Урок № 8.

Тема уроку: Інструктаж з БЖД. Криптографічні методи захисту інформації. Контроль цілісності програмних та інформаційних ресурсів.

На цьому уроці ти дізнаєшся про криптографічні методи захисту інформації та про контроль цілісності інформаційних ресурсів.

Правила поведінки за комп'ютером:

Пам’ятай:

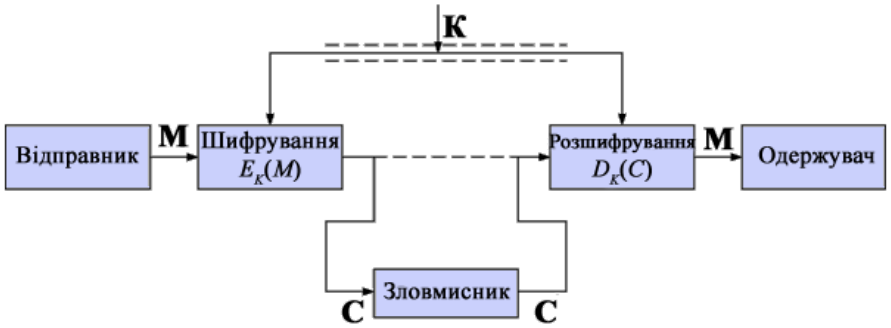
- Робоче місце за комп'ютером потрібно тримати у порядку.
- Не клади зайвих речей на стіл біля комп'ютера.
- Прибирай пил з комп'ютера спеціальною ганчіркою, коли він вимкнений.

Виконуй:

- Слідкуй за осанкою (спина повинна бути прямою).
- Очі мають бути на відстані 50 – 60 см від екрану монітору.
- Кожні 30 хвилин роби перерву в своїй роботі.

Проблема захисту інформації шляхом її перетворення, що виключає її прочитання сторонньою особою, хвилювала людський розум з давніх часів. Історія криптографії - ровесниця історії людської мови. Більше того, спочатку писемність сама по собі була криптографічною системою, тому що в стародавніх суспільствах нею володіли лише обрані. Священні книги Стародавнього Єгипту, Стародавньої Індії тому є прикладами.

Криптографічні методи захисту інформації - це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. Криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї. Даний метод захисту реалізується у вигляді програм або пакетів програм.



Сучасна криптографія включає в себе чотири великих розділи:

1.*Симетричні криптосистеми*.

У симетричних криптосистемах і для шифрування, і для дешифрування використовується один і той самий ключ. (Шифрування - перетворювальний процес. Оригінальний текст, який носить також назву відкритого тексту, замінюється шифрованих текстом, дешифрування - зворотний шифруванню процес. На основі ключа шифрований текст перетворюється у початковий);

2.Криптосистеми з відкритим ключем. У системах з відкритим ключем використовуються два ключі - відкритий і закритий, які математично пов'язані один з одним. Інформація шифрується за допомогою відкритого ключа, який доступний всім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачу повідомлення.

3.*Електронний підпис.* Системою електронного підпису називається його криптографічне перетворення, що приєднуються до тексту і дозволяє при отриманні його іншим користувачем перевірити авторство і достовірність повідомлення.

4.Управління ключами. Це процес системи обробки інформації, який полягає в складанні та розподілі ключів між користувачами.

Основні напрямки використання криптографічних методів - передача конфіденційної інформації по каналах зв'язку (наприклад, електронна пошта), встановлення автентичності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому вигляді.

Вимоги до криптосистем.

Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, проте їй притаманні такі переваги: висока продуктивність, простота, захищеність тощо. Програмна реалізація більш практична, допускає відому гнучкість у використанні.

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті *вимоги*:

✔ зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа;

✔ число операцій, необхідних для визначення використаного ключа шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, має бути не менше загального числа можливих ключів;

✔ число операцій, необхідних для розшифрування інформації шляхом перебору різноманітних ключів повинно мати сувору нижню оцінку і не виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень);

✔ знання алгоритму шифрування не повинно впливати на надійність захисту;

✔ незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа;

✔ структурні елементи алгоритму шифрування повинні бути незмінними;

✔ додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути повністю та надійно сховані в зашифрованому тексті;

✔ довжина шифрованого тексту повинна бути рівною довжині вихідного тексту;

✔ не повинно бути простих і легко встановлюваних залежностей між ключами, що послідовно використовуються в процесі шифрування.

Симетричні криптосистеми.

Все різноманіття існуючих криптографічних методів у симетричних криптосистемах можна звести до наступних класів перетворень:

- **підстановка** - символи тексту, що шифрується, замінюються символами того ж або іншого алфавіту відповідно до заздалегідь визначеного правила;
- **перестановка** - символи тексту, що шифрується, переставляються по деякому правилу в межах заданого блоку переданого тексту;
- **аналітичне перетворення** - текст, що шифрується, перетворюється по деякому аналітичному правилу, наприклад, гамування - полягає в накладені на вихідний текст деякої псевдовипадкової послідовності, що генерується на основі ключа;
- **комбіноване перетворення** - представляє собою послідовність (з можливим повторенням і чергуванням) основних методів перетворення. Застосовується до блоку (частини) тексту, що шифрується. Блокові шифри на практиці зустрічаються частіше, ніж "чисті" перетворення того чи іншого класу в силу їх більш високої криптостійкості.

Системи з відкритим ключем.

