2.3. Сліди злочинів у сфері використання електронно-обчислювальних засобів, телекомунікаційних систем і комп'ютерних мереж

На сьогодні злочини у сфері використання інформаційних технологій[1] (комп`ютерні злочини, кіберзлочини) – це одна з най-

[1] Примітка : У Законі України «Про Національну програму інформатизації» указано, що «інформаційною технологією (ІТ) є цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, доступ до інформації незалежно від місця її розташування» (див.: Про Національну програму інформатизації : Закон України № 74/98-ВР від 04.02.1998 // Відомості Верховної Ради України. – № 27-28. – Ст. 181. Редакція від 01.08.2016. [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80).

динамічніших груп суспільно небезпечних посягань[1]. Щороку збільшуються їх кількість та суспільна небезпечність[2]. Це зумовлене постійним і стрімким розширенням сфери застосування інформаційних технологій в усіх галузях діяльності людини.

Боротьба зі злочинами у сфері використання комп'ютерних технологій вимагає використання адекватних засобів протидії, інтенсивного впровадження інновацій[3] у роботу правоохоронних органів для своєчасного їх виявлення, кваліфікованого розслідування і профілактики.

Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (статті 361-363 розділу 16 Кримінального Кодексу України) розподіляються на такі види:

– несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних

---

[1] Див.: Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації : рішення РНБО України від 29 грудня 2016 року. Введено в дію Указом Президента України від 13 лютого 2017 року № 32/2017 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/n0015525-16.

[2] Примітка : За даними міжнародної організації Group-IB, що 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 із СНД складають 2,5 млрд доларів, тобто «комп'ютерні» злочинці країн СНД контролюють більш ніж третину світового ринку кіберзлочинності. На 2014 рік зростання заробітку даних 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).

[3] Примітка : інновації — новостворені (застосовані) і (або) вдосконалені конкурентноздатні 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 № 40-IV від 04.07.2002 // Відомості Верховної Ради України. – № 36. – ст. 266. Редакція від 05.12.2012. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/40-15).

машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

– несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;

– 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;

– перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Питанням дослідження проблем боротьби зі злочинами у сфері використання інформаційних технологій учені-криміналісти (Т. В. Авер'янова, О. Р. Росинська, В. О. Мєщєряков, В. Б. Вєхов, В. В. Крилов, І. Ю. Михайлов, М. В. Салтевський 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 в цьому напрямку для уточнення окремих наукових положень, в т. ч. – виокремлення специфічних слідів комп'ютерних злочинів та розробки інноваційних способів їх виявлення.

У науках кримінально-процесуального циклу термін «слід» використовується в двох значеннях – процесуальному і криміналістичному. Процесуальне значення сліду полягає у тому, що інформація, одержана за його допомогою, використовується для формування доказової бази за кримінальною справою і знаходить своє відбиття у процесуальних документах. Криміналістичне розуміння сліду більш широке й охоплює всю сукупність одержаної інформації, що використовується для здійснення розшукових дій,

висунення пошукових та інших версій, визначення напряму дій слідчого[1].

Існуюча в криміналістиці традиційна класифікація слідів вчинення тих чи інших злочинів практично не охоплює ті її види, що виникли при появі нових видів злочинів (зокрема, у сфері використання інформаційних технологій). Важливу роль у формуванні слідової картини злочинів у сфері інформаційних технологій відіграють способи вчинення злочинів цієї категорії.

Одним із способів вчинення злочину у сфері комп'ютерних технологій є використання зі злочинною метою шкідливих програмних продуктів. Заражені «комп'ютери-жертви» без згоди на це їх власників стають учасниками botnet-мереж[2]. Крадіжка особистих персональних і комерційних авторизаційних даних користувачів, конфіденційної інформації, ключів захисту, використання апаратного ресурсу «комп'ютера-жертви» з подальшою можливістю проведення DDoS-атак[3], несанкціонованої розсилки повідомлень і виконання «брехливих» транзакцій[4] 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,

---

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

[2] Примітка : Botnet – це комп'ютерна мережа, що складається з деякої кількості пристроїв (як правило, 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 із використанням ресурсів зараженого комп'ютера.

