КІБЕРЗЛОЧИННІСТЬ

Юрлакова І., ст. гр. Е-11-21, доц. Фастовець В.І.
ХНАДУ

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

Останнім часом в Україні значно зросла чисельність Інтернет користувачів, адже підключення до глобальної мережі стало доступним та зручним. Сьогодні особистий комп'ютер, КПК, мобільний телефон з підключенням до Інтернету сприймається наче належне та необхідне.

Популярність Інтернету невипадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, змога проведення банківських, торгових, біржових операцій, переказування коштів і пребагато іншого. Інтернет – це чудовий засіб для зв'язку та спілкування. Для багатьох людей він став цілим світом, віртуальним світом. Як і в реальному світі, так і в віртуальному, де панує комп'ютерна інформація, трапляються, злочини, кіберзлочини.

На сьогоднішній день комп'ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань . Стрімко збільшуються показники розповсюдження цих злочинів, а також без перерви зростає їх суспільна небезпечність. Це зумовлено прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосовування комп'ютерної техніки.

Треба зауважити, що український законодавець приділяє значну увагу цій проблемі: новий Кримінальний кодекс України вперше передбачив не підпорядкований розділ про ці злочини - розділ XVI «Злочини у сфері застосування електронно-обчислювальних машин

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

Кіберзлочинність - це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера, у якому перебувають дані про особ, приладдя, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а заразом іншого носія, навмисне призначеного для їхнього зберігання, обробки й передачі.

Родовим об'єктом злочинів, передбачених у розділі XVI КК України, є одиниця інформаційних відносин, які можливо визначити як інформаційні взаємини, засобом забезпеки яких є ЕОМ, системи, комп'ютерні мережі та мережі електрозв'язку.

По-іншому кажучи, злочини, передбачені цим розділом, посягають на певну частину інформаційних відносин – інформаційні відносини, які пов'язані із застосуванням спеціальних технічних засобів. У чинному кримінальному законі зараз 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 здійснювати розрахунки без участі людини;
- автоматизована система – організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей і персоналу, котрий здійснює цю діяльність;
- комп'ютерна сітка – комплекс територіально розосереджених систем опрацювання даних, засобів і (або) систем зв'язку та передавання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне користування цих ресурсів;
- телекомунікаційна мережа (мережа електрозв'язку) – комплекс технічних засобів телекомунікацій і споруд, призначених для маршрутизації, комутації, передавання та/або затвердження знаків, сигналів, письмового тексту, зображень і звуків чи повідомлень будь-якого роду

за допомогою радіо, проводових, оптичних чи інших електромагнітних систем між кінцевим обладнанням.

Відповідно до Конвенції про кіберзлочинність, яка є частиною українського законодавства з 11.10.2005 р., кіберзлочини умовно поділяються на чотири види.

Перший вид. До цього виду належать правопорушення супроти конфіденційності, цілісності та доступності комп'ютерних даних і систем.

Сюди можна віднести всі злочини, спрямовані против комп'ютерних систем і даних (наприклад, нарочитий доступ до комп'ютерної системи або її частини; свідоме пошкодження, знищення, погіршення, модифікація або приховування комп'ютерної інформації; навмисне вчинення, не маючи на це права, виготовлення, продажу, здобуття для використання, поширення або надання для застосування іншим чином пристроїв, включаючи комп'ютерні програми).

Другий вид. До другого виду кіберзлочинів відносять правопорушення, пов'язані з комп'ютерами. Такі злочини характеризуються умисним діянням, що призводить до втрачання майна іншої особи в наслідок будь-якого введення, зміни, знищення чи приховування комп'ютерних даних чи будь-якого вторгнення у роботу комп'ютерної системи, з шахрайською або нечесною метою придбання не маючи на це права, економічних переваг для себе чи іншої особи.

Третій вид. Цей вид кіберзлочинів охоплює правопорушення, пов'язані зі змістом (контентом), що полягає у здійсненні умисних незаконних дій з приводу вироблення, пропонування або надання доступу, поширення дитячої порнографії, а також володіння такими файлами у своїй системі кіберзлочинів охоплює правопорушення, пов'язані зі змістом, який полягає у здійсненні умисних незаконних дій стосовно вироблення, пропонування чи то надання доступу, поширення дитячої порнографії, а заразом володіння такими файлами у своїй системі.

