Комп'ютерні системи обробки інформації як об'єкти захисту

Інформація - це результат відображення і обробки в людській свідомості різноманіття навколишнього світу. Відомості, якими обмінюється людина через ЕОМ з іншою людиною або з ЕОМ, і є предметом захисту. Однак захисту підлягає не будь-яка інформація, а тільки та, яка має ціну. Цінним стає та інформація, володіння якою дозволить її наявному й потенційному власнику отримати будь-якої виграш: моральний, матеріальний, політичний і т. і. Оскільки в людському суспільстві завжди існують люди, охочі незаконним шляхом отримати цінну інформацію, у її власника виникає необхідність в її захисті.

Актуальність і важливість проблеми забезпечення захисту інформації обумовлена наступними причинами:

а) різке збільшення обчислювальної потужності сучасних комп'ютерів, що веде до значного збільшення обсягів оброблюваної інформації, в тому числі такої, втрата якої може привести до серйозних проблем;

б) спрощення експлуатації сучасних комп'ютерів, що веде до значного розширення кола користувачів (що не завжди володіють достатньою для усвідомлення проблем захисту інформації кваліфікацією), які мають доступ до обчислювальних ресурсів, засобів розробки програм і даних;

в) зосередження в єдиних базах даних інформації різного призначення і різної приналежності (тобто належить різним користувачам);

г) бурхливий розвиток програмних засобів, які не задовольняють навіть мінімальним вимогам безпеки і зростання кількості програмістів;

д) повсюдний розвиток мережевих технологій, об'єднання локальних мереж і їх використання для передачі даних, а також об'єднання мереж в глобальні комп'ютерні мережі, що надає потенційну можливість віддаленого порушення безпеки комп'ютерних систем.

Комп'ютерна система обробки інформації (КСОІ) - локалізований або розподілений апаратно-програмний комплекс і обслуговуючий його персонал, здійснюють генерування, введення, зберігання, обробку.

Основні компоненти КСОІ:

а) апаратні засоби - ЕОМ і їх компоненти, периферійні пристрої, лінії зв'язку та мережеве обладнання;

б) програмне забезпечення: BIOS, операційні системи, прикладне програмне забезпечення, мови програмування;

в) дані (електронні та ті, що зберігаються в твердій копії);

г) персонал.

Об'єктами КСОІ називають пасивні компоненти систем, які зберігають і передають інформацію (приклади об'єктів КСОІ - накопичувачі інформації, канали і пристрої зв'язку).

Суб'єктами КСОІ називають активні компоненти систем, які можуть стати причиною потоку інформації від об'єкта КСОІ до будь-якого суб'єкта КСОІ або причиною зміни стану КСОІ (приклади суб'єктів КСОІ - користувачі, програми, процеси).

Безпека КСОІ - її захищеність від випадкового або навмисного втручання в нормальний процес функціонування, а також від спроб розкрадання, зміни або руйнування її компонентів.

Властивості інформації в контексті її захисту:

а) конфіденційність - властивість бути відомою тільки допущеним і тим, які пройшли перевірку - авторизованим користувачам, програмам і процесам;

б) цілісність - інформація вважається цілісної, якщо дані в семантичному відношенні не відрізняються від вихідних даних, тобто якщо не відбулося випадкового або навмисного спотворення або руйнування даних.

Доступ до інформації - ознайомлення з інформацією і / або її обробка, зокрема, копіювання, модифікація або знищення.

Типи доступу:

а) санкціонований - що не порушує встановлені правила розмежування доступу, які представляють собою систему заходів (апаратних, програмних, адміністративних, законодавчих і морально-етичних), що регламентують доступність об'єктів КСОІ і ступінь доступу (права) суб'єктів КСОІ до цих об'єктів;

б) несанкціонований доступ (НСД) - порушує встановлені для КСОІ правила розмежування доступу.

