Урок №8. **Криптографічні методи захисту інформації. Контроль цілісності програмних та інформаційних ресурсів.**

Вивчення нового матеріалу

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. 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.

Криптографія - наука про способи перетворення (шифрування) інформації з метою її захисту від незаконних користувачів.

Криптоаналіз - наука (і практика її застосування) про методи і способи розкриття шифрів.

Криптографія – це захист, тобто розробка шифрів, а криптоаналіз – це напад, тобто атака на шифри. Однак ці дві дисципліни пов'язані між собою – не буває гарних криптографів, що не володіють методами криптоаналізу.

Сучасна криптографія включає в себе чотири великі 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 шифрованим текстом, дешифрування - зворотний шифруванню процес. На основі ключа шифрований текст перетворюється у початковий).

2.Криптосистеми з відкритим ключем. У системах із відкритим ключем використовуються два ключі - відкритий і закритий, які математично пов'язані один із одним. Інформація шифрується за допомогою відкритого ключа, який доступний всім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачу повідомлення (Ключ - інформація, необхідна для безперешкодного шифрування і дешифрування текстів).

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.

Зашифрування — процес перетворення звичайної інформації (*відкритого тексту*) в незрозумілий текст - «сміття» (тобто, *шифротекст або криптограму*).

Розшифрування — це зворотній процес відтворення інформації із шифротексту.

Шифрування – називається пара алгоритмів шифрування / дешифрування.

Криптографічний алгоритм, або шифр, — це математична формула, що описує процеси шифрування і розшифрування**.**

Ключ — це секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення. Ключ забезпечує конфіденційність шифротексту. Ключі, як правило, — це дуже великі числа. Знання ключа шифрування дозволяє виконати правильне розшифрування шифротексту.

Криптостійкість - це характеристика шифру, що визначає його стійкість до дешифрування без знання ключа (тобто криптоаналізу).

Дешифрування (розкриття шифру) – процес одержання інформації із шифротексту без знання застосованого ключа.

Криптографічний алгоритм, або шифр, — математична формула, що описує процеси шифрування і розшифрування. Щоб зашифрувати відкритий текст, криптоалгоритм працює в сполученні з ключем — словом, числом або фразою. Те саме повідомлення одним алгоритмом, але різними ключами буде перетворюватися в різний шифротекст. Захищеність шифротексту цілком залежить від двох речей: стійкості криптоалгоритму і таємності ключа. Криптоалгоритм плюс усілякі ключі і протоколи, що приводять їх у дію, складають криптосистему.

Розрізняється шифрування двох типів:

- симетричне шифртування;
- асиметричне шифрування.

Несиметричне шифрування складніше, але й надійніше. Для його реалізації потрібні два взаємозалежні ключі: відкритий і закритий. Одержувач повідомляє всім бажаючим свій відкритий ключ, що дозволяє шифрувати для нього повідомлення. Закритий ключ відомий тільки одержувачеві повідомлення. Коли комусь потрібно послати зашифроване повідомлення, він виконує шифрування, використовуючи відкритий ключ одержувача. Одержавши повідомлення, останній розшифровує його за допомогою свого закритого ключа. За підвищену надійність несиметричного шифрування приходиться платити: оскільки обчислення в цьому випадку складніше, то процедура розшифровки займає більше часу.

Коли надійність криптографічного алгоритму забезпечується за рахунок збереження в таємниці суті самого алгоритму, такий алгоритм шифрування називається обмеженим. Обмежені алгоритми становлять значний інтерес з погляду історії криптографії, однак зовсім непридатні при сучасних вимогах, які висуваються до шифрування. Адже, в цьому випадку, кожна група користувачів, які

бажають обмінюватися секретними повідомленнями, повинна мати свої оригінальні алгоритми шифрування.

При симетричному шифруванні створюється ключ, файл разом з цим ключем пропускається через програму шифрування та отриманий результат пересилається адресатові, а сам ключ передається адресатові окремо, використовуючи інший (захищений або дуже надійний) канал зв'язку. Адресат, запустивши ту ж саму шифрувальну програму з отриманим ключем, зможе прочитати повідомлення. Симетричне шифрування не таке надійне, як несиметричне, оскільки ключ може бути перехоплений, але через високу швидкість обміну інформацією воно широко використовується, наприклад, в операціях електронної торгівлі.

В основі криптографічного контролю цілісності лежать два поняття:

- хеш-функція;
- електронний цифровий підпис (ЕЦП).

Хеш-функція - це складнозворотнє перетворення даних (однобічна функція), реалізована, як правило, засобами симетричного шифрування зі зв'язуванням блоків. Результат шифрування останнього блоку (що залежить від усіх попередніх) і слугує результатом хеш-функції.

Хешування (англ. hashing) - перетворення вхідного масиву даних довільної довжини в вихідну бітову послідовність фіксованої довжини, яку можна використати для порівняння даних.

Одностороня хеш-функція отримує ввід довільної довжини, називаний прообразом. У цьому випадку, повідомлення будь-якого розміру (хоч тисячі або мільйони біт) і генерує строго залежне від прообразу значення фіксованої довжини, наприклад, 160 біт. Хеш-функція гарантує, що якщо інформація буде будь-як змінена — навіть на один біт, — у результаті вийде зовсім інше хеш-значення.

Електронний цифровий підпис (ЕЦП) (англ. *digital signature*) — вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Оригіналом електронного документа вважається електронний примірник з електронним цифровим підписом автора.

Електронний цифровий підпис є складовою частиною інфраструктури відкритих ключів.

Електронний цифровий підпис призначений для використання фізичними та юридичними особами-суб'єктами електронного документообігу:

- для аутентифікації підписувача;
- для підтвердження цілісності даних в електронній формі.