Четвертий вид. Четвертим видом є умисні дії, пов'язані з порушенням авторських та суміжних прав, згідно до вимог Бернської Конвенції про захист літературних і художніх творів, Угоди про

торговельні аспекти прав інтелектуальної власності та Угоди BOIB про авторське право, а заразом національного законодавства України.

В Україні політика з приводу кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених органів діють відповідні підрозділи.

Хакери мають значні можливості, щоб скористатися вразливістю кібербезпеки та досягти своїх злочинних цілей. На нинішній день можна виділити такі основні (найпопулярніші) способи:

• Фішинг – один з видів інтернет-шахрайства, коли «жертві» надсилаються сповіщення від імені відомих компаній або організацій одначе у дійсності вони не є справжніми. задум фішингу – отримання доступу до конфіденційних даних користувачів (паролів, логінів, даних особових рахунків і банківських карт). Зазвичай використовується метод проведення масових розсилок від імені популярних компаній або організацій, які містять посилання на фейкові сайти, які важко зовні відрізнити від справжніх. У листах особу ввічливо просять оновити чи підтвердити правильність персональної інформації чи то інформують про які-небудь проблеми з даними, а після цього перенаправляють на підроблений сайт, де треба ввести облікові дані. коли «жертва» вводить особисті дані на таких сайтах, то злочинцям стають відомі ці відомості та вони можуть використати їх з метою крадіжки персональних даних, персональних коштів або іншого. Фішинг є одним з найпоширеніших видів кібератак.

• Вірус – це програма, яка встановлюється без відома та проти волі користувача на його комп'ютер чи інакший пристрій. Комп'ютерний вірус можна «схопити» по-різному. Скажімо, вебсторінки та поштові вкладення можуть застосовуватися для безпосереднього запуску вірусу в систему. Зчаста вірус буває вбудований у завантажену з інтернету програму, яка «випускає» вірус на волю, пізніше як «жертва» її встановлює. Після зараження вірусом програма може заблоковувати доступ до файлів та системи з метою отримання

викупу. При цьому сплата викупу не завжди гарантує відновлення роботи системи.

• Соціальна інженерія – це підхід до злому, який не залежить від технологій і полягає у застосуванні шахраями тактики, завдяки якій вони переконують «жертву» розкрити конфіденційну інформацію. Тактики можуть бути різними: від видавання себе за співробітника банку, знайомого або товариша до різноманітних погроз із вимогою встановити шкідливе ПЗ.

• Шкідливе ПЗ (Malware) – до таких програм належать так звані «трояни», програми-шпигуни чи рекламне ПЗ. Достатньо часто вони встановлюються разом з іншою, корисною програмою, яку вирішила завантажити «жертва». Такі програми можуть таємно записувати всі натискання на клавіші, сканувати файли на жорсткому диску і читати cookie-файли браузера.

• Злам – це умисна дія, спрямована на несанкціоноване проникнення у ПЗ або систему шляхом обходу механізму безпеки, з метою отримання несанкціонованого доступу до певного ПЗ або системи.

• Вішинг – це майже той самий фішинг, однак виманювання реквізитів картки зловмисники здійснюють за допомогою телефонних дзвінків (шахраї часто представляються працівниками банку й намагаються вивідати у власника картки ПІН-код чи примусити здійснити якісь дії зі своїм рахунком).

• Скімінг – копіювання даних платіжної картки за допомогою спеціального пристрою (скімера). Зазвичай відбувається під час здійснення карткових операцій із банкоматами. Для отримання даних злочинці використовують міні-камери або змінні клавіатури.

• Шимінг – модернізований різновид скімінгу. У цьому разі шахраї використовують майже непомітний прилад, який розміщують усередині картридера. Таким чином дані кредитки копіюються непомітно.

• Онлайн-шахрайство – фальшиві інтернет-аукціони, інтернет-магазини, сайти й телекомунікаційні засоби зв’язку.

• Піратство – протиправне розповсюдження об’єктів інтелектуальної власності в Інтернеті.

• Мальваре – створення та поширення вірусів і шкідливого програмного забезпечення.

• Протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства.

• Рефайлінг – незаконна підміна телефонного трафіку.

Таким чином, кіберзлочинність – це проблема, з якою зіштовхнулась планета у 21 столітті, і яка обіцяє зростати та поглинати дедалі більше коштів. Незважаючи на усі заходи, що їх приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи достатки порушників та зменшуючи вміст кишень пересічних громадян. Через те сьогодні насамперед важливо переглянути усі існуючі кроки та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців.