Поліщук Віталій В'ячеславович, курсант навчально-наукового інституту № 2 Національної академії внутрішніх справ
Науковий керівник: старший викладач кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2 Національної академії внутрішніх справ ***Волошин О. Г.***

ВИДИ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ І ХАРАКТЕРИСТИКА КОМП'ЮТЕРНИХ ЗЛОЧИНЦІВ

Сучасний світ неможливо уявити без телекомунікацій та високих технологій, зокрема і комп'ютерних мереж. У зв'язку з цим сьогодні в Україні спостерігається різке збільшення інтересу до обчислювальних систем. Без сумніву, це зумовлено, в першу чергу, розвитком банківського бізнесу і широким упровадженням сучасних обчислювальних і комунікаційних засобів як у державному так і в приватному секторі.

Глобальна комп'ютерна мережа Інтернет у всьому світі щоденно поповнюється тисячами користувачів, які користуються WEB-технологіями для обміну інформацією. Як відомо, інформація на сьогодні стає об'єктом пильної уваги кримінального середовища, особливо для завоювання нових сфер впливу. Збільшення кількості суб'єктів зв'язку супроводжується, на жаль, поширенням протиправних дій, які завдають шкоди не лише користувачам, а й провайдерам комп'ютерної інформації та державним установам.

Комп'ютерна злочинність сучасного світу не знає кордонів. Віртуальні злочини є транснаціональними не лише тому, що для комп'ютерних мереж не існує кордонів, а й через відсутність цілісної законодавчої бази щодо кримінальної відповідальності суб'єктів таких злочинів.

Проблема комп'ютерної злочинності набирає оберти і в Україні. У зв'язку з цим у правоохоронних органів виникло доволі широке коло проблем, які мають переважно технічний та процесуальний характер. Одна з таких проблем полягає у відсутності чіткої класифікації злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також у недостатній підготовці слідчих для проведення огляду місць вчинення злочинів з використанням комп'ютерної техніки.

Серед елементів криміналістичної характеристики злочинів у сфері комп'ютерної інформації варто виділити: спосіб вчинення і приховування протиправного діяння, знаряддя (засоби), обстановку і місце вчинення злочину; типові сліди злочинних дій; предмет злочинного посягання; особу, що вчиняє протиправні дії в сфері комп'ютерної інформації; потерпілих від даних злочинів.

Види комп'ютерних злочинів можна поділити за способом їх вчинення. Ці способи поділені на три групи.

Перша група – це способи безпосереднього доступу. При їх реалізації інформація знищується, блокується, модифікується, копіюється, а також може порушуватися робота ОЕМ. Безпосередній доступ може здійснюватися як особами, що працюють з інформацією, так і осіб, що спеціально проникають у закриті зони та приміщення, де проводиться опрацювання інформації. Іноді злочинець з метою вилучення інформації, залишеної користувачами після роботи ОЕМ, обстежує робочі місця програмістів у пошуках чорнових записів, роздруківок, ділового листування (так зване «прибирання сміття») або здійснює перегляд і відновлення стертих файлів. При цьому необхідно відзначити, що такий спосіб у даний час менш поширений у зв'язку з тим, що комп'ютерну

інформацію легше перехопити при її передачі на телекомунікаційних каналах і комп'ютерних мережах, ніж при безпосередньому проникненні в приміщення.

Друга група включає способи віддаленого доступу до комп'ютерної інформації. До них можна віднести:

– підключення до лінії зв'язку законного користувача (наприклад, до телефонної лінії) і одержати тим самим доступ до його одержаної і переданої інформації;

– проникнення до чужих інформаційних мереж шляхом автоматизованого перебору (сканування) віддалених локальних комп'ютерів, які в даний час знаходяться в з'єднанні «dial-up», перебір здійснюється доти, поки на іншому кінці лінії не «відповість» чужий комп'ютер;

– електронний злом, який здійснюється, як правило, через комп'ютерну мережу. При спробі неправомірного доступу один несанкціонований користувач може бути легко виявлений, тому злом здійснюється одночасно з декількох робочих місць. У заданий час більше десяти персональних комп'ютерів одночасно починають спробу несанкціонованого доступу. При такій кількості комп'ютерів, що проводять «атаку» одночасно, навіть найнадійніші системи захисту від несанкціонованого доступу не встигають адекватно відреагувати на створену позаштатну ситуацію. Це може призвести до того, що декілька комп'ютерів, які «атакують», відсікаються системою захисту, а інші одержують необхідний доступ. Один комп'ютер, що «прорвався», блокує систему статистики мережі, яка фіксує всі спроби доступу, внаслідок чого інші комп'ютери, що «прорвалися», не можуть бути виявлені і зафіксовані. Частина з них приступає до «зламу» потрібного сектору мережі, а інші займаються фіктивними операціями з метою дезорганізації роботи підприємства, організації, установи та приховування злочину;

