

Бакунець Євген
Види загроз небе

Коток Дарина

Види загроз і небезпеки Види небезпек в Інтернеті різноманітні: від шкідливого ПЗ (віруси, хробаки, програми-вимагачі) та шахрайства (фішинг, соціальна інженерія), що краде дані й гроші, до кібербулінгу (цькування в мережі), дезінформації, недоречного контенту (порнографія, насильство) та ризиків приватного життя, коли публікація особистих даних призводить до реальних загроз.

Технічні загрози (Шкідливе ПЗ):

- **Віруси:** Приєднуються до файлів, пошкоджують дані.
- **Черв'яки:** Самостійно розповсюджуються мережею, сповільнюють роботу.
- **Трояни:** Маскуються під корисні програми, надаючи зловмисникам доступ.
- **Програми-вимагачі (Ransomware):** Шифрують файли, вимагаючи викуп.
- **Шпигунські програми (Spyware) / Рекламне ПЗ (Adware):** Збирають інформацію, показують нав'язливу рекламу.

Психологічні та соціальні загрози:

- **Фішинг:** Оманливі листи й сайти, що виманюють паролі, номери карток.
- **Соціальна інженерія:** Маніпуляції людьми для отримання секретної інформації.
- **Кібербулінг:** Цькування, приниження, провокації в соцмережах, іграх.
- **Тролінг:** Розпалювання конфліктів в онлайн-дискусіях.
- **Небезпечне спілкування:** Зв'язки з шахраями, сектантами, небезпечними незнайомцями.

Контентні та інформаційні загрози:

- **Дезінформація:** Поширення неправдивих новин, що може впливати на думки.
- **Шкідливий контент:** Насильство, порнографія, матеріали, що пропагують ненависть, суїцид.
- **Інтернет-залежність**

- ## Види небезпек і загроз в інтернеті

Інтернет-загрози – це шкідливе ПЗ (віруси, трояни, шпигуни), фішинг, кібербулінг, шахрайство (крадіжка даних, коштів, особистості), DDoS-атаки та небезпечний контент (порнографія, насильство, неправда). Вони становлять небезпеку для особистої безпеки (залежність, спілкування з шахраями, протиправні дії) та фінансової/інформаційної цілісності (витік даних, крадіжки). Захист включає антивірус, сильні паролі, обережність з посиланнями, налаштування приватності та цифрову етику. **інформаційна безпека** — стан захищеності інформаційного середовища суспільства, який забезпечує конфіденційність, доступність і цілісність даних.

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

Омельковець Артем

Види загроз і небезпеки в інтернеті
Види загроз в Інтернеті включають
шкідливе програмне забезпечення
(віруси, трояни, хробаки,
шифрувальники), фішинг та соціальну
інженерію (шахрайство з метою
викрадення даних), хакерські атаки
(DoS-атаки, несанкціонований доступ),
витоки та крадіжки персональних даних
і фінансів, а також небезпечний контент
(кібербулінг, насильство, недостовірна
інформація), що може завдати шкоди
користувачам, особливо дітям, і
порушити роботу систем.

Технічні загрози

- **Шкідливе ПЗ (Malware):** Віруси, хробаки, трояни, шпигунське ПЗ, рекламні програми (adware), програми-вимагачі (ransomware), які крадуть дані або блокують доступ до комп'ютера, вимагаючи викуп.
- **[DoS/DDoS атаки](#):** Перевантаження сервера для зупинки роботи сервісу.
- **[Несанкціонований доступ](#):** Отримання доступу до систем, даних, керування ними.

Соціальні та фінансові загрози

- **Фішинг:** Шахрайські електронні листи чи сайти, що видають себе за відомі компанії для виманювання паролів, даних карток.

- Соціальна інженерія: Маніпуляції людьми для отримання конфіденційної інформації.
- **Шахрайство**: Крадіжка коштів, особистих даних, розповсюдження недостовірної інформації.

Блог вчителя інформатики Гудімової Оксани Степанівни розташований за адресою <https://hudimova.blogspot.com/>.

На цьому блозі можна знайти різноманітні матеріали, зокрема:

- Інформація про вчителя: освіта, спеціальність, посада (вчитель інформатики Тинненського ліцею).
- Навчальні матеріали: завдання та вправи для учнів 5-6 класів, тести, матеріали з програмування мовою Java, тощо.
- Методичні розробки: презентації (наприклад, "Історія дитячої іграшки: від ляльки-мотанки до Майнкрафт").
- Корисні посилання: добірка сервісів (Wordwall, Genially, Interacty), електронних підручників та інших освітніх ресурсів.
- Новини та поради: інформація про курси з програмування для дітей, День безпечного Інтернету, тощо.

Булейко Софія

Види небезпек і загроз в Інтернеті

Матюк Поліна

сновні небезпеки в Інтернеті включають технічні загрози (віруси, шкідливі програми, фішинг, шахрайство, крадіжка даних), соціальні ризики (кібербулінг, онлайн-шантаж, грумінг, небезпечні знайомства, маніпуляції), інформаційні ризики (неправдива інформація, недостовірний контент, пропаганда насильства/наркотиків) та психологічні проблеми (залежність від ігор чи соцмереж, ізоляція). Ці загрози стосуються всіх користувачів, але особливо вразливими є діти та підлітки.

