Безпека в Інтернеті
(методичні рекомендації для адміністрацій закладів загальної середньої освіти, вчителів інформатики, завідуючих кабінетами інформатики)

Інтернет — це феноменальний за своїми можливостями засіб.

В даних методичних рекомендація мова піде про небезпеки пов’язані використанням Інтернет технологій.

Інтернет охоплює майже весь світ, а отже ця мережа доступна і для тих людей, які мають далеко не найкращі наміри. Проблема збільшується ще й тому, що після підключення комп'ютера до мережі, а особливо до Інтернету, виникає ризик вторгнення зловмисника до цього комп’ютера та подальшого використання його для атак на інші комп’ютерні системи.

Злочинці послуговуються чужими комп’ютерами, щоб уникнути відповідальності за свої дії, бо в такому в такому разі визначити справжнє джерело нападу буває дуже складно. Тому захист від зловмисників став одною з основних проблем користувачів Інтернету. Існують й інші види небезпек, наприклад стеження через Інтернет за діяльністю людини чи організації.

Як захистити комп'ютер від атак зловмисників?

Існують різні види небезпек, пов'язаних із користуванням Інтернетом. Одні зловмисники прагнуть отримати вашу персональну інформацію та скориставшись нею, зашкодити вам. Інші вибирають об'єктом атак вашу комп'ютерну систему та намагаються вивести її з ладу або використати для приховування своїх шкідливих дій.

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.

Хакери

Спочатку слово хакер було сленговою назвою комп'ютерного ентузіаста. Однак з часом воно набуло негативного значення, й тепер так називають людину, яка без дозволу проникає до чужої комп'ютерної системи з наміром викрасти або зруйнувати дані. Більшість подібних хакерів воліють, щоб їх називали кракерами — від англійського слова «crack», тобто «злом».

Існує багато способів, за допомогою яких «хакери» проникають до чужих систем. Найбільш поширеними є такі :

- **Троянські коні**. Це шкідливі програми, які розповсюджуються шляхом обману. Так, вам може надійти електронною поштою лист, де буде сказано, що програма, яка знаходиться у вкладенні, виконує якусь корисну функцію. Якщо ви запустите її на виконання, ваш комп'ютер буде заражений. Троянські коні відкривають хакерам доступ до системи, можуть спричинити руйнування інших та виконання інших програм.
- **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.
- **Підміна адрес**. Хакер підмінює адреси сайтів у такий спосіб, що коли користувач зводить у браузері адресу якогось сайту, його спрямовують до зовсім іншого сайту. Іноді на такому альтернативному сайті міститься негативна інформація про власника того сайту, який збирався відвідати користувач.

- **Аналіз пакетів**. За допомогою спеціальної програми хакер читає певну інформацію що міститься у пакетах, які передаються мережею. Загалом програми - аналізатори пакетів призначені для контролю за мережею, проте вони ж використовуються хакерами для несанкціонованого збирання інформації.
- **Соціотехніка**. Цей термін використовується для позначення шахрайських дій, спрямованих на отримання інформації, яка дає змогу проникнути до певної системи та даних, що в ній знаходяться. Соціотехніка зазвичай є грою хакера на довірі людини. Для цього використовуються сфальсифіковані сайти та фіктивні електронні повідомлення від імені реальних компаній з проханням надати особисту інформацію.
- **Підміна веб-сторінки**. Хакер дістається сайту та змінює на ньому певну веб-сторінку, після чого на ній відображається інша інформація.

ПРИМІТКА

Перед передаванням мережею інформацію завжди поділяють на маленькі порції - так звані пакети з яких після прибуття до місця призначення знову утворюється єдине ціле. Щоб кожний пакет був доставлений до місця призначення до нього додається заголовок який містить номер пакета, адресу призначення та іншу необхідну інформацію.

УВАГА!!!

Отримавши електронного листа з проханням повідомити персональну інформацію, ніколи не надавайте цю інформацію.

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. Такий вірус потрапляє до комп'ютерної системи, власник якої про це й гадки не має. До того ж іноді вірус якийсь час залишається затаєним, жодним чином себе не викриваючи, і лише після настання певної дати чи події активізується та завдає шкоди комп'ютерній системі.
- **Хробаки**. Хробак схожий на вірус тим, що розмножується, роблячи власні копії, але на відміну від останнього він не потребує носія й існує сам по собі. Часто хробаки передаються через електрону пошту. Хоча спершу хробаки не були шкідливими, нинішні їхні різновиди спричиняють значні перенавантаження мереж і можуть руйнувати файли. Найбільш нищівний з усіх хробаків на ім'я I LOVE YOU завдав збитків на 7 млрд. доларів.

