Розділ V. ПРОБЛЕМИ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ ТА ПРАВООХОРОННА ДІЯЛЬНІСТЬ ОРГАНІВ ВНУТРІШНІХ СПРАВ

УДК 343.98

Г.К. Авдєєва

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У БОРОТЬБІ З КОМП'ЮТЕРНОЮ ЗЛОЧИННІСТЮ

Статтю присвячено питанням використання спеціальних знань у боротьбі з найбільш поширеними видами комп'ютерних злочинів і способам виявлення їх слідів. Наведено приклади успішного розслідування шахрайства завдяки огляду електронного листування злочинців та SMS-повідомлень. Проаналізовано сліди комп'ютерних злочинів у вигляді результатів роботи антивірусних і тестових програм. Запропоновано способи виявлення слідів несанкціонованого доступу до роботи електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж і баз даних.

Ключові слова: *спеціальні знання, комп'ютерні злочини, сліди злочину, інформаційні технології*

Постановка проблеми. На сучасному етапі розвитку суспільство стає все більше залежним від роботи комп'ютерних систем для автоматичної обробки інформації. Це стосується різних сфер діяльності людини. Усі найважливіші функції, так чи інакше, здійснюються з використанням комп'ютерів, автоматизованих систем та комп'ютерних мереж [1].

Завдяки динамічному розвитку комп'ютерних систем з'являються нові можливості для вчинення невідомих раніше правопорушень, а також традиційних злочинів з використанням інформаційних технологій. Щороку збільшуються їх кількість та суспільна небезпека [2]. Це зумовлено постійним і стрімким розширенням сфери застосування інформаційних технологій в усіх галузях діяльності людини.

Злочини у сфері використання електронно-обчислювальних засобів, телекомунікаційних систем і комп'ютерних мереж (ст. ст. 361–363 розділу 16 Кримінального кодексу України) розподіляються на такі види: 1) несанкціонований доступ до роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, баз даних; 2) створення з метою використання, поширення або збуту шкідливих програмних продуктів або технічних засобів, а також їх розповсюдження або збут; 3) несанкціонований збут або поширення інформації з обме-

женим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; 4) злочини, що здійснені шляхом використання комп'ютерної системи як засобу досягнення злочинної мети тощо.

Комп'ютерна злочинність – це особливий вид злочинів, пов'язаних із незаконним використанням сучасних інформаційних технологій і засобів комп'ютерної техніки. [1] Однією з характерних особливостей цього виду злочинів є їхня латентність, спричинена небажанням користувачів мережі інформувати про такі злочини через недовіру до потенційних можливостей правоохоронних органів, а також небажанням публічно визнати слабкі місця у власних системах безпеки. Тому боротьба з ними вимагає використання адекватних засобів протидії, інтенсивного впровадження інновацій у роботу правоохоронних органів та найбільш широкого використання спеціальних знань для своєчасного їх виявлення, кваліфікованого розслідування й профілактики.

Аналіз останніх досліджень і публікацій. Питанням дослідження проблем використання спеціальних знань у боротьбі зі злочинами у сфері використання інформаційних технологій учені-криміналісти (О.Р Росинська, В.О. Мещеряков, В.Б. Вехов , В.О. Голубєв, І.Ю. Михайлов , А.І. Усов, В.Ю. Шепітько та ін.) приділяють значну увагу останні два десятиліття, однак у звязку зі стрімким розвитком інформаційних технологій і швидкими змінами поколінь комп`ютерної техніки та програмного забезпечення існує нагальна потреба в подальшому дослідженні цього напряму для уточнення окремих наукових положень, зокрема– виокремлення специфічних слідів комп`ютерних злочинів та розроблення способів їх виявлення з використанням спеціальних знань.

У науках кримінально-процесуального циклу термін «слід» вживається в двох значеннях – процесуальному і криміналістичному. Процесуальне значення сліду полягає в тому, що інформація, одержана за його допомогою, використовується для формування доказової бази за кримінальним провадженням і знаходить своє відображення в процесуальних документах. Криміналістичне розуміння сліду більш широке й охоплює всю сукупність одержаної інформації, яка використовується для здійснення розшукових дій, висунення пошукових та інших версій, визначення напряму дій слідчого [4].

