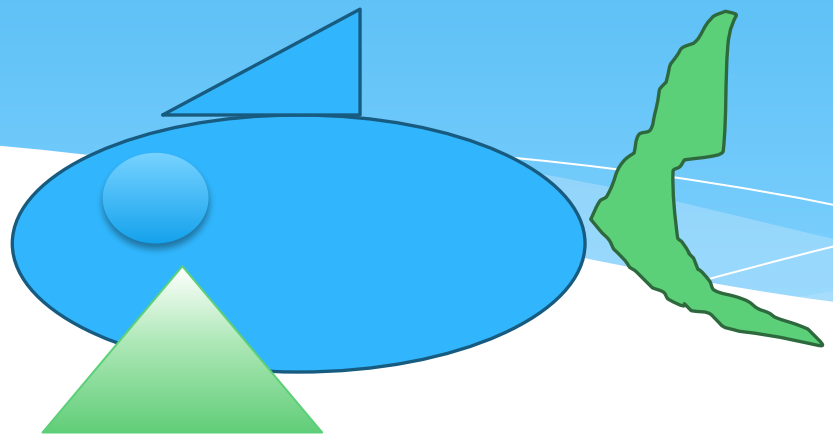
Безпека в інтернеті

Приготувала Соловей Катерина з 1-в класу



У цьому проекті ви отримаєте відповіді на такі запитання:

* Хто прагне проникнути до мого комп'ютера?
Хто за мною спостерігає?
Як уберегтися від непроханих візитерів?
Як саме й навіщо люди здобувають інформацію про мене?
Як уберегти персональну інформацію від викрадення?
Хто і як може завдати мені шкоди?
Як убезпечити себе в Інтернеті?

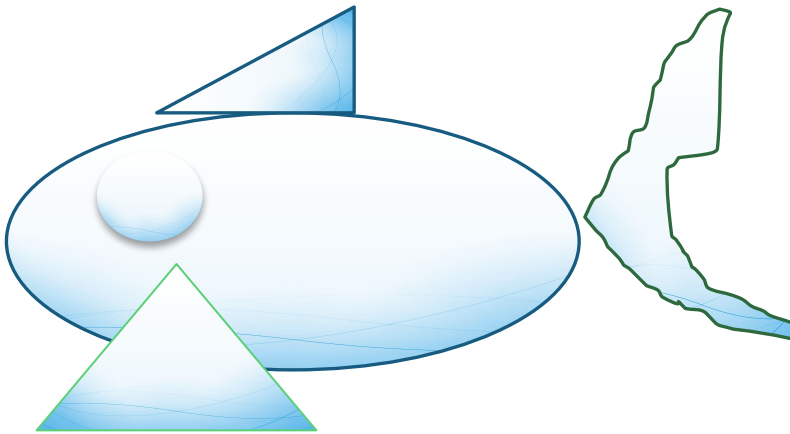
Хто прагне проникнути до мого комп'ютера?

Кожен користувач Інтернету повинен мати чітке уявлення про основні джерела безпеки, що йому загрожують. Це насамперед діяльність хакерів, а також віруси та спам.

* Хакер - тепер так називають людину, яка без дозволу проникає до чужої комп'ютерної системи з наміром викрасти або зруйнувати дані.

Способи проникнення Хакерів до чужих систем

* **1.Троянські коні.** Це шкідливі програми, які розповсюджуються шляхом обману.
2. **Перевантаження сайту або мережі.** Генеруючи багато запитів довільного змісту до сайту або мережі, хакер збільшує їхнє робоче навантаження внаслідок чого цей сайт або мережа не можуть нормально функціонувати.
* 3. **Підміна адрес.**
4. Аналіз пакетів. 5. Соціотехніка. 6. Підміна веб-сторінки.



Віруси та хробаки

Існують програми, що мандрують Інтернетом та, потрапивши на комп'ютер чи до локальної мережі, завдають тієї чи іншої шкоди. Особливо небезпечними є два види таких програм — віруси та хробаки.

Віруси. Програми названі на ім'я біологічних організмів, бо вони досить малі, розповсюджуються, роблячи копії з самих себе, та не можуть існувати без носія.