Хакери створюють вірусоподібні програми, бажаючи продемонструвати свою владу над інформаційними системами. Навіть найменш шкідливі з цих програм можуть призвести до великих неприємностей, а завдані ними збитки іноді оцінюються в мільйони доларів.

УВАГА!!!

Нові віруси та інші методи вторгнення до вашої комп’ютерної системи виникають майже щодня. Тому регулярно перевіряйте наявність оновлень на сайті своєї антивірусної програми. Повідомлення про нові віруси та інші небезпеки з’являються в Інтернеті постійно.

Фішинг

Чи отримували ви коли-небудь електронне повідомлення нібито з банку чи іншого популярного онлайн-сервісу, який вимагав «підтвердити» дані облікового запису, номер кредитної картки чи іншу конфіденційну інформацію? Якщо так, ви вже знаєте, як виглядає фішинг-атака. Ціль фішингу — отримання цінних даних, які можуть бути продані або використані для зловмисних цілей, таких як вимагання, викрадення грошей або особистих даних.

Фішинг існує впродовж багатьох років, за цей час кіберзлочинці розробили широкий спектр методів інфікування жертв.

Найчастіше зловмисники, які займаються фішингом видають себе за банки чи інші фінансові установи, щоб змусити жертву заповнити фальшиву форму та отримати дані облікових записів.

У минулому для виманювання даних користувачів кіберзлочинці часто використовували неправильно написані або оманливі доменні імена. Сьогодні зловмисники використовують більш складні методи, завдяки чому фальшиві сторінки дуже схожі на свої легітимні аналоги.

Як захиститися від фішингу?

Щоб уникнути подібних атак, звертайте увагу на описані вище ознаки, за допомогою яких можна виявити фішингові повідомлення.

Дотримуйтеся таких рекомендацій

1. Дізнавайтесь про нові методи фішингу: читайте засоби масової інформації для отримання нової інформації про фішингові атаки, оскільки кіберзлочинці постійно знаходять нові методи для виманювання даних користувачів.
2. Не надсилайте облікові дані: будьте особливо уважні, коли у електронному листі начебто перевірені організації запитують ваші облікові або інші конфіденційні дані. У разі необхідності перевірте вміст повідомлення, відправника або організацію, яку вони представляють.
3. Не натискайте на підозрілі кнопки та посилання: якщо підозріле повідомлення містить посилання або вкладення, не натискайте та не завантажуйте вміст. Це може призвести до переходу на шкідливий веб-сайт або інфікувати ваш пристрій.
4. Регулярно перевіряйте облікові записи: навіть якщо ви не маєте підозр, що хтось намагається викрасти ваші облікові дані, перевірте банківські та інші облікові записи в Інтернеті на наявність підозрілої активності.
5. Використовуйте надійне рішення для захисту від фішингових атак. Дотримання цих рекомендацій допоможе Вам насолоджуватися безпекою.

Незаконний майнінг

Незаконний майнінг використовує потенційно небажаний або шкідливий код, який призначений для споживання обчислювальної потужності певного пристрою з метою прихованого майнінгу. При цьому дії зловмисників приховуються або виконуються у фоновому режимі без отримання згоди користувача або адміністратора.

Як забезпечити захист від загроз незаконного майнінгу та криптоджекінгу?

1. Для захисту робочих станцій, серверів та інших пристроїв використовуйте багаторівневі рішення з безпеки, які здатні виявляти потенційно небажані програми для майнінгу, включаючи трояни.

2. Для виявлення загроз використовуйте програмне забезпечення, яке допомагає виявити підозрілі мережеві комунікації, які пов'язані з незаконним майнінгом

(заражені домени, вихідні з'єднання на типових портах, таких як 3333, 4444 або 8333, ознаки стійкості тощо).

3. Покращуйте видимість мережевого трафіка за допомогою віддаленої консолі управління для забезпечення політики безпеки, моніторингу стану системи, а також захисту робочих станцій та серверів компанії.

4. Підвищуйте обізнаність співробітників у сфері кібербезпеки (включаючи керівників організації та адміністраторів мережі), наприклад щодо створення надійних паролів та використання двофакторної аутентифікації для підвищення захисту систем компанії у випадку викрадення паролів.

5. Дотримуйтесь принципу надання мінімальних привілеїв. Користувачі повинні мати облікові записи з обмеженою кількістю дозволів, потрібних для виконання певних щоденних завдань. Цей підхід значно знижує ризик маніпулювання користувачами та адміністраторами з метою відкриття або встановлення шкідливих програм на пристрої в мережі компанії.

6. Використовуйте контроль програм, який дозволяє зменшити кількість запусків програмного забезпечення до мінімуму, запобігаючи встановленню шкідливої програми для майнінгу.

