Математичні методи захисту інформації: курс лекцій. Частина 1

Завадська Л.О., Савчук М.М.

11 травня 2014 р.

Розділ 1

Задачі, напрямки та методи захисту інформації. Поняття про криптографічний захист інформації

1.1 Області застосування, мета, методи захисту інформації

Протягом свого існування людство пережило декілька інформаційних революцій: створення і розвиток мов, винахід писемності, винахід та широке застосування друкарства, створення комп'ютера та новітніх електронних технологій, що радикально змінили суспільство в усіх галузях, на всіх рівнях суспільного розвитку. Кількість інформації, що була доступна та використовувалась, постійно зростала, а за періоди інформаційних революцій — на декілька порядків. Володіння інформацією і в минулому і нині давало можливість досягти швидкого розвитку і успіху у різних галузях як у глобальному масштабі, так і в конкретних справах. Сьогодні світ переживає період, коли накопичено колосальний об'єм знань, що дозволяє перейти до здійснення справді революційних технологічних рішень. Основою розвитку нині може бути, перш за все, процес пізнання, і він посильний тільки високоосвіченому суспільству, в якому праця приймає все більш інтелектуальні форми. Технологіям майбутнього потрібні широко освічені люди, які здатні орієнтуватися в нових умовах дійсності, що стрімко змінюється.

Однією з галузей, що найбільш динамічно змінюються протягом останніх десятиліть, є технології електронної обробки інформації, телекомунікацій, комп'ютерних мереж, технології захисту інформації.

В Україні широкий попит на методи і засоби захисту інформації почав виявлятися у другій половині 80-х років XX ст. З часом виникла нагальна потреба використання криптографічних та технічних методів захисту також у приватному секторі. Сьогодні велика кількість конфіденційної інформації передається в електронному вигляді, на електронних носіях, між

ЕОМ звичайними лініями зв'язку. Інформація може продаватися та купуватися, мати ціну, що незрівнянно перевищує ціну матеріального носія. Часто володіння інформацією дає переваги, ціну яких неможливо підрахувати, наприклад, у військовій справі. Термін збереження секретності інформації може коливатися від декількох годин до багатьох десятиліть. Тому вкрай потрібні спеціалісти, які володіють криптографічними, технічними, комплексними методами захисту, знають відповідні стандарти, здатні використовувати (або розробляти) програмне й апаратне забезпечення для гарантування таємності та цілісності конфіденційної інформації. Криптографічні методи захисту вважаються одними з найбільш надійних та ефективних.

- Області застосування захисту інформації (відповідно — види таємниці):

  1. Військова;
  2. Дипломатична;
  3. Фінансова;
  4. Банківська;
  5. Комерційна;
  6. Промислова;
  7. Наукова;
  8. Юридична;
  9. Медична;
  10. Особиста таємниця.

- Мета і головні задачі захисту інформації:

  1. Конфіденційність (секретність) інформації;
  2. Цілісність інформації;
  3. Автентичність інформації;
  4. Доступність інформації.

- Напрямки, аспекти, методи і засоби захисту інформації:

  1. Юридичні, правові;
  2. Методично-нормативні;
  3. Організаційні;
  4. Безпосередні (фізичні);
  5. Технічні — захист від витоку по технічним каналам:
     (a) електромагнітному
     (b) оптичному
     (c) акустичному
     (d) віброакустичному;
  6. Стеганографічні;
  7. Криптографічні. Методи математичного захисту інформації;
  8. Методи квантової криптографії;
  9. Морально-етичні норми.

1.2 Перші поняття криптографічного захисту інформації

Визначення 1.2.1 (Криптографічний захист інформації)**.** Криптографічний захист інформації — це різновид захисту інформації, який реалізується за допомогою криптографічних перетворень, спеціальних ключових даних з метою приховування та відновлення змісту інформації, підтвердження достовірності, авторства, запобігання несанкціонованому використанню тощо.

Визначення 1.2.2 (Криптографічне перетворення)**.** Криптографічне перетворення — це перетворення інформації відповідно до певних правил (логічних, математичних) з метою забезпечення функціонування криптографічних протоколів.

