформаційними є сліди модифікації інформації (баз даних, програм, текстових файлів), що містяться на жорстких дисках ЕОМ, дискетах, магнітних стрічках, лазерних і магнітооптичних дисках; сліди знищення чи модифікації інформації (видалення з каталогів імен файлів, стирання чи додавання окремих записів, фізичне руйнування або розмагнічування носіїв); результати роботи антивірусних і тестових програм (ці сліди може бути виявлено під час вивчення комп'ютерного обладнання, робочих записів програмістів, протоколів роботи антивірусних програм, а також програмного забезпечення). Власне інформаційні сліди є відображенням об'єктивної сторони складу злочину у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Особливості інформаційних слідів полягають у такому:

– місцезнаходження – окремий матеріальний носій комп'ютерної інформації, матеріальний носій в автоматизованій (комп'ютерній) системі, реалізованій на основі автономного комп'ютера, комп'ютерної або телекомунікаційної мережі;

[1] Середа Г. П. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Інформаційна безпека людини, суспільства, держави.* 2011. № 2 (6). С. 109.

– вигляд – кодований цифровий запис графічного, звукового, текстового та іншого характеру на магнітному або оптичному носії, сукупність електронних імпульсів у мережі;

– потреба дотримання певних технологічних процедур виявлення, фіксації та вилучення інформації (в електронному вигляді інформація легко піддається зміні, перекрученню, а інформація у вигляді електронних імпульсів загалом існує лише в окремі моменти реального часу);

– потреба використання наукових, технічних й інших спеціальних знань, а також програмно-технічних засобів і відповідних технологій, призначених для виявлення, фіксації та відтворення інформації у вигляді, придатному для сприймання людиною[1].

Матеріальними слідами злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можна вважати:

– сліди-відображення зовнішнього фізичного впливу на комп'ютерні системи, периферійні пристрої та мережі (сліди рук, ніг, знарядь злому тощо);

– сліди-речовини у вигляді витратних матеріалів (тонерів, фарб, різних мастил, що використовуються в комп'ютерних системах, їх мережах та периферійних пристроях);

– сліди-предмети: змінні диски та стрічки, апаратно реалізовані закладні пристрої, пристрої дистанційного зняття інформації, роздруківки на паперових носіях та

[1] Середа Г. П. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Інформаційна безпека людини, суспільства, держави.* 2011. № 2 (6). С. 109.

документи на електронних носіях, кабелі та роз'єми, пристрої фізичного знищення комп'ютерів і їх мереж[1].

Зазначимо, що копіювання, зміна, модифікація, виток, знищення інформації можуть бути викликані не тільки умисними неправомірними діями, але й помилками, неумисною неправильною поведінкою персоналу організації-жертви. Указані особливості мають бути враховані при вирішенні питання про початок досудового розслідування та визначенні кваліфікації кримінального правопорушення за КК України[2].

Зауважимо, що відповідно до частини 3 ст. 214 КПК України у невідкладних випадках до внесення відомостей до ЄРДР може проводитися лише огляд місця події, який здійснюється в порядку, визначеному ст. 237 КПК України. Мета цієї слідчої (розшукової) дії полягає у виявленні та фіксації відомостей щодо обставин учинення кримінального правопорушення, а також огляду місцевості, приміщення, речей та документів[3].

Під час проведення зазначеної процесуальної дії можна встановити такі факти:

– збереження й оброблення комп'ютерної інформації, яка зазнала злочинного впливу (наприклад, у разі незаконного втручання в роботу ЕОМ (комп'ютерів), їх систем чи комп'ютерних мереж);

---

[1] Середа Г. П. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Інформаційна безпека людини, суспільства, держави.* 2011. № 2 (6). С. 109.

[2] Європіна І. В. Особливості порушення кримінальних справ про комп'ютерні злочини. *Адвокат*. 2011. № 3 (126). С. 35.

[3] Кримінальний процесуальний Кодекс України від 13 квітня 2012 року № 4651-VI. URL : http://zakon3.rada.gov.ua/laws/show/4651-17 (дата звернення : 17.03.2018).

– знаходження комп'ютерного обладнання, яке використовувалося при вчиненні злочину (у разі поширення комп'ютерного вірусу після незаконного проникнення в комп'ютерну мережу);

– збереження інформації, отриманої в злочинний спосіб (у разі заволодіння комп'ютерною інформацією через викрадення, привласнення, вимагання, шахрайство чи зловживання службовим становищем);

– порушення правил експлуатації ЕОМ, комп'ютерної системи або мережі;

– настання шкідливих наслідків (знищення, блокування, модифікації, копіювання комп'ютерної інформації, порушення роботи комп'ютера, комп'ютерної системи або мережі)[1].

Огляд місця події вимагає ретельної підготовки й вирішення низки організаційних і технічних питань:

1. Забезпечення участі фахівців. Їхні знання потрібні для оперативного аналізу інформації та кваліфікованого її вилучення із засобів комп'ютерної техніки. Профіль потрібного фахівця визначають залежно від завдань огляду з урахуванням первинних даних про характер злочину.

2. Залучення понятих, які розуміються на комп'ютерній техніці хоча б на рівні користувача.

3. Підготовка обладнання, яке буде використано для огляду, перевезення й зберігання вилученої інформації. Основні труднощі при проведенні огляду за цією категорією злочинів полягають у тому, що інформаційні

[1] Тарасюк А. В. Актуальні питання тактики проведення окремих слідчих дій при розслідуванні комп'ютерних злочинів. *Інформаційна безпека людини, суспільства, держави.* 2011. № 3 (7). С. 66.

сліди може бути виявлено й вилучено тільки при використанні спеціального апаратного й програмного забезпечення. До того ж застосування таких засобів не врегульовано в кримінально-процесуальному законі[1].

Під час огляду комп'ютерної інформації та її вилучення треба виділити такі аспекти:

1. Перед проведенням огляду потрібно скопіювати всю інформацію, що міститься у відповідних журналах і каталогах, на жорстких дисках, дискетах тощо.

2. Усі маніпуляції із засобами комп'ютерної техніки мають строго фіксуватися в протоколі.

Під час перегляду журналів системи або оцінок часу файлів зафіксовані дані дадуть змогу пізніше ідентифікувати системні зміни, що були викликані діями слідчого.

Для уникнення можливих негативних наслідків збереження доказової інформації вироблено певні правила дій на завершальній стадії огляду: вилучення, упакування, опечатування підконтрольних об'єктів і, в разі потреби, транспортування до місця зберігання. На цьому етапі оформляють протокол огляду, до якого додають плани й схеми приміщення, що оглядається, і розташування комп'ютерного обладнання.

Слідчий огляд становить цілеспрямовану діяльність, що має бути належно організована, завчасно продумана, виважена та підготовлена[2].

---

[1] Козак Н. С., Цимбал П. В., Данкович Н. О. Криміналістичні аспекти виявлення комп'ютерних злочинів. *Науковий вісник Національного університету ДПС України (економіка, право).* 2010. № 4 (51). С. 255.

[2] Козак Н. С., Цимбал П. В., Данкович Н. О. Криміналістичні аспекти виявлення комп'ютерних злочинів. *Науковий вісник Національного університету ДПС України (економіка, право).* 2010. № 4 (51). С. 256-257.

Огляд дає змогу встановити великий обсяг доказів, які належать до складу злочину – об'єкта, об'єктивної сторони, суб'єкта та суб'єктивної сторони[1].

Під час огляду місця події до внесення відомостей до ЄРДР треба також звертати увагу й на такі елементи обстановки:

– сліди, що вказують на зміни в заданій файловій структурі (перейменування каталогів і файлів, зміна розмірів і змісту файлів, зміна стандартних реквізитів файлів, поява нових каталогів і файлів, видалення з каталогів імен файлів, стирання або додавання окремих записів, фізичне знищення або розмагнічування носіїв інформації, поява нових реєстраційних даних, які комп'ютер робить автоматично тощо);

– сліди, що є результатом роботи антивірусних і тестових програм (наприклад, результати роботи програми DrWeb відбиваються у файлі report.web, зміст якого можна легко переглянути);

– сліди, що відбивають зміни в заданій конфігурації комп'ютера (зміна кольору і файлів, поява нових і видалення старих мережних пристроїв, зміна порядку взаємодії з периферійними пристроями (принтером, модемом тощо);

– сліди, що характеризують незвичні прояви в роботі ЕОМ (уповільнене або некоректне завантаження операційної системи, уповільнена реакція машини на введення з клавіатури, уповільнена робота машини з накопичувачами при записі й зчитуванні інформації, неадекватні реакції ЕОМ на команди користувача, поява на екрані нестандартних символів, знаків тощо);

[1] Тарасюк А. В. Актуальні питання тактики проведення окремих слідчих дій при розслідуванні комп'ютерних злочинів. *Інформаційна безпека людини, суспільства, держави.* 2011. № 3 (7). С. 66.