ЕЦП як спосіб ідентифікації підписувача електронного документу, дозволяє однозначно визначати походження інформації, що міститься у документі. Завдяки цьому ЕЦП є також надійним засобом розмежування відповідальності за інформаційну діяльність у суспільстві, зокрема, відповідальності за дезінформування.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. За правовим статусом він прирівнюється до власноручного підпису (печатки). Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.

За умови правильного зберігання власником секретного (особистого) ключа його підробка неможлива. Електронний документ також не можливо підробити: будь-які зміни, не санкціоновано внесені в текст документу, будуть миттєво виявлені.

Особистий ключ ЕЦП

Особистий ключ ЕЦП формується на підставі абсолютно випадкових чисел, що генеруються давачем випадкових чисел, а відкритий ключ обчислюється з особистого ключа ЕЦП так, щоб одержати другий з першого було неможливо.

Особистий ключ ЕЦП є унікальною послідовністю символів довжиною 264 біти, яка призначена для створення Електронного цифрового підпису в електронних документах. Працює особистий ключ тільки в парі з відкритим ключем. Особистий ключ необхідно зберігати в таємниці, адже будь-хто, хто дізнається його, зможе підробити ЕЦП.

Документ підписується ЕЦП за допомогою особистого ключа ЕЦП, який існує в одному екземплярі тільки у його власника. Цьому особистому ключу відповідає відкритий ключ, за допомогою якого можна перевірити відповідність ЕЦП його власнику.

Відкритий ключ ЕЦП і Сертифікат відкритого ключа

Відкритий ключ використовується для перевірки ЕЦП одержуваних документів (файлів). Відкритий ключ працює тільки в парі з особистим ключем. Відкритий ключ міститься в Сертифікаті відкритого ключа, і підтверджує приналежність відкритого ключа ЕЦП певній особі. Крім самого відкритого ключа, Сертифікат відкритого ключа містить в собі персональну інформацію про його власника (ім'я, реквізити), унікальний реєстраційний номер, термін дії Сертифікату відкритого ключа. З метою забезпечення цілісності представлених у Сертифікаті даних він підписується особистим ключем Центру сертифікації ключів. Сертифікат

відкритого ключа може публікуватися на сайті відповідного ЦСК відповідно до Договору про надання послуг ЕЦП.

Підписання електронного документу ЕЦП

Управління ключами складається з процедур, що забезпечують:

- включення користувачів у систему;
- виробництво, розподіл та введення в апаратуру ключів;
- контроль використання ключів;
- зміну та знищення ключів;
- архівування, зберігання і відновлення ключів.

Управління ключами грає найважливішу роль в криптографії як основа для забезпечення конфіденційності обміну інформацією, ідентифікації та цілісності даних. Важливою властивістю добре спроектованої системи управління ключами є зведення складних проблем забезпечення безпеки численних ключів до проблеми забезпечення безпеки кількох ключів, яка може бути відносно просто вирішена шляхом забезпечення їх фізичної ізоляції у виділених приміщеннях і захищеному від проникнення обладнанні. У разі використання ключів для забезпечення безпеки інформації, що зберігається суб'єктом, може бути єдиний користувач, який здійснює роботу з даними в послідовні проміжки часу. Управління ключами в мережах зв'язку включає, принаймні, двох суб'єктів — відправника і одержувача повідомлення.

Генерація ключів

Генерація ключів повинна здійснюватись апаратними генераторами випадкових чисел або криптографічно стійкими генераторами псевдовипадкових чисел. Якщо можлива атака на генератор псевдовипадкових чисел, то можливе дешифрування криптограм зі складністю, меншою ніж складність атаки грубою силою навіть при відсутності вразловостей у алгоритмах шифрування.

Зберігання та використання ключів

Ключі повинні зберігатись і використовуватись у апаратних криптографічних модулях, смарт-картках та токенах, які не дозволяють експорт ключа у незашифрованому вигляді.

Знищення ключів

Після виведення з дії ключі повинні знищуватись способом, який не допускає їх відновлення. Найнадійнішим способом є знищення носія ключів (механічне, термічне тощо). Допускається повний перезапис носія.

• Під *контролем цілісності інформації* розуміють процес перевірки наявності викривлень цієї інформації, незалежно від причин їх походження (навмисні чи ненавмисні).

Причини порушення цілісності

- помилки користувачів, які викликають викривлення чи втрату інформації;
- навмисні дії осіб, які не мають прав доступу до автоматизованої системи;
- збої обладнання, які викликають викривлення чи втрату інформації;
- фізичні впливи на носії інформації;
- вірусні впливи.

У більшості операційних систем є механізми ідентифікації користувача, які забезпечують той чи інший рівень захисту інформації. Основні методи захисту інформації в операційних системах наступні:

• захист інформації за допомогою матриці управління доступом та списків управління доступом;

• захист інформації за допомогою «паролів»;

• захист інформації за допомогою шифрування-дешифрування (криптографія).

Недоліки двох перших методів полягають у тому, що «ключі» доступу зберігаються в самій системі. Це може призвести до того, що підготовлений недобросовісний користувач може їх розкрити і скористатись секретною інформацією. При шифруванні інформації ключ кодування не повинен зберігатись у системі. Користувач вводить його тільки тоді, коли зашифровує або розшифровує інформацію.

Причини порушення цілісності

- Помилки користувачів, які викликають викривлення чи втрату інформації.
- Навмисні дії осіб, які не мають прав доступу до втоматизованої системи.
- Збої обладнання, які викликають викривлення чи втрату інформації.
- Фізичні впливи на носії інформації.