Урок № *2 Інформаційна безпека 10(11) клас вибірковий модуль*

Тема. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій. Інформація та інформаційні відносини. Суб'єкти інформаційних відносин, їх інтереси та безпека, шляхи нанесення їм шкоди. Безпека інформаційних технологій.

1. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій.

Більше 4 млрд. людей користуються комп'ютерами і Інтернетом. Комп'ютеризації торкнулись майже всі аспекти діяльності людини: від укладення договорів до особистих відносин, від придбання товарів через Інтернет-магазин до навчання. Набирає обертів IoT (Інтернет речей) і скоро Ваш холодильник сам через Інтернет буде замовляти доставку продуктів.

Відбувається стрімке впровадження комп'ютерної техніки та інформаційних технологій майже в усі сфери діяльності людини - біржова та банківська справа, страхування, медицина тощо. У зв'язку цим зростає кількість злочинів, спрямованих проти інформаційної безпеки.

Велику зацікавленість з боку кібер-злочинців викликає діяльність і державних структур, і комерційних підприємств. Їхньою метою є розкрадання, розголошення конфіденційної інформації, підрив ділової репутації, порушення працездатності і, як наслідок, доступності інформаційних ресурсів організації. Такі дії завдають величезних моральних і матеріальних збитків.

Насправді ризик чатує не лише на крупні компанії, але й на окремих користувачів. За допомогою різних засобів злочинці дістають доступ до персональних даних – номерів банківських рахунків, кредитних карт, паролей, виводять обчислювальну систему з ладу або дістають повний доступ до комп'ютера. Надалі такий комп'ютер може використовуватися як частина зомбі-мережі – мережі заражених комп'ютерів, які використовують зловмисники для проведення атак на сервери, розсилки спаму, збору конфіденційної інформації, розповсюдження нових вірусів і троянських програм. Одним з найбільших бажань користувача – бажання заховати свої особисті документи, програми і інші дані подалі від чужих очей.

Проблема захисту інформації у автоматизованих системах (АС) визначається наступними чинниками:

- високими темпами зростання засобів обчислювальної техніки і зв'язку, розширенням областей використання електронно-обчислювальних машин (ЕОМ);
- залученням в процес інформаційної взаємодії все більшого числа людей і організацій;

- ставленням до інформації, як до товару, переходом до ринкових відносин, з властивою ним конкуренцією і промисловим шпигунством, в області створення і збуту (надання) інформаційних послуг;
- концентрацією великих обсягів інформації різного призначення і приналежності на електронних носіях;
- наявністю інтенсивного обміну інформацією між учасниками цього процесу;
- зростанням числа кваліфікованих користувачів обчислювальної техніки і можливостей по створенню ними програмно-технічних впливів на систему;
- розвитком ринкових відносин (в області розробки, постачання, обслуговування обчислювальної техніки, розробки програмних засобів, в тому числі засобів захисту).

Отже, сьогодні всі визнають, що інформація є цінним надбанням і підлягає захисту.

2. Інформаційні відносини. Об’єкти та суб’єкти інформаційних відносин, їх інтереси та безпека, шляхи нанесення їм шкоди

Найважливішими компонентами інформаційної діяльності є:

- Інформація та інформаційні системи;
- суб’єкти – учасники інформаційних процесів;
- правові відносини виробників – споживачів інформаційної продукції;

Інформаційні відносини – це можливість доступу суб’єктів інформаційної безпеки до об’єктів, що визначаються певними правилами

Об’єкт – пасивний компонент системи, який зберігає, приймає або передає інформацію. Доступ до об'єкту означає доступ до інформації, яка міститься в ньому. У якості **об'єктів інформаційної безпеки** [information security object], необхідно розглядати: інформацію і інформаційні ресурси, носії інформації, процеси обробки інформації. До соціальних об'єктів інформаційної безпеки звичайно відносять особистість, колектив, суспільство, державу, світове товариство.

Суб’єкт – це активний компонент інформаційної системи, який може стати причиною потоку інформації від об'єкта до суб'єкта або зміни стану системи.

До суб'єктів інформаційної безпеки [information security subject] відносяться:

- держава, що здійснює свої функції через відповідні органи;
- громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства.

Суб’єкт інформаційних відносин може постраждати (зазнати збитки та/або

одержати моральний збиток) не тільки від несанкціонованого доступу, але й від несправності системи, що викликала перерву в роботі.

3. Безпека інформаційних технологій.

Слово "безпека" латинського походження - secure (securus).Потім в англійській мові воно отримало написання "security".

Загальновідомо, що "безпека" - це відсутність небезпеки; стан діяльності, при якій з певною ймовірністю виключено заподіяння шкоди здоров'ю людини, будівель, приміщень та матеріально-технічних засобів у них.

Безпека об'єкта проявляється через безпеку його найбільш важливих властивостей або властивостей структурних складових.

Якщо об'єктом безпеки є *людина*, то його безпека полягає в захищеності від загроз йому, як живому організму, захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ і т. ін.

Якщо об'єктом безпеки є *суспільство* (спільність людей на певній території, яка характеризується економічною і духовною єдністю), то його безпека буде полягати в захищеності від загроз його членів, а також відносинами, що історично склалися між людьми.

Інформаційна безпека організації — спрямована на захист інформаційного середовища організації та забезпечення її нормального функціонування і динамічного розвитку.

Відповідно, в змісті *національної безпеки* розрізняють державну, економічну, суспільну, оборонну, інформаційну, екологічну та іншу безпеку.

Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи і т. ін.) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси і т. ін.) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Під ***безпекою інформації*** (Information security) або ***інформаційною безпекою*** розуміють захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних впливів природного або штучного характеру, здатних завдати шкоди безпосередньо даним, їхнім власникам і користувачам інформації та інфраструктурі, що підтримує інформаційну безпеку.

Під термінами "захист інформації" та "інформаційна безпека" мається на увазі сукупність методів, засобів і заходів, спрямованих на виключення

спотворень, знищення і несанкціонованого використання накопичуваних, оброблюваних і збережених даних.

Розглянемо принципи, на яких базується інформаційна безпека (рис. 2).

Стандартною моделлю безпеки даних може слугувати модель із трьох категорій:

1. **Конфіденційність** означає, що доступ до конкретної інформації здійснюють тільки ті особи, що мають на нього право (коло осіб узгоджено з власником інформації).

2. **Цілісність** означає, що в ході передавання й зберігання інформація зберігає зміст і структуру; створювати, знищувати або змінювати дані має право лише власник. Цілісність - цеуникнення несанкціонованої зміни даних та існування даних у неспотвореному вигляді.

3. **Доступність** означає здатність забезпечувати своєчасний і безперешкодний доступ повноправних користувачів до необхідної інформації. Достовірність означає неможливість викривлення чи спотворення інформації.

Інформаційна безпека полягає в захисті систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації.

Домашнє завдання

1) **Опрацювати** конспект
2) **Підготувати** індивідуальні чи групові повідомлення (міні-проекти) про загрози безпеці: інтернет-шахрайство; спам-розсилки; бот-мережі (botnet), DDoS-атаки, крадіжка коштів, «крадіжка особистості».
3) **Творче завдання**: Створити скрайб - видео (візуалізація інформації, де картинка йтиме за вами під час розповіді) за інформацією уроку (AnimizAnimatorMaker).