– сліди руху пакетів інформації в мережі Інтернет, де кожний забезпечується адресою комп'ютера-одержувача, і способом передачі проходить декілька вузлових комп'ютерів (серверів), на яких залишаються сліди реєстрації проходження пакетів і сліди, залишені в результаті неправомірних дій злочинця. Крім того, при відвідуванні Web-вузла браузер (програма) пише електронну адресу цієї сторінки в безліч файлів, що містяться на жорсткому диску. Це кеш-файли, файли-сценарії, файли-історії та файли Windows Registry (наприклад, файли-сценарії при перегляді Web-вузла реєструють кожний натиск на мишу і файл, що був використаний як буфер адреси вузлів, які висилали код, і зберігають інформацію про це в папці Windows/Cookies; при роботі з Internet Explorer URL файли-історії зберігають послідовність дій оператора в папці Windows/History); сліди, що залишаються на «робочому місці» злочинця, так звані сліди засобів для налагодження програм проникнення (наприклад, які-небудь рукописні записи, списки паролів, коди, таблиці шифрування, чернетки, роздруківки тощо);

– сліди, що залишаються на засобах захисту інформації (спеціальних електронних картках, електронних ключах доступу до персонального комп'ютера, пристроях ідентифікації користувача за геометричними ознаками руки, почерку, голосу);

– сліди знарядь зламу, пальців рук, мікрочасток, паперові носії: роздруківки на принтері, записи кодів, паролів тощо при проникненні сторонніх осіб у приміщення, за місцем розміщення комп'ютерного (мережного) устаткування, носіїв інформації та засобів доступу до віддалених мереж (модемів, засобів телефонного і супутникового зв'язку)[1].

[1] Європіна І. В. Особливості порушення кримінальних справ про комп'ютерні злочини. *Адвокат*. 2011. № 3 (126). С. 36.

При огляді та описанні слідів комп'ютерного (мережного) обладнання та місця події варто також звернути увагу на:

– знаряддя вчинення злочинів у сфері комп'ютерної інформації, якими є засоби комп'ютерної техніки, зокрема спеціальне програмне забезпечення, за допомогою яких здійснюється безпосередній або опосередкований (віддалений) доступ. До знарядь безпосереднього доступу належать носії комп'ютерної інформації (USB Flash накопичувачі, лазерні диски, дискети, касети з магнітною стрічкою для стримера), різноманітне периферійне устаткування (друкувальний пристрій, CD-ROM – накопичувач, стример, дисководи), а також електронні ключі, особисті ідентифікаційні коди тощо.

До знарядь опосередкованого (віддаленого) доступу належить передусім мережне устаткування, а також засоби доступу до віддалених мереж (модеми, засоби телефонного й супутникового зв'язку).

Подібно до знарядь можна класифікувати й способи доступу до комп'ютерної інформації. При реалізації способів безпосереднього доступу інформація знищується, блокується, модифікується, копіюється, а також може порушуватися робота ЕОМ, системи ЕОМ або їх мережі через віддання відповідних команд з комп'ютера, на якому інформація міститься. Безпосередній доступ можуть здійснювати як особи, які працюють з інформацією, так і особи, котрі спеціально проникають у закриті зони та приміщення, де провадиться обробка інформації. Іноді злочинець для вилучення інформації, залишеної користувачами після роботи ЕОМ, обстежує робочі місця програмістів у пошуках чорнових записів, роздруківок, ділового листування (так зване «прибирання сміття») або здійснює перегляд і відновлення стертих програм.

Проте такий спосіб на сьогодні менш поширений з огляду на те, що комп'ютерну інформацію легше перехопити при її передаванні телекомунікаційними каналами й комп'ютерними мережами, ніж при безпосередньому проникненні в приміщення[1].

При реалізації способів опосередкованого (віддаленого) доступу до комп'ютерної інформації відбувається вмикання до лінії зв'язку законного користувача (наприклад, до телефонної лінії) і одержання тим самим доступу до його системи; проникнення в чужі інформаційні мережі способом автоматичного перебору абонентських номерів з дальшим з'єднанням з певним комп'ютером. Перебір здійснюється доти, аж доки на іншому кінці лінії не «озветься» чужий комп'ютер. Вельми важливими при вирішенні питання про реєстрацію в ЄРДР та початок досудового розслідування[2] є пояснення співробітників (персоналу) організації-жертви: адміністраторів мережі, інженерів-програмістів, розробників програмного забезпечення та осіб, які його обслуговують, операторів, спеціалістів, які здійснюють експлуатацію та ремонт комп'ютерного обладнання, системних програмістів, інженерів засобів зв'язку й телекомунікаційного обладнання, спеціалістів з інформаційної безпеки та інших.

Що ж до отримання пояснень від заявника та інших осіб, які мають стосунок до події злочину, то під час безпосереднього спілкування з ними треба з'ясовувати обставини, що могли передувати вчиненню вказаного кримінального правопорушення (для встановлення

[1] Європіна І. В. Особливості порушення кримінальних справ про комп'ютерні злочини. *Адвокат*. 2011. № 3 (126). С. 36.

[2] Про затвердження Положення про порядок ведення Єдиного реєстру досудових розслідувань : наказ ГПУ України від 06.04.2016 № 139.

кола підозрюваних), події про виявлення цього факту (його ознак, способів і засобів, негативних наслідків), наявність і стан функціонування системи інформаційного захисту, її недоліки, інші причини й умови, які могли бути задіяні для вчинення протиправних діянь.

Типовий перелік запитань, відповіді на які потрібно отримати під час відібрання пояснень:

– чи не було розкрадань носіїв інформації;

– чи не чинив будь-хто із числа тих, хто працює, необґрунтованих маніпуляцій з інформацією;

– чи не було порушень заданого режиму функціонування комп'ютерних систем, мереж, комп'ютерів або іншого обладнання;

– чи не було випадків спрацювання засобів захисту комп'ютерних систем, мереж, обладнання та інформації, котра в них оброблюється;

– чи не з'являлися в приміщенні, де розташовані технічне устаткування, ЕОМ, інші засоби комп'ютерної техніки та носії інформації, сторонні особи (радіотелемеханік, зв'язківець, працівники позавідомчої охорони, санепідемстанції, енергонагляду тощо);

– чи не було порушень правил ведення журналів обліку часу роботи комп'ютерних систем, мереж, обладнання;

– чи не виявляв будь-хто інтерес до інформації, яка не належить до його безпосередньої діяльності? Що відомо про вчинений злочин, підозрюваних осіб, підготування злочину, з яких джерел виходить ця поінформованість? Яка інформація зазнала впливу, її призначення та зміст;

– які розміри збитку від впливу на інформацію та які наслідки, що можуть спричинити шкідливі для ЕОМ, системи ЕОМ та їх мережі програми й технічні засоби?

У випадках, коли персонал організації-жертви (зазвичай співробітники служби безпеки) самостійно провів перевірку зі встановлення осіб, причетних до злочину, та окреслив коло підозрюваних осіб, під час первинної перевірки проводиться комплекс заходів щодо виявлення підозрюваної особи (групи осіб) і, якщо змога, затримання її з поличним (наприклад, у момент отримання в установі банку чи банкоматі викрадених грошових сум; або замовлених через Інтернет речей, придбаних на викрадені «електронні гроші» тощо). Інколи при затриманні вилучаються комп'ютерне обладнання, носії інформації, на яких містяться сліди вчиненого злочину; до того ж спеціалісти проводять лабораторне дослідження вмісту вилученого[1].

Крім того, у процесі попередньої перевірки за наявності повідомлення про комп'ютерний злочин можуть проводитись експрес-дослідження, які застосовуються для встановлення:

– ознак злочину;

– способу та місця здійснення неправомірного доступу (копіювання, модифікація, знищення інформації, унесення шкідливих програм; зсередини організації або ззовні) і його ознаки;

– засоби вчинення злочину (технічні, програмні, носії інформації); способи подолання захисту (підбір ключів і паролів, викрадання паролів, відмикання засобів захисту тощо)[2].

[1] Європіна І. В. Особливості порушення кримінальних справ про комп'ютерні злочини. *Адвокат*. 2011. № 3 (126). С. 36-37.

[2] Пашнєв Д. В., Рудик М. В. Особливості виявлення та кримінально-правова кваліфікація злочинів, що посягають на комп'ютерну інформацію з обмеженим доступом. *Ученые записки Таврического национального университета им. В. И. Вернадского*. Серия «Юридические науки». 2009. Т. 22 (61). № 1. С. 232.

Перевірка зібраних матеріалів перед реєстрацією злочину в ЄРДР проводиться в тісній взаємодії з особами, які здійснюють перевірку інформації про злочин, та фахівця, котрий повинен виявляти всі необхідні комп'ютерні сліди. Це пов'язано з ужиттям потрібних заходів щодо виявлення, вилучення, закріплення й дослідження слідів злочину, що є умовою його успішного розслідування та розкриття. Отже, метою такої взаємодії є негайне отримання орієнтувальної інформації від фахівця. Одержані дані використовують для висунення розшукових версій та визначення способів пошуку злочинця за «гарячими слідами», виявлення носіїв комп'ютерних слідів, які перебувають поза місцем події, з'ясування механізму та обставин учиненого злочину тощо[1].