Аналіз останніх досліджень і публікацій показав, що існуюча в криміналістиці традиційна класифікація слідів практично не охоплює сліди нових видів злочинів (зокрема – у сфері використання інформаційних технологій). Це пояснюється специфікою таких слідів та зумовлює актуальність дослідження слідів комп'ютерних злочинів з використанням спеціальних знань.

Формування цілей. Метою статті є розкриття можливостей використання спеціальних знань у боротьбі з комп'ютерною злочинністю, особливо – під час виявлення та дослідження слідів комп'ютерних злочинів.

Виклад основного матеріалу. Важливу роль у формуванні слідової картини злочинів у сфері інформаційних технологій відіграють способи вчинення злочинів цієї категорії.

Одним із способів вчинення комп'ютерного злочину є використання із злочинною метою шкідливих програмних продуктів. Заражені «комп'ютери-жертви» без згоди на це їх власників стають учасниками botnet-мереж [5]. Крадіжка особистих персональних і комерційних авторизаційних даних користувачів, конфіденційної інформації, ключів захисту, використання апаратного ресурсу «комп'ютера-жертви» з подальшою можливістю проведення DDoS-атак [6], несанкціонованої розсилки повідомлень і виконання «брехливих» транзакцій [7] є найбільш поширеними правопорушеннями в банківській сфері України. На сьогодні в усьому світі кількість злочинів з використанням телекомунікаційних мереж і мережевих технологій (кіберзлочинність) складає 30–40% від загальної кількості злочинів. Метою зловмисників є заволодіння «великими» грошима, протизаконне отримання яких не потребує безпосередньої участі правопорушника.

На сьогодні в мережі Інтернет розміщені пропозиції хакерів [8] про можливе здійснення DDoS-атак «на замовлення», вказано певні розцінки на цей вид «послуг». Співробітники Служби безпеки України 25 травня 2014 року під час позачергових виборів Президента України в Києві затримали групу таких хакерів, які мали намір за допомогою спеціалізованого обладнання фальсифікувати результати виборів [9].

Термін «злочини, що здійснюються з використанням комп'ютерних технологій» охоплює всі дії, що передбачають використання досягнень цих технологій і ті, які зазіхають на комп'ютерну інформацію. У криміналістичному аспекті таке визначення дозволило розробити типові прийоми, засоби і методи виявлення, фіксації та дослідження комп'ютерної інформації з використанням спеціальних знань.

Одним з найважливіших визначальних чинників у боротьбі з такими злочинами є галузь їх здійснення – кіберпростір. Кіберпростором називають сферу існування комп'ютерної інформації, що утворена сукупністю засобів комп'ютерної техніки. Комп'ютерна інформація [10] залежно від характеру злочинних діянь виступає як предмет посягання і як галузь можливого збереження слідів злочинної діяльності.

Специфічними властивостями комп'ютерної інформації є такі: 1) відсутність нерозривного зв'язку з матеріальним носієм; 2) динамічність, можливість миттєвого перенесення в просторі (у тому числі з однієї частини земної кулі в іншу); 3) можливість зміни і знищення інформації будь-якого об'єму за короткі проміжки часу (зокрема – за допомогою видаленого доступу) [11]; 4) складність застосування в розслідуванні кіберзлочинів «традиційних» методів та засобів.

Крім того, оригінал і всі копії комп'ютерної інформації (незалежно від виду носія) є ідентичними.

Комп'ютерна інформація як джерело доказу є новим об'єктом криміналістичного дослідження, а тому її аналіз потребує використання спеціальних знань. Вивчення кримінальних проваджень з розслідування комп'ютерних злочинів показав, що до проведення огляду, допиту, залучення експерта та ін. слідчих дій у більшості випадків залучається спеціаліст, який під час слідчої дії надає допомогу слідчому, роз'яснюючи останньому питання, що містять відомості технічного характеру.

