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

Лекція 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.

Зміст