Проведення перевірочних досліджень елементів комп'ютерних технологій у взаємодії зі слідчим або працівниками уповноважених оперативних підрозділів набуває великого значення при збиранні комп'ютерних слідів. Адже іноді неможливо без дослідження інформації на електронному носії виявити сліди вмикання з віддаленого доступу до комп'ютерної системи, під час яких було вчинено злочин, а також на їх основі прослідкувати мережний маршрут між елементами ЕОМ, що були засобом та предметом злочину, й зібрати всі сліди цього злочину на всіх точках маршруту.

У такому разі доцільно розпочати пошук слідів комп'ютерного злочину з виявлення мережних під'єднань засобів комп'ютерної техніки, що знаходяться на

[1] Пашнєв Д. В., Рудик М. В. Особливості виявлення та кримінально-правова кваліфікація злочинів, що посягають на комп'ютерну інформацію з обмеженим доступом. *Ученые записки Таврического национального университета им. В. И. Вернадского*. Серия «Юридические науки». 2009. Т. 22 (61). № 1. С. 232.

місці події і в яких виявлено сліди злочину, та дослідження інформації, пов'язаної з цими під'єднаннями. Після чого діяти так:

Ситуація 1. Якщо ЕОМ апаратно не під'єднано до мережі, або в інформації про мережні під'єднання відсутні ознаки, що вказують на віддалений доступ до неї під час учинення злочину, то, наймовірніше, ця ЕОМ є і предметом злочинного посягання, і засобом учинення злочину.

Ситуація 2. Якщо ЕОМ під'єднана до мережі й в інформації про мережні під'єднання наявні ознаки, що вказують на віддалений доступ до неї під час учинення злочину, то залежно від інформації, що міститься в записах під'єднань, слід визначити наступну точку пошуку слідів та діяти в ній згідно із ситуацією 1.

У результаті цього пошук може привести до ЕОМ, які є кінцевими точками маршруту. Усі сліди на точках маршруту фіксуються, при потребі досліджуються та вилучаються за допомогою фахівця.

Зауважимо, що в разі вчинення конкретного комп'ютерного злочину йтиметься про індивідуальну слідову картину. Але все ж таки можна виділити певну специфіку слідової картини цього виду комп'ютерних злочинів. Вона, в основному, буде характеризуватися наявністю на носії комп'ютерної інформації зловмисника файлів, які вміщують інформацію з обмеженим доступом, що стала предметом злочину, програмні й технічні засоби подолання захисту, отримання інформації в спосіб перехоплення активного чи пасивного, її декодування, а також іншого спеціального обладнання й програмного забезпечення для отримання комп'ютерної інформації та виготовлення її носіїв, розповсюдження й збуту: сканерів, цифрових фотоапаратів, принтерів, записувальних пристроїв для компакт-дисків, відповідних загото-

вок, чистих носіїв інформації, засобів під'єднання до мережі локальної й глобальної (Інтернет) тощо[1].

Дальшим істотним джерелом інформації про обставини, що свідчать про вчинення кримінального правопорушення, передбачених XVI розділом КК України, можуть бути матеріали оперативно-розшукової діяльності.

У визначеному контексті оперативно-розшукові справи (далі – ОРС) заводяться тільки стосовно осіб, щодо яких є дані про участь у підготовці до вчинення кримінального правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. За наявності достатніх даних про факт готування до вчинення цих злочинів начальник оперативного підрозділу звертається до начальника органу досудового розслідування про закріплення за цією ОРС слідчого для забезпечення методичного супроводження її реалізації та надання практичної допомоги. Після чого начальник оперативного підрозділу з дотриманням режиму таємності надає слідчому потрібні матеріали ОРС для вивчення та надання в разі потреби рекомендацій щодо фіксації додаткових фактичних даних про подію злочину, окремих осіб та злочинних угрупувань. У подальшому матеріали ОРС розглядають на оперативній нараді за участю начальників оперативного та слідчого підрозділів, а також працівників, які брали участь у їх підготовці, на якій визначають повноту зібраних матеріалів і приймають рі-

[1] Пашнєв Д. В., Рудик М. В. Особливості виявлення та кримінально-правова кваліфікація злочинів, що посягають на комп'ютерну інформацію з обмеженим доступом. *Ученые записки Таврического национального университета им. В. И. Вернадского*. Серия «Юридические науки». 2009. Т. 22 (61). № 1. С. 232-233.

шення про занесення відомостей про це правопорушення до ЄРДР[1].

Досудове розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку здійснюється слідчими, які спеціалізуються на розслідуванні кримінальних правопорушень зазначеного виду.

Матеріали оперативного підрозділу, у тому числі Департаменту кіберполіції Національної поліції України, його структурного підрозділу, який діє за міжрегіональним принципом, де зафіксовано фактичні дані про кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку, що направляються до слідчого підрозділу для початку та здійснення досудового розслідування, мають містити:

1) письмове пояснення заявника, в якому зафіксовані відомі заявнику дані про вчинення кримінального правопорушення з відповідними додатками, що містять відомості, які підтверджують його вчинення (роздруківки або скріншоти (програмне фотографування зображення з екрана монітора) вікон програм), а також у разі наявності документи, що підтверджують право власності потерпілого на комп'ютерну інформацію та інформацію, що передається мережами електрозв'язку, чи програмно-технічні засоби;

[1] Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07 липня 2017 року № 575.

2) установлені ідентифікаційні дані про використані електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі та мережі електрозв'язку (логін і пароль для доступу до мережі Інтернет, IP-адреса, WEB-адреса, номер абонента мережі електрозв'язку чи номер телефону, за допомогою яких було здійснено такий доступ, тощо).

Утворення СОГ за участю оперативних працівників Департаменту кіберполіції Національної поліції України, його структурних підрозділів, які діють за міжрегіональним принципом, для розслідування кримінальних правопорушень у сфері використання комп`ютерів, систем та комп`ютерних мереж і мереж електрозв`язку здійснюється за спільним наказом керівників органу досудового розслідування та Департаменту кіберполіції Національної поліції України. Утворення СОГ у кримінальному провадженні, досудове розслідування у якому здійснюється Головним слідчим управлінням Національної поліції України, здійснюється за наказом Голови Національної поліції України або за наказом заступника Голови Національної поліції України - начальника Головного слідчого управління, погодженим керівництвом Департаменту кіберполіції Національної поліції України. Старшим СОГ є слідчий, якого керівником органу досудового розслідування визначено здійснювати досудове розслідування кримінального правопорушення.

Керівник Департаменту кіберполіції Національної поліції України, його структурного підрозділу, який діє за міжрегіональним принципом, оперативний працівник якого включений до складу СОГ або за матеріалами якого розпочато кримінальне провадження, забезпечує взаємодію з органом досудового розслідування Національної поліції України, який здійснює розслідування

кримінальних правопорушень зазначеної категорії[1].

Заключним етапом усіх указаних ситуацій за наявності приводів і підстав, визначених у ст. 214 КПК України, є внесення відомостей про кримінальне правопорушення до ЄРДР. Наведена інформація має містити:

1) час та дату надходження заяви, повідомлення про кримінальне правопорушення або виявлення з іншого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення;

2) прізвище, ім'я, по батькові (найменування) потерпілого або заявника;

3) інше джерело, з якого виявлені обставини, що можуть свідчити про вчинення кримінального правопорушення;

4) короткий виклад обставин, що можуть свідчити про вчинення кримінального правопорушення, наведених потерпілим, заявником чи виявлених з іншого джерела;

5) попередню правову кваліфікацію кримінального правопорушення із зазначенням статті (частини статті) закону України про кримінальну відповідальність;

6) передачу матеріалів та відомостей іншому органу досудового розслідування або за місцем проведення досудового розслідування (частина п'ята статті 36, частина сьома статті 214, статті 216, 218 КПК України);

7) прізвище, ім'я, по батькові керівника прокуратури, органу досудового розслідування, слідчого, прокурора, який вніс відомості до Реєстру та розпочав досудове розслідування та/або здійснює досудове розслідування чи процесуальне керівництво;

[1] Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07 липня 2017 року № 575.

8) дату затримання особи;

9) обрання, зміну та скасування запобіжного заходу (статті 176–178, 200, 202, 492, 493, 508КПК України);

10) час та дату повідомлення про підозру, зміну повідомлення про підозру, особу, яку повідомлено про підозру, правову кваліфікацію кримінального правопорушення, у вчиненні якого підозрюється особа, із зазначенням статті (частини статті) закону України про кримінальну відповідальність (частина четверта статті 278, стаття 279 КПК України);

11) час та дату складання повідомлення про підозру, особу, стосовно якої складено повідомлення про підозру, правову кваліфікацію кримінального правопорушення, у вчиненні якого підозрюється особа, із зазначенням статті (частини статті) закону України про кримінальну відповідальність у разі неможливості повідомлення такій особі про підозру з об'єктивних причин (стаття 277 КПК України);

12) юридичну особу, щодо якої можуть застосовуватися заходи кримінально-правового характеру (частина восьма статті 214 КПК України)[1].