7. Застосовуйте надійні політики оновлення програмного забезпечення та встановлення виправлень для зниження ризиків інфікування пристроїв за допомогою раніше виявлених уразливостей, оскільки багато загроз незаконного майнінгу використовують відомі експлойти для розповсюдження, наприклад EternalBlue.

8. Здійснюйте моніторинг систем компанії щодо надмірного споживання енергії, що може вказувати на небажану активність шкідливих програм для майнінгу.

Бекдор

Шкідлива програма для отримання доступу до робочої станції, сервера, пристрою чи мережі шляхом обходу аутентифікації, а також інших стандартних методів та технологій безпеки.

Як працює бекдор?

Найчастіше це шкідливе програмне забезпечення проникає на пристрій жертви під час завантаження користувачем файлів. Деякі види загрози можуть бути інтегрованими в програму або додаток, у такому випадку проникають в систему під час інсталяції та активуються після запуску.

Відомі приклади

Одними з найвідоміших атак з використанням бекдорів були атаки, які здійснювала група кіберзлочинців TeleBots. Зловмисники стали відомими завдяки глобальному поширенню NotPetya — загрози, яка спричинила збитки в розмірі мільярдів доларів США.

Способи захисту

Для безпеки пристрою рекомендують регулярно перевіряти актуальність всього встановленого програмного забезпечення та своєчасно завантажувати оновлення.

Крім цього, спеціалісти рекомендують завантажувати додатки лише з офіційних магазинів та звертати увагу на відгуки та рейтинг ПЗ, яке ви плануєте інсталювати.

Експлойт

Це шкідливий код, який використовує уразливості в системі безпеки програмного забезпечення для поширення кіберзагроз.

Як забезпечити захист від експлойтів?

Експлойти часто є початковою точкою для інфікування системи шкідливими програмами.

Для виправлення помилок, які зловмисники можуть використати у своїх цілях, варто регулярно здійснювати оновлення всіх програм та операційної системи.

Також на пристроях рекомендується встановити надійне рішення з безпеки, яке здатне виявляти та блокувати шкідливе програмне забезпечення, а також захищає від цілеспрямованих атак на веб-браузери, PDF-редактори, поштові клієнти та інші програми.

Рекламне програмне забезпечення

Це різні спливаючі рекламні оголошення, які відображаються на комп'ютері чи мобільному пристрої користувача. Також рекламне ПЗ може використовуватися у зловмисних цілях, наприклад, для завантаження вірусів та шпигунських програм на пристрої.

Як видалити рекламне програмне забезпечення?

Крім того, що потрібно бути уважним під час натискання на різні спливаючі вікна та банери, важливо не забувати і про захист пристрою від цього виду загроз.

Варто зазначити, що існує багато безкоштовних інструментів для видалення рекламного ПЗ, однак не всі з них є безпечними та якісними.

Тому для ефективного захисту пристроїв від подібних загроз рекомендується використовувати надійне антивірусне рішення, яке допоможе запобігти інфікуванню шкідливим програмним забезпеченням, а також очистити пристрій від нього.

Не забудьте створити резервну копію файлів та даних перед скануванням пристрою на наявність шкідливого ПЗ.трій, або для отримання доступу до Вашого браузера.

Спам

Спамом називають небажану електронну пошту, тобто пошту, що надходить без вашої згоди. Майже нічого не коштує розіслати такі повідомлення мільйонам людей по всьому світу, й ніякі Хакери тут не потрібні. А от боротися зі спамом дуже складно навіть корпорації, спроможні щорічно витрачати мільйони доларів на антивірусне програмне забезпечення, не здатні зупинити потік рекламних та інших небажаних повідомлень, які призводять до перенавантаження мережних каналів та зайвих витрат дискового простору. І хоча повністю припинити надходження спаму досить важко, існують методи, що дозволяють істотно зменшити його кількість. Люди отримують спам з різних причин. Проте часто вони самі є винуватцями того, що їхня електронна адреса потрапляє до спамерів. Щоб з вами такого не сталося, треба знати, як відбувається полювання за адресами. Зазвичай спамери використовують спеціальні програми-павуки, які обстежують Веб і відшукують всі адреси електронної пошти, що там з'являються. Тому пам'ятайте: як тільки ви вкажете де-небудь адресу своєї електронної пошти, чекайте надходження спаму.