На сьогодні з використанням спеціальних знань розроблена значна кількість ефективних сучасних засобів пошуку (відновлення) знищеної електронної інформації. Практика показує, що якнайповніше доказову базу можна сформувати, залучаючи фахівців у галузі інформаційних технологій, які постійно використовують у своїй повсякденній діяльності новітні програмні засоби. Зокрема, судовими експертами України на сьогодні використовуються такі сучасні програмні продукти, як X-Ways Forensics, EnCase Forensics, FTK, AccessData Forensic Toolkit, Forensic Disk Decryptor, MailPro, FileLister та ін.

Сліди злочинів у сфері використання інформаційних технологій утворюються за результатами зовнішнього доступу до комп'ютерної інформації, що викликає певні зміни, пов'язані з подією злочину. Такими змінами можуть бути сліди знищення, модифікації, копіювання інформації, блокування інформаційної системи. Сліди змін залишаються на машинних носіях інформації і відображають зміни в інформації, яка в них зберігається (порівняно з попереднім станом). Часто злочинці здійснюють модифікації баз даних, програм, текстових файлів, що містяться на стаціонарних і змінних носіях інформації, призначених для багаторазового її перезапису. Інформація може зберегти сліди її часткового знищення або модифікації (видалення з каталогів імен файлів, видалення або додавання окремих записів, фізичного руйнування або розмагнічування носіїв тощо). Інформаційними слідами є також результати роботи антивірусних і тестових програм. Такі сліди можуть бути виявлені при експертному дослідженні комп'ютерного обладнання, протоколів роботи операційних систем, додатків, антивірусних програм, програмного коду тощо.

Сліди неправомірного доступу до інформації можна виявити в мережі Інтернет, а згодом, виходячи з їх ознак – встановити вихідне підключення і технічний засіб, з якого здійснювалося правопорушення. Найменування й адреса інтернет-провайдера [12], за допомогою якого правопорушник підключений до мережі Інтернет, можна вільно отримати через спеціальну службу Whois (у мережі Інтернет). У загальнодоступному режимі за адресою www.ripe.net у будь-який час можна отримати електронну адресу (IP) «атакуючого» комп'ютера. Час роботи користувача в мережі можна встано-

вити за спеціальним log-файлом (журналом). Додаткові відомості про вид, порядок і час підключень користувача до мережі Інтернет і збіг цих даних з log-файлом провайдера може слугувати вагомим доказом несанкціонованого доступу в певну комп'ютерну систему.

Сліди несанкціонованого доступу до інформації містяться в журналах операційних систем і окремих програмних продуктів, які створюють резервні копії файлів і файли-звіти, зберігають інформацію про останні проведені операції та виконані програми, а також містять іншу інформацію, що має значення для розслідування злочину. Слідами, які вказують на сторонній доступ до комп'ютерної інформації, можуть слугувати такі: перейменування каталогів і файлів, зміна розмірів і вмісту файлів, їх атрибутів, поява нових каталогів, файлів, зміна часу останнього доступу до інформації, її модифікація тощо.

Певну інформаційну цінність мають SMS [13] – повідомлення, що автоматично фіксуються і накопичуються на сервері мобільного оператора. Співробітники правоохоронних органів мають можливість отримати в оператора мобільного зв'язку роздрук переліку телефонних дзвінків на певний телефонний номер і текстів SMS -повідомлень.

У 2006 році вивчення і аналіз текстів SMS-повідомлень дозволили слідчим МВС Запорізької області знешкодити організовану злочинну групу, яка в Харкові, Києві, Запоріжжі та інших містах України за допомогою різних шахрайських дій і «театральних вистав» шантажувала багатих людей і протягом декількох років отримувала від них величезні суми грошових коштів. Злочинна група імітувала дорожньо-транспортні події, убивства з необережності, тяжкі тілесні ушкодження, провокувала осіб на статеві зносини з особами, які не досягли статевої зрілості тощо. Окремі члени злочинної групи виконували роль «трупів», інші – співробітників правоохоронних органів. Організація кожного нового злочину супроводжувалася зміною номерів мобільних телефонів кожного члена злочинної групи. Учасникам групи дозволялося телефонувати з «робочого» телефону лише «жертві» злочину або один одному і було заборонено телефонувати рідним і близьким, проте одного дня один з таких «артистів» зателефонував своїй дружині. Отримавши інформацію про це від оператора мобільного зв'язку, співробітники правоохоронних органів почали «відпрацьовувати» зв`язки абонентів, що слугувало підґрунтям для розкриття серії аналогічних злочинів, здійснених на території України.

Важливу інформацію можна отримати при вивченні даних електронного листування і сервісів обміну миттєвими повідомленнями. У багатьох випадках саме ці сліди дозволяють встановити організаційні схеми злочинів. Так, аналіз електронних повідомлень і листування в 2010 році на території м. Харкова і інших міст України дозволив встановити канали постачання сировини для виготовлення сумішей для паління та енергетиків, основу яких складала синтетична речовина «JWH» (при вживанні викликає ефект, порівняний з

дією марихуани), рекомендації з їх виробництва, упакування, особливості та факти реалізації. Правоохоронними органами України припинена злочинна діяльність мережі реалізації цієї продукції. Лише у м. Харкові співробітники правоохоронних органів виявляли по 50-60 торгівельних точок на місяць, найбільша кількість яких знаходилася поблизу початкових шкіл.

Останні роки спостерігається стрімке зростання правопорушень у системах дистанційного банківського обслуговування (ДБО). ДБО – це комплекс сервісів видаленого доступу клієнтів до банківських послуг. При цьому клієнт видалено (без візиту в банк) передає необхідні розпорядження, використовуючи інформаційні технології.

Системи ДБО в Україні розподіляються на такі види: система «Клієнт-банк» (PC-banking, remote banking, direct banking, home banking); інтернет-банкинг; мобільний банкинг. Шахрайська схема розкрадання грошових коштів складається з трьох основних етапів: отримання конфіденційної інформації для здійснення неправомірного доступу в систему ДБО, проведення шахрайської операції від імені користувача з використанням його авторизаційних даних і ключів електронних засобів захисту, отримання готівки. Для розкрадання персональних (авторизаційних) даних користувача системи ДБО (логіна, пароля і ключів підпису) правопорушники часто використовують спеціальне шкідливе програмне забезпечення. Найчастіше це – модифікації добре відомих троянських програм з додатковими функціями, що дозволяють після певних неправомірних дій повністю «самоліквідуватися» без можливості відновлення.

Спеціалісти в галузі комп'ютерних мереж вважають, що умовами,які сприяють розкраданню персональних (авторизаційних) даних є такі:

– використання суб'єктами підприємницької діяльності, державними установами неліцензійного програмного забезпечення (особливо операційних систем та програм захисту інформації), «зараження» інформації комп'ютера користувачами локальної мережі установи;

– недостатній захист комп'ютерно-технічних засобів, які працюють в системах ДБО, від зовнішнього інтернет-середовища локальної мережі установи. Це надає можливість правопорушникам отримувати контроль над інформацією, що міститься на інтернет-ресурсах фінансових установ, маніпулювати апаратними можливостями комп'ютерно-технічних засобів з метою об'єднання їх в botnet-мережі для поширення спаму [14] або організації DDos-атак. Так, у низці випадків з аналізу журналів операційної системи, журналів програм захисту операційної системи комп'ютера, фактичної наявності вірусних і троянських кодів і програм стає зрозумілим, що передумовою злочину (наприклад, незаконної транзакції) є те, що злочинці при підготовці до правопорушення вивчають роботу й технічні можливості роботи комп'ютерної системи потенційної жертви; блокують її роботу в мережі й «заражають» інформацію користувача для здобуття дистанційно-

го контролю над певними технологічними процесами. Самостійно користувач (зазвичай співробітник бухгалтерії) не може оцінити рівень небезпеки несподіваних затримок у роботі комп'ютера і телекомунікаційних засобів, а також з'ясувати причини завантаження не оригінальної WEB-сторінки [15] ресурсу банківської установи;

– недотримання суб'єктами підприємницької діяльності, державними установами вимог щодо нерозповсюдження конфіденційних даних (авторизаційних даних користувачів Інтернет-банкинга, вміст ключів електронних засобів захисту), доступ сторонніх осіб до конфіденційної інформації підприємства. Так, наприклад, судові експерти в більшості випадків при дослідженні комп'ютерного засобу легко відшукують вміст авторизаційних даних для підключення до системи Інтернет-банкинга, вміст закритого ключа, яким засвідчується документ для виконання транзакції користувачем.