Після внесення відомостей до ЄРДР реєстратор проводить накладення електронного цифрового підпису. Використання електронного підпису здійснюється відповідно до Закону України «Про електронний цифровий підпис».

Формування Реєстру розпочинається з внесення до нього слідчим, прокурором відповідних відомостей про кримінальне правопорушення, зазначених у заяві чи повідомленні про його вчинення або виявлених ними самостійно з будь-якого джерела. Усні заяви заносить слідчий або прокурор до протоколу, який підписує заявник.

[1] Про затвердження Положення про порядок ведення Єдиного реєстру досудових розслідувань : наказ ГПУ України від 06.04.2016 № 139.

Відомості про кримінальне правопорушення, викладені в заяві, повідомленні чи виявлені з іншого джерела мають відповідати вимогам п. 4 ч. 5 ст. 214 Кримінального процесуального кодексу України, зокрема мати короткий виклад обставин, що можуть свідчити про вчинення кримінального правопорушення[1].

Особу, яка подає заяву чи повідомляє про кримінальне правопорушення, під розпис попереджають про кримінальну відповідальність за завідомо неправдиве повідомлення, крім випадків надходження заяви, повідомлення поштою або іншими засобами зв'язку.

Заява чи повідомлення про кримінальне правопорушення вважаються поданими з моменту попередження особи про кримінальну відповідальність (за винятком випадків, коли таке попередження неможливо зробити з об'єктивних причин: надходження заяви, повідомлення поштою, іншим засобом зв'язку).

Після внесення та перевірки цих даних керівником прокуратури або органу досудового розслідування в Реєстрі автоматично фіксується дата обліку інформації та присвоюється номер кримінального провадження.

Також до Реєстру підлягають унесенню відомості, що характеризують кримінальне правопорушення. Факт унесення цих відомостей відображається в Реєстрі та вони є доступними для перегляду прокуророві відповідного рівня.

При внесенні до Реєстру фабули кримінального правопорушення в обов'язковому порядку зазначається дата, час, адреса, місце, спосіб, знаряддя (комп'ютерна

[1] Кримінальний процесуальний Кодекс України від 13 квітня 2012 року № 4651-VI. URL : http://zakon3.rada.gov.ua/laws/show/4651-17 (дата звернення : 17.03.2018).

техніка, програмне забезпечення), засоби та інші особливості вчинення кримінального правопорушення, розмір збитків, прізвище фізичної особи (осіб) або дані про юридичну особу (осіб), яка є потерпілою, дані про осіб, які вчинили кримінальні правопорушення, інші потрібні відомості.

Із занесенням відомостей про вчинення кримінального правопорушення до ЄРДР, усі заяви й повідомлення, якщо вони надходили до чергової частини територіального органу поліції, негайно реєструє оперативний черговий відразу після їх надходження та вносить до Єдиного обліку, а також до інформаційної підсистеми «ФАКТ» – інтегрованої інформаційно-пошукової системи органів Національної поліції (ІП «ФАКТ» ІІПС).

РОЗДІЛ 5. ТИПОВІ СЛІДЧІ СИТУАЦІЇ, ВЕРСІЇ ТА ВІДПОВІДНИЙ ЇМ АЛГОРИТМ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПОЧАТКОВОГО ЕТАПУ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Слайди до розділу 5

Залежно від характеру вихідних даних при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку на початковому етапі розслідування можуть складатися різноманітні слідчі ситуації, які залежно від змісту вихідної інформації можна умовно поділити на дві групи.

Першу групу складають ситуації вчинення зазначеного виду злочинів в умовах так званої «очевидності», коли вихідна інформація містить дані про конкретну особу, яка вчинила кримінальне правопорушення[1]. Такими, зокрема, можуть бути:

1. Виявлено факт учинення злочину у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, способи його вчинення й приховування, свідки та матеріально фіксовані сліди; відомо, що злочин учинений групою осіб, одна з яких затримана на місці злочину в момент або безпосередньо після його вчинення, решта злочинців зникла з місця події або їхнє місцезнаходження невідоме; місцезнаходження частини викрадених грошових коштів відоме.

2. Виявлено факт учинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, відомі способи його вчинення й приховування, свідки та матеріально фіксовані сліди злочину, установлена особа злочинця, але він зник з місця вчинення

Відеокоментар до розділу 5

[1] Див.: Коваленко В. В., Анапольська А. І. Розслідування шахрайств та пов'язаних з ними злочинів, учинених у сфері функціонування електронних розрахунків : монографія / МВС України, ЛДУВС ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2013. С. 81.; Веліканов С. В. Класифікація слідчих ситуацій у криміналістичній методиці : дис. … канд. юрид. наук : 12.00.09. Харків, 2002. 204 с.

злочину, місцезнаходження викрадених грошових коштів невідоме.

3. Виявлено факт учинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, відомі способи його вчинення й приховування, установлені свідки та матеріально фіксовані сліди злочину, особа злочинця (злочинців), але її (їхні) дії завуальовані під вигляд законних фінансових операцій, місцезнаходження викрадених грошових коштів або їх частини відоме.

До другої групи належать ситуації вчинення комп'ютерних злочинів в умовах «неочевидності», коли вихідна інформація не містить даних про незаконне заволодіння грошовими коштами конкретною особою, відомий лише факт учинення злочину. Процес розслідування в цьому випадку утруднюється дефіцитом інформації передусім про особу злочинця та подію злочину; потребою одночасної перевірки багатьох слідчих версій та проведення значного обсягу слідчих (розшукових) та негласних слідчих (розшукових) дій для встановлення невідомих обставин. Прикладами названих ситуацій можуть бути такі:

1. Виявлено факт учинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, до того ж інформація про спосіб його вчинення й особу правопорушника відсутня, свідків не встановлено, матеріально фіксованих слідів не виявлено, місцезнаходження викрадених грошових коштів не встановлено.

2. Виявлено факт учинення злочинів у сфері використання електронно-обчислювальних машин (комп'юте-

рів), систем та комп'ютерних мереж і мереж електрозв'язку, є дані про спосіб його вчинення, установлені свідки, але немає матеріально фіксованих слідів учинення злочину та відомостей про особу злочинця.

З огляду на аналіз та оцінки наведених вище типових ситуацій висуваються різні версії, будуються ймовірні уявні моделі (гіпотези) розслідуваної події, засновані на конкретних матеріалах кримінального провадження, зокрема:

1) щодо співучасті злочинців висувають версії про те, що: а) мала місце змова злочинця зі співробітником підприємства, установи, організації; б) мала місце змова декількох осіб у межах підприємства, установи, організації; в) злочинець діяв одноосібно;

2) щодо взаємодії злочинців версії можуть бути такі: а) комп'ютерний злочин учинено групою осіб; б) кримінальне правопорушення вчинено одноосібно;

3) якщо злочинець переховується, можна висунути версії щодо його місцезнаходження: а) у друзів, знайомих; б) у будь-кого з далеких родичів; в) за місцем постійного проживання; г) у близьких родичів; д) виїхав за кордон; е) у колег по роботі, партнерів по бізнесу;

4) розшукові версії можна виділити залежно від місцезнаходження знарядь учинення злочину, інших речових доказів: а) за місцем роботи злочинця; б) за місцем проживання злочинця; в) у родичів, друзів, знайомих, партнерів по бізнесу; г) у гаражі, на складі, в інших підсобних та службових приміщеннях.

Зазначені переліки версій залежно від конкретної ситуації може бути доповнено або змінено. Проте всі вони мають бути перевірені слідчим паралельно.

Для слідчих ситуацій, що склалися в умовах «очевидності», характерний такий алгоритм слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій:

1) огляд місця події із залученням відповідних спеціалістів (спеціаліста-криміналіста, спеціаліста з банківської справи, спеціаліста з комп'ютерних технологій та інших);

2) особисті обшуки затриманих, їхніх робочих місць і місць проживання;

3) аудіо-, відеоконтроль особи, накладення арешту на кореспонденцію, огляд і виїмка кореспонденції, зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем як тих, що можуть надати істотну допомогу в розкритті зазначеного різновиду злочинів[1];

4) допит підозрюваних;

5) огляд документів, що засвідчують особу затриманих, а так само документів, що характеризують ті виробничі операції, у процесі яких допущено порушення та вчинено злочинні дії;

6) допит осіб, названих у документах, переданих до органів досудового розслідування, як тих, що вчинили злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

7) перевірка підозрюваних за обліками органів Національної поліції;

8) тимчасове вилучення:

– документів, що характеризують порядок та організацію роботи на підприємстві, в установі чи в організації

– місці виявлення слідів злочину;

[1] Див.: Гапотченко Г. М. Удосконалення кримінально-процесуальної діяльності щодо отримання та перевірки інформації про злочини. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* Спеціальний випуск у 2-х частинах. 2008. № 1. Ч. 2. С. 140.