Далі наведений перелік типових дій, які можуть призвести до того, що ваша адреса стане надбанням спамерів:

запис до гостьової книги на якомусь з сайтів із зазначенням своєї електронної адреси;

- підписка на безкоштовне отримання електронною поштою прайс-листів, новин та іншої подібної інформації;

- відповідь на спам, що надійшов на вашу адресу (цим ви підтверджуєте, що адреса дійсно комусь належить);
- публікування свого імені та електронної адреси в онлайновому довіднику типу «жовтих сторінок»;
- надання згоди на участь у групі новин;
- реєстрація свого доменного імені, яка вимагає надання персональної інформації;
- заповнення онлайнових форм;
- участь у чаті.

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.

Таке програмне забезпечення має багато функцій. Воно може 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.

Інформацію про відвідувані веб-сторінки також можна отримати із cookie-файлів.

Adware і spyware

Термін adware не має перекладу українською мовою, так називають програми, які під час своєї роботи виводять на екран рекламні стрічки-банери. Подібні програми сповільнюють роботу вашої системи.

Програми типу spyware без вашого дозволу надсилають комусь інформацію про те, що ви робите в Інтернеті. Зазвичай це здійснюється в рекламних цілях. Програмне забезпечення типу spyware також сповільнює роботу системи і навіть призводить до її збоїв. Програми цього типу можуть також збирати без вашого дозволу інформацію з комп'ютера, само встановлюватися на ваш комп'ютер і змінювати файли в його системі.

Існує декілька програм, що застосовуються з метою блокування програмного забезпечення типу adware і spyware. Це, зокрема, такі:

- Spybot Search & Destroy: http://www.safernetworking.org (англомовна, є free версія)
- Lavasoft Ad-aware: http://lavasoft.element5.com (англомовна, є free версія)
- Spyware Doctor 2.0: http://www.pctools.com (англомовна, потрібен ключ)
- NoAdware: http://www.noadware.net (англомовна, потрібен ключ)
- Spyware Eliminator: http://www.aluriasoftware.com (англомовна, потрібен ключ)
- Spyware C.O.P:http://www.noadware.net (англомовна, потрібен ключ)

Cookie-файли

Хоча cookie-файли ми розглядаємо в даному розділі це зовсім не шпигунський засіб, і коли вони застосовуються за призначенням, то значно полегшують ваше перебування в Інтернеті. Це маленькі текстові файли, що містять дані, а не програми і тим більше не віруси. Навіть для розповсюдження вірусів вони не застосовуються.

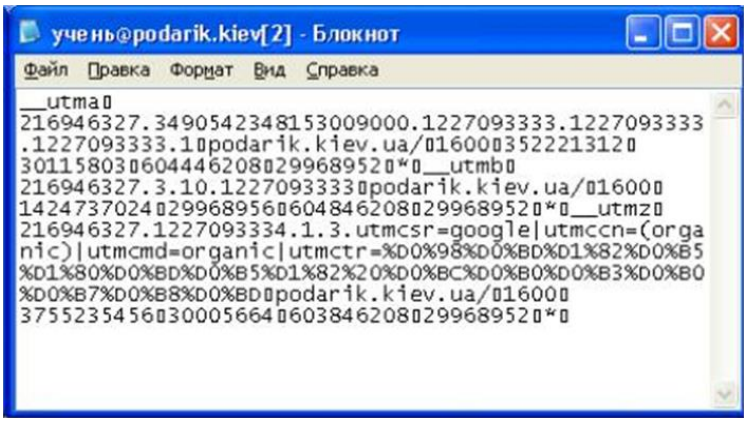

Рис. 4.1. Cookie - файл

У cookie-файлах міститься багато різної інформації. Наприклад, коли ви налаштуєте для себе домашню сторінку сайту My MSN, то вона під час відкриття набуватиме бажаного вигляду автоматично. Це стає можливим завдяки тому, що відповідні настройки зберігаються в cookie-файлі на вашому комп'ютері, і програмне забезпечення сайту читає їх під час завантаження сторінки. Сайти, призначені для купівлі товарів через Інтернет, можуть зберігати кошик для покупок у вигляді cookie. Прочитати cookie-файл може лише програмне забезпечення сайту, який його створив.

Шпигунські програми

Існує безліч причин, з яких певні особи застосовують шпигунські програми, що стежать за вашими діями, аналізують вашу електронну пошту та фіксують адреси відвідуваних вами веб-сторінок. Найбільшими користувачами цих засобів є ФБР (у США), корпорації, які стежать за своїми робітниками, та навчальні заклади, що спостерігають за учнями чи студентами.

У ФБР застосовується система під назвою DCS 1000, більш відома як Carnivore.

Це інтернет-еквівалент підслуховуючого пристрою, що може здійснювати аналіз електронної пошти користувача й стежити за відвідуванням веб-сайтів.

