Дарина ВАСЯНОВИЧ
здобувач вищої освіти ОС «бакалавр»,
спеціальність «Фінанси, банківська справа та страхування»,
Подільський державний аграрно-технічний університет,
м. Кам'янець-Подільський
Андрій ПЕЧЕНЮК
канд .екон. наук, доцент кафедри фінансів, банківської справи,
страхування та електронних платіжних систем,
Подільський державний аграрно-технічний університет,
м. Кам'янець-Подільський

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Захист інформації є однією з вічних проблем. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми – комп'ютерні злочини стали характерною ознакою сьогодення.

Комп'ютерними називають злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби.

Серед причин комп'ютерних злочинів і пов'язаних з ними викрадень інформації головними є такі:

– швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;

– широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;

– постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць.

Сьогодні ніхто не може назвати точну цифру загальних збитків від комп'ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. [1]

Варто також ураховувати й морально-психологічні наслідки для користувачів, персоналу і власників інформаційних систем та інформації. Що ж

до порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей.

Згідно із Законом України «Про захист інформації в автоматизованих системах» захист інформації — це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

У літературі вживаються також споріднені терміни «безпека інформації» та «безпека інформаційних технологій». [2]

Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання інформаційних технологій, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. [4]

Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів.

Із цього погляду основними випадками порушення безпеки інформації можна назвати такі:

– несанкціонований доступ — доступ до інформації, що здійснюється з порушенням установлених в інформаційних системах (ІС) правил розмежування доступу;

– витік інформації — результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;

– втрата інформації — дія, внаслідок якої інформація в ІС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;

– підробка інформації — навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в ІС;

– блокування інформації — дії, наслідком яких є припинення доступу до інформації;

– порушення роботи ІС — дії або обставини, які призводять до спотворення процесу обробки інформації.

Зауважимо, що порушенням безпеки можна вважати і дії, які не призводять безпосередньо до втрати або відпливу інформації, але передбачають втручання в роботу системи.

Загалом найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту. Співробітники служб комп'ютерної безпеки поділяють усіх порушників на чотири групи стосовно жертви: сторонні, які не знають фірму; сторонні, які знають фірму, та колишні співробітники; співробітники-непрограмісти; співробітники-програмісти. [3]

Межа між програмістами та простими користувачами з погляду небезпечності останнім часом стирається. Останні становлять більшість співробітників, звичайно мають базову комп'ютерну підготовку і можуть скористатися спеціальним програмним забезпеченням, яке має дружній інтерфейс. За твердженнями експертів, тільки чверть співробітників цілком лояльна, чверть настроєна до фірми вороже і не має моральних обмежень, лояльність решти залежить від обставин. Тому нелояльні співробітники, які мають доступ до комп'ютерів і знайомі з системою, становлять серйозну загрозу. Передусім це організаційна проблема, технологія тут може відігравати тільки допоміжну роль.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про проблеми захисту інформації в комп`ютерних мережах. URL: http://ua-referat.com/.

2. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб. / За заг. ред. проф. Я.Ю. Кондратьєва. Київ, 2014.

3. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. Київ, 2006.

4. Електронна комерція: Навч. посіб. / Береза А.М., Козак Г.А., Левченко Ф.А. К: КНЕУ, 2002. 328с.

5. Артемов В. Ю. Нормативно-правовий довідник з охорони інформації в Україні. У 4-х томах / Артемов В. Ю., Лєнков О. С., Пашков А. С., Стаднік О. М., Хорошко В. О. Київ : Вид. ДУІКТ, 2010.