Конспект учня

Інформаційна безпека – розділ інформатики, що вивчає закономірності забезпечення захисту інформаційних ресурсів від втрати, порушення функціонування, пошкодження, спотворення, несанкціонованого копіювання та використання.

Основні складові інформаційної безпеки:

- **Доступність** – забезпечення доступу до загальнодоступних даних усім користувачам, захист цих даних від спотворення та блокування зловмисниками.
- **Конфіденційність** – забезпечення доступу до даних на основі розподілу прав доступу.
- **Цілісність** – захист даних від зловмисного або випадкового видалення чи спотворення.

Класифікація загроз інформаційної безпеки:

- **В залежності від** обсягів **збитків:**
  - **нешкідливі** – не завдають збитків;
  - **шкідливі** – завдають значних збитків;
  - **дуже шкідливі** – завдають критичних збитків інформаційній системі, що призводить до повного або тривалого в часі припинення роботи інформаційної системи.
- **За метою:**
  -
  - зловмисні;
  - випадкові.
- **За місцем виникнення:**
  -
  - зовнішні;
  - внутрішні.
- **За походженням:**
  -
  - природні
  - техногенні;
  - зумовлені людиною.

Основні загрози інформаційної безпеки

- знищення та спотворення даних;
- отримання доступу до секретних або конфіденційних даних;
- пошкодження пристроїв інформаційної системи;
- отримання прав на виконання дій, що передбачені тільки для окремих керівних осіб;
- отримання доступу до здійснення фінансових операцій замість власників рахунків;
- отримання повного доступу до керування інформаційною системою.

Етичні та правові основи захисту даних

Етичні норми – не використовувати комп’ютерну техніку та програмне забезпечення на шкоду іншим людям, не порушувати авторських прав.

Правова основа захисту даних – правові акти.

Акти, що утверджують права та свободи людини:

- **Загальна декларація прав людини** (прийнята Генеральною Асамблеєю ООН 10.12.1948 року): *«Стаття 19. Кожна людина має право на … свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів»;*
- **Конвенція про захист прав людини і основоположних свобод** (прийнята Радою Європи 04.11.1950 року) проголошує, що *свобода вираження поглядів може обмежуватися законодавством «…для запобігання розголошенню конфіденційної інформації»;*
- **Конституція України:** *«Стаття 32…. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом…». «Стаття 54. Громадянам гарантується свобода літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав…».*

Кримінальним кодексом України передбачено кримінальну відповідальність за:

- Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер»;
- Незаконне відтворення, розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, … їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації»;
- Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення»;
- Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;
- Створення з метою використання, «розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;
- Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації» тощо.

Заходи реалізації організаційних принципів захисту даних

ЦІЛІ ЗАХИСТУ ДАНИХ	ЗАХОДИ
Захист від втрати даних внаслідок стихійних явищ, збоїв у роботі електричних мереж, некомпетентності працівників тощо	Використання додаткових пристроїв автономного електроживлення, створення копій особливо важливих даних і зберігання їх у захищених місцях
Захист від умисного пошкодження комп'ютерного та мережевого обладнання, викрадення даних безпосередньо з пристроїв	Створення системи охорони з розмежуванням доступу до особливо важливого обладнання

Захист від викрадення даних власними працівниками	Введення різних рівнів доступу до даних, використання персональних захищених паролів, контроль за діяльністю працівників
Захист від викрадення, спотворення чи знищення даних з використанням спеціальних комп’ютерних програм	Використання спеціального антишпигунського та антивірусного програмного забезпечення, шифрування даних, що передаються мережами, використання паролів доступу та обов’язкового дублювання даних