Інтернет. Безпека в інтернеті.

Презентацію виконала
Учениця 10-А класу
Гімназії №117
Мазур Дарина

Що таке інформаційна безпека

Під інформаційною безпекою розуміється захищеність інформації та підтримує її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктурі.

Складові інформаційної безпеки

· Конфіденційність - стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на нього право;

· Цілісність - уникнення несанкціонованої модифікації інформації;

· Доступність - уникнення тимчасового або постійного захування інформації від користувачів, що отримали права доступу.

Що загрожує інформаційній системі?

Хакери.

Спам.

Комп'ютерні віруси.

Дії, здійснювані авторизованими користувачами.

Трояни.

Загрози природного характеру .

Спам

Спам - це масові розсилки, реклама, та будь-яка інша інформація, яка надходить до нас всупереч нашій волі. Спамом можуть бути в першу чергу електронні листи, пости та коментарі на блогах, форумах, інших сайтах, а також оффлайнова реклама.

Вебмайстри винайшли чимало способів незаконної реклами. Серед них - власне, сама реклама, антиреклама, т.зв. "нігерійські листи" (листи із закликом вислати гроші, щоб отримати взамін щось набагато більше), фішинг та інше.

Фішинг - це засоби та дії, які імітують поведінку будь-кого іншого. Метою зловмисників у випадку фішингу є викрадення паролів або пін-кодів, щоб в кінці перевести гроші жертви на свій рахунок.

Засоби захисту від спаму

- без потреби не публікуйте свою e-mail адресу будь-де.
- без потреби не реєструйтесь на сайтах, форумах чи блогах - ви також передаєте їм свою інформацію, тим більше не треба реєструватись на підозрілих сайтах.
- не відповідати на спам чи переходити за посиланнями, що містяться в ньому.
- користуватись останніми версіями браузерів, котрі самі визначають чи підозрюється сайт у фішингу (Firefox 3/Opera 9.5), а також останньою версією антивірусу.
- не тримати важливу інформацію в одному місці, завести хоча б кілька другорядних електронних скриньок.

Хакери

Хакери - це користувачі, що добре володіють всіма програмами по злому персональних комп'ютерів через мережу Інтернет. Хакери своїми діями намагаються отримати незаконний доступ до комп'ютерних даних іншого користувача.

Хакер зламує комп'ютер користувача шляхом програми шпигуна, яку він відправляє жертві в спамерському листі. І після прочитання такого листа програма успішно потрапляє в систему комп'ютера.

Як захиститися від хакерів

1. Користуйтеся складними паролями.

2. Користуйтесь антивірусним програмним забезпеченням. Обов'язкова умова - його постійне оновлення.

3. Працюйте з комп'ютером у режимі користувача. Якщо після встановлення операційної системи ви продовжуєте використовувати комп'ютер в режимі «Адміністратор», ви створюєте додаткові ризики зараження комп'ютера вірусами, які пропустила антивірусна система.

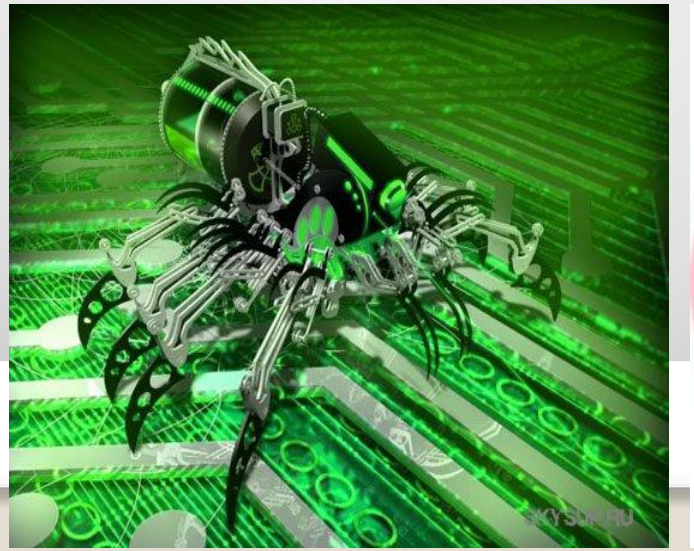
4. Виявляйте обережність при спробі підвищити власну анонімність.

Комп’ютерні віруси

Комп'ютерний вірус - це невелика програма, що написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій.

Основними джерелами вірусів є:

- дискета, на якій знаходяться заражені вірусом файли;
- комп'ютерна мережа, в тому числі система електронної пошти та Internet;
- жорсткий диск, на який потрапив вірус в результаті роботи з зараженими програмами;
- вірус, що залишився в оперативній пам'яті після попереднього користувача.

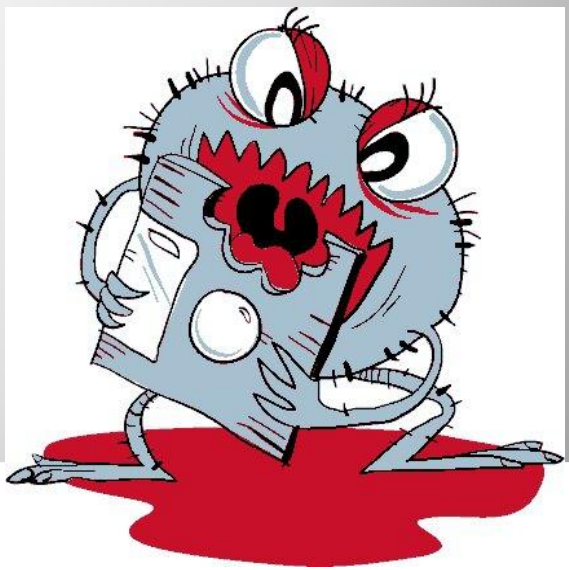


Види вірусів

- завантажувальні віруси або BOOT-віруси: заражають boot-сектори дисків. Дуже небезпечні, можуть призвести до повної втрати всієї інформації, що зберігається на диску;
- файлові віруси: заражають файли. Поділяються на:
  - віруси, що заражують програми
  - макровіруси: віруси, що заражують файли даних
  - віруси-супутники: використовують імена інших файлів;
  - віруси сімейства DIR: спотворюють системну інформацію про файлові структури;
- завантажувально-файлові віруси: здатні вражати як код boot-секторів, так і код файлів;

Види вірусів

- віруси-невидимки або STEALTH-віруси: фальсифікують інформацію прочитану з диска так, що програма, якій призначена ця інформація отримує невірні дані.
- ретровіруси: заражують антивірусні програми, намагаючись знищити їх або зробити непрацездатними;
- віруси-хробаки: заражують невеликі повідомлення електронної пошти, так званим заголовком, який по своїй суті є всього навсього лише Web-адресою місцезнаходження самого вірусу. При спробі прочитати таке повідомлення вірус починає зчитувати через глобальну мережу Internet своє 'тіло', яке після завантаження починає свою деструктивну дію.



Заходи захисту від вірусів

- резервне копіювання інформації (створення копій файлів і системних областей жорстких дисків);
- уникнення користування випадковими й невідомими програмами. Найчастіше віруси розповсюджуються разом із комп'ютерними вірусами;
- перезавантаження комп'ютера перед початком роботи, зокрема, у випадку, якщо за цим комп'ютером працювали інші користувачі;
- обмеження доступу до інформації, зокрема фізичний захист дискети під час копіювання файлів із неї.

До програмних засобів захисту належать різні антивірусні програми (антивіруси). Антивірус - це програма, яка виявляє й знешкоджує комп'ютерні віруси.

Трояни

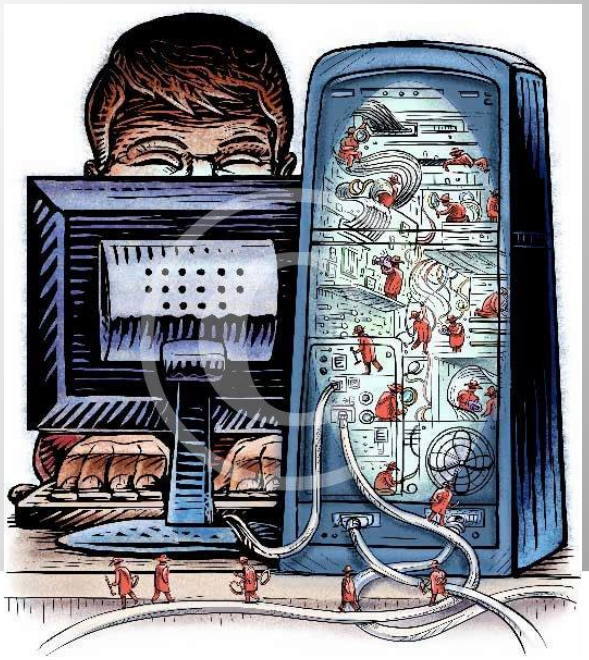
Троянські віруси — це комп'ютерні програми, які добре вміють маскуватися під програмні продукти, а насправді виконують різні користувачем дії (збирають та пересилають, змінюють або псують інформацію, використовують ресурси комп'ютера на власний розсуд).

Ці віруси самостійно не розмножуються. Вони видають себе за корисні програми, провокуючи користувача самостійно їх встановити.

Adware та Spyware

Adware (англ. Ad, Advertisement — реклама і Software — програмне забезпечення) — програмне забезпечення, яке в процесі свого використання показує користувачеві рекламу.

Spyware - шпигунське програмне забезпечення програмне забезпечення для відстежування (моніторингу) дій користувача, що вживається несанкціоновано



Авторське право і плагіат

Плагіат — привласнення авторства на чужий твір науки, літератури, мистецтва або на чуже відкриття, винахід чи раціоналізаторську пропозицію, а також використання у своїх працях чужого твору без посилання на автора.

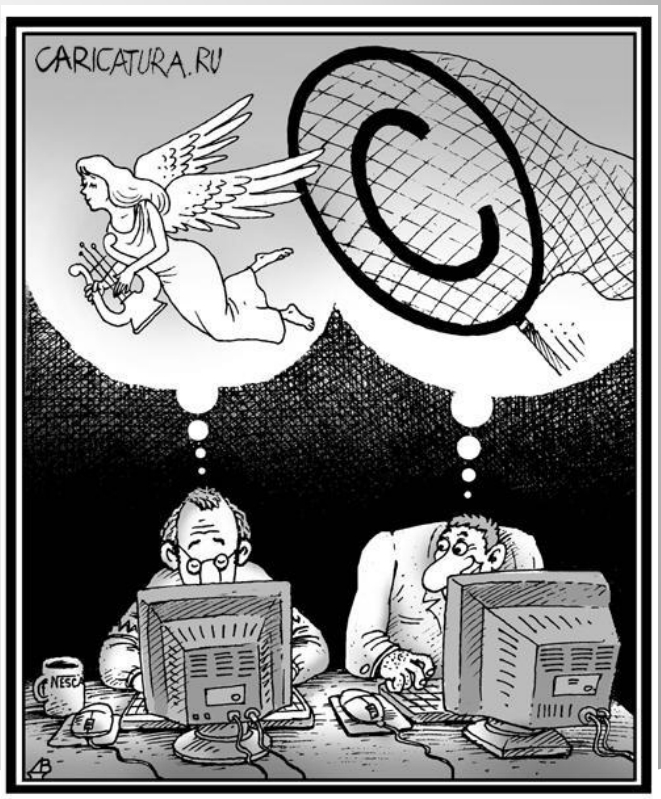
Плагіатом вважається:

- крадіжка ідеї або слова іншої людини і видача їх за власні;
- використання результатів роботи іншої людини без вказання джерела, звідки вони були взяті;
- повна або часткова крадіжка мистецького, наукового або іншог твіру чи роботи та видача їх за свою;
- представлення вже існуючої ідеї або продукту як новий та оригінальний .

Авторське право і плагіат

Авторське право — набір виключних прав, які дозволяють авторам отримати соціальні блага від результатів своєї творчої діяльності. АП історично виникло внаслідок потреби захистити права авторів літературних творів та творів мистецтва.

Зі збільшенням кількості Інтернет-ЗМІ плагіат як приписування собі чужої інтелектуальної власності або її творче використання: переклад, адаптація, аранжування без отримання належного дозволу набуває все більших масштабів. Копіпастери нехтують застереженням автора про заборону вільно використовувати його матеріал, як того вимагає ст. 21 Закону України „Про авторське право й суміжні права”



Дозвілля в інтернеті

Якщо у 2003 році в інтернеті проводили свій час лише 2% українців, то тепер це чи не найпопулярніший спосіб проведення вільного часу для 27% українців, грають у комп'ютерні ігри вже не 5—10%, а 15—25% молоді.

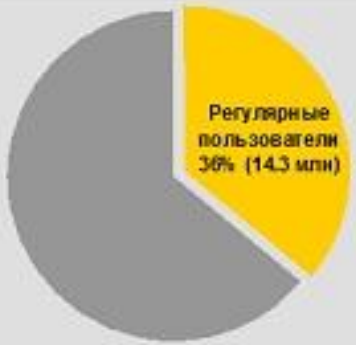
Так само активно змінює інтернет і практики спілкування. У мережі приймають і відправляють повідомлення електронною поштою, спілкуються в соціальних мережах, в чатах, на форумах, блогах, знайомляться на сайтах. Відбувається активне перенесення дозвілля молоді в інтернет-мережу. Інтернетизація життя значною мірою це життя змінює.

По-перше, людина може «лазити» в інтернеті по всьому світу, якщо знає іноземну мову. По-друге, це дає можливості об' єднуватися за інтересами, збиратися разом, створювати якісь групи. Звичайно, є і негативні наслідки — зменшення фізичної активності, а відповідно — погіршення здоров'я.

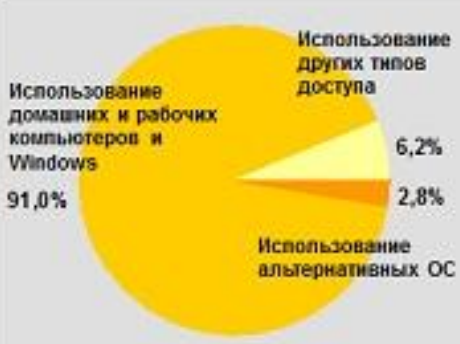
Статистика

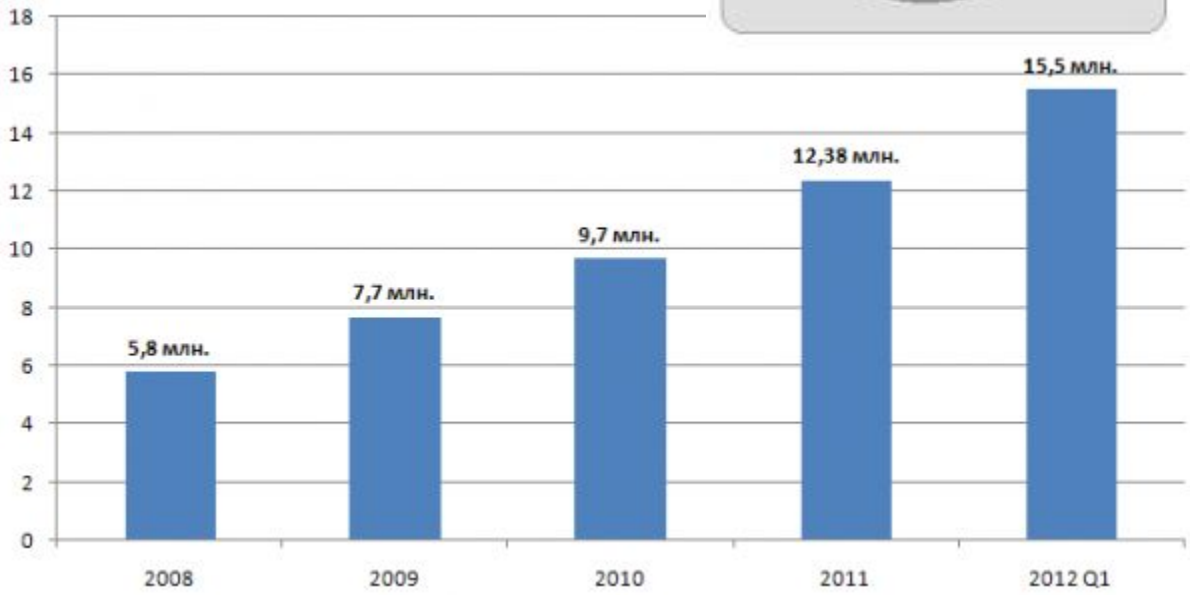
14,3 млн украинцев в возрасте 15+ лет пользуются интернет не реже раза в месяц

Доля и численность пользователей



В панель включены пользователи, использующие для выхода в Интернет домашний или рабочий компьютер и ОС Windows.





Використані джерела:

http://kaspersky-antivirus.kiev.ua/reshenija/infosecur.html

http://www.ukrreferat.com/index.php?referat=36222

http://pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi

http://h.ua/story/114317/

http://kaspersky-antivirus.kiev.ua/ugroz/xack.html

http://komphelp.net/Virus/Index1.htm

http://uchni.com.ua/informatika/5621/index.html

http://bibliofond.ru/view.aspx?id=439369

http://www.referatcentral.org.ua/sociology_load.php?id=255

Дякую за увагу!