УДК 658.336:007:681.3.06

Володимир Ковальов

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ В ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ

У статті розглядаються основні особливості захисту інформації в інформаційно-обчислювальних мережах, наводиться аналіз несанкціонованого доступу та способи вирішення можливих проблем щодо захисту цілісності комп'ютерної мережі.

В статье рассматриваются основные особенности защиты информации в информационно-вычислительных сетях, приводится анализ несанкционированного доступа и способы решения возможных проблем по защите целостности компьютерной сети.

The article reviews the main features of protection of information in computer networks, an analysis of the unauthorized access and how to solve potential problems in protecting the integrity of a computer network.

Ключові слова: захист інформації, несанкціонований доступ, вимоги до захисту інформації.

ВСТУП

Завдання забезпечення інформаційної безпеки в даний час є особливо актуальним. Це пов'язано із широким впровадженням комп'ютерних систем передачі, збереження й обробки інформації. Комп'ютерні системи застосовуються у всіх галузях промисловості, фінансових операціях тощо. Проблема забезпечення інформаційної безпеки і захисту інформації у зв'язку з тенденцією об'єднання локальних комп'ютерних мереж у глобальну мережу і використання її як середовища передачі інформації при взаємодії різних офісів чи представництв великого підприємства набуває особливого значення. Використання ресурсів мережі Internet при організації такої взаємодії дозволяє здійснювати централізоване керування всією інформаційною інфраструктурою підприємства і швидко передавати дані між представництвами, що знаходяться в різних країнах.

Практика експлуатації і розширення таких систем ведеться за принципом послідовного приєднання з забезпеченням інформаційної прозорості. Це означає, що наявний парк комп'ютерів поєднується мережею. Нові ж робочі станції включаються безпосередньо в мережу через

комутатори чи за допомогою віддаленого доступу. Як правило, проблема інформаційної безпеки при цьому не вирішується.

1. Аналіз способів несанкціонованого доступу до локальної обчислювальної мережі

Для оцінки інформаційної безпеки та вразливих місць інформаційної системи розглянемо можливі способи несанкціонованого доступу до інформаційних ресурсів.

Під несанкціонованим доступом до інформації мають на увазі такий доступ, що порушує правила використання інформаційних ресурсів комп'ютерної системи, встановлені для її користувачів.

Обчислювальні системи є територіально розподілені комп'ютерні мережі, які поєднують за допомогою каналів зв'язку різні комп'ютери і локальні мережі. Вразливість таких систем істотно перевищує вразливість автономних комп'ютерів. Це пов'язано, насамперед, з відкритістю і масштабністю комп'ютерних мереж, що використовуються на залізниці. Відповідно існує чимало способів атак на ці комп'ютерні мережі.

Усі можливі способи несанкціонованого доступу до інформації в комп'ютерних системах, що захищаються, можна класифікувати за такими ознаками:

1. За принципом несанкціонованого доступу: фізичний несанкціонований доступ, логічний несанкціонований доступ.

Фізичний несанкціонований доступ може бути реалізований одним з таких способів: подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів, розкрадання документів і носіїв інформації, візуальне перехоплення інформації, виведеної на екрани моніторів і принтери, а також підслуховування, перехоплення електромагнітних випромінювань.

Логічний несанкціонований доступ припускає логічне подолання системи захисту ресурсів активної комп'ютерної мережі. З огляду на те, що переважна більшість інформації може бути реалізована лише у процесі функціонування обчислювальної системи, а також те, що логічний несанкціонований доступ є найбільш результативним для зловмисника, він і буде основним предметом аналізу. Способи фізичного несанкціонованого доступу далі розглядатися не будуть.

2. За розташуванням джерела несанкціонованого доступу: несанкціонований доступ, джерело якого розташоване у локальній мережі, несанкціонований доступ, джерело якого розташоване поза локальною мережею.

3. За режимом виконання несанкціонованого доступу: атаки, що проводяться при постійній участі людини; атаки, що проводяться спеціально розробленими програмами без особистої участі людини.