Висновки. Виявлення слідів комп'ютерних злочинів здійснюється криміналістами на основі дослідження технічного характеру вчинення протиправних дій.

Інформативність та доказова значущість виявлених слідів комп'ютерних злочинів залежить від обсягу використаних спеціальних знань та рівня обізнаності спеціаліста (експерта), якого залучено до огляду (дослідження) комп'ютерної інформації.

У зв'язку з швидким розвитком інформаційних технологій особливої уваги потребує розробка новітніх технічних засобів і прийомів виявлення, вилучення, фіксації і дослідження слідів комп'ютерних злочинів з використанням спеціальних знань.

Використані джерела:

1. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку / Офіційний сайт Верховного суду України. – [Електронний ресурс]. – Режим доступу : http://www.scourt.gov.ua. – Заголовок з екрану.

2. *Примітка.* За даними міжнародної організації Group-IB, яка досліджує стан комп'ютерної злочинності на пострадянському просторі, зазначено, що фінансові збитки світового ринку через комп'ютерні злочини за минулий рік перевищили 7 млрд. доларів США, а доходи злочинців з СНД складають 2,5 млрд. доларів, тобто «комп'ютерні» злочинці країн СНД контролюють більш як третину світового ринку кіберзлочинності. На 2014 рік зростання заробітку зловмисників прогнозується до 3,7 млрд. доларів. – Див.: Основные услуги и тарифы на рынке киберпреступности в странах СНГ. – [Електронний ресурс]. – Режим доступу : http://www.interface.ru. – Заголовок з екрану.

3. *Примітка.* Інновації – новостворені (застосовані) і (або) вдосконалені конкурентоздатні технології, продукція або послуги, а також організаційно-технічні рішення виробничого, адміністративного, комерційного або іншого характеру, що істотно поліпшують структуру та якість виробництва і (або) соціальної сфери. – Див.: Про інноваційну діяльність. Закон України // Відомості Верховної Ради України (ВВР). – 2002. – № 36. – ст. 266 (Із змінами та доповненнями).

4. Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. Криминалистика : [учебник] / [Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р.] ; под ред. Р. С. Белкина. – М. : Норма, 2001. – 990 с.

5. *Примітка.* Botnet – це комп'ютерна мережа, що складається з деякої кількості хостів (зазвичай, комп'ютерів або пристроїв, що підтримують сервіс «клієнт-сервер») із запущеними ботами – програмним забезпеченням, що працює автономно. Встановлений бот на комп'ютері «жертви» дозволяє зловмисникові виконувати певні дії з використанням ресурсів зараженого комп'ютера.

6. *Примітка.* DDoS-атака (атака типу «відмова в обслуговуванні», від англ. Distributed Denial of Service) - атака одночасно з великої кількості комп'ютерів на обчислювальну систему з метою створення таких умов, за яких легальні користувачі системи не можуть дістатися системних ресурсів (серверів). – Див.: Дремлюга Р. И. Интернет-преступность : [моногр.] / Р. И. Дремлюга. – Владивосток : Изд-во Дальневост. ун-та, 2008. – С. 23.

7. *Примітка.* Транзакція - банківська операція, що полягає в переказі грошових коштів з одного рахунку на інший. – Див.: Финансовый словарь. – [Електронний ресурс]. – Режим доступу : http://finance.sci-lib.com/. – Заголовок з екрану.

8. *Примітка.* Хакер [англ. hacker < to hack – рубити, прорубати] – комп'ютерний зломщик – той, хто за допомогою свого комп'ютера втручається в інформаційні мережі банків, фінансових, промислових і інших організацій для здобуття необхідної інформації, зараження цих мереж вірусами тощо. – Див. : Крысин Л. П. Толковый словарь иноязычных слов. – М. : Эксмо, 2008. – 944 с.