Корпорації та навчальні заклади часом використовують різні методи стеження за перебуванням співробітників чи учнів на веб-сайтах. Простіші програми створюють журнальні файли, де фіксується інформація про те, коли, хто і який сайт відвідував.

Більш складні програми (клавіатурні шпигуни) здатні відстежувати кожне натискання клавіші на комп'ютері та надсилати цю інформацію особі, що здійснює стеження. Існує багато засобів, які утруднюють несанкціоноване отримання персональної інформації. **Серед них - програми батьківського контролю, що є дуже популярними**. Ними користуються не лише батьки, щоб вберегти своїх дітей від відвідування сайтів з небажаним вмістом, а й керівники корпорацій та навчальних закладів, з аналогічною метою. Мандруючи мережею Веб, учні у такому разі стикаються з блокуванням у випадках, коли сторінка, яку вони намагаються відкрити, містить слова, розцінені блокуючою програмою як образливі чи неприйнятні для дитячої або підліткової аудиторії.

На деяких інтернет-порталах, зокрема на MSN, також є засоби блокування доступу до подібних інтернет-ресурсів. Існує багато програм, які містять функції блокування. Крім того, у більшість браузерів вбудовано функції, що дозволяють користувачеві підключатися до певних сайтів лише після введення паролю.

Усі такі програми діють майже однаково. Програма встановлюється на комп'ютер. Коли користувач вводить адресу сайту, програма її перевіряє, звертаючись до бази даних заборонених сайтів. Якщо ця адреса є в базі даних, програма блокує доступ до

сайту, і користувач не зможе до нього підключитися, доки не введе пароль. Якщо ж адреси в базі даних немає, програма сканує сам сайт у пошуку певних заборонених слів і тільки після цього надає користувачеві доступ до сайту. Більшість подібних програм щомісяця оновлюють свою базу даних, завдяки чому ця інформація завжди актуальна, незважаючи на швидке зростання кількості інтернет-ресурсів.

НАЙПОПУЛЯРНІШІ:

Norton Safety Minder 1.2.0.55 – ліцензія Freeware (безкоштовно)

Norton Safety Minder пов'язує Ваш комп'ютер з онлайн-сервісом Norton Online Family, який дозволяє батькам блокувати доступ дітей до небажаних веб-сайтів за типом контенту або на основі «чорних» списків.

За допомогою Norton Online Family можна обмежувати час перебування малолітніх користувачів в Інтернеті і відслідковувати їх дії в режимі реального часу.

З Norton Safety Minder Ви будете мати можливість контролювати онлайн-активність Ваших дітей, використовуючи аккаунт Norton Online Family.

Crawler Parental Control – ліцензія Freeware (безкоштовно)

www.crawlerparental.com – офіційний сайт – українського, російського інтерфейсу немає.

КиберМама – промоверсія безкоштовна

http://www.cybermama.ru/download.php

може:

- вирішувати або забороняти дитині доступ в мережу Інтернет;
- забороняти використання певних програм (у тому числі і комп'ютерних ігор);
- встановлювати обмеження часу використання комп'ютера дитиною (обмеження по сумарному щоденному часу використання, обмеження за часом безперервного використання);

Salfeld Child Control - програма обмежує час, що проводиться вашими дітьми за комп'ютером, як тільки виділене їм час закінчиться, комп'ютер автоматично вимкнеться і повторний вхід буде можливий тільки після введення пароля. Обмеження можна ввести як по загальному часу (наприклад, не більше 1 години на день), так і по періоду часу, коли можна працювати (наприклад, з 22:00 до 8:00 доступ заборонений). Крім цього, програма дозволяє заборонити відвідування небажаних сайтів, а також заблокувати доступ до певних дисках і теках.

Можна встановити блокування запуску тих чи інших програм та внесення змін до реєстру. Програма веде лог-файл всіх подій.

KinderGate – Shareware (потрібен ключ)

Просте і зручне рішення для домашніх користувачів, за допомогою якого батьки можуть контролювати і обмежувати використання неповнолітніми дітьми мережі Інтернет. Функціонал продукту включає можливість фільтрації ресурсів за категоріями, автоматичну і ручну блокування сайтів, моніторинг мережевої активності користувача, формування статистики, розмежування прав і установку режимів доступу.

NetPolice – Shareware (потрібен ключ) є версія Lite (5 базових функцій).

«Один дома» Shareware (потрібен ключ)

Просте і зручне рішення для домашніх користувачів, за допомогою якого батьки можуть контролювати і обмежувати використання неповнолітніми дітьми мережі Інтернет. Функціонал продукту включає можливість фільтрації ресурсів за

категоріями, автоматичну і ручну блокування сайтів, моніторинг мережевої активності користувача, розмежування прав і установку режимів доступу.