4. За несанкціонованим доступом: атаки, орієнтовані на використання прямого стандартного шляху доступу до комп'ютерних ресурсів, атаки;

орієнтовані на використання прихованого нестандартного шляху доступу до комп'ютерних ресурсів.

5. За безпосереднім місцем розташування кінцевого об'єкта атаки: на інформацію, що зберігається на зовнішніх запам'ятовуючих пристроях, на інформацію, передану по лініях зв'язку, атаки на інформацію, оброблювану в основній пам'яті комп'ютера.

6. За безпосереднім об'єктом атаки: на політику безпеки і процес адміністративного керування, на постійні компоненти системи захисту, на змінні елементи системи безпеки, напади на протоколи взаємодії, напади на функціональні елементи комп'ютерної системи.

2. Вимоги до системи захисту інформації в локальних обчислювальних мережах

Доцільно виділити такі групи вимог до систем захисту інформації: загальні вимоги, організаційні вимоги, конкретні вимоги до підсистем захисту, технічного і програмного забезпечення, документування, способів, методів і засобів захисту.

Загальні вимоги

Насамперед необхідна повна ідентифікація користувачів, терміналів, програм, а також основних процесів і процедур. Крім того, варто обмежити доступ до інформації, використовуючи сукупність таких способів: ієрархічна класифікація доступу, класифікація інформації по важливості і місцю її виникнення, зазначення обмежень до інформаційних об'єктів, наприклад, користувач може здійснювати лише читання файлу без права запису в нього, визначення програм і процедур, наданих лише конкретним користувачам.

Як правило, загальні вимоги характеризуються: за способами побудови СЗІ або її окремих компонентів (до програмного, програмно-апаратного, апаратного), архітектурою ІС, застосуванням стратегії захисту, витратами ресурсів на забезпечення СЗІ, надійністю функціонування СЗІ, кількістю ступенів таємності інформації, підтримуваних СЗІ, забезпеченням швидкості обміну інформацією в ІС, у тому числі з обліком використовуваних криптографічних перетворень, кількістю підтримуваних СЗІ рівнів повноважень, можливостями СЗІ обслуговувати певну кількість користувачів, тривалістю процедури генерації програмної версії СЗІ, тривалістю процедури підготовки СЗІ до роботи після подачі живлення на компоненти ІС, можливістю СЗІ реагувати на спроби несанкціонованого доступу, або на «небезпечні ситуації», наявністю і забезпеченням автоматизованого робочого місця адміністратора захисту інформації в ІС, складу використовуваного програмного і лінгвістичного забезпечення, до його сумісності з іншими програмними платформами, до можливості модифікації тощо, використовуваними закупленими компонентам СЗІ (наявність ліцензії, сертифіката і т.п.).

Організаційні вимоги

Організаційні вимоги до системи захисту передбачають реалізацію сукупності адміністративних і процедурних заходів. Вимоги щодо забезпечення схоронності мають виконуватися, насамперед, на адміністративному рівні. Організаційні заходи, проведені з метою підвищення ефективності захисту інформації, повинні передбачати такі процедури: обмеження несупроводжуваного доступу до обчислювальної системи, здійснення контролю за зміною в системі програмного забезпечення, виконання тестування і верифікації змін у системі програмного забезпечення і програмах захисту, організація і підтримання взаємного контролю за виконанням правил захисту даних, обмеження привілею персоналу, що обслуговує ІС, здійснення запису протоколу про доступ до системи, гарантія компетентності обслуговуючого персоналу, розробка послідовного підходу до забезпечення схоронності інформації для всієї організації, організація чіткої роботи служби стрічкової і дискової бібліотек, комплектування основного персоналу на базі інтегральних оцінок і необхідних знань, організація системи навчання і підвищення кваліфікації обслуговуючого персоналу.

Вимоги до підсистем захисту інформації

Доцільно СЗІ умовно розділити на підсистеми: керування доступом до ресурсів ІС (містить також функції керування системою захисту в цілому), реєстрація й облік дій користувачів (процесів), криптографічна підсистема, забезпечення цілісності інформаційних ресурсів і конфігурації ІС.