Першим відомим "хробаком" прийнято вважати програму Роберта Морріса , студента Корнелського університету. За 90 хвилин, використовуючи помилку переповнювання буфера, Morris Worm заразив 6000 комп'ютерів Глобальної Мережі.

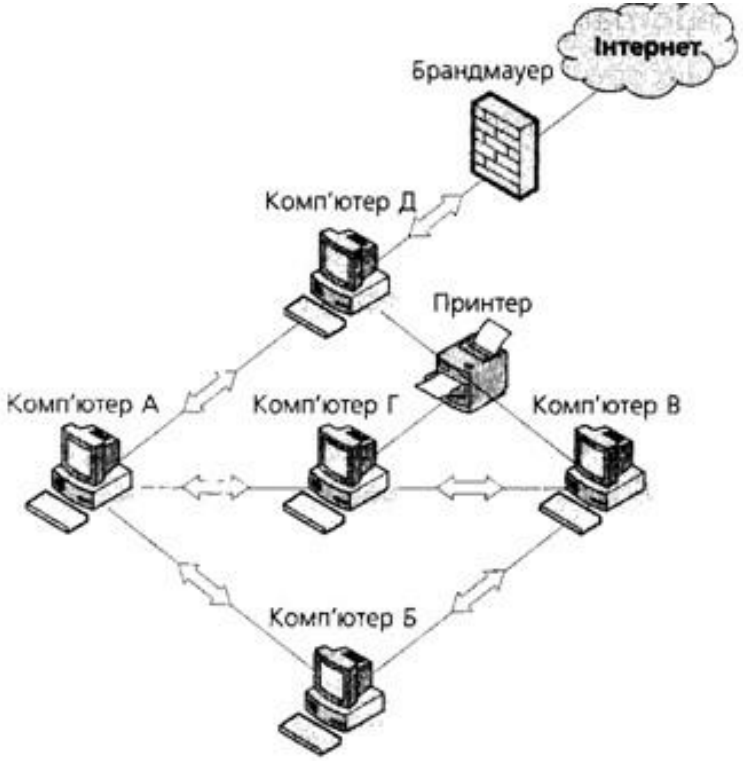
Хто за мною спостерігає?

* Крім програм, за допомогою яких певні люди намагаються проникнути до вашої системи, існують також засоби, що застосовуються для спостереження за вами. Це насамперед програмне забезпечення, яке зазвичай називають adware та spyware, шпигунські програми, програми для батьківського контролю, блокуючи програми тощо.
* Ці програми можуть відстежувати ваші звички стосовно мандрування Інтернетом, надсилати комусь дані без вашого дозволу, змінювати адресу домашньої сторінки вашого браузера і навіть змінювати системні файли комп’ютера.

Як уберегтися від непроханих візитерів?