КСОІ	**Порушення конфіденційності інформації**	**Порушення цілісності інформації**	**Порушення працездатності системи**
Апаратні засоби	НСД - підключення і використання апаратних ресурсів, розкрадання носіїв інформації	НСД - зміна режимів роботи апаратури, яке тягне за собою зміну інформації	НСД - зміна режимів роботи апаратури, яке тягне за собою висновок апаратури з ладу
Програмне забезпечення	НСД - копіювання, розкрадання, підслуховування	НСД - зміна конфігурації програмного забезпечення, комп'ютерні віруси	НСД - зміна конфігурації програмного забезпечення, "мережеві черв'яки"
Дані	НСД - копіювання, розкрадання, перехоплення, "троянські коні",	НСД - спотворення, модифікація	НСД - спотворення, підміна, видалення даних
Персонал	Розголошення, передача відомостей про захист, недбалість	Вербовка, підкуп персоналу	Відхід з робочого місця, фізичне усунення

НСД - несанкціонований доступ

Рис. 1. Можливі шляхи реалізації навмисних загроз безпеки КСОІ

Загроза безпеки КСОІ - потенційно можливе навмисне чи випадкова подія, яка може негативно впливали на КСОІ.

Типи загроз безпеки КСОІ щодо впливу на інформацію:

а) загрози порушення конфіденційності інформації (відбувається завжди при НСД);

б) загрози порушення цілісності інформації;

в) загрози порушення працездатності КСОІ (відмова в обслуговуванні - Deny Of Service - DOS).

Типи загроз безпеки КСОІ за характером виникнення:

а) випадкові:

- відмови і збої апаратури;
- перешкоди на лініях зв'язку від впливів зовнішнього середовища;
- помилки людини як ланки системи;
- схемні і системотехнічні помилки розробників;
- структурні, алгоритмічні та програмні помилки;
- аварійні ситуації та інші впливи.

б) навмисні - пов'язані з цілеспрямованими діями порушника, вмотивованими, наприклад, прагненням отримати права на доступ до об'єктів КСОІ, не передбачені для нього правилами розмежування доступу КСОІ, отриманням матеріальних вигід від використання інформації КСОІ, конкурентною боротьбою і шпигунством, прагненням до самоствердження та інш.

Комплекс заходів щодо забезпечення безпеки КСОІ: частковий і комплексний підходи до забезпечення безпеки КСОІ. Переваги фрагментарного підходу - висока вибірковість і ефективність до конкретної загрози, мінімальний час реагування на конкретну загрозу. Важливо використання і комплексного і фрагментарного підходу.

Етапи побудови комплексної системи захисту КСОІ:

1. Аналіз можливих загроз КСОІ;

2. Планування системи захисту:

а) визначення законодавчих актів, що забезпечують захист КСОІ і передбачають відповідальність за її порушення та ознайомлення з ними користувачів КСОІ.

б) визначення морально-етичних заходів захисту КСОІ - створення здорового морально-етичного клімату в колективі користувачів КСОІ, матеріальні і моральні заохочення користувачів, що підвищують престиж організації, що виконують усі вимоги безпеки КСОІ, що не дозволяють невиправданого використання ресурсів КСОІ і ін.

в) визначення адміністративних заходів захисту, що регламентують:

- загальна схему функціонування КСОІ - функціональні блоки і їх взаємозв'язок;
- вибір персоналу КСОІ і визначення порядку взаємодії користувачів з системою;
- використання ресурсів КСОІ і визначення прав доступу персоналу до них.

г) визначення фізичних заходів захисту:

- механічних (розташування компонентів КСОІ і контроль доступу до них)
- забезпечення гарантованого електроживлення КСОІ;
- визначення засобів захисту від пожеж, повеней та інших стихійних лих;
- визначення засобів відео і аудіо спостереження.

д) визначення апаратно-програмних засобів захисту:

- забезпечення ідентифікації (розпізнавання) і аутентифікації (перевірки справжності) суб'єктів КСОІ;
- розмежування доступу до ресурсів КСОІ;
- контроль цілісності даних КСОІ;
- забезпечення конфіденційності даних КСОІ;
- аудит і аналіз подій КСОІ;
- резервування ресурсів і компонентів КСОІ.

3. Реалізація системи захисту інформації КСОІ.

4. Супровід системи захисту КСОІ, контроль і аналіз подій з метою виявлення проломи, корекції системи захисту та ін.

Основні принципи забезпечення безпеки інформації:

- економічна ефективність засобів захисту - вартість захисту повинна бути менше вартості інформації, що захищається;
- проектування системи захисту з урахуванням принципу "ворожого оточення";
- виключення з кола контрольованих системою захисту користувачів її розробників;
- визначення особистої відповідальності осіб, які займаються забезпеченням безпеки КСОІ;
- забезпечення користувачам за замовчуванням мінімальних прав і привілеїв, достатніх для їх нормальної роботи;
- поділ об'єктів і суб'єктів КСОІ на групи і управління захистом на рівні груп;
- забезпечення постійного аудиту використання об'єктів і роботи суб'єктів КСОІ;
- забезпечення прийняття рішення людиною, а не автоматизованого прийняття рішення в найбільш важливих ситуаціях;
- система захисту інформації повинна відключатися тільки адміністратором і тільки в екстрених випадках;
- приховування, по можливості, факту існування системи захисту.

Соціальна інженерія - область знань, яка використовується хакерами і крекерами для забезпечення їх несанкціонованого доступу до КСОІ інакше, ніж через злом ПЗ. Мета атакуючого - обхитрувати користувачів КСОІ з метою отримання їх паролів і ключів доступу до КСОІ.

Класичне шахрайство включає дзвінки по телефону в організацію для визначення атакується жертви і подальшого дзвінка адміністратору від її імені з проханням організувати негайний доступ до КСОІ (наприклад, змінивши пароль).

Класифікація атак класу соціальної інженерії:

За засобом зв’язку:

- телефон;
- електронна пошта;
- повідомлення Internet реального часу;
- звичайна пошта;
- особиста зустріч.

За рівнем соціального ставлення до об'єкта:

- офіційний стиль спілкування;

- товариський стиль спілкування;
- дружній стиль спілкування.

За ступенем доступу жертви до КСОІ:

- адміністратор КСОІ - високий ступінь доступу;
- керівник КСОІ (ланки КСОІ) (часто секретар керівника) - середній ступінь доступу;
- користувач КСОІ - низький ступінь доступу;
- знайомі адміністратора, начальника, користувача

Приклади атак класу соціальної інженерії:

1. Дзвінок адміністратору від імені користувача, який не може увійти в систему (можливо, забув пароль). Адміністратор запитує ім'я користувача (воно відомо атакуючому через e-mail адресу або в результаті попередніх дзвінків в організацію), атакуючий повідомляє ім'я і отримує пароль. Він може тепер від імені адміністратора КСОІ повідомити жертві новий пароль і входити в систему від її імені.

2. Атакуючий дзвонить користувачеві КСОІ і представляється адміністратором системи, повідомляє, що в системі виконані зміни і користувач повинен бути повторно зареєстрований, при цьому атакуючий запитує, а жертва повідомляє по телефону своє ім'я входу в КСОІ і пароль;

3. Атака на адміністратора - атакуючий, отримавши ім'я користувача КСОІ і пароль (наприклад, одним з вищеописаних способів), дзвонить адміністратору КСОІ який працює, наприклад, під ОС UNIX, і повідомляє, що він не може чомусь виконати зазвичай дозволених для нього дій, наприклад , переглянути файли в своєму домашньому каталозі (це виконується командою ls). Адміністратор, зареєстрований в системі як root (з найвищими привілеями), входить в каталог користувача і виконує успішно програму ls. Якщо у змінній PATH адміністратора розташований поточний каталог (точка), то від імені адміністратора буде виконана програма, яку створив атакуючий, назвав її ls і розмістив в домашньому каталозі користувача-жертви. Така програма може порушувати конфіденційність і цілісність інформації в КСОІ, і надавати НСД до її об'єктів.