Якими б не були складними та надійними криптографічні системи - їх слабке місце при практичній реалізації - проблема розподілу ключів. Для того, щоб був можливий обмін конфіденційною інформацією між двома суб'єктами інформаційної системи (ІС), ключ повинен бути згенерований одним з них, а потім якимось чином знову ж таки в конфіденційному порядку переданий іншому.

Тобто в загальному випадку для передачі ключа знову ж потрібне використання деякої криптосистеми. Для вирішення цієї проблеми на основі результатів, отриманих класичною та сучасною алгеброю, були запропоновані системи з відкритим ключем. Суть їх полягає в тому, що

кожним адресатом ІС генеруються два ключі, зв'язані між собою за певним правилом. Один ключ оголошується відкритим, а інший закритим. Відкритий ключ публікується і доступний кожному, хто бажає послати повідомлення адресату. Секретний ключ зберігається в таємниці.

Оригінальний текст шифрується відкритим ключем адресата і передається йому. Зашифрований текст у принципі не може бути розшифрований тим же відкритим ключем.

Дешифрування повідомлення можливе тільки з використанням закритого ключа, який відомий тільки самому адресату.

Криптографічні системи з відкритим ключем використовують, так звані, незворотні або односторонні функції, які мають наступну властивість: при заданому значенні x відносно просто обчислити значення $F(x)$, однак якщо $y = F(x)$, то немає простого шляху для обчислення значення x. Безліч класів незворотних функцій і породжує все розмаїття систем з відкритим ключем.

Електронний підпис.

В чому полягає проблема аутентифікації даних? Наприкінці звичайного листа або документа виконавець або відповідальна особа зазвичай ставить свій підпис. Подібна дія зазвичай переслідує дві мети.

По-перше, одержувач має можливість переконатися в істинності листа, звіривши підпис з наявним у нього зразком. По-друге, особистий підпис є юридичним гарантом авторства документа. Останній аспект особливо важливий при укладанні різного роду торгових угод, складанні довіреностей, зобов'язань тощо.

Якщо підробити підпис людини на папері дуже непросто, а встановити авторство підпису сучасними криміналістичними методами - технічна деталь, то з підписом електронним справа полягає в іншому. Підробити ланцюжок бітів, просто його скопіювавши, або непомітно внести нелегальні виправлення в документ зможе будь-який користувач.

Управління ключами.

Крім вибору підходящої для конкретної ІС криптографічного системи, важлива проблема - управління ключами. Як би не була складна і надійна сама криптосистема, вона заснована на використанні ключів. Якщо для забезпечення конфіденційного обміну інформацією між двома користувачами процес обміну ключами тривіальний, то в ІС, де кількість користувачів становить десятки і сотні управління ключами - серйозна проблема. Під ключовою інформацією розуміється сукупність всіх діючих в ІС ключів. Якщо не забезпечено досить надійне управління ключовою інформацією, то заволодівши нею, зловмисник отримує необмежений доступ до всієї інформації. Управління ключами - інформаційний процес, що включає в себе три елементи:

•генерацію ключів;

•накопичення ключів;

•розподіл ключів.

Генерація ключів.

На самому початку розмови про криптографічні методи було сказано, що не варто використовувати невипадкові ключі з метою легкості їх запам'ятовування. У серйозних ІС використовуються спеціальні апаратні і програмні методи генерації випадкових ключів. Як правило використовують датчики ПВЧ (псевдовипадкових чисел).

Накопичення ключів.

Під накопиченням ключів розуміється організація їх зберігання, обліку та видалення. Оскільки ключ є найпривабливішим для зловмисника об'єктом, який відкриває йому шлях до конфіденційної інформації, то питанням накопичення ключів слід приділяти особливу увагу. Секретні ключі ніколи не повинні записуватися в явному вигляді на носії, який може бути зчитаний або скопійований. У досить складній ІС один користувач може працювати з великим об'ємом ключової інформації і іноді, навіть, виникає необхідність організації міні-баз даних по ключовій інформації.

Розподіл ключів.

Розподіл ключів - найвідповідальніший процес в управлінні ключами. До нього пред'являються дві вимоги:

•Оперативність і точність розподілу;

•Скритність ключів, що розподіляються.

Реалізація криптографічних методів.

Проблема реалізації методів захисту інформації має два аспекти:

•розробку засобів, що реалізують криптографічні алгоритми;

•методику використання цих засобів.

Кожен з розглянутих криптографічних методів можуть бути реалізовані або програмним, або апаратним способом. Можливість програмної реалізації обумовлюється тим, що всі методи криптографічного перетворення формальні і можуть бути представлені у вигляді кінцевої алгоритмічної процедури.

При апаратній реалізації всі процедури шифрування і дешифрування виконуються спеціальними електронними схемами. Найбільшого поширення набули модулі, що реалізують комбіновані методи. Більшість зарубіжних серійних засобів шифрування засновані на американському стандарті DES.

Основною перевагою програмних методів реалізації захисту є їх гнучкість, тобто можливість швидкої зміни алгоритмів шифрування. Основним же недоліком програмної реалізації є істотно менша швидкодія в порівнянні з апаратними засобами (приблизно в 10 разів). Останнім часом стали з'являтися комбіновані засоби шифрування, так звані програмно-апаратні засоби. В цьому випадку в комп'ютері використовується своєрідний «криптографічний співпроцесор" - обчислювальний пристрій, орієнтований на виконання криптографічних операцій. Міняючи програмне забезпечення для такого пристрою, можна вибирати той чи інший метод шифрування.

Таким чином, вибір типу реалізації криптозахисту для конкретної ІС в істотній мірі залежить від її особливостей і повинен спиратися на всебічний аналіз вимог, що пред'являються до системи захисту інформації.