Теоретичний матеріал до теми: "Проблеми інформаційної безпеки. Загрози при роботі в Інтернеті і їх уникнення "

Сьогодні наслідки від пошкодження або знищення інформації (даних) є більш значними, ніж втрата матеріальних ресурсів. Нерідко вартість інформації, втраченої, наприклад, під час природного лиха або техногенної аварії, може в сотні разів перевищувати вартість будівель. Тому на цьому уроці ми розглянемо принципи інформаційної безпеки, види загроз інформаційній безпеці та правила безпечної роботи в Інтернеті.

Інформаційна безпека — це стан захищеності систем передавання, опрацювання та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність даних.

Під конфіденційністю розуміють забезпечення доступу до даних на основі розподілу прав доступу, захист від несанкціонованого ознайомлення. Доступність означає забезпечення доступу до загальнодоступних даних усім користувачам і захист цих даних від блокування зловмисниками. Цілісність передбачає захист даних від їх зловмисного або випадкового знищення чи спотворення.

З технічної точки зору, залежно від результату шкідливих дій, можна виділити такі види загроз інформаційній безпеці:

• отримання несанкціонованого доступу до секретних або конфіденційних даних;

• порушення або повне припинення роботи комп’ютерної інформаційної системи;

• отримання несанкціонованого доступу до керування роботою комп’ютерної інформаційної системи;

• знищення та спотворення даних.

Значна частина загроз інформаційній безпеці виникає внаслідок користування ресурсами Інтернету. Серед них основними загрозами є такі:

• потрапляння в інформаційну систему шкідливого програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем;

• інтернет-шахрайство, наприклад фішинг — вид шахрайства, метою якого є виманювання персональних даних у клієнтів;

• несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем;

• потрапляння комп'ютера до ботнетмережі через приховане встановлення програмного забезпечення, яке використовується зловмисником для виконання певних, найчастіше протиправних, дій з використанням ресурсів інфікованих комп'ютерів.

Такими діями можуть бути розсилання спаму, добір паролів перебором усіх можливих варіантів, отримання персональних даних про користувачів, крадіжка номерів кредитних карток, паролів доступу, атаки з метою відмови в обслуговуванні — так звані DDoS-атаки, щоб порушити доступ до деякого інтернет-сервісу шляхом перевантаження його обчислювальних ресурсів;

• «крадіжка особистості» — несанкціоноване заволодіння персональними даними особи, що дає можливість зловмиснику здійснювати діяльність (підписувати документи, отримувати доступ до ресурсів, користуватися послугами, знімати кошти з банківських рахунків тощо) від її імені.

Для того щоб максимально уникнути загроз під час роботи в Інтернеті, варто дотримуватися правил:

1. Використовуйте тільки ліцензійне програмне забезпечення. Установлюйте програми тільки з офіційних джерел. Перед установленням читайте відгуки інших користувачів, якщо вони доступні.

2. Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп'ютери. Бажано, щоб оновлення антивірусних баз здійснювалося регулярно та автоматично.

3. Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.

4. Використовуйте надійні паролі. Не використовуйте на різних інтернет-ресурсах один і той самий пароль, змінюйте його регулярно.

5. Приєднуйтеся тільки до перевірених Wi-Fi-мереж. Не відправляйте важливі дані через публічні та незахищені Wi-Fi-мережі.

6. Установіть фільтр спливаючих вікон у браузері.

7. Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузера та URL-адреси веб-сайтів, щоб визначити,чи не підроблений сайт ви відвідуєте.

8. Не відкривайте повідомлення електронної пошти від невідомих вам осіб і прикріплені до них файли, яких ви не очікуєте.

9. Подумайте про можливі ризики для вас перед тим, як викласти щось у мережу Інтернет.

10. Створюйте резервні копії важливих для вас даних, зберігайте їх на носіях даних, відключених від мережі Інтернет.