– документів, що відображають роботу суб'єкта з комп'ютерною інформацією – журналу оператора ЕОМ, електронного журналу фіксації вчинених операцій, електронного реєстру з'єднань абонентів у зв'язку з ЕОМ або електрозв'язку;

9) допит осіб, причетних до відповідних електронних операцій або підозрюваних у зв'язках з особами, які вчинили злочинні дії;

10) аналіз одержаної інформації й вирішення питання про потребу клопотати перед слідчим суддею про залучення до кримінального провадження відповідного експерта, проведення ревізії, документальної або іншої перевірки, зокрема повторної (з яких позицій, за який період і за участю яких фахівців).

У вирішенні ситуацій, що склалися в умовах «неочевидності», зазвичай планують та проводять такі початкові слідчі (розшукові), негласні слідчі (розшукові) та інші процесуальні дії:

1) допит заявника й осіб, на яких указано в початковій інформації як на можливих свідків;

2) огляд місця події із залученням відповідних спеціалістів (спеціаліста-криміналіста, спеціаліста з банківської справи, спеціаліста з комп'ютерних технологій та інших);

3) тимчасове вилучення й дальший огляд засобів комп'ютерної техніки, предметів, матеріалів і документів (зокрема тих, що містяться в електронній формі на машинних носіях), які характеризують електронну операцію, під час якої за наявними даними вчинені злочинні дії;

4) вирішення питання про потребу клопотати перед слідчим суддею про залучення до кримінального провадження відповідної експертної установи або експерта для проведення комп'ютерно-технічних, бухгалтерських та інших експертиз;

5) вирішення питання про можливість установлення особи злочинців та затримання злочинця на місці злочину й потрібні з огляду на це заходи;

6) проведення негласних слідчих (розшукових) дій для виявлення осіб, винних у вчиненні злочину, а також слідів та інших речових доказів;

7) допити свідків (очевидців), установлених під час проведення розслідування;

8) допити підозрюваних (свідків), відповідальних за проведення операцій, пов'язаних з електронними розрахунками;

9) обшуки на робочих місцях і за місцем проживання підозрюваних[1].

Дальші дії слідчий планує з огляду на інформацію, одержану в процесі проведення вищевказаних слідчих (розшукових) та негласних слідчих (розшукових) дій.

Якщо під час розслідування зібрано достатню кількість доказів для складання обвинувального акта стосовно певної особи, таку ситуацію прийнято вважати сприятливою. У такому разі досудове розслідування визнається закінченим. У протилежному ж випадку ми отримуємо одну з проміжних ситуацій, яка, як і початкова, є вихідною для висування версій, планування розслідування, проведення слідчих (розшукових), негласних слідчих (розшукових) дій та оперативно-розшукових заходів.

[1] Див.: Коваленко В. В., Анапольська А. І. Розслідування шахрайств та пов'язаних з ними злочинів, учинених у сфері функціонування електронних розрахунків : монографія / МВС України, ЛДУВС ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2013. С. 85.

РОЗДІЛ 6. ТАКТИКА ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Слайди до розділу 6

Як свідчить аналіз слідчої та судової практик, найбільш типовими слідчими (розшуковими) діями при розслідуванні злочинів у сфері використання інформаційних технологій є огляд, обшук, допит та судова експертиза.

Огляд і обшук. Значення огляду та обшуку в кримінальному провадженні складно переоцінити. Вони дають змогу отримати первісну інформацію про подію, установити наявність ознак злочину, виявити сліди та речові докази тощо. Указані слідчі (розшукові) дії розглянемо сукупно, оскільки тактика їх проведення в кримінальних провадженнях щодо розслідування злочинів у сфері використання інформаційних технологій суттєво не різниться. Вибір між ними залежить від слідчої ситуації та

особливостей конкретного кримінального провадження. Зазвичай огляд проводять на підприємствах, в установах, організаціях щодо яких було вчинено злочин. Їхні керівники та відповідальні особи заінтересовані у виявленні злочинця та якнайшвидшому розслідуванні злочину, тому дають добровільну згоду на дослідження ЕОМ, місця, де вона розташована тощо. Якщо ж планують дослідження комп'ютерної техніки, що належить підозрюваному, то доцільно проводи обшук, оскільки відповідно до ч. 6 ст. 236 КПК України при його здійсненні дозволено примусове проникнення до приміщення. Такий обшук доречно проводити в межах тактичної операції, що охоплює затримання підозрюваного, обшук місця, де було розміщено комп'ютерну техніку, яку використовували для вчинення злочину, допит підозрюваного.

У процесі розслідування злочинів у сфері використання інформаційних технологій огляд (обшук) зазвичай проводять на місці:

– збереження й оброблення комп'ютерної інформації, яка зазнала злочинного впливу (наприклад, у разі незаконного втручання в роботу ЕОМ (комп'ютерів), їх систем чи комп'ютерних мереж);

Відеокоментар до розділу 6

– знаходження комп'ютерного обладнання, яке використовували при вчиненні злочину (у разі поширення комп'ютерного вірусу після незаконного проникнення в комп'ютерну мережу);

– збереження інформації, отриманої в злочинний спосіб (у разі заволодіння комп'ютерною інформацією через викрадення, привласнення, вимагання, шахрайство чи зловживання службовим становищем);

– порушення правил експлуатації ЕОМ, комп'ютерної системи або мережі;

– настання шкідливих наслідків (знищення, блокування, модифікації, копіювання комп'ютерної інформації, порушення роботи комп'ютера, комп'ютерної системи або мережі)[1].

Будь-яка слідча (розшукова) дія може стати результативною лише за умов її ретельної попередньої підготовки. Підготовка до огляду (обшуку) під час розслідування аналізованих злочинів складається з двох стадій.

На першій стадії підготовчого етапу (до виїзду на місце проведення огляду (обшуку), слідчому потрібно:

– з огляду на наявну інформацію про подію злочину визначити коло осіб, які візьмуть участь у слідчій (розшуковій) дії. Окрім учасників СОГ (слідчого, оперативного співробітника, спеціаліста-криміналіста), залучають спеціалістів у галузі комп'ютерних технологій, представників юридичних осіб або потерпілого.

У нескладних випадках, коли йдеться про один комп'ютер, що знаходиться у власності громадянина, підозрюваного у вчиненні злочину у сфері використання інформаційних технологій, слідчий може обмежитися залученням до участі у відповідній слідчій (розшуковій) дії спеціаліста-криміналіста. У такому разі комп'ютер доцільно ви-

[1] Див.: Тарасюк А. В. Актуальні питання тактики проведення окремих слідчих дій при розслідуванні комп'ютерних злочинів. *Інформаційна безпека людини, суспільства, держави.* 2011. № 3 (7). С. 66.

лучити, не проводячи з ним ніяких маніпуляцій, і направити на експертне дослідження для вирішення питань, які цікавлять слідство.

Якщо слідчу (розшукову) дію мають проводити в якійсь установі, організації чи підприємстві, треба мати на увазі, що комп'ютери можуть бути з'єднані в комп'ютерну мережу. Комп'ютерна мережа – це сукупність комп'ютерів, з'єднаних за допомогою каналів передавання даних та/або засобів комунікацій в єдину систему для обміну повідомленнями та доступу користувачів до програмних, технічних й інформаційних ресурсів мережі. Розрізняють локальні (зазвичай у межах одного підприємства чи установи) та глобальні (об'єднують комп'ютери і комп'ютерні мережі, розташовані на значній відстані один від одного). Для забезпечення функціонування мережі виділяють сервер (спеціальний комп'ютер) або кілька серверів, які містять основну (базову) інформацію.

Треба також ураховувати, що в комп'ютерах можуть бути спеціальні засоби захисту від несанкціонованого доступу, які, не отримавши у встановлений час спеціального коду, автоматично знищують усю інформацію або інші засоби захисту від несанкціонованого доступу. Це може призвести до втрати електронних доказів, які мають значення для справи. У загальному «електронні докази» – це сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв і в електронних засобах. Особливість цих доказів полягає в тому, що вони не можуть сприйматися безпосередньо, а мають бути інтерпретовані певним чином та проаналізовані за допомогою спеціальних технічних засобів і програмного забезпечення[1].

[1] Голубєв В. О. Проблеми розслідування комп'ютерних злочинів. *Правові проблеми боротьби зі злочинністю :* кн. 2. Харків : Східно-регіон. центр гуманіт. –освіт. ініціатив, 2002. С. 243.

У таких випадках є доцільним залучення до участі в слідчій (розшуковій) дії групи різнопрофільних спеціалістів у складі спеціаліста-криміналіста та спеціаліста в галузі комп'ютерних технологій. У разі потреби до цієї групи можна ввести також системного інженера, системного аналітика тощо. Якщо треба провести значний обсяг роботи, то до участі в таких слідчих (розшукових) діях доцільно залучити декількох спеціалістів у галузі комп'ютерних технологій, які разом зі спеціалістом-криміналістом під час виконання своїх обов'язків доповнюватимуть один одного, набуваючи додаткових навичок.

