Програмно-технічні аспекти безпеки в Інтернет

Ободяк В.К.,
доцент кафедри комп'ютерних наук
Сумського державного університету

Основні шляхи попадання шкідливих програм (вірусів) на комп'ютер з мережі Інтернет:

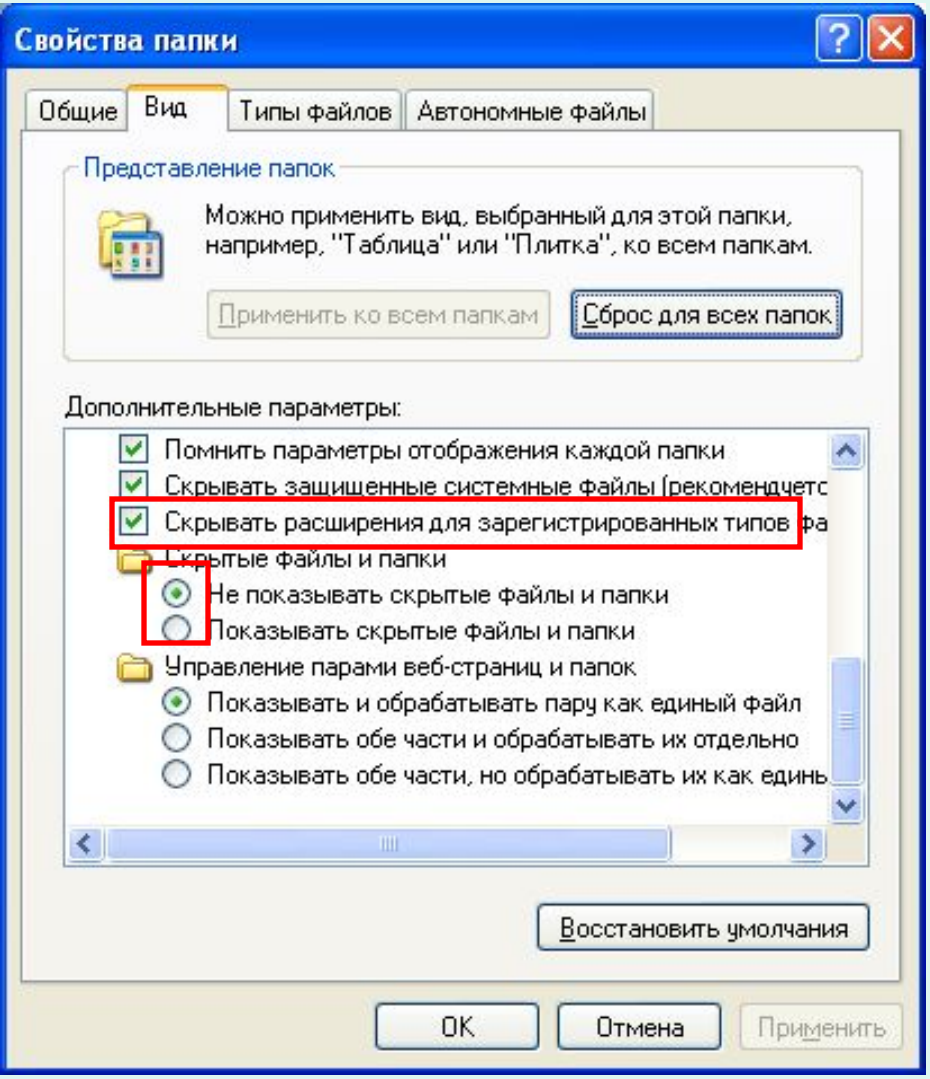
1) зараження вірусами через поштові повідомлення з вкладеннями;
2) зараження вірусами через веб-сторінки.

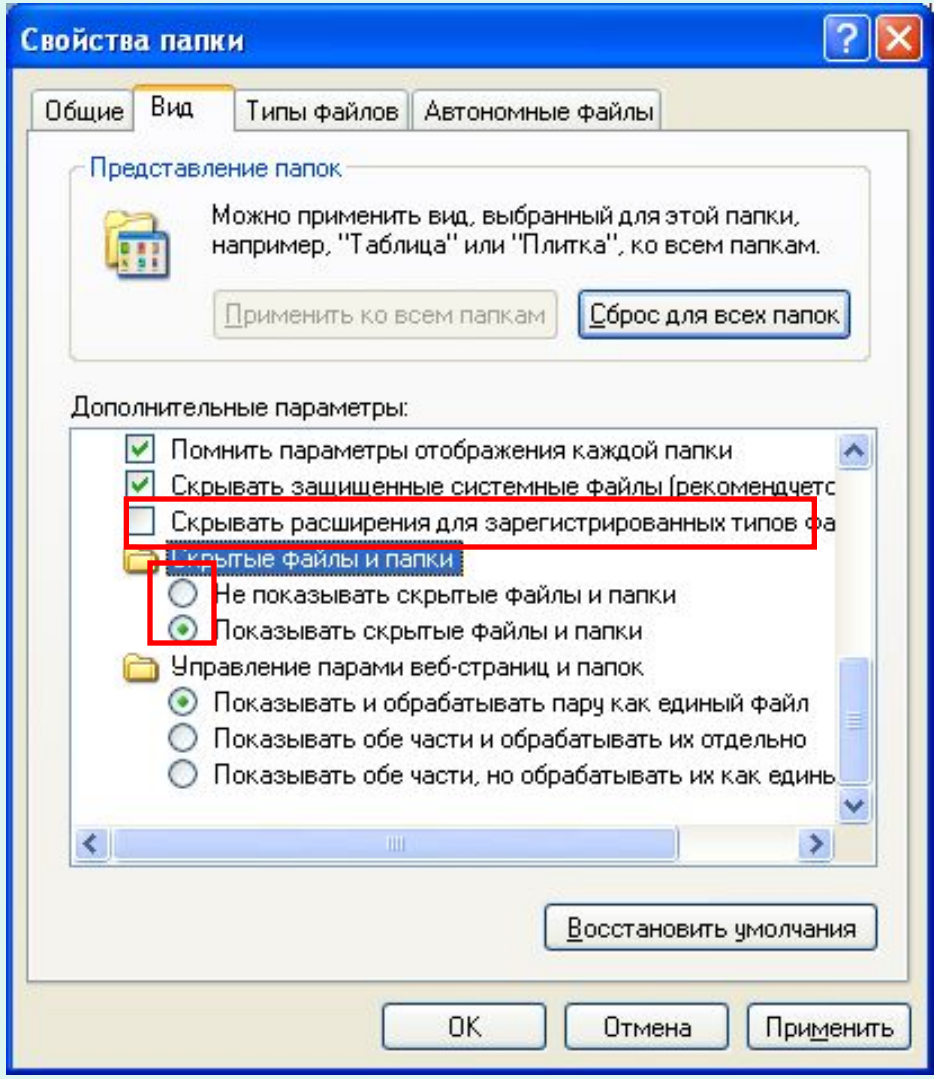
1. **Зараження вірусами через поштові повідомлення з вкладеннями**

Ніколи не відкривайте таких повідомлень від невідомих осіб, або якщо є сумнів, щодо безпечності вкладення (якщо вкладенням є файл з розширенням exe, cmd, bat).

Бажано завжди показувати в папках розширення файлів.

Це можна зробити у властивостях папки.





Властивості папки до і після змін

При скачуванні файлів з відеоматеріалами:

- **потрібно звертати увагу, що в цих файлах не повинно бути розширення exe;**
- **при скачуванні файлів з розширення rar, zip потрібно бути уважним;**
- **після завантаження необхідно перевірити файли антивірусною програмою.**

Ніколи не потрібно відповідати на листи, в яких пропонується ввести ваші персональні дані, логіни, паролі.

2. Зараження вірусами через веб-сторінки

Гру можете скачувати з сайту розробника.

При роботі з файлообмінниками необхідно отримати додаткову інформацію від інших користувачів.

На моніторі може відображатись вікно з повідомленнями типу «Ваш програвач застарів і потребує оновлення». Ні в якому разі не можна клацати по кнопкам в цьому вікні.

Уважно використовуйте адреси сайтів.

Може надійти пропозиція перейти на якийсь ресурс за посиланням. Посилання може бути відкритим, наприклад, http://vkontakte.ru або закритим – Знайди нових друзів! .

Але при цьому може використовуватись хибне посилання, а саме може бути змінені імена сайтів. При помилках в іменах сайтів (якщо замість vkontakte.ru буде vk0ntakte.ru) можна потрапити на підроблений сайт. Така технологія використовується в трьох випадках:

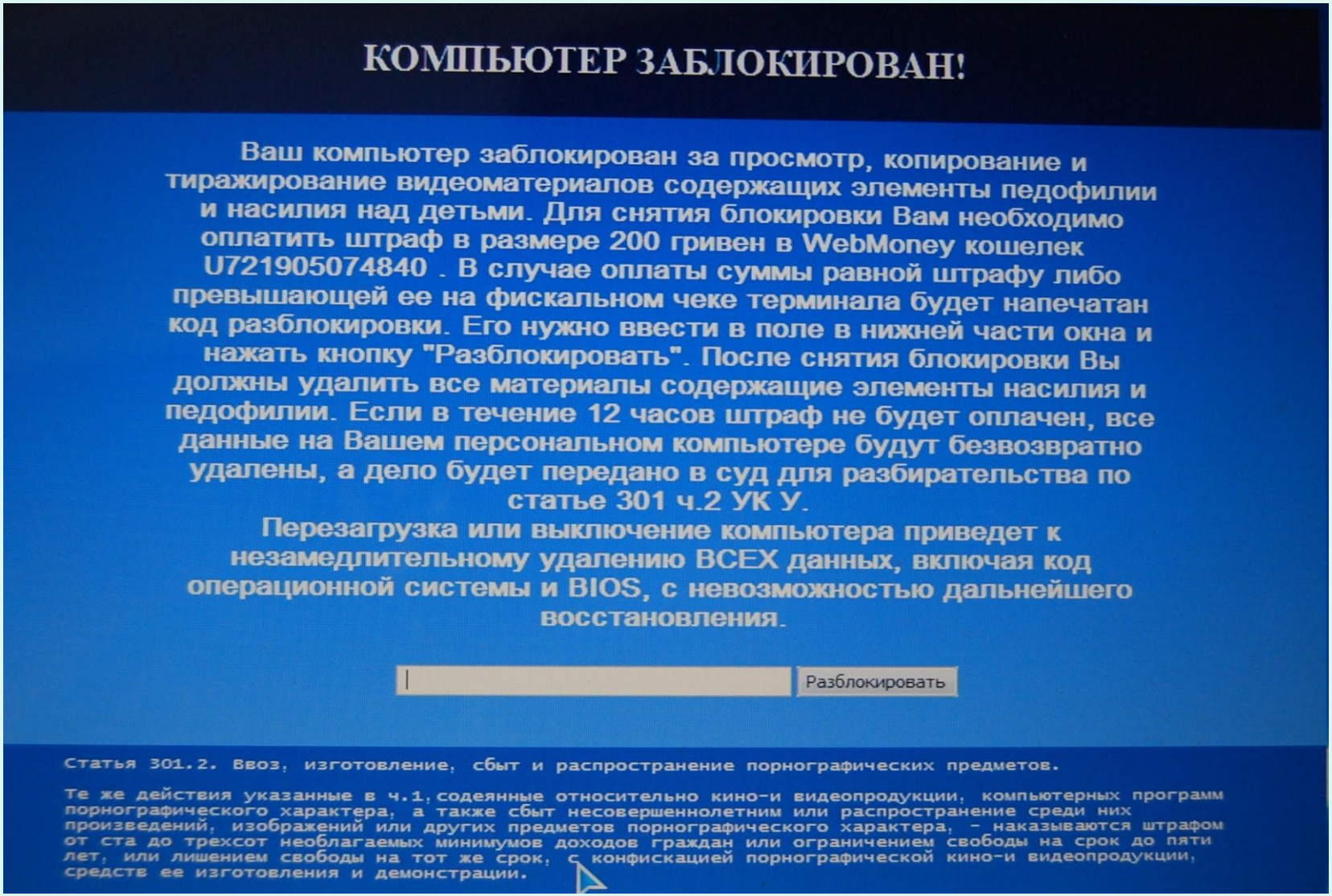
1) якщо цей сайт схожий на оригінальний, то він використовується для викрадення вашої приватної інформації, включаючи логін і пароль;

2) таким чином можуть рекламуватись сторонні веб-сторінки, в тому числі порнографічні;

3) для завантаження вірусів.

Потрібно скопіювати гіперпосилання в Word і перевірити, чи відповідає посилання реальній адресі ресурсу або ігнорувати подібні посилання.

За допомогою скриптових вірусів шкідливе програмне забезпечення потрапляє на ваш комп’ютер при відвідуванні сайту без будь-яких ваших додаткових дій. Прикладом можуть бути програми-здирники, які блокують роботу комп’ютера, вимагаючи кошти за розблокування.



Методи боротьби з попаданням на комп’ютер вірусів наступні:

- якщо пошукова система повідомляє про можливу загрозу сайту – не потрібно його відкривати;

- необхідно оновлювати антивірусну базу автоматично при появі нових баз;

- необхідно вчасно встановлювати оновлення операційної системи.

Антивірусне забезпечення

Можна встановити комерційне, якщо ви згодні платити приблизно 300-400 гривень на рік.

Можна обмежитись безкоштовним, але воно буде менш надійним.

Паролі потрібно пам’ятати.

Є варіант, коли набирається пароль із великої кількості символів (більше 15) англійськими літерами фразу, яка кирилицею не є загальновідомою, але вас зачепила: пароль Dectkt_rhfot_ptktyjuj отримуєте, якщо набрати Веселе_краще_зеленого.

Не варто погоджуватись на пропозицію деяких сайтів і програм «Зберегти пароль».

Для безпечної роботи в мережі Інтернет необхідно працювати під обліковим записом без прав адміністратора.

Висновки

Антивірус повинен бути з актуальними базами.

Не заходити на сайти, про можливу шкідливість яких попереджують пошукові системи, або браузер.

Не відкривати поштових повідомлень із вкладеннями від незнайомих адресатів.

Не переходити за вкладеними гіперпосиланнями без перевірки або ігнорувати подібні посилання.

Скачувати програмне забезпечення або від виробника, або на файлообмінному ресурсі при великій кількості позитивних відгуків і відсутності негативних повідомлень про деструктивні дії даного файлу.

Не працювати в Інтернеті під обліковим записом адміністратора.

Потрібно пам’ятати, що жоден антивірус не дає повну гарантію і потрібно виконувати весь комплекс заходів.

Більше інформації про безпеку в Інтернет можна знайти на сайтах

http://www.onlandia.org.ua/pages/v_turvallisesti_netin
http://urokinfo.ho.ua/view_post.php?id=47