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.

Брандмауери

Взагалі брандмауер – це стіна з вогнестійкого матеріалу, що розташована між буквами й захищає їх від пожежі. Якщо вогонь вируватиме зовні то така стіна не дозволить йому досягти будинку. В комп'ютерній мережі брандмауером називати програмне та апаратне забезпечення, яке захищає локальну мережу від небезпек. Брандмауер розташовують між локальною мережею та Інтернетом або між окремими ланками локальної мережі. Він відстежує й аналізує весь потік пакетів з даними що надходить до нього, і пропускає лише дозволені пакети. Таким чином, небезпечний код з Інтернету не може потрапити до локальної мережі. Принцип дії Брандмауера ілюструє рис. 4.2.

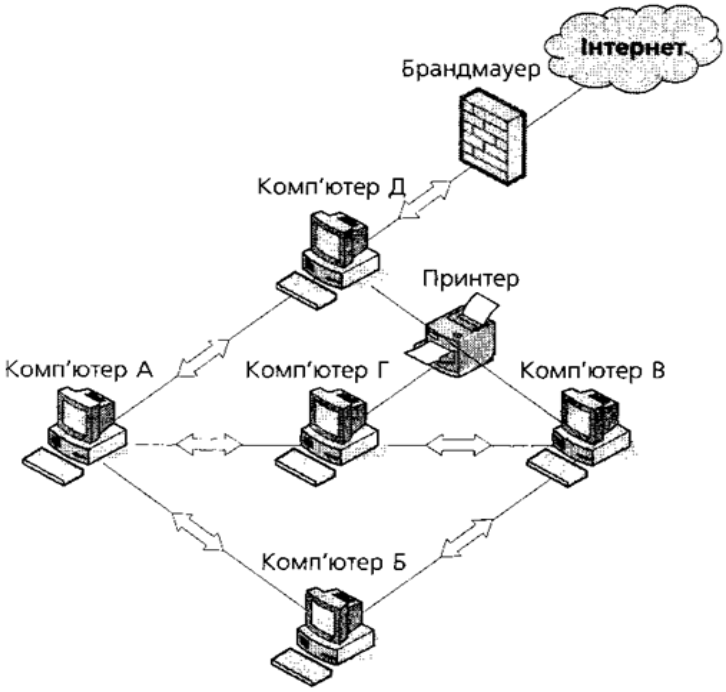

Рис. 4.2. Брандмауер у мережі

Корпоративні брандмауери, що застосовуються в мережах підприємств та установ складаються з апаратного та програмного забезпечення, завдяки чому вони надійно захищають внутрішні мережі. Для захисту домашніх комп'ютерів використовують так звані персональні брандмауери, які зазвичай реалізовані у вигляді програм.

Вибір домашнього брандмауера

Брандмауер потрібний у будь-якій локальній мережі, в тому числі й у домашній. Вже зараз у вас є можливість ознайомитися з відомостями про наявне програмне забезпечення на відповідних сайтах.

- Symantec Firewall: http://www.symantec.com (безкоштовна)
- McAfee Personal Firewall: http://us.mcafee.com (безкоштовна)
- Kerio Personal Firewall: http://www.kerio.com (потрібно ліцензія)

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 флеш-накопичувачів.

Більшість виробників антивірусних програм пропонують пробні версії, які можна завантажити на комп'ютер і використовувати протягом певного часу. Пробними версіями можуть бути укомплектовані також нові комп'ютери.

Незалежно від того, яку з антивірусних програм ви оберете, важливо постійно її оновлювати. Зазвичай за певну річну оплату ви можете завантажувати оновлення з сайту виробника. Більшість програм самостійно щоденно підключаються до свого сайту й перевіряють, чи нема там «свіжих» оновлень.

Центр забезпечення безпеки Windows

Після того як корпорацією Microsoft для операційної систем Windows XP був розроблений пакет оновлень Service Pack 2 (SP2), процес підтримки цієї операційної системи значно спростився. Основними нововведеннями цього пакету є Центр забезпечення безпеки, за допомогою якого користувач може встановити бажаний рівень захисту комп'ютера, а також вбудований засіб блокування спливаючих вікон у браузері Microsoft Internet Explorer.

Центр забезпечення безпеки складається з трьох компонентів: брандмауера, засобу автоматичного оновлення системи та засобу антивірусного захисту. Центр регулярно виконує перевірку комп’ютера й нагадує користувачеві, що певна важлива функція вимкнена чи застаріла. Для доступу до Центру забезпечення безпеки потрібно з меню Пуск визвати команду Панель керування та вибрати посилання Центр обеспечения безопасности (Центр забезпечення безпеки). Після цього відкриється діалогове вікно, показане на рис. 4.3

Рис 4.3. Центр забезпечення безпеки

Брандмауер Windows, настройки якого показані на рис. 4.4, стежить за всіма застосуваннями та іншими потенційно небезпечними для комп’ютера компонентами. На рис. 4.5 ви бачите вікно з настройками браузера.

