Сучасні інформаційні технології: теорія, практика, досвід та перспективи розвитку : матеріали міжрегіонального семінару (17 квітня 2013 р.). – Житомир: Вид-во ЖДУ ім. Івана Франка, 2013. – 90 с. – С. 16-20

Вакалюк Т.А.,

старший викладач,

Житомирський державний університет імені Івана Франка

Загрози безпеки інформаційних ресурсів у комп'ютерних системах

Зростання ролі й відповідальності інформаційних технологій у життєдіяльності людини неминуче спричиняє відповідальне відношення до забезпечення надійної, безпечної роботи автоматизованих комп'ютерних систем. Помилки у функціонуванні автоматизованих комп'ютерних систем можуть призвести до досить серйозних наслідків. Захищена від зовнішніх і внутрішніх загроз автоматизована комп'ютерна система – це те, до чого прагнуть керівники великих підприємств і власники домашніх персональних комп'ютерів.

Інформаційні ресурси – це відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх подання. Інформаційні ресурси поділяються на: відкритого та обмеженого доступу. До обмеженого доступу відносять: державну таємницю та конфіденційну інформацію, яка поділяється на: службову таємницю (адвокатська таємниця, таємниця суду і слідства тощо); комерційну таємницю (банківська); персональні дані (відомості про факти, події і обставини життя громадянина, що дозволяють ідентифікувати його особу).

Основними характеристиками інформаційних ресурсів є: ***1) конфіденційність інформаційних ресурсів*** – це відомість змісту тільки тим суб'єктам, які мають відповідні повноваження; 2) ***цілісність інформаційних ресурсів*** – це незмінність інформаційних ресурсів в умовах їх випадкового і (або) навмисного викривлення або руйнування; 3) ***доступність інформаційних ресурсів*** – це здатність забезпечення безперешкодного доступу суб'єктів до інформаційних ресурсів, що їх цікавить.

Захистом інформаційних ресурсів називають діяльність щодо запобігання витоку інформаційних ресурсів, несанкціонованих і ненавмисних дій на ці інформаційні ресурси.

Під ***витоком*** розуміють неконтрольоване поширення інформаційних ресурсів шляхом їх розголошення, несанкціонованого доступу до них та отримання розвідками. ***Розголошення*** – це доведення інформаційних ресурсів до неконтрольованої кількості одержувачів інформаційних ресурсів (наприклад, публікація відомостей на відкритому сайті в мережі Інтернет або у відкритій пресі). ***Несанкціонований доступ*** – отримання інформаційних ресурсів зацікавленим суб'єктом з порушенням правил доступу до них.

Несанкціонований вплив на інформаційні ресурси – вплив з порушенням правил їх зміни (наприклад, навмисне впровадження в інформаційні ресурси шкідливого програмного коду чи навмисна підміна електронного документу).

Під ***ненавмисним впливом*** на інформаційні ресурси розуміють вплив на них через помилки користувача, збій технічних чи програмних засобів, природних явищ, інших нецілеспрямованих впливів (наприклад, знищення документів у результаті відмови накопичувача на жорсткому магнітному диску комп'ютера).

Під ***загрозою безпеки інформаційних ресурсів*** розуміється потенційно можлива подія, процес або явище, які можуть привести до знищення, втрати цілісності, конфіденційності або доступності інформаційних ресурсів.

Потенційні загрози безпеки інформаційних ресурсів у КС поділяються на два класи (див. рис. 1).

Загрози, які не пов'язані з навмисними діями зловмисників і реалізуються у випадкові моменти часу, називають ***випадковими загрозами***.

Реалізація загроз цього класу приводить до найбільших втрат інформаційних ресурсів, при цьому можуть відбуватися знищення, порушення цілісності і доступності інформаційних ресурсів, рідше порушується конфіденційність інформаційних ресурсів, проте при цьому створюються передумови для зловмисної дії на інформаційні ресурси.

Стихійні лиха і аварії несуть найбільш руйнівні наслідки для КС, оскільки останні піддаються фізичному руйнуванню, інформаційні ресурси втрачаються або доступ до них стає неможливим.