Основними завданнями спеціалістів у галузі комп'ютерних технологій при розслідуванні злочинів у сфері використання інформаційних технологій є:

– виконання всіх маніпуляцій з комп'ютерною технікою (умикання – вимикання, розбирання – збирання тощо); надання допомоги слідчому в описі комп'ютерної техніки та периферійного устаткування в протоколах слідчих (розшукових) дій; проведення експрес-аналізу комп'ютерної інформації; виявлення інформаційних слідів злочину; запобігання знищення чи ушкодження комп'ютерної інформації; вилучення комп'ютерної інформації тощо;

– залучення понятих. Як понятих доцільно запрошувати осіб, які володіють певним рівнем знань у галузі комп'ютерних технологій. Якщо такої змоги немає, то дії слідчого (спеціаліста) з дослідження ЕОМ чи комп'ютерної інформації треба детально пояснювати їм;

– підготування необхідної комп'ютерної техніки, обладнання та програмного забезпечення, що буде використовуватися для зчитування й збереження вилученої інформації. Зазвичай технічні засоби для застосування під час проведення відповідної слідчої (розшукової) дії

готують відповідні спеціалісти, проте слідчий має пересвідчитися в їх наявності та справності, оскільки саме він несе персональну відповідальність за повноту огляду (обшуку), належну фіксацію виявленої інформації;

– проведення інструктажу з учасниками огляду (обшуку), під час якого довести до їх відома мету та завдання проведення слідчої (розшукової) дії, роз'яснити їхні права та обов'язки. До того ж доцільно звернути увагу на необхідність вжиття заходів обережності під час перебування на місці огляду (обшуку).

Уже на цьому етапі починається спільна діяльність спеціаліста-криміналіста й спеціаліста в галузі комп'ютерних технологій. До того ж спеціаліст-криміналіст доповнить слідчого щодо питань про порядок і етапи проведення огляду (обшуку), про типові та нетипові ситуації, які можуть при цьому виникати, і про необхідні в таких випадках дії (особливо при спробах знищити комп'ютерну інформацію та інші сліди злочину). Спеціаліст у галузі комп'ютерних технологій пояснить, на яких носіях може знаходитися цікава для слідства інформація (лазерні компакт-диски, флеш-накопичувачі, знімні жорсткі диски тощо), як ці носії виглядають і які існують правила поводження з ними тощо.

З огляду на думку спеціалістів слідчий складає план проведення слідчої (розшукової) дії, у якому потрібно зазначити як кінцеві, так і проміжні цілі й завдання огляду (обшуку), дії кожного зі спеціалістів у вирішенні конкретних завдань, порядок і особливості застосування відповідних науково-технічних засобів. Варіанти дій спеціалістів мають бути передбачені з урахуванням типових ситуацій, які можуть складатися в процесі проведення слідчої (розшукової) дії (комп'ютери працюють

чи вимкнені, під'єднані до мережі чи ні тощо)[1].

На другій стадії підготовчого етапу (після прибуття на місце проведення огляду (обшуку) слідчому потрібно:

– вивести з місця проведення слідчої (розшукової) дії сторонніх осіб та забезпечити його охорону, зокрема ЕОМ, серверу, пунктів вимкнення живлення тощо;

– унеможливити стороннім особам користування технічними засобами, які можуть за допомогою бездротових технологій унести зміни або знищити інформацію;

– опитати потерпілого (заявника), свідків про те, що відбулось. Значну допомогу в цьому може надати спеціаліст у галузі комп'ютерних технологій. Він може з'ясувати, які використовуються паролі, коди доступу, що собою являє мережа, у яку з'єднані комп'ютери, де знаходиться сервер тощо. Серйозна увага в бесіді має бути звернена на встановлення типології (конфігурації з'єднання елементів комп'ютерної мережі). Від цього залежатиме вибір тактики огляду (обшуку).

Робочий етап огляду (обшуку) починається з фіксації обстановки, що склалася на момент проведення слідчої (розшукової) дії. Спеціаліст-криміналіст робить оглядову фотозйомку приміщення, яке оглядається, і комп'ютерного устаткування, що знаходиться в ньому. Після цього доцільно:

а) визначити, чи з'єднано комп'ютери, що розміщено в приміщенні, у локальну мережу. За наявності локальної комп'ютерної мережі найбільший інтерес являє центральний комп'ютер – сервер, на якому зберігається велика частина інформації й до якого мають доступ усі ЕОМ. Цей комп'ютер треба обстежувати більш ретельно

[1] Коваленко В. В. Застосування науково-технічних засобів спеціалістами при проведенні слідчих дій : монографія. Луганськ, 2007. С. 205-207.

й обережно;

б) установити, чи існують з'єднання комп'ютера з устаткуванням або обчислювальною технікою поза приміщенням, що оглядається. На це можуть указувати кабелі й проводи, що йдуть від комп'ютера до інших приміщень або будівель. Якщо комп'ютер під'єднаний до локальної мережі, спеціаліст у галузі комп'ютерних технологій має встановити кількість під'єднаних до сервера робочих станцій – комп'ютерів, вид зв'язку, кількість серверів у мережі; якщо можна, то організувати паралельний огляд з'єднаних у локальну мережу комп'ютерів. Якщо такої можливості немає, треба забезпечити їх зупинку та далі проводити огляд за схемою огляду комп'ютера, що не працює.

У процесі огляду (обшуку) можуть бути виявлені «дзеркальні» вінчестери, що знаходяться на значній відстані від основних. Зміст «дзеркального» вінчестера є точною копією основного. Найчастіше «дзеркальні» вінчестери встановлюють у фірмах, які використовують захист від несанкціонованого доступу. Якщо, приміром, був уведений неправильний пароль, то вся інформація, що знаходиться на основному вінчестері, автоматично знищується, але зберігається на «дзеркальному», який може знаходитися в іншому приміщенні, бути ретельно замаскованим і охоронятись;

в) визначити, чи запущено програми на ЕОМ і які саме. До того ж виконання основної частини технічної роботи покладено на спеціаліста в галузі комп'ютерних технологій, який визначає, яка програма виконується на початок проведення слідчої (розшукової) дії; після зупинки виконання програми здійснюють вихід в операційну систему для з'ясування, якщо можна, яку програму викликали востаннє; установлюють наявність у комп'ютера зовнішніх пристроїв віддаленого доступу

до системи (під'єднання до локальної мережі, наявність модему); комп'ютер від'єднують від мережі й вимикають модем; за потреби здійснюють копіювання програм та інформації на машинний носій.

Найпростішим і найзручнішим для слідчого є вилученням інформації разом із носієм. Проте відповідно до абзацу 2 ч. 1 ст. 159 КПК України тимчасовий доступ до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку має здійснюватися через зняття копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення, і це спеціально фіксується в протоколі огляду (обшуку).

Відповідно до ч. 2 ст. 168 КПК тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, здійснюють лише у разі, якщо вони безпосередньо зазначені в ухвалі суду.

Заборонено тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, або якщо такі об'єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення, а також якщо доступ до них обмежує їхній власник, володілець або утримувач.

У разі потреби слідчий чи прокурор здійснює копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста.

Усі зазначені дії спеціаліст-криміналіст має зафіксувати із застосуванням відеозапису, а слідчий – описати в протоколі.

Якщо комп'ютер не працює, то в протоколі слідчої (розшукової) дії фіксують місцезнаходження комп'ютера, який цікавить слідство, і його периферійних пристроїв, указують кожен пристрій (назва, серійний номер, комплектація: наявність і тип дисководів, мережевих карт, рознімань тощо), наявність з'єднання з локальною мережею і (чи) мережами, телекомунікації, стан пристроїв (зі слідами чи без слідів розкриття тощо). У цей час спеціаліст-криміналіст допомагає слідчому описати в протоколі порядок з'єднання між собою зазначених пристроїв, кількість сполучних рознімань, проводи, кабелі, а також порти, з якими кабель з'єднується; здійснюють пошук і фіксацію на комп'ютері та його пристроях, поблизу комп'ютерного устаткування й в інших місцях службового приміщення або на квартирі слідів пальців рук, мікрочастинок та інших предметів, знімних машинних носіїв інформації; паперових носіїв інформації – роздруківок, записів, записників, у яких можуть міститися паролі доступу тощо.

Після проведення дій щодо відшукання слідів пальців рук, мікрочастинок на знімних носіях інфорації, їх треба оглянути. Надання допомоги слідчому в огляді цих предметів доцільно доручити спеціалістові-криміналісту і спеціалістові в галузі комп’ютерних технологій. До того ж потрібно дотримуватися всіх вимог кримінального процесуального законодавства та правил експлуатації технічних засобів, щоб носій інформації, який оглядають, не втратив під час роботи з ним доказове значення; постаратися якнайповніше ознайомитися зі змістом файлів і отримати при цьому максимум інформації, яка цікавить.

Треба мати на увазі, що на пристроях запам'ятовування, які видаються на перший погляд чистими, може знаходитися прихована або знищена інформація. Такі файли можна спробувати відновити із застосуванням спеціальних програм.

На заключній стадії огляду (обшуку) за допомогою спеціаліста, ураховуючи дані про використання комп'ютера, треба визначити, які знаряддя злочину чи джерела доказів і які носії інформації потрібно вилучити (за умови, якщо про тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження безпосередньо зазначено в ухвалі суду). Вилучаються ті носії, які містять або з найбільшою ймовірністю можуть містити докази вчиненого злочину. Такими є: системні блоки комп'ютера, у яких установлені жорсткі диски (недоцільно вилучати жорсткі диски окремо від системного блоку), переносні комп'ютери «Ноутбук»; принтери (що мають плати пам'яті, у яких зберігаються завдання на друк), а також у разі потреби й інші компоненти комп'ютера; знімні машинні носії інформації.

