Інформаційна безпека. Загрози при роботі в Інтернеті і їх уникнення

Теорія:

Проблема захисту даних від втрати, викрадення, спотворення або пошкодження потребує посиленої уваги оскільки зростає роль ***інформаційно-комунікаційних технологій*** у сучасному суспільстві.

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

Конфіденційність — забезпечення доступу до даних на основі розподілу прав доступу, захист від несанкціонованого ознайомлення.

Дані можуть бути відкриті (право доступу мають усі користувачі), до деяких даних має доступ тільки певна група людей, а деякі дані — особисті, до них доступ може мати тільки одна людина.

Доступність — забезпечення доступу до загальнодоступних даних усім користувачам і захист цих даних від блокування зловмисниками.

Цілісність — захист даних від їх зловмисного або випадкового знищення чи спотворення.

Інформаційна безпека включає в себе комплекс заходів, які повинні забезпечити захищеність даних від несанкціонованого доступу, використання, оприлюднення, внесення змін чи знищення.
Види загроз інформаційній безпеці:

- отримання доступу до секретних або конфіденційних даних;
- порушення або повне припинення роботи комп'ютерної інформаційної системи;
- отримання доступу до керування роботою комп'ютерної інформаційної системи;
- знищення або спотворення даних.

Деструкція — порушення або руйнування нормальної структури чого-небудь.

Існує досить багато **загроз**. Основні з них:
• Потрапляння в інформаційну систему шкідливого програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем.
• Атаки хакерів.
• **BotNet** — це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням.
• **DdoS** — атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS-attack (Distributed) Denial-of-service attack) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.
• **Фішинг** — вид шахрайства, метою якого є виманювання персональних даних у клієнтів онлайн-аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо.
Для **смартфонів** характерні ті самі загрози, що і для стаціонарних комп’ютерів: віруси, троянські програми, мережеві хробаки, рекламні модулі тощо, орієнтовані на різні типи мобільних пристроїв.

Зверни увагу!

Основні правила безпечної роботи в Інтернеті:

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

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

• Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.

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

• Приєднуйтеся тільки до перевірених Wi-Fi-мереж. Не відправляйте важливі дані (дані кредитних карток, онлайн-банкінгу тощо) через публічні та незахищені Wi-Fi-мережі.

• Установіть фільтр спливаючих вікон у браузері.

• Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузера.

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

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

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

Для користувачів смартфонів є окремі рекомендації: не телефонуйте на незнайомі номери; уважно контролюйте послуги, на які ви підписуєтеся; установлюйте мобільні додатки лише з офіційних магазинів: PlayMarket (Android), AppStore (iOS), Marketplace (WindowsPhone); уважно стежте за тим, які дозволи вимагає програма під час установлення та оновлення програмного забезпечення на мобільних пристроях.

Джерела:

Інформатика (рівень стандарту): підруч. для 10-го (11-го) кл. закл. заг. серед, освіти / Й.Я. Ривкінд [та ін.]. — Київ : Генеза, 2018. — 144 с. : іл.

https://testinform.in.ua/category/10-11-klas/10-11kl-tema2/

http://it-science.com.ua/article.php?id=12&table=school9_11

Морально-етичні правила

- Використовуйте тільки ліцензоване програмне забезпечення
- Робіть посилання на використані ресурси
- Використовуйте антивірусні програми
- Створюйте надійні паролі під час реєстрації акаунтів
- Обмежуйте доступ сторонніх осіб до власного комп'ютера
- Не розголошуйте приватну інформацію стороннім особам
- Не відкривайте листи і файли, отримані від посторонніх осіб

Правова сторона

1. Закон України «Про інформацію»
2. Закон України «Про захист інформації в ІТ системах»
3. Закон України «Про державну таємницю»
4. Закон України «Про захист персональних даних»

Морально-етичні правила

- Використовуйте тільки ліцензоване програмне забезпечення
- Робіть посилання на використані ресурси
- Використовуйте антивірусні програми
- Створюйте надійні паролі під час реєстрації акаунтів
- Обмежуйте доступ сторонніх осіб до власного комп'ютера
- Не розголошуйте приватну інформацію стороннім особам
- Не відкривайте листи і файли, отримані від посторонніх осіб