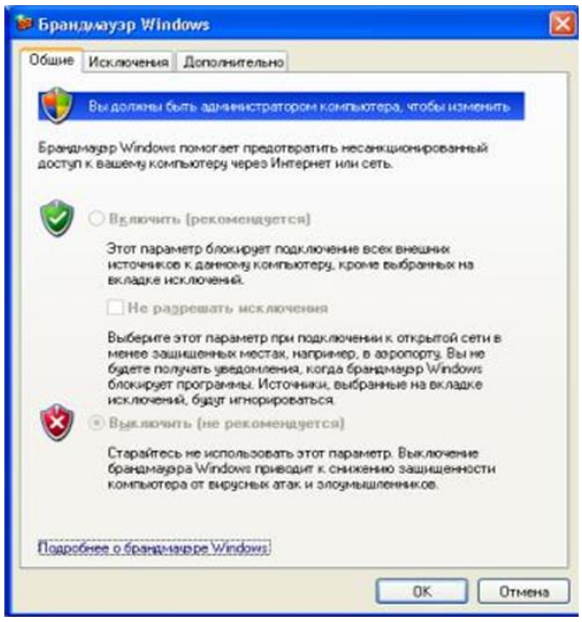

Рис. 4.4. Брандмауэр Windows

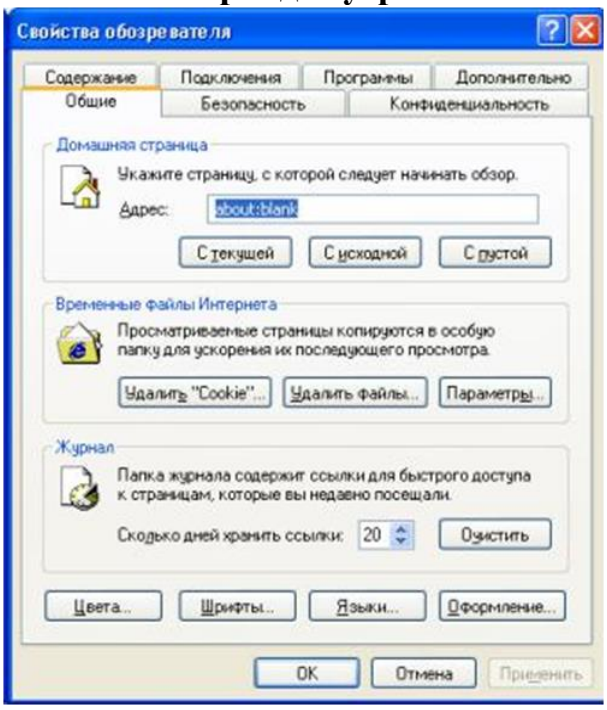

Рис. 4.5. Настройки браузера

Автоматичне оновлення Windows

Автоматичне оновлення Windows — це засіб, що демонструє турботу корпорації Microsoft про безпеку користувачів. Фахівці корпорації доклали багато зусиль, щоб операційна система Windows була захищеною, швидкою і потужною та водночас дружньою до користувача. Завдяки Центру забезпечення безпеки Windows процедури завантаження та встановлення оновлень значно спростилися. Користувачеві треба лише переконатись, що компонент Автоматичне оновлення Windows ввімкнено (за умовчанням це саме так), і за потреби змінити час, коли він виконуватиме перевірку наявності оновлень на сайті Microsoft, їх завантаження та встановлення на комп'ютер. Потрібно лише, щоб комп’ютер у цей час був увімкнений та підключений до Інтернету.