Для підготовки до вилучення намічених апаратних засобів потрібно:

– завершити роботу комп'ютерної системи;

– вимкнути електроживлення;

– промаркувати пристрої комп'ютера перед тим, як від'єднати й вилучити;

– наклеїти липкі аркуші чи стрічки із зазначенням дати й підписами слідчого, спеціаліста, понятих і власника (користувача) цих апаратних засобів. Пристрої, з'єднані з одним центральним процесором, треба позначати одним номером. Кожен пристрій має мати наклейку в тих місцях, де приєднано кабелі;

– від'єднати всі кабелі, попередньо зафіксувавши їх положення (за допомогою фото- чи відеозйомки). Усі кабелі, що з'єднують пристрої комп'ютера, які вилучають, також маркують з обох кінців і вилучають. Липкою стрічкою з підписами учасників огляду (обшуку) пломбують всі наявні рознімання та кнопки для того, щоб унеможливити вмикання комп'ютера та його пристроїв без порушення пломбування;

– опломбувати корпус апаратного пристрою так, щоб унеможливити його розкриття;

– роз'єднати пристрої комп'ютера й упакувати окремо, із зазначенням на пакуванні знімних машинних носіїв місця їх виявлення. Роз'єднання треба починати з периферійних пристроїв.

Після огляду комп'ютерного устаткування спеціалісти нададуть допомогу слідчому в описі всіх виконаних дій та пакуванні вилучених об’єктів.

Допит. Однією з умов успішного допиту при розслідуванні будь-якого злочину є ретельна підготовка до його проведення. Приймаючи рішення про допит особи як свідка, потерпілого чи підозрюваного, слідчий має визначити, яку інформацію він має отримати від допитуваного. При плануванні допиту потрібно скласти орієнтовний перелік запитань, які будуть ставитися допитуваному.

У кримінальних провадженнях щодо розслідування злочинів у сфері використання інформаційних технологій під час допитів серед іншого необхідно з’ясовувати безліч технічних питань, тому до планування цієї слідчої (розшукової) дії доцільно залучити спеціаліста в галузі комп’ютерних технологій.

При допиті **свідків (потерпілих)** у кримінальних

провадженнях щодо розслідування зазначеного різновиду злочинів з'ясуванню підлягають такі типові обставини:

– чи не виявляв хто-небудь інтерес до комп'ютерної інформації, програмного забезпечення, комп'ютерної техніки цього підприємства, організації, установи, фірми або компанії;

– чи не з'являлися в приміщенні, де розташована комп'ютерна техніка, сторонні особи, чи не зафіксовано випадки роботи співробітників з інформацією, що не належить до їхньої компетенції;

– чи не було збоїв у роботі програм, викрадень носіїв інформації й окремих комп'ютерних пристроїв;

– чи зафіксовано збої в роботі комп'ютерного устаткування, електронних мереж, засобів захисту комп'ютерної інформації;

– хто зі співробітників працював у неробочий час, хто виявляв зацікавленість до інформації, що не стосується їхньої безпосередньої діяльності;

– чи зафіксовано останнім часом випадки спрацьовування засобів захисту комп'ютерної інформації;

– як часто перевіряють програми на наявність вірусів та які результати останніх перевірок;

– як часто поновлюють програмне забезпечення, у який спосіб це здійснюють;

– як здійснюють придбання комп'ютерної техніки, її ремонт і модернізацію;

– у який спосіб на підприємстві, в організації, установі або фірмі проводять роботу з інформацією, як вона надходить, обробляється й передається каналами зв'язку;

– хто ще є абонентом комп'ютерної мережі, до якої під'єднано комп'ютери цього підприємства, організації

чи установи, як здійснюють доступ у мережу, хто з користувачів має право на роботу в мережі, повноваження цих користувачів по роботі з інформацією;

– як здійснюють захист комп'ютерної інформації, які застосовують засоби й методи захисту тощо[1].

Допит підозрюваного. Під час допиту підозрюваних у кримінальних провадженнях щодо розслідування злочинів у сфері використання інформаційних технологій з'ясуванню підлягають такі типові обставини:

– освіта, місце роботи, посада, стаж роботи на посаді, рівень кваліфікації;

– до якої комп'ютерної інформації та до якого програмного забезпечення має доступ;

– коли (дата та час), у який спосіб, із використанням яких технічних засобів та із використанням якого програмного забезпечення здійснив неправомірний доступ до комп'ютерної інформації;

– з якого джерела або від кого конкретно та коли дізнався про зміст інформації, до якої здійснив неправомірний доступ;

– яким способом, із використнням яких програмних засобів «зламав» пароль доступу до інформації, або із якого джерела (від кого) дізнався пароль;

– з якою метою здійснив неправомірний доступ до комп'ютерної інформації, та в який спосіб скористовля нею тощо[2].

З огляду на специфіку розслідування злочинів у сфері використання інформаційних технологій, потребу з'ясування складних технічних питань, використання спеціальної термінології бажаною є участь спеціаліста в

[1] Голубєв В.О. Розслідування комп'ютерних злочинів :монографія. Запоріжжя : ЗІДМУ, 2003. С. 129–130.

[2] Більш детально див.: Розслідування комп'ютерних злочинів :монографія. Запоріжжя : ЗІДМУ, 2003. С. 140-142.

галузі комп'ютерних технологій не лише в плануванні допиту, а й безпоседньо у проведенні цієї слідчої (розшукової) дії. Відповідно до ч. 4 ст. 71 КПК України спеціаліст має право ставити запитання, звертати увагу на певні обставини тощо. Така участь спеціаліста надасть слідчому реальну допомогу в отриманні повної та всебічної інформації про обставини злочину й причетних до нього осіб.

Судова експертиза

Тести до розділів 3-6

Експертиза комп'ютерної техніки і програмних продуктів. Відповідно до Інструкції про призначення та проведення судових експертиз й експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень, затверджених Наказом МЮ України від 08.10.1998 № 53/5[1], до основних завдань експертизи комп'ютерної техніки й програмних продуктів належать:

а) установлення робочого стану комп'ютерно-технічних засобів;

[1] Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 08.10.1998 № 53/5. URL : http://zakon4.rada.gov.ua/ laws/show/z0705-98

б) установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;

в) виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;

г) установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку тощо.

Орієнтовний перелік вирішуваних питань:

– чи є на цьому носії інформація щодо (зазначити, яка інформація цікавить) і в якому вигляді;

– чи містить носій досліджуваного комп'ютера інформацію про певні (зазначити, які саме) дії користувача;

– чи піддавався досліджуваний накопичувач певним процедурам для знищення інформації;

– чи могло бути створено зазначену інформацію на цьому комп'ютері чи перенесено з іншого носія;

– у який спосіб інформацію (зазначити, яка саме) перенесено до досліджуваного комп'ютера (носія);

– яка технологія та хронологія створення електронного документа (зазначити електронний документ та певний зміст);

– які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію стосовно... (зазначити зміст);

– чи містить накопичувач інформації досліджуваного комп'ютера певне (зазначити, яке саме – установлене, не встановлене) програмне забезпечення;

– які функціональні несправності має це комп'ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання загалом;

– чи можливе виконання певних дій за допомогою цього програмного продукту;

– чи можливе вирішення певного завдання за допомогою цього програмного продукту;

– чи реалізовано в цьому програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?

Об'єктами комп'ютерно-технічної експертизи є:

– зібрані комп'ютери, їх системні блоки;

– периферійні пристрої (монітори, принтери, дисководи, модеми, сканери, клавіатури, маніпулятори тощо), комунікаційні прилади комп'ютерів та обчислювальних мереж;

– магнітні носії інформації (жорсткі диски й флопі-диски, оптичні диски);

– роздруківка програмних і текстових файлів;

– словники пошукових ознак систем (тезауруси), класифікатори та інша технічна документація, наприклад, технічні завдання і звіти;

– планшетні комп'ютери, смартфони, комунікатори, мобільні телефони, мр-3 програвачі, інші електронні носії текстової або цифрової інформації, технічна документація до них;

– пристрої, що не є комп'ютерами в класичному розумінні – електронні касові апарати, гральні автомати, карт-рідери тощо.

Для дослідження інформації, що міститься на комп'ютерних носіях, експертові надають комп'ютерний носій, а за потреби комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій).

Щоб зберегти інформацію в робочому стані, її носії надають в окремих пакуваннях. Системні блоки персональних комп'ютерів надають в пакуваннях, що унеможливлюють доступ до носіїв інформації безпосередньо чи під'єднання системного блока до мережі живлення.

Для встановлення відповідності програмних продуктів певним параметрам експертові надають носій з копією досліджуваного програмного продукту або програмного коду.

Для дослідження робочого стану комп'ютерно-технічних засобів експертові надають ці комп'ютерно-технічні засоби, а також технічну документацію до них.