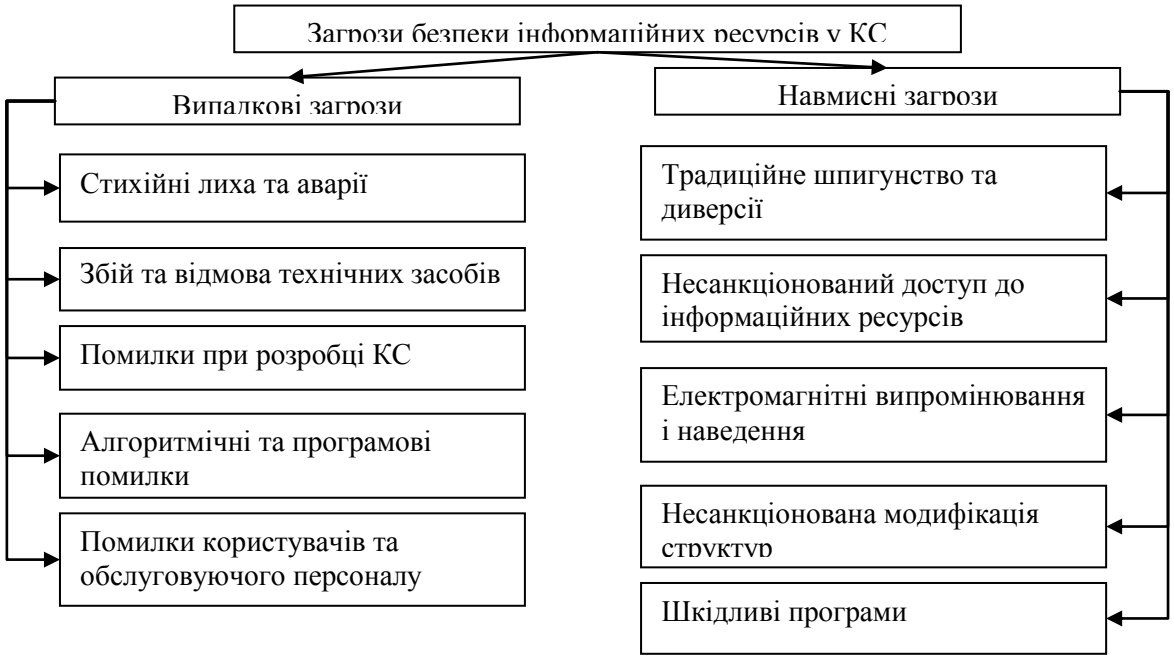

Рис. 1. Потенційні загрози безпеки інформаційних ресурсів у КС

Збої і відмови складних систем неминучі. В результаті збоїв і відмов порушується працездатність технічних засобів, знищуються і спотворюються дані і програми, порушується алгоритм роботи пристроїв, конфіденційність інформаційних ресурсів. Наприклад, збої і відмови засобів видачі інформаційних ресурсів можуть привести до несанкціонованого доступу до них шляхом несанкціонованої їх видачі в канал зв'язку, на принтер тощо.

Помилки при розробці КС, алгоритмічні і програмні помилки приводять до наслідків, аналогічних наслідкам збоїв і відмов технічних засобів. Особливу небезпеку представляють помилки в операційних системах (ОС) і в програмних засобах захисту інформаційних ресурсів.

Згідно аналізу даних, 65% випадків порушення безпеки інформаційних ресурсів відбувається в результаті помилок користувачів і обслуговуючого персоналу: некомпетентне, недбале або неуважне виконання функціональних обов'язків співробітниками приводять до знищення, порушення цілісності і конфіденційності інформаційних ресурсів.

Характеризуючи загрози інформаційних ресурсів у КС, не пов'язані з навмисними діями, в цілому, слід зазначити, що механізм їх реалізації вивчений досить добре, накопичений значний досвід протидії цим загрозам. Сучасна технологія розробки технічних і програмних засобів, ефективна система експлуатації КС, що включає обов'язкове резервування інформації, дозволяють значно понизити втрати від реалізації загроз цього класу.

Другий клас загроз безпеці інформації в КС складають ***навмисно створювані загрози***.

Даний клас загроз вивчений недостатньо, дуже динамічний і постійно поповнюється новими загрозами.

Як джерела небажаної дії на інформаційні ресурси як і раніше актуальні методи і засоби шпигунства і диверсій, які використовувалися і використовуються для добування або знищення інформаційних ресурсів. Найчастіше вони використовуються для здобуття відомостей про систему захисту з метою проникнення в КС, а також для розкрадання і знищення інформаційних ресурсів. До методів шпигунства і диверсій відносяться: підслуховування; візуальне спостереження; розкрадання документів і машинних носіїв інформаційних ресурсів; розкрадання програм і атрибутів системи захисту; підкуп і шантаж співробітників; збір і аналіз відходів машинних носіїв інформаційних ресурсів; підпали; вибухи.