Технічні загрози

Шкідливе ПЗ: Віруси, черв'яки, трояни, програми-вимагачі (ransomware), шпигунське ПЗ (spyware), що крадуть дані, блокують системи або показують нав'язливу рекламу (adware).

Фішинг: Спроби виманити паролі, номери карток через підроблені сайти або листи від імені відомих компаній.

Шахрайство: Несанкціонований доступ до систем, крадіжки коштів, різні схеми обману, які часто використовують соціотехніки.

Соціальні та психологічні ризики

- [Кібербулінг](#): Цькування, залякування, приниження в мережі.
- Онлайн-грумінг та шантаж: Зловмисники входять у довіру до дітей, щоб отримати інтимні фото (сексторшн), а потім шантажують ними.

- **Небезпечні знайомства:** Контакти з незнайомцями, які видають себе за інших, з метою виманювання інформації про сім'ю, місце проживання, статки.
- **Залежність:** Інтернет-залежність, ігроманія, що призводять до соціальної ізоляції та проблем зі здоров'ям

Види небезпек і загроз в Інтернеті

Одарчук Соломія

В інтернеті існують різні види небезпек та загроз, які можна поділити на технічні (шкідливе програмне забезпечення, фішинг), соціальні (кібербулінг, соціальна інженерія) та контентні (образливий, недостовірний контент). Ці загрози можуть призвести до крадіжки особистих даних, фінансових збитків, а також завдати шкоди психічному здоров'ю

Технічні загрози

- **Шкідливе програмне забезпечення:**
 - **Віруси:** Самостійно розмножуються та пошкоджують файли на комп'ютері.
 -
 - **Черв'яки:** Самостійно розповсюджуються мережею, створюючи копії себе.
 -
 - **Троянські програми:** Маскуються під корисні програми, але виконують шкідливі дії, наприклад, надають зловмисникам доступ до даних.
 -
 - **Програми-вимагачі (ransomware):** Шифрують файли та вимагають викуп за їх відновлення.
 -
- **Фішинг:** Спроби отримати конфіденційну інформацію (паролі, дані карток) через підроблені веб-сайти та листи, що імітують відомі компанії.
- **Несанкціонований доступ:** Несанкціонований доступ до інформаційних ресурсів та систем, що може призвести до поширення, зміни або видалення даних.

Види небезпек і загроз інтернеті

Види небезпек і загроз в Інтернеті

Миронець Софія

Види небезпек і загроз різноманітні і класифікуються за походженням (природні, техногенні, соціальні, політичні), сферою впливу (екологічні, економічні, інформаційні), масштабом (індивідуальні, суспільні, державні) та характером (фізичні, хімічні, біологічні, кібер). До них належать стихійні лиха, промислові аварії, епідемії, тероризм, кібератаки (віруси, фішЗагрозиинг) та соціальні конфлікти, які можуть призводити до руйнувань, жертв та порушення стабільності.

- Природні: Землетруси, повені, урагани, метеорити, сонячна активність.
- Антропогенні/Техногенні: Промислові аварії (хімічні, радіаційні), транспортні катастрофи, війни, забруднення довкілля.
- Соціальні: Злочинність, безробіття, алкоголізм, тероризм, конфлікти на міжнаціональному ґрунті, протести, міграційні кризи.
- Політичні: Тероризм, війни, ідеологічні конфлікти, політичне гноблення

КостюкСофія Небезпеки в Інтернеті включають технічні загрози (віруси, черв'яки, трояни, програми-вимагачі, шпигунське ПЗ), соціальні маніпуляції (фішинг, кібербулінг, тролінг, шахрайство), небажаний контент (насильство, порнографія, ненависницькі матеріали), загрози особистій безпеці (онлайн-хижаки, кіберзалежування, секстинг) та залежності (ігрова, Інтернет-залежність). Це може призвести до втрати даних, фінансових збитків, психологічних травм та компрометації персональної інформації.

Віруси: Програми, що поширюються, прикріплюючись до інших файлів, і можуть знищувати системи.

- Троянські програми: Маскуються під корисні програми, надаючи зловмисникам доступ до системи.
- Програми-вимагачі (Ransomware): Шифрують файли та вимагають викуп за їх розблокування.
- Шпигунське ПЗ (Spyware): Збирає конфіденційну інформацію (паролі, дані карток).
- Рекламне ПЗ (Adware): Показує нав'язливу рекламу.

2. Загрози соціальної інженерії та шахрайство

- Фішинг: Обман шляхом створення фальшивих сайтів для викрадення паролів та фінансових даних.
- [Соціальна інженерія](#): Маніпулювання людьми для отримання конфіденційної інформації.
- Кібербулінг: Цькування, залякування, поширення чуток в мережі.
- Тролінг: Провокування конфліктів та негативних емоцій онлайн.
- Онлайн-шахрайство: Різні схеми обману з метою отримання грошей або даних.

Матюк Арт