У кримінальних провадженнях з цієї категорії злочинів можуть призначати й інші експертизи: *трасологічну*; *дактилоскопічну*; с*удово-економічні (фінансово-економічну й бухгалтерську); техніко-криміналістичну експертизу документів; фоноскопічну тощо.*

Практичний приклад. *Цю частину розділу підготували працівники Кіберполіції. Вона являє собою стислий опис основних проблемних аспектів, з якими стикаються правоохоронці під час досудового розслідування конкретного злочину. Також наводимо QR-код з посиланням на вирок у цій справі.*

Посилання на обвинувальний вирок за підсумками судового розгляду цієї справи

У нашому випадку був виявлений користувач хакерського форуму, який продавав прихований майнер. Згодом він виклав його безкоштовно, об'єднавши до того ж цей файл з іншим шкідливим файлом (тобто всі, хто хотіли завантажити безкоштовно прихований майнер, щоб заразити ним інших, самі ставали жертвами). Для документування цього факту було проведено огляди веб-сторінок сайтів з документуванням гаманців, email адрес, номерів телефону, ніків згаданого хакера. Викладений ним безкоштовно

файл було завантажено під час огляду, записано на диск і відправлено на експертизу.

Закупівлю зробив свідок як інтернет-провайдер для захисту власних користувачів (клієнтів), щоб упевнитися в тому, що ця людина дійсно продає шкідливе програмне забезпечення. Гроші за придбання вірусу свідок переказав на картковий рахунок близької родички хакера. Чек і сам вірус, а також листування з хакером у скайпі провайдер надав оперативним співробітникам під час допиту.

Далі був проведений обшук за місцем проживання хакера, під час якого було встановлено наявність його персонального комп'ютера. Під час огляду комп'ютера перевіряли кожен текстовий документ і щодо кожного файлу ставилися запитання хакерові. У підсумку був знайдений один із файлів, який містив посилання на канал YouTube з трьома відео. Сам хакер пояснив, що канал створив він, і під кожним з відео розмістив файли, які є шкідливими, уточнивши, що розмістив їх саме для зараження інших користувачів. Усі вилучені під час обшуку предмети (комп'ютер, флешка) було відправлено на КТЕ в ДЕНДКЦ у м. Київ.

Звернемо увагу на кілька важливих моментів щодо призначення комп'ютерно-технічної експертизи. Перед призначенням експертизи потрібно отримати консультацію спеціаліста для якомога точнішого визначення предмета дослідження. Не можна надсилати носій, наприклад, вінчестер, який може містити тисячі виконувальних файлів і ставити запитання на кшталт: «Чи є серед виконувальних файлів на представленому носії шкідливе програмне забезпечення?». Таке запитання неминуче призведе до затягування строків проведення експертизи.

До того ж для встановлення специфічних ознак предмета злочину, що описується в ч.1 ст. 361-1 КК України, експертові треба сформулювати питання щодо функціонального призначення певних файлів. Зокрема, на експертизу надсилалися два DVD диски й комп'ютер. Нижче наведено запитання, які ставили експертові:

1. Чи є на DVD-R диску (диск № 1, сейф-пакунок № 3969647) для лазерних систем зчитування серед наявних файли, які антивірусне програмне забезпечення визначає як «шкідливі»? Якщо так, то яке їх основне функціональне призначення?

2. Чи є на DVD-R диску (диск № 2, сейф-пакунок № 3969636) для лазерних систем зчитування серед наявних файли, які антивірусне програмне забезпечення визначає як «шкідливі»? Якщо так, то яке їх основне функціональне призначення?

3. У разі, якщо на диску № 1 (сейф-пакунок № 3969647) та диску № 2 (сейф-пакунок № 3969636) виявлено програмне забезпечення, що визначається антивірусним програмним забезпеченням як «шкідливе», то просимо повідомити, до яких дій під час запуску та подальшої роботи вони призводять?

4. Чи містяться на жорсткому диску наданого на дослідження ноутбуку серед наявних файли з такими ключовими словами: «4149 4978 6501 8263», «380506943477», «1652si7FTmWQkweNZWivPexNPiT3kSW2kW», «xmr.pool.minergate.com:45560», «igor.davydenko.2013@mail.ru»? Якщо так, то просимо скопіювати виявлені дані на оптичний диск.

5. Чи міститься на наданому на дослідження технічному пристрої історія обміну електронними повідомленнями в програмах Viber, Skype, Telegram? Якщо так, то просимо скопіювати виявлені дані на оптичний диск.

6. Який вміст файлів архівів «builder.rar», «RCC v1.3.rar», «Аватария.rar», що знаходяться на робочому столі облікового запису в операційній системі «Microsoft Windows» у папці з назвою «ютуб» на жорсткому диску наданого для дослідження ноутбуку (пароль для розархівування «Sliv»), а також файлів, наданих на дослідження на DVD-R дисках для лазерних систем зчитування, які мають назву «podv.rar» (диск № 2, сейф-пакунок № 3969636, пароль для розархівування «12345») та «Билдер.rar» (Диск № 1, сейф-пакунок № 3969647, пароль для розархівування «hh»)?

7. Чи є в заархівованих контейнерах «builder.rar», «Аватария.rar» серед наявних файли, які антивірусне програмне забезпечення визначає як «шкідливі»? Якщо так, то яке їх основне функціональне призначення?

8. Які дії будуть виконані, якщо запустити файл, який міститься в архіві «RCC v1.3.rar», та чи є цей файл шкідливим програмним забезпеченням?

9. Чи є серед вмісту виконувальних файлів (файли типу «.exe»»), які були розархівовані з файлів «builder.rar», «RCC v1.3.rar», «Аватария.rar», файли типу «.exe», «.bat» «.cmd», «.vbs», ідентичні файлам серед вмісту виконувальних файлів, які були розархівовані з файлів «podv.rar», «Билдер.rar» на DVD-R дисках для лазерних систем зчитування?

Висновки експертизи

Окремо звернемо увагу на те, що стаття 361-1 КК України передбачає відповідальність за посягання, що за

ступенем тяжкості належать до злочинів невеликої тяжкості (ч.1 ст. 361-1) та середньої тяжкості (ч. 2 ст. 361-1 КК). Тому маємо відомі процесуальні обмеження у використанні НСРД, що є типовими для злочинів, пов'язаних із збутом певних об'єктів. У нашому випадку вихід було знайдено в спосіб допиту провайдера, який для виконання завдань інформаційної безпеки своїх клієнтів придбав шкідливе програмне забезпечення. Безсумнівно, наш випадок є локальним розв'язанням проблеми та лише підкреслює актуальність унесення змін до законодавства в частині скасування залежності можливості проведення НСРД під час розслідування злочинів, пов'язаних з використанням інформаційних технологій.

ЗАМІСТЬ ПІСЛЯМОВИ

У посібнику зроблено спробу представити основні питання кримінально-правового та криміналістичного забезпечення протидії злочинам у сфері використання інформаційних технологій. Деякі аспекти проблеми не розглянуто або розглянуто не досить детально. Упевнені, що за час підготовки праці до друку з'явилися нові способи вчинення «комп'ютерних злочинів». Ці посягання змінюються кількісно та якісно. Виникають принципово нові проблеми, пов'язані з автономними транспортними засобами, штучним інтелектом, розвитком технологій імплантів тощо. Обстановка протидії злочинам у сфері використання інформаційних технологій постійно та динамічно змінюється.

Ваша думка важлива!

В означених умовах виникають нові вимоги до якості та оперативності професійної комунікації. Пропонуємо всім небайдужим долучатися до обговорення кримінально-правових і криміналістичних проблем протидії ІТ-злочинності на форумі нашого посібника.

Запрошуємо до спілкування!

ЗМІСТ

Навчальне видання

Карчевський Микола Віталійович
Коваленко Володимир Вітокрович
Комлєв Віктор Євгенович
Мартиш Олександр Юрійович
Невгад Віталій Вікторович
Токарев Олексій Олексійович
Усманов Руслан Абдішекурович
Чубаєвський Віталій Іванович
Яковенко Микола Олексійович

Протидія злочинам у сфері використання інформаційних технологій

Інтегрований навчально-практичний посібник

За редакцією авторів.
Технічний редактор *А. С. Кудінов*
Комп'ютерне верстання *А. С. Кудінов*
Підписано до друку 20.12.2018.
Формат 60х84 1/16 Ум. друк. арк. 10,4.
Тираж 300 прим. Зам. № 20/12.

Адреса редакції та видавця:
Луганський державний університет внутрішніх справ імені Е.О. Дідоренка,
вул. Донецька, 1, м. Сєвєродонецьк, Луганська область, Україна, 93401;
тел. (06452) 9-07-77; адреса електронної пошти: oonr_lduvs@meta.ua;
сайт: http://lduvs.edu.ua

Виготовлено згідно з наданим оригінал-макетом:
ФОП Пронькіна Катерина Володимирівна
вул. Гущенка, 14, м. Лисичанськ, Луганська обл., 93100
Свідоцтво В03 № 959630 від 25.12.2009