Урок №1. **Безпека інформаційних технологій. Інформація та інформаційні відносини. Безпека суб'єктів інформаційних відносин**

-

Властивості інформації:

- **Конфіденційність** (англ. confidentiality) — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем.
- **Цілісність** (англ. integrity) — означає неможливість модифікації неавторизованим користувачем.
- **Доступність** (англ. availability) — властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час.
- **Апелювання** (англ. non-repudiation) — можливість довести, що автором є саме заявлена людина (юридична особа), і ніхто інший.
- **Вірогідність** (англ. reliability) — властивість інформації, яка визначає ступінь об'єктивного, точного відображення подій, фактів, що мали місце.
- **Автентичність** (англ. authenticity) — властивість, яка гарантує, що суб'єкт або ресурс ідентичні заявленим.

Вивчення нового матеріалу

Основні поняття в області безпеки інформаційних технологій

Інформаційне середовище представляється як сукупність інформації, що оточує людину, незалежно від форми її подання.

- Яким може бути інформаційне середовище?

Під безпекою інформаційного середовища розуміється захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого отримання) інформації, модифікації або фізичного руйнування її компонентів, тобто здатність протидіяти різним підступним впливам на ІС.

Інформаційна загроза - потенційна можливість певним чином порушити інформаційну безпеку.

- Про які інформаційні загрози вам відомо?

Інформаційна небезпека - обставини, при яких інформація або її похідні можуть вплинути на людину або обставини таким чином, що це призведе до її погіршення або неможливості її функціонування і розвитку.

Інформаційний захист - процес забезпечення інформаційної безпеки.

Інформаційна безпека особистості - це стан і умови життєдіяльності особистості, при яких реалізуються її інформаційні права і свободи.

- Чи важливо забезпечити інформаційну безпеку особистості?

Інформаційна безпека суспільства - це стан суспільства, в якому йому не може бути завдано істотної шкоди шляхом впливу на його інформаційну сферу.

- Що може трапитися, якщо не забезпечити інформаційну безпеку суспільства?

Інформаційна війна - використання і управління інформацією з метою отримання конкурентної переваги над противником. Інформаційна війна може включати в себе збір тактичної інформації, забезпечення безпеки власних інформаційних ресурсів, поширення пропаганди або дезінформації, щоб деморалізувати противника і населення, підрив якості інформації противника і попередження можливості збору інформації противником.

Інформаційний тероризм - гранично небезпечне соціальне явище, спрямоване на дезорієнтацію свідомості людей з метою деструктивного видозмінювання істинності знань, світогляду і думок мирного населення шляхом застосування інформаційних ресурсів і систем.

- У чому відмінність між інформаційною війною та тероризмом?

Інформаційна залежність - залежність від різних джерел інформації, нав'язливе бажання отримувати інформацію будь-яким доступним способом і хвороблива нездатність відмовитися від безперервного отримання інформації усіма можливими способами.

- Чи траплялося вам спостерігати інформаційну залежність?
- Наведіть приклади.

Автоматизована система - це організаційно-технічна система, що реалізує інформаційну технологію і поєднує у собі:

- обчислювальну систему;
- фізичне середовище;
- персонал;
- інформацію, яка обробляється

Будь-яка інформація, що обробляється та зберігається в інформаційних системах, чогось варта при умові її достовірності та гарантованості, а тому інформація має бути надійно захищена.

Причинами виникнення загроз для функціонування ІС є наступне:

- *інформація - товар*: має ціну, вартує грошей, може купуватись і продаватись, загалом представляє інтереси багатьох груп людей, бізнесу, може цікавити конкурентів, опонентів тощо;
- *інформація - гроші*: реальні гроші у вигляді файлових структур, електронних документів тощо;

- *відкритість інформаційних каналів*: використання глобальних мереж передачі інформації, кожен клієнт є учасником одного загального цілого і фізично з допомогою телекомунікацій має доступ до решти учасників процесу.

Несприятливий вплив - вплив, що призводить до зменшення цінності інформаційних ресурсів.

Загроза - будь-які обставини, чи події, що можуть спричинити порушення політики безпеки інформації та нанесення збитків ІКС.

Атака - це спроба реалізації загрози. Якщо атака є успішною, це називають проникненням. Наслідком успішної атаки є порушення безпеки інформації в системі, яке називають компрометацією.

Вразливість системи - нездатність системи протистояти реалізації певної загрози або ж сукупності загроз.