Підсистема керування доступом має забезпечувати: ідентифікацію, аутентифікацію і контроль за доступом користувачів (процесів) до системи, терміналів, вузлів мережі, каналів зв'язку, зовнішніх пристроях, програм, каталогів, файлів, записів і т.д.; керування потоками інформації, очищення областей, що звільняються, оперативної пам'яті і зовнішніх накопичувачів.

Підсистема реєстрації й обліку виконує: реєстрацію й облік доступу до ІС, видачу вихідних документів, запуск програм і процесів, доступ до файлів, що захищаються; передачу даних по лініях і каналах зв'язку, реєстрацію зміни повноважень доступу, створення об'єктів доступу, що підлягають захисту, облік носіїв інформації, оповіщення про спроби порушення захисту.

Криптографічна підсистема передбачає: шифрування конфіденційної інформації, шифрування інформації, що належить різним суб'єктам доступу (групам суб'єктів), з використанням різних ключів, використання атестованих (сертифікованих) криптографічних засобів.

Підсистема забезпечення цілісності здійснює: забезпечення цілісності програмних засобів і оброблюваної інформації, фізичну охорону засобів обчислювальної техніки і носіїв інформації, наявність адміністратора (служби) захисту інформації в ІС, періодичне тестування СЗІ, наявність засобів відновлення СЗІ, використання сертифікованих засобів захисту, контроль за цілісністю, оперативне відновлення функцій СЗІ після збоїв,

тестування засобів захисту інформації, виявлення і блокування поширення вірусів, резервне копіювання програмного забезпечення і даних, контроль доступу до інформації, що дає впевненість у тому, що тільки авторизований користувач використовує наявні робочі програми й інформацію, контроль дій з персональною авторизацією, що забороняє операції, які роблять операційне середовище вразливим, захист програмного забезпечення, що виключає ушкодження інстальованих програм, використання тільки ліцензійного програмного продукту з метою забезпечення захисту від вбудованих модулів руйнування інформаційного середовища і дискредитації систем захисту, захист комунікацій для забезпечення неприступності переданої інформації.

Вимоги до технічного забезпечення

У цій групі формулюються вимоги за такими параметрами: місцеві застосування засобів захисту, способами їхнього використання, розмірами контрольованої зони безпеки інформації, необхідна величина показників захищеності, що враховує реальну обстановку на об'єктах ІС, застосування способів, методів і засобів досягнення необхідних показників захищеності, проведення спеціальної перевірки технічних об'єктів ІС, метою якої є виявлення спеціальних електронних (заставних) пристроїв.

Вимоги до програмного забезпечення

Програмні засоби захисту інформації повинні забезпечувати контроль доступу, безпеку і цілісність даних і захист самої системи захисту. Для цього слід виконати такі умови: об'єкти захисту повинні ідентифікуватися в очевидному вигляді при використанні паролів, пропусків і ідентифікації по голосу; система контролю доступу має бути досить гнучкою для забезпечення різноманітних обмежень і різних наборів об'єктів, кожен доступ до файлу даних чи пристрою повинен простежуватися через систему контролю доступу для того, щоб фіксувати і документувати будь-яке звертання.

Вимоги до документування

Можна виділити три групи вимог до документування системи захисту інформації. Це протоколювання, тестування програм і обробка погроз.

Основні специфічні вимоги: необхідність записів будь-якого руху даних, що захищаються, можливість відтворення при необхідності ретроспективи використання об'єкта, що захищається, для реалізації якої забезпечується запам'ятовування станів програми і навколишнього середовища, нагромадження статистики по протоколах використання інформації в системі.

ЛІТЕРАТУРА

1. *Кулаков Ю. А., Луцкий Г. М.* Компьютерные сети. – К.: Юниор, 1998. – 380 с.
2. *Бэрри Нанс.* Компьютерные сети / Пер. с англ. – К.: Бином, 1995. – 214 с.