– проникнення до комп'ютерної системи з використанням чужих паролів, коли незаконний користувач видає себе за законного користувача. При цьому незаконний користувач здійснює набір пароля для доступу до чужого комп'ютера, використовуючи спеціально розроблені програми, придбані на «чорному» ринку. Підібравши необхідний пароль, незаконний користувач одержує доступ до комп'ютерної інформації і може проводити з нею будь-які дії під виглядом законного користувача: копіювати, модифікувати, видаляти, викрадати конфіденційну інформацію.

До способів віддаленого доступу до комп'ютерної інформації відносять такі методи перехоплення інформації:

– безпосереднє перехоплення – найпростіший спосіб неправомірного доступу. Перехоплення здійснюється як через телефонні канали зв'язку, так і шляхом підключення до комп'ютерних локальних мереж. При цьому об'єктами безпосереднього перехоплення (підслуховування) є різноманітні системи – кабельні, наземні мікрохвильові, супутникові та спеціально виділені.

– електромагнітне перехоплення – спосіб доступу до інформації за рахунок перехоплення випромінювань центрального процесора, дисплея, комунікаційних каналів принтера тощо, не використовуючи безпосереднє підключення до комп'ютерної системи. Таке перехоплення можна здійснити із сусіднього приміщення або навіть із сусіднього будинку, оскільки сучасні технічні засоби дозволяють прийняти і розшифрувати випромінювання працюючого принтера на відстані до 150 м, а випромінювання моніторів і з'єднання кабелів – до 500 м. Допоміжним засобом електромагнітного перехоплення є встановлення в комп'ютерному обладнанні «жучків» – чутливих мікрофонів з метою

прослуховування розмов обслуговуючого персоналу про роботу комп'ютерної мережі, коди доступу до неї, заходи безпеки тощо.

Третю групу складають змішані способи, що можуть здійснюватися як шляхом безпосереднього, так і віддаленого доступу. До таких відносяться:

– підміна даних (заміна або введення нових даних), як правило, коли інформація вводиться або виводиться з ОЕМ;

– таємне введення в чужу машину таких команд, що допомагають їй здійснювати нові, незаплановані функції при одночасному зберіганні її працездатності («троянський кінь»). Наприклад, така програма може виконувати копіювання файлів, але одночасно знищувати дані про фінансову діяльність підприємства;

– модифікація програм шляхом таємного впровадження в програму відповідних команд, що повинні спрацювати за певних умов через деякий час («логічна бомба»). Наприклад, як тільки програма незаконно перераховує кошти на підставний рахунок, вона самознищується і при цьому знищує всю інформацію про здійснену операцію;

– здійснення доступу до баз даних і файлів законного користувача за рахунок знаходження слабких місць у системах захисту. Системи, які не мають засобів автентичної ідентифікації (наприклад, за фізіологічними характеристиками: за відбитками пальців, малюнка сітчатки ока, голосом тощо), залишаються без захисту проти цього прийому. Найпростіший напрям здійснення – одержати коди та інші ідентифікаційні шрифти законних користувачів. Виявивши їх, з'являється можливість читати й аналізувати наявну в системі інформацію, копіювати її, повертатися до неї в міру необхідності. Таким чином, можна звертатися до баз даних конкуруючої фірми з тим, щоб мати перспективи її розвитку. Одержання такої інформації дає безсумнівну перевагу в конкурентній боротьбі;

– використання помилок у логіці побудови програми і виявлення «прогалин». Для злочинців дані помилки в програмах чи програмному забезпеченні – як «відкриті ворота» до інформації законного користувача;

– поширення у комп'ютерних мережах або шляхом продажу неліцензійних програм, що призводять до знищення або блокування інформації, порушення працездатності ОЕМ, системи ОЕМ чи їх мережі, включаючи переважну більшість комп'ютерних вірусів.

У літературі часто поділяють осіб, які вчинюють злочини в сфері комп'ютерної інформації, на три групи.