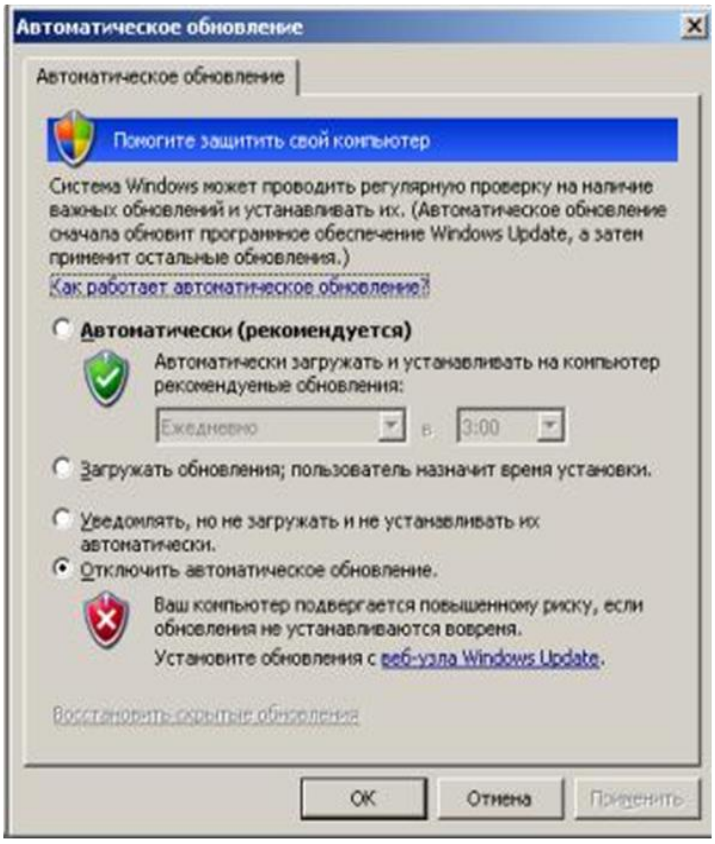

Рис. 4.6. Автоматичне оновлення Windows

Блокування спливаючих вікон

Спливаючі вікна з'являються під час перегляду багатьох сайтів. Деякі такі вікна містять лише рекламу, проте є вікна, разом з якими без вашого відома може завантажуватися та встановлюватися програмне забезпечення типу Spyware.

Як зазначалося вище, операційна система Windows XP із встановленим пакетом оновлень SP2 має засіб блокування спливаючих вікон, який вбудований в Internet Explorer. Користувач може обрати потрібний варіант: блокувати всі такі вікна, блокувати лише ті, що належать до безпечних сайтів, або ж не блокувати жодні. Для доступу до даного засобу відкрийте у програмі Internet Explorer меню Сервіс «Блокирование всплывающих окон» (Сервіс «Блокування спливаючих вікон»). Воно містить команду-перемикач Включить/Выключить блокирование всплывающих окон (Ввімкнути/Вимкнути блокування спливаючих вікон), а також команду Параметри блокирования всплывающих окон (Параметри блокування спливаючих вікон), яка доступна лише за умови, що блокування спливаючих вікон ввімкнене. Коли таке вікно блокується, у верхній частині вікна Internet Explorer виводиться інформаційна панель.

Також є додаткові програмні продукти які забороняють відкриття спливаючих вікон.

Найбільш поширеними є такі:

- Adblock (розповсюджується вільно)
- AdSweep (розширення можливостей переглядача Opera, розповсюджується вільно)
- Adblock Plus (розширення можливостей переглядача для Mozilla Firefox розповсюджується вільно)
- Adguard (потребує ліцензію – платна)
- Ad Muncher (платна ліцензія)
- Netpolice (Pro - потребує ліцензію – платна, Lite – безкоштовна ліцензія)
- Zero PopUp Killer XP 7.7 (потребує ліцензію – платна)

- A1Tech AdsGone 2004 Popup Killer 4.9.4 (потребує ліцензію – платна)
- GuardPrivacy PopUps Blocker 3.23.103 (потребує ліцензію – платна)
- IHatePopups 1.5.335 (потребує ліцензію – платна)
- PopSwat 1.4.15 (потребує ліцензію – платна)
- Popup XP 2.0.446 (потребує ліцензію – платна)

Антиспамове програмне забезпечення

Програми даного типу застосовуються для фільтрації електронної пошти, вони аналізують усі повідомлення, які надходять до вашого комп'ютера, з метою виявлення та видалення спаму. Зазвичай у таких програмах є можливість задавати правила, за якими бажана пошта буде відокремлюватися від небажаної. У цих правилах може враховуватися наявність певних слів та адрес відправника у заголовках поштових повідомлень або наявність певних слів у самих повідомленнях.

Існує також програмне забезпечення, яке розширює антиспамові можливості поштового клієнта. Воно буває різним: одні програми просто ізолюють підозрілі повідомлення, а інші відокремлюють усі повідомлення із зворотними адресами, яких немає у сформованому вами списку.

Антиспамове програмне забезпечення

SpamPepper 4.34

SpamPepper на 100% процентов заблокирует весь спам вам только нужно вовремя обновлять фильтры

Хочу особо обратить внимание на то, что в настройках почтового клиента НИЧЕГО менять не надо. Просто вводите в SpamPepper 'е нужные аккуанты. И через него будет проходить вся почта.

Также программа обладает функцией автоответа и умеет искать badwords (плