Тема. Загрози безпеці інформації в автоматизованих системах. Основні джерела і шляхи реалізації загроз.

Коли користувач вмикає комп'ютер і мандрує сторінками сайтів, здійснює покупки за електронні гроші чи використовує прикладні програми, то хоче бути впевненим, що доступ до його даних знаходиться під його контролем, тобто що інформація захищена. Але, як ми вже з'ясували, під час користування Інтернетом часто виникають загрози інформаційній безпеці.

Сьогодні ми познайомимося з поняттям загрози інформаційної безпеки, різновидами загроз та шляхами їх реалізації. Отже, тема нашого уроку «Загрози безпеці інформації», ми дізнаємося які загрози можуть виникати під час роботи з комп'ютером.

Вивчення нового матеріалу

1. Загрози безпеці інформації

Під загрозою розуміють будь-які обставини та події, що виникають у зовнішньому середовищі, які у відповідних умовах можуть викликати появу небезпечної події.

Інформаційна загроза — це потенційна можливість певним чином порушити інформаційну безпеку та (або) нанесення збитків АС. Загрози самі по собі не виявляються. Всі загрози можуть бути реалізовані тільки при наявності яких-небудь слабких місць - вразливостей, властивих об'єкту інформатизації.

Вразливість системи: нездатність системи протистояти реалізації певної загрози або сукупності загроз.

Атака на ком'ютерну систему – це дія, що робиться зловмисником для пошуку і використанні тієї або іншої уразливості системи. Таким чином, атака – це реалізація загрози безпеки.

2. Класифікація загроз

Залежно від обсягів завданих збитків загрози інформаційній безпеці поділяють на:

Нешкідливі – не завдають збитків;

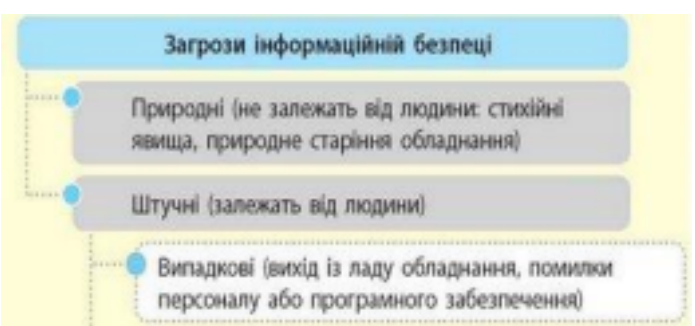
Шкідливі – завдають значних збитків;

Дуже шкідливі – задають критичних збитків інформаційній системі. Загрози можуть мати як природний, так і штучний характер. А вони, у свою чергу, можуть бути або випадковими, або навмисними. Слід зазначити, що

серед усіх загроз найбільший відсоток за масштабом і ступенем пошкодження даних припадає на людський чинник.

Загрози пошкодження даних можна *класифікувати за природою їх виникнення.*

- **Природні (об'єктивні, не залежать від людини)** стихійні явища, природне старіння обладнання, відмова елементів



ОС;

- **Штучні (суб'єктивні, залежать від людини)**
  - Випадкові (вихід із ладу обладнання, помилки персоналу або програмного забезпечення)
  - Навмисні (перехоплення даних, маскування під дійсного користувача, фізичне руйнування системи)

За *метою впливу* розрізняють наступні основні типи загроз безпеки (відповідно до відомої моделі безпеки даних):

1. **Загроза порушення конфіденційності (розкриття)** полягає в тому, що дані стають відомими тому, хто не має права доступу до них. Вона виникає щоразу, коли отримано доступ до деяких секретних даних, що зберігаються в комп'ютерній системі чи передаються від однієї системи до іншої. Іноді, у зв'язку із загрозою порушення конфіденційності, використовується термін «витік даних».
2. **Загроза порушення цілісності** передбачає будь-яку умисну зміну даних, що зберігаються в комп'ютерній системі чи передаються з однієї системи в іншу. Вона виникає, коли зловмисники навмисно змінюють дані, тобто порушується їхня цілісність, може відбутися її повне або часткове знищення, спотворення, фальсифікація, дезінформація). Цілісність даних також може бути порушена внаслідок випадкової помилки програмного або апаратного забезпечення.
3. **Загроза відмови служб (загроза доступності)** виникає щоразу, коли в результаті навмисних дій, які виконує інший користувач або зловмисник, блокується доступ до деякого ресурсу комп'ютерної системи, відбувається порушення часткове або повне працездатності системи. Блокування буває постійним, якщо доступ до запитуваного ресурсу ніколи не буде отримано, або воно може викликати тільки затримку запитуваного ресурсу, досить довгу для того, щоб він став непотрібним. У цих випадках говорять, що ресурс вичерпано.

Джерела загроз:

1. **Людський чинник.** Ця група загроз пов'язана з діями людини, що має санкціонований або несанкціонований доступ до інформації. Загрози цієї групи можна розділити на:

- *зовнішні* — дії кібер-злочинців, хакерів, інтернет шахраїв, недобросовісних партнерів, кримінальних структур;
- *внутрішні* — дії персоналу компаній і також користувачів домашніх комп'ютерів. Дії даних людей можуть бути як умисними, так і випадковими.

2. **Технічний чинник.** Ця група загроз пов'язана з технічними проблемами – фізичне і моральне старіння устаткування, неякісні програмні і апаратні засоби опрацювання інформації. Все це приводить до відмови устаткування втрати інформації.
3. **Стихійний чинник.** Ця група загроз включає природні катаклізми, стихійні лиха і інші форс-мажорні обставини, незалежні від діяльності людей.

Розглядають й інші класифікації загроз: **за метою** (зловмисні, випадкові), **за місцем виникнення** (внутрішні, зовнішні), **за походженням** (природні, техногенні, зумовлені людиною) тощо.

Всі ці джерела загроз необхідно обов'язково враховувати при розробці системи захисту інформаційної безпеки.

Шляхи поширення загроз (людський чинник)

1. **Глобальна мережа Інтернет** унікальна тим, що не є чиєюсь власністю і не має територіальних меж. Це багато в чому сприяє розвитку численних веб ресурсів і обміну інформацією. Зараз будь-яка людина може дістати доступ даним, що зберігаються в Інтернеті, або створити свій власний веб-ресурс. Ці особливості глобальної мережі надають зловмисникам можливість скоєння злочинів в Інтернеті, затрудняючи їх виявлення і покарання. Зловмисники розміщують віруси і інші шкідливі програми на веб-ресурсах, «маскують» їх під корисне і безкоштовне програмне забезпечення.

   Скрипти, що автоматично запускаються при відкритті веб-сторінки, можуть виконувати шкідливі дії на вашому комп’ютері, включаючи зміну системного реєстру, крадіжку особистих даних і встановлення шкідливого програмного забезпечення. Використовуючи мережеві технології, зловмисники реалізують атаки на віддалені комп’ютери та сервери компаній. Результатом таких атак може бути отримання повного доступу до ресурсу, а отже, до даних, що зберігаються на ньому, або виведення його з ладу.
2. **Локальна мережа (Інтранет**) – це внутрішня мережа, спеціально розроблена для управління інформацією усередині компанії або приватної домашньої мережі. Це єдиний простір для зберігання, обміну і доступу до інформації для всіх комп'ютерів мережі. Тому, якщо якій-небудь з комп'ютерів мережі заражений, решту комп'ютерів піддано величезному ризику зараження. Щоб уникнути виникнення таких ситуацій необхідно захищати не лише периметр мережі, але й кожний окремий комп'ютер.

3. **Електронна пошта**. Наявність поштових застосунків практично на кожному комп'ютері і використання шкідливими програмами вмісту електронних адресних книг для виявлення нових жертв забезпечують сприятливі умови для

розповсюдження шкідливих програм. Користувач зараженого комп'ютера, сам того не підозрюючи, розсилає заражені листи адресатам, які у свою чергу відправляють нові заражені листи і т.д. Нерідкісні випадки, коли заражений файл-документ унаслідок недогляду потрапляє в списки розсилки комерційної інформації якої-небудь крупної компанії. В цьому випадку страждають сотні або навіть тисячі абонентів таких розсилок, які потім поширять заражені файли десяткам тисячам своїх абонентів.

4. **Знімні носії інформації** — CD-диски, флеш-карти — широко використовують для зберігання і поширення інформації. При активуванні файлу знімного носія, що містить шкідливий код, є загроза пошкодити дані на вашому комп'ютері і розповсюдити вірус на інші носії інформації або комп'ютери мережі.