1. Першу групу складають «хакери». Саме з «хакерами» пов'язана сама поява комп'ютерної злочинності. Їх метою може бути спочатку спортивна зацікавленість у вирішенні завдання «зламу» захисту програмного продукту або створення комп'ютерних вірусів тільки для самовираження особистості. Їх відрізняє високий професіоналізм, який поєднується зі специфічним комп'ютерним фанатизмом. Варто підкреслити, що характерною рисою злочинців цієї групи є відсутність у них чітко виражених протиправних намірів. Практично всі дії направлені на прояв особистих інтелектуальних здібностей. До цієї ж групи належать професійні програмісти, які мають високий інтелект і характеризуються нестандартним мисленням. Розробка заходів безпеки для власних комп'ютерних систем і «злам» чужих засобів захисту є для них єдиним завданням, яке цікаве само по собі. Деякі з них можуть переорієнтуватися на отримання від своєї роботи певної матеріальної вигоди. Так, може бути поєднано створення нових вірусів з одночасною розробкою антивірусної програми для їх

знешкодження. Таким чином, ця програма буде користуватися попитом і знаходити свого покупця.

До особливостей, які вказують на вчинення комп'ютерного злочину особами розглянутої категорії, можна віднести такі: відсутність цілеспрямованої, продуманої підготовки до злочину; оригінальність способу; невжиття заходів для приховування злочину; факти невмотивованого бешкетництва.

2. Особи, які страждають інформаційними хворобами (так званими «комп'ютерними» фобіями). Ця категорія захворювань пов'язана з порушеннями в інформаційному режимі людини під впливом зовнішніх або внутрішніх дестабілізуючих факторів як природженої, так і набутої властивості. Внаслідок прискореного ритму життя, інформаційного вибуху, до якого багато людей виявилися непідготовленими, інтенсифікації праці за рахунок комп'ютерних технологій, багато службовців потрапляють до різних стресових ситуацій, деякі з них закінчуються формуванням комп'ютерних фобій і неврозів (страху перед втратою контролю над своїми діями). Власне кажучи, це є не що інше, як професійне захворювання. Основні симптоми його прояву: швидка стомлюваність, різкі стрибки артеріального тиску при контакті з комп'ютерною технікою, підвищене потовиділення, запаморочення і головні болі, тремтіння в кінцівках, утрудненість подиху, непритомності тощо. Дії, що здійснюються особами цієї категорії, спрямовані переважно на фізичне знищення або пошкодження засобів комп'ютерної техніки без наявності злочинного наміру при частковій або повній втраті контролю над своїми діями.

3. Професійні злочинці – особи, у діяннях яких яскраво виражена корислива мета. Вони володіють стійкими злочинними навичками. Злочини мають серійний, багатоепізодний характер, обов'язково супроводжуються діями для приховування злочину. Це, як правило, висококваліфіковані фахівці з вищою математичною, інженерно-технічною або економічною освітою, що входять до організованих злочинних груп і співтовариств, технічно оснащені на високому рівні (нерідко – спеціальною оперативною технікою). Цією групою вчинюються більшість особливо небезпечних посадових злочинів, що вчинені з використанням засобів комп'ютерної техніки, присвоєння коштів в особливо великих розмірах, шахрайства тощо.

Узагальнюючи вищевикладене, можна охарактеризувати «комп'ютерних злочинців» у такий спосіб. Переважна більшість – це чоловіки (приблизно 80 %), але частка жінок швидко збільшується у зв'язку з оволодінням комп'ютерною технікою секретарями, діловодами, бухгалтерами, касирами тощо. Вік більшості правопорушників складає 15–45 років (вік 33 % злочинців не перевищує 20 років). Фахова освіта не є обов'язковою.

Серед мотивів і мети здійснення протиправних діянь можна виділити: корисливі (присвоєння коштів і майна); політичні (шпигунство, діяння, спрямовані на підрив фінансової і грошово-кредитної політики, валютної системи країни); дослідницький інтерес; хуліганські спонукання і бешкетництво; помста тощо.

На сьогодні комп'ютерні злочини – це одна з найбільш динамічних груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Варто зауважити, що український законодавець приділяє значну увагу цій проблемі: Кримінальний кодекс України передбачив самостійний розділ про ці злочини – розділ XVI «Злочини у сфері використання електронно-

обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж»; двічі положення цього розділу змінювалися і доповнювалися – це свідчить про актуальність цієї проблеми в суспільстві.