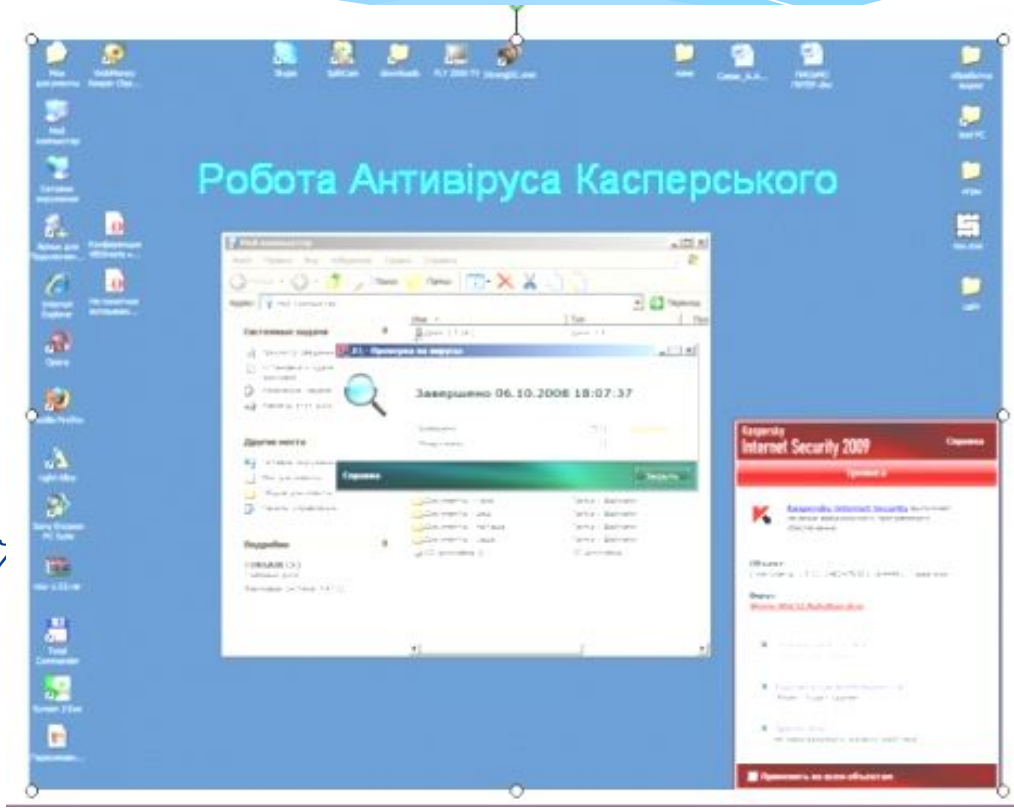
Отже, ви мали змогу впевнитись, що є багато людей, які намагаються отримати доступ до чужих комп'ютерів. Проте існують засоби, що утруднюють цей процес або навіть унеможливлюють його. Найпоширеніші з них — брандмауери, а також антивірусне та антиспамове програмне забезпечення. Велике значення має також дотримання користувачами правил безпеки під час роботи в Інтернеті

Взагалі брандмауер — це стіна з вогнестійкого матеріалу, що розташована між буквами й захищає їх від пожежі. В комп'ютерній мережі брандмауером називати програмне та апаратне забезпечення, яке захищає локальну мережу від небезпек.



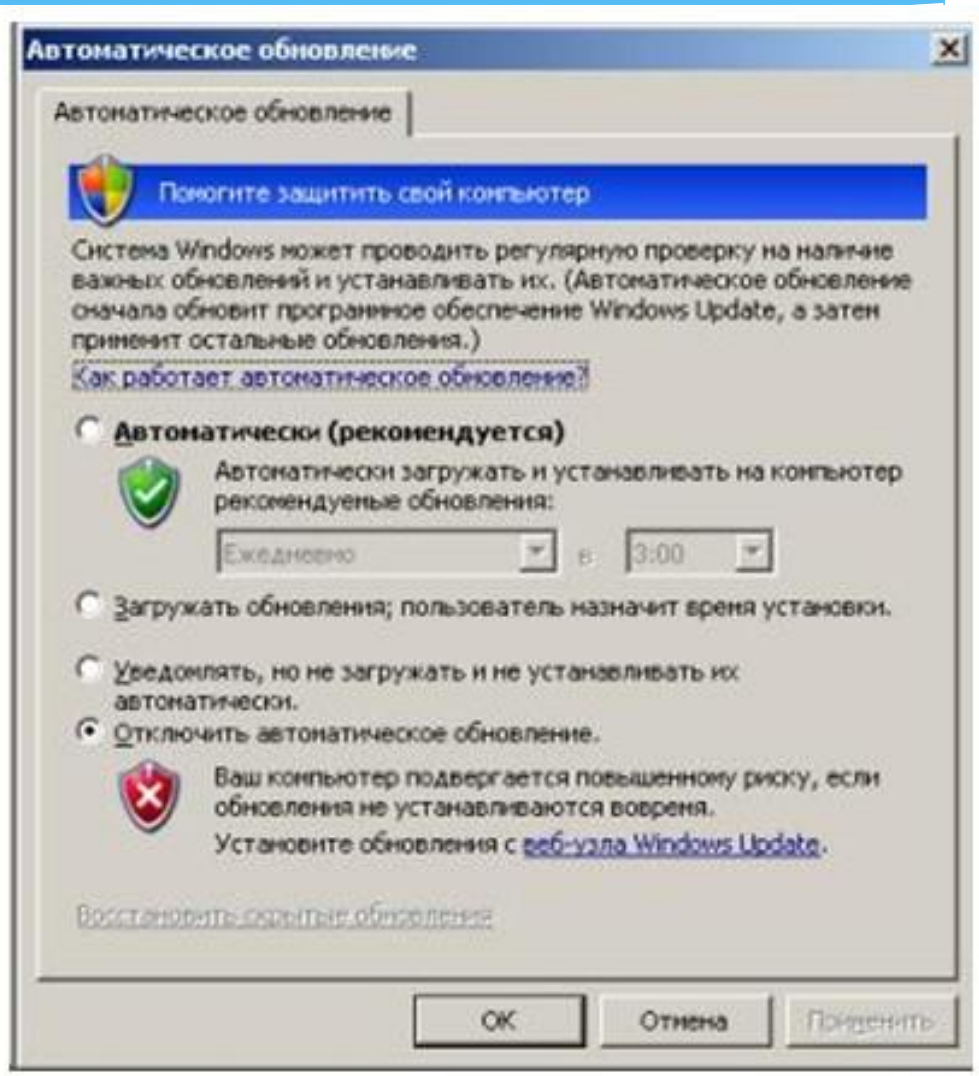
Антивірусне програмне забезпечення

* Однією з найбільших загроз для комп'ютерних систем є віруси. Для боротьби з ними можна придбати програмне забезпечення, що називається антивірусним. Воно працюватиме у вашій системі й перевірятиме на вміст вірусів усі файли, які ви отримуєте електронною поштою, завантажуєте з Інтернету, переписуєте на жорсткий диск або запускаєте на виконання з компакт-дисках чи дискети. Це Антивірус Касперського, Symantec Antivirus, McAfee VirusScan, AVG Anti-Virus.



Автоматичне оновлення Windows

* Автоматичне оновлення Windows — це засіб, що демонструє турботу корпорації Microsoft про безпеку користувачів.



Як захиститися від тих, хто хоче використати мою Персональну інформацію?

* Крім хакерів, які намагаються завдати шкоди вашому комп’ ютеру, існують зловмисники, що прагнуть отримати вашу персональну і конфіденційну інформацію та, використовуючи її, завдати вам шкоди.

* ***Як саме й навіщо люди здобувають інформацію про мене?***
* Певна категорія людей здійснює атаки на чужі комп'ютери задля отримання персональної інформації. Зазвичай їхніми об’ єктами стають бази даних великих корпорацій, де зберігаються такі відомості, як персональні ідентифікаційні номери, номери банківських рахунків та кредитних карток клієнтів.

Як уберегти персональну інформацію від викрадення?

* Не надавайте більше інформації, ніж потрібно. В кожному випадку треба бути впевненим, що одержувач інформації надійний. Не завадить також переконатися, що сайт захищений і на ньому використовуються технології шифрування.

Як захиститися від людей, які прагнуть завдати мені шкоди?

* ***Хто і як може завдати мені шкоди?***
* Існують особи, які через Інтернет знайомляться з молодими людьми, здобувають їхню довіру, випитують особисті дані й призначають зустріч. Тож пам'ятайте, що ваш приятель із чату, який, скажімо, відрекомендувався 15-річним підлітком, що шукає друзів, насправді може виявитися дуже небезпечною людиною.

Як убезпечити себе в Інтернеті?

* В Інтернеті дійсно можна зустріти багато суб'єктів з недобрими намірами, але це не є приводом для того, щоб відмовитися від користування цією мережею. Дотримуйтесь кількох простих правил, і ви будете гарантовані, що жодна людина з нечесними намірами не отримає доступу до вашої персональної інформації.
* Завжди звертайтеся до батьків чи учителів з будь-яких питань, пов'язаних із користуванням Інтернетом.

Висновки

* З початком широкого використання міжнародних мереж передачі даних загального користування темпи росту мережної злочинності зростають в геометричної прогресії. За оцінками експертів Міжнародного центру безпеки Інтернет (CERT) кількість інцидентів пов'язаних з порушенням мережної безпеки зросла в порівнянні з 2000 роком майже у 10 разів.
* Основними причинами, що провокують ріст мережної злочинності є недосконалі методи і засоби мережного захисту, а також різні уразливості у програмному забезпеченню елементів, що складають мережну інфраструктуру.