[3] 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, при яких легальні користувачі системи не можуть дістатися системних ресурсів (серверів) (див.: Дремлюга Р. И. Интернет-преступность : монографія / Р. И. Дремлюга. – Владивосток : Изд-во Дальневост. ун-та, 2008. – С. 23).

[4] 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/).

протизаконне отримання яких не потребує безпосередньої участі правопорушника.

На сьогодні в мережі Інтернет розміщені пропозиції хакерів[1] про можливе здійснення DDoS-атак «на замовлення», вказано певні розцінки на цей вид «послуг». Співробітниками Служби безпеки України 25 травня 2014 р. під час позачергових виборів Президета України в Києві затримано групу таких хакерів, які мали намір за допомогою спеціалізованого обладнання фальсифікувати результати виборів[2].

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

Одним із найважливіших визначальних чинників у боротьбі із зазначеними злочинами є галузь їх вчинення – кіберпростір. Кіберпростором називають сферу існування комп'ютерної інформації, що утворена сукупністю засобів комп'ютерної техніки. Комп'ютерна інформація[3] залежно від характеру злочинних діянь є предметом посягання і галуззю можливого збереження слідів злочинної діяльності.

Специфічними властивостями комп'ютерної інформації є такі:

– відсутність нерозривного зв'язку з матеріальним носієм;
– динамічність, можливість миттєвого перенесення в просторі (у тому числі з однієї частини земної кулі в іншу);

[1] Примітка : Хакер [англ. hacker < to hack – рубити, прорубати] – комп'ютерний зломщик, особа, яка за допомогою свого комп'ютера втручається в інформаційні мережі банків, фінансових, промислових й інших організацій із метою здобуття необхідної інформації, зараження цих мереж вірусами та ін. (див.: Крысин Л. П. Толковый словарь иноязычных слов / Л. П. Крысин. – М.: Эксмо, 2008. – 944 с.).

[2] Див.: У Києві затримали хакерів, які хотіли зламати системи ЦВК [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua/news/2014/05/25/7026530/.

[3] Примітка : Комп'ютерною інформацією є інформація в електронному (цифровому) вигляді, що може бути зафіксована на певному носієві, в електронно-обчислювальній машині (ЕОМ), телекомунікаційній системі або мережі ЕОМ.

– можливість зміни і знищення інформації будь-якого обсягу за стислі проміжки часу (зокрема, за допомогою видаленого доступу)[1];
– 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 є новим об'єктом криміналістичного дослідження, а комп'ютерна техніка (техніко-криміналістичний засіб для роботи з комп'ютерною інформацією) надає цій інформації значення джерела доказу.

На сьогодні 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 дії на комп'ютерну інформацію шляхом зовнішнього доступу до неї, 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, що в них зберігається (в порівнянні з вихідним станом). Часто злочинцями здійснюються 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

[1] Криминалистика : учебник / под ред. Т. А. Седовой, А. А. Эксархопуло. – СПб.: Лань, 2001. – С. 370.

з каталогів імен файлів, видалення або додавання окремих записів, фізичного руйнування або розмагнічування носіїв та ін.). Інформаційними слідами є також результати роботи антивірусних і тестових програм. Дані сліди можуть бути виявлені при експертному дослідженні комп'ютерного обладнання, протоколів роботи операційних систем, додатків, антивірусних програм, програмного коду та ін.