Загрози, які можуть завдати шкоди інформаційній безпеці організації, можна розділити на кілька категорій (мал. 2).

1) До ***дій, що здійснюються авторизованими користувачами***, належать: цілеспрямована крадіжка або знищення даних на робочій станції чи сервері; пошкодження даних користувачами в результаті необережних дій.

2) ***Дії хакерів***: Хакер — кваліфікований IT фахівець, який знається на комп'ютерних системах і втручається в роботу комп'ютера, щоб без відома власника дізнатися деякі особисті відомості або пошкодити дані, що зберігаються в комп'ютері. Їхні мотиви можуть бути різними: помста, самовираження (дехто робить це задля розваги, інші — щоб показати свою кваліфікацію), винагорода. Останнім часом поняття «хакер» використовується для визначення мережевих зломщиків, розробників комп'ютерних вірусів й інших кіберзлочинців. У багатьох країнах злом комп'ютерних систем, розкрадання інформаційних даних, створення та поширення комп'ютерних вірусів і шкідливого програмного забезпечення переслідується законодавством.

3) Окрема категорія електронних методів впливу — ***комп'ютерні віруси та інші шкідливі програми (***Malware***)***. Вони становлять реальну небезпеку, широко використовуючи комп'ютерні мережі, Інтернет й електронну пошту.

4) **DoS-атакою, або DDos-атакою** (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack — атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні) - напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких

комп’ютерна система була призначена.

5) **Спам** — небажані рекламні електронні листи, повідомлення на форумах, телефонні дзвінки чи текстові повідомлення, що надходять без згоди користувача.Не будучи джерелом прямої загрози, небажана кореспонденція збільшує навантаження на поштові сервери, створює додатковий трафік, засмічує поштову скриньку користувача, веде до втрати робочого часу і тим самим наносить значні фінансові втрати. Зловмисники стали використовувати так звані спамерські технології масового розповсюдження, щоб примусити користувача відкрити лист, перейти по посиланню з листа на якийсь інтернет ресурс. Отже, можливості фільтрації спаму важливі не лише самі по собі, але і для протидії інтернет-шахрайству і розповсюдженню шкідливих програм.
6) ***Фішинг*** — один з найпопулярніших і прибуткових (для тих, хто його реалізує) видів атак. Сценарій атак фішингу: зловмисник створює сайт, який у точності копіює дизайн і можливості сайта будь-якого банку,інтернет-магазину або платіжної системи. Далі він замовляє спам-розсилку листів, у яких переконує своїх жертв зайти за посиланням на сайт і заповнити будь-яку форму з внесенням персональних даних. Здебільшого причиною запиту даних зазначається повідомлення про збій в інформаційній системі й загрозу блокування профілю користувача, якщо не буде надано дані. Мета — збір конфіденційної інформації — паролі, коди тощо.
7) ***Кардинг*** - У зв’язку з появою кредитних карт, електронних грошей і можливістю їхнього використання через Інтернет інтернет-шахрайство стало одним з найбільш поширених злочинів.
8) ***Інтернет шахрайство***
9) ***бот-мережі (botnet)*** **–** це мережа повязаних між собою вірусом комп’ютерів, які керуються зловмисниками з командного центру.
10) «крадіжка особистості» (Identity Theft)

Формування практичних умінь і навичок

Увага! ***Під час роботи з комп’ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.*** (Інструктаж з правил техніки безпеки)

Завдання 1.Виконайте інтерактивну вправу «Чинники загроз безпеці даних» (розділ Захист інформації) http://LearningApps.org/3944076.

Завдання 2.Виконайте інтерактивну вправу «Класифікація загроз безпеці» (розділ Захист нформації)https://learningapps.org/6278374).

Завдання 3.Виконайте інтерактивну вправу «Загрози безпеці та пошкодження даних у комп’ютерних системах» (розділ Захист нформації) https://learningapps.org/5745146.

Завдання 4. Створити спільну презентацію про загрози, використовуючи можливості Google Диску.

Обговорюємо .

- На які види поділяються загрози інформаційній безпеці залежно від обсягів завданих збитків?
- На які види поділяються загрози інформаційній безпеці залежно від результатів шкідливих дій?
- Які чинники можуть становити загрозу комп'ютеру?

Домашнє завдання

1) Опрацювати конспект