Термін "несанкціонований доступ до інформаційних ресурсів" (НСДІР) визначений як доступ до інформаційних ресурсів, що порушує правила розмежування доступу з використанням штатних засобів обчислювальної техніки або автоматизованих систем. Несанкціонований доступ до інформаційних ресурсів можливий лише з використанням штатних апаратних і програмних засобів в наступних випадках: відсутня система розмежування доступу; збій або відмова в КС; помилкові дії користувачів або обслуговуючого персоналу комп'ютерних систем; фальсифікація повноважень.

Процес обробки і передачі інформації технічними засобами КС супроводжується електромагнітними випромінюваннями в навколишній

простір і наведенням електричних сигналів в лініях зв'язку, сигналізації, заземленні і інших провідниках. Найбільший рівень електромагнітного випромінювання в КС властивий працюючим пристроям відображення інформаційних ресурсів на електронно-променевих трубках. Вміст екрану такого пристрою може бути видимим за допомогою звичайного телевізійного приймача, доповненого нескладною схемою, основною функцією якої є синхронізація сигналів. Для добування даних зловмисник може використовувати також "просочування" інформаційних сигналів в ланцюзі електроживлення технічних засобів КС. Електромагнітні випромінювання використовуються зловмисниками не лише для здобуття інформаційних ресурсів, але і для їх знищення. Електромагнітні імпульси здатні знищити дані на магнітних носіях.

Велику загрозу безпеці інформації в КС представляє несанкціонована модифікація алгоритмічної, програмної і технічної структур системи. Несанкціонована зміна структури КС на етапах розробки і модернізації отримала назву "***закладка***". В процесі розробки КС "закладки" упроваджуються, як правило, в спеціалізовані системи, призначені для експлуатації в якій-небудь фірмі або державних установах. Алгоритмічні, програмні і апаратні "закладки" використовуються або для безпосередньої шкідливої дії на КС, або для забезпечення неконтрольованого входу в систему. Шкідливі дії "закладок" на КС здійснюються при здобутті відповідної команди ззовні і при настанні певних подій в системі (перехід на певний режим роботи, настання встановленої дати, досягнення певного напрацювання тощо).

Одним із основних джерел загроз безпеці інформації в КС є використання спеціальних програм, що отримали загальну назву "Шкідливі програми". Залежно від механізму дії шкідливі програми діляться на чотири класи: "логічні бомби"; "черв'яки"; "троянські коні"; "комп'ютерні віруси".

"Логічні бомби" – це програми або їх частини, що постійно знаходяться в ЕОМ або обчислювальних системах (ОС) і виконувані лише при дотриманні певних умов.

"Черв'яками" називаються програми, які виконуються кожного разу при завантаженні системи, володіють здатністю переміщатися у ОС або мережі і самовідтворювати копії, що приводить до перевантаження каналів зв'язку, пам'яті і, зрештою, до блокування системи.

"Троянські коні" – це програми, отримані шляхом явної зміни або додавання команд в призначені для користувача програми. При подальшому виконанні призначених для користувача програм поряд із заданими функціями виконуються несанкціоновані, змінені або якісь нові функції.

"Комп'ютерні віруси" – це невеликі програми, які після впровадження в ЕОМ самостійно поширюються шляхом створення своїх копій, а при виконанні певних умов надають негативну дію на КС.

Можливості здійснення шкідливих дій у великій мірі залежать від статусу зловмисника по відношенню до КС. Зловмисником може бути: розробник КС; співробітник з числа обслуговуючого персоналу; користувач; стороння особа.

Розробник володіє якнайповнішою інформацією про програмні і апаратні засоби КС і має можливість впровадження "закладок" на етапах створення і модернізації систем. Користувач може здійснювати збір даних про систему захисту даних методами традиційного шпигунства, а також робити спроби несанкціонованого доступу до інформаційних ресурсів. В розпорядженні сторонньої особи є дистанційні методи традиційного шпигунства і можливість диверсійної діяльності, вона може здійснювати шкідливі дії з використанням електромагнітних випромінювань і наведень, а також каналів зв'язку. Великі можливості надання шкідливих дій на інформаційні ресурси в КС мають фахівці, обслуговуючі ці системи. Причому, фахівці різних підрозділів володіють різними можливостями зловмисних дій. Найбільшої шкоди можуть завдати працівники служби безпеки інформаційних ресурсів, далі йдуть системні програмісти, прикладні програмісти і інженерно-технічний персонал.

На практиці небезпека зловмисника залежить також від фінансових, матеріально-технічних можливостей і кваліфікації зловмисника.

Список використаних джерел:

1. Мельников В. В. Защита информации в компьютерных системах /В. В. Мельников. – М. : Финансы и статистика; Электронинформ, 1997. – 368 с.