Сліди неправомірного доступу до інформації можна виявити в мережі Інтернет, а згодом, виходячи з їх ознак, установити вихідне підключення і технічний засіб, з якого здійснювалося це правопорушення. Найменування й адресу інтернет-провайдера[1], 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 в будь-який час можна отримати електронну адресу (IP) «атакуючого» комп'ютера. Час роботи користувача в мережі можна встановити за спеціальним log-файлом (журналом). Додаткові відомості про вид, порядок і час підключень користувача до мережі Інтернет і збіг цих даних із 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, що 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, що 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 та ін.

[1] Примітка : Інтернет-провайдер (провайдер; від англ. internet service provider, скор. ISP – постачальник інтернет-послуги) – організація, що надає послуги доступу до мережі Інтернет.

Певну інформаційну цінність мають SMS1– 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 р. вивчення й аналіз 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, протягом кількох років отримуючи величезні суми грошових коштів. Дана злочинна група імітувала дорожньо-транспортні події, вбивства з необережності, тяжкі тілесні ушкодження, провокувала осіб на статеві зносини з особами, які не досягли статевої зрілості, та ін. Окремі члени злочинної групи виконували роль «трупів», інші – співробітників правоохоронних органів. Організація кожного нового злочину супроводжувалася зміною номерів мобільних телефонів членів злочинної групи. Учасникам даної групи дозволялося телефонувати з «робочого» телефону лише «жертві» злочину або один одному і 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 підгрунтям для розкриття серії аналогічних злочинів, учинених 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

[1] Примітка : SMS (англ. Short Messaging Service — «служба коротких повідомлень») – технологія, що здійснює приймання та передавання коротких текстових повідомлень за допомогою мобільного телефону (див.: Масловский Е. К. Англо-русский словарь по вычислительной технике и программированию / Е. К. Масловский (The English-Russian Dictionary of Computer Science). – 8-е изд., испр. и доп. ABBYY, 2008. [Электронная версия]. (CD-ROOM).

організаційні схеми злочинів. Так, аналіз електронних повідомлень і листування в 2010 р. на території м. Харкова й інших міст України дозволив установити канали постачання сировини з метою виготовлення сумішей для паління та енергетиків, основу яких складала синтетична речовина «JWH» (при вживанні викликає ефект, порівнянний із дією марихуани), технологію їх виробництва й упакування, особливості та факти реалізації. Правоохоронними органами України припинена злочинна діяльність мережі реалізації цієї продукції. Лише у м. Харкові співробітниками правоохоронних органів виявлялося по 50-60 торгівельних пунктів на місяць, найбільша кількість яких знаходилася поблизу початкових шкіл.

Протягом останніх 2–3 років в усьому світі спостерігається стрімке зростання правопорушень у системах дистанційного банківського обслуговування (ДБО). Широке використання систем ДБО пояснюється можливістю здійснювати фінансові операції за допомогою комп'ютерів, планшетів та мобільних телефонів з будь-яких місць перебування особи без візиту до банку. Єдиною умовою для можливості здійснення таких дій є наявність точки доступу до мережі Internet.

Системи ДБО в Україні розподіляються на такі види: система «Клієнт-банк» (PC-banking, remote banking, direct banking, home banking); інтернет-банкинг; мобільний банкинг. Доступ до здійснення банковских операцій клієнти отримують після введення своїх персональних даних, які дозволяють системі ДБО його ідентифікувати.

Умовами, що сприяють розкраданню персональних (авторизаційних) даних, є такі:

– не дотримання суб'єктами підприємницької діяльності, державними установами вимог щодо нерозголошення конфіденційних даних (авторизаційних даних користувачів Інтернет-банкинга, вмісту ключів електронних засобів захисту), доступ сторонніх осіб до конфіденційної інформації підприємства. Так, наприклад, судові експерти в більшості випадків при досліджен-

ні комп'ютерного засобу легко відшукують вміст авторизаційних даних для підключення до системи Інтернет-банкинга, вміст закритого ключа, яким засвідчується документ для виконання транзакції користувачем;

– недостатній захист комп'ютерно-технічних засобів, що працюють у 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 із метою об'єднання їх в botnet-мережі для поширення спаму[1] 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 і технічні можливості роботи комп'ютерної системи потенційної жертви; блокують її роботу в мережі і «заражають» інформацію користувача з метою здобуття дистанційного контролю над певними технологічними процесами. Самостійно користувач (як правило, 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[2] ресурсу банківської установи;

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

---

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

[2] Примітка : WEB-сторінка (англ. Web page) – документ або інформаційний ресурс мережі Інтернет.

У наш час для вирішення проблем боротьби з комп'ютерними злочинами криміналістами досліджується технічний характер їх вчинення. Особливу увагу приділено розробці новітніх технічних засобів і прийомів виявлення, вилучення, фіксації і дослідження слідів злочинів із використанням комп'ютерних технологій. Однак боротьба з комп'ютерною злочинністю не обмежується встановленням кримінальної відповідальності злочинців. Багато уваги приділено захисту комп'ютерної інформації та іншим засобам запобігання злочинам у сфері використання інформаційних технологій.

На сьогодні активно здійснюється побудова міжнародної системи боротьби із зазначеними видами злочинів, об'єднуються необхідні кадри, розробляються методики розслідування злочинів цієї категорії, уточнюються процедури взаємодії із міжнародними структурами і правоохоронними органами різних країн (зокрема, за допомогою телекомунікаційних засобів і систем). Це зумовлює проведення подальших досліджень щодо розробки інноваційних способів виявлення слідів злочинів у сфері використання інформаційних технологій.

Національна академія правових наук України

Науково-дослідний інститут вивчення проблем злочинності
імені академіка В. В. Сташиса

ІННОВАЦІЙНІ ЗАСАДИ ТЕХНІКО-КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ КРИМІНАЛЬНОЇ ЮСТИЦІЇ

Монографія

За редакцією
академіка НАПрН України В. Ю. Шепітька,
члена-кореспондента НАПрН України В. А. Журавля

Харків
2017

УДК 343.98 : 001.895
ББК 67.52
І 67

Рекомендовано до друку вченою радою Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса Національної академії правових наук України (протокол № 11 від 26 жовтня 2016 р.)

Рецензенти:
Коновалова В. О. – професор кафедри криміналістики Національного юридичного університету іменні Ярослава Мудрого, доктор юридичних наук, професор, академік Національної академії правових наук України
Степанюк Р. Л. – завідувач кафедри криміналістики та судової експертології факультету №1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор

Колектив авторів:
Шепітько В. Ю. – Передмова, §§ 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 3.1, 3.2; Журавель В. А. – Передмова, §§ 1.2, 4.1, 4.2, 4.3, 4.4; Авдєєва Г. К. – §§ 1.1, 1.2, 1.3, 1.4, 1.5, 2.3, 3.2, 3.3, 3.4; Білоус В. В. – §§ 2.1, 2.4; Великанов С. В. – §§ 2.5, 3.5; Гетьман Г. М. – § 2.2; Затенацький Д. В. – §§ 2.7, 2.8; Керик Л. І. – § 2.6; Павлюк Н. В. – §§ 4.2; 4.4; Резнікова О. І. – §§ 4.1; 4.4.

І 67 Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції : Монографія / кол. авт. В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. – Х.: Вид. агенція «Апостіль», 2017. – 260 с.

Монографію присвячено проблемам розроблення інноваційних засад техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції. У роботі розкрито сутність інновацій у техніко-криміналістичному забезпеченні діяльності органів кримінальної юстиції, досліджено проблеми застосування новітніх інформаційних технологій у діяльності органів досудового розслідування, інноваційні підходи до використання спеціальних знань у правозастосовній діяльності та питання техніко-криміналістичного забезпечення розслідування кримінальних правопорушень корупційної спрямованості.

Для науковців, працівників правоохоронних та судових органів, викладачів, аспірантів та студентів юридичних навчальних закладів.

ББК 67.52

ISBN