Визначення 1.2.3 (Криптографічний ключ)**.** Криптографічний ключ — це параметр, який використовується в криптографічному алгоритмі для вибору конкретного криптографічного перетворення; ключі можуть бути таємними або відкритими.

Визначення 1.2.4 (Криптографічний протокол)**.** Криптографічний протокол — це послідовність узгоджених дій згідно з деякими правилами, у відповідності з якими відбувається обмін інформацією між сторонами або учасниками протоколу та її перетворення з використанням криптографічних методів і засобів. Простий приклад криптографічного протоколу – це зашифрування та розшифрування повідомлення.

Визначення 1.2.5 (Криптографія)**.** Криптографія — науково-технічна дисципліна, яка вивчає принципи, методи і засоби криптографічного захисту інформації і інформаційних технологій, предметом якої є розробка криптографічних систем.

Визначення 1.2.6 (Криптоаналіз)**.** Криптоаналіз — це науково-технічна дисципліна, яка вивчає методи, способи і засоби аналізу криптографічного захисту інформації: криптографічних систем, криптографічних алгоритмів, протоколів з метою знайти способи їх розкриття без знання секретних ключів і, можливо, будови криптосистем, знайти способи несанкціонованого доступу, підробки даних тощо. Криптоаналіз оцінює складність таких способів розкриття (злому) і стійкість криптографічного захисту інформації. Фахівця, який займається криптоаналізом будемо називати криптоаналітиком.

Визначення 1.2.7 (Криптологія)**.** Криптологія за найбільш поширеною сучасною термінологією, об'єднує в собі дисципліни криптографію і криптоаналіз.

Зауваження 1. *Не всі країни дотримуються останньої термінології щодо дисциплін. Так, наприклад, в Росії назва „криптографія" об'єднує в собі власне криптографію (криптосинтез) у вище наведеному розумінні і криптоаналіз, а криптологія розглядається як галузь криптографії, що вивчає математичні моделі криптографічних систем, і також поділяється на криптосинтез та криптоаналіз.*

1.3 Етапи розвитку технологічних засобів криптографії

1. “Ручна” криптографія (із давнини до середини-кінця XIX століття)

   Основні види шифрів — заміни і перестановки.

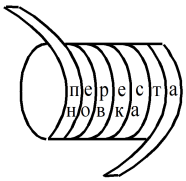

Рис. 1.1: Шифр Скитала

Перший шифр перестановки, застосування якого зафіксоване у військовій справі, (Спарта, V ст. до н.е.) – шифр Скитала (рис. 1.1). Таємний ключ – діаметр барабана.

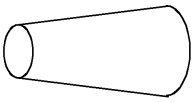

Рис. 1.2: Засіб криптоаналізу шифру Скитала

Для шифрування на стрічці, що намотувалась на барабан (скитал), писалось вздовж барабана повідомлення. Після знімання з барабану на стрічці була зовні випадкова послідовність літер – шифроване повідомлення. Криптоаналіз шифру Скитала запропонував Арістотель за допомогою барабана змінного діаметру (рис. 1.2): якщо на намотаній на нього стрічці з шифрованим повідомленням у деякому місці вгадувались якісь частини слів, то цьому місцю відповідав діаметр справжнього барабану.

Прикладом шифру заміни є шифр Цезаря — заміна кожної букви повідомлення на букву циклічно віддалену в алфавіті на фіксоване число позицій.

2. Застосування телеграфу для шифрування і кодування (з середини XIX ст.)
3. Використання механічних машин (кінець XIX ст. – 20і роки XX ст.)
4. Електромеханічні машини (з 20-х років XX ст. – середина XX ст.)

   Приклад — ENIGMA — основна шифрувальна машина Вермахту у Другій світовій війні.

5. Електронні машини (з кінця 40-х років XX ст.)
6. Напівпровідникові криптосистеми
7. Криптосистеми, засновані на мікросхемах

8. Використання комп'ютерної техніки для криптографічного захисту
9. Квантова криптографія

1.4 Про розвиток теоретичної криптографії

Зміст