9. *Примітка.* У Києві затримали хакерів, які хотіли зламати системи ЦВК. – [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua/news/2014/05/25/7026530/. – Заголовок з екрану.

10. *Примітка.* Комп'ютерною інформацією є інформація в електронному (цифровому) вигляді, яка може бути зафіксована на певному носієві, в електронно-обчислювальній машині (ЕОМ), у телекомунікаційній системі або мережі ЕОМ.

11. Криминалистика : [учебник] / Под ред. Т. А. Седовой, А. А. Эксархопуло. – СПб. : Издательство «Лань», 2001. – С. 370.

12. *Примітка.* Інтернет-провайдер (провайдер; від англ. internet service provider, скор. ISP – постачальник інтернет-послуги) – організація, що надає послуги доступу до мережі Інтернет й інші пов'язані з Інтернетом послуги.

13. SMS [англ. Short Messaging Service – «служба коротких повідомлень»] – технологія, що здійснює приймання та передавання коротких текстових повідомлень за допомогою мобільного телефону. – Див.: Англо-русский словарь по вычислительной технике и программированию (The English-Russian Dictionary

of Computer Science) : около 55 тыс. статей. – 8-е изд., испр. и доп. © ABBYY, 2008; © Масловский Е. К., 2008. [Электронная версия]. – Заголовок з екрану.

14. *Примітка.* Спам (англ. spam) – розсилка комерційної та іншої реклами або інших видів повідомлень особам, які не мають бажання їх отримувати.

15. *Примітка.* WEB-сторінка (англ. Web page) – документ або інформаційний ресурс мережі Інтернет.

Авдеева Г.К. Использование специальных знаний в борьбе с компьютерной преступностью

Статья посвящена вопросам использования специальных знаний в борьбе с наиболее распространенными способами совершения компьютерных преступлений и способам выявления их следов. Приведены примеры успешного расследования мошенничества благодаря осмотру электронной переписки преступников и их SMS-сообщений. Проанализированы следы компьютерных преступлений в виде результатов работы антивирусных и тестовых программ. Предложены способы выявления следов несанкционированного доступа к работе электронно-вычислительных машин, автоматизированных систем, компьютерных сетей и баз данных.

Ключевые слова: *специальные знания, компьютерные преступления, следы преступления, информационные технологии.*

Avdeeva G.K. Use of special knowledge in the fight against computer crimes

The article is devoted to questions of use of special knowledge in the fight against the most common ways of committing computer crimes and identification of their traces. Placed the examples of successful investigation of crimes with by research of electronic correspondence of criminals and SMS. Are listed an innovative ways of detection of signs of criminal access in computers and in automated systems, in computer networks and in databases.

Ways of computer crimes is the use of harmful software products, telecommunication networks and net-work technologies, implementation of DDoS-attacks «to order», etc. Traces of computer crimes in the form of the results of the virus programs and of test programs can be identified by the results of the expert study of computer hardware, protocols, operating systems, antivirus programs, software code, etc.

Traces of illegal access to information can be found on the Internet, and subsequently, proceeding from their properties it is possible to establish a source of connection and a concrete technical tool. The traces of unauthorized access to computer information are a renaming of directories and of files, a change of size and of contents of files them of attributes, the emergence of new directories, files, change of time of last access to information, its modification, etc.

Some informational importance is having SMS messages. They are recorded on the server of the mobile operator. Law enforcement officers can take from mobile operator the phone numbers and texts of SMS. Important information you can obtain when studying e-mails and instant messages, as also a traces of offences in

remote banking systems (RBS). In many cases these traces allow us to establish the organizational scheme of crime.

The law enforcement agencies are building the international system of combating this type of crimes, they are creating methods of investigation of crimes of this category, they are strengthening cooperation with international institutions and law enforcement agencies of different countries (including via telecommunication means and systems). This makes topical further research on the development of innovative methods of detection and research of traces of crimes in the sphere of using of information technologies.

Key words: *special knowledge, computer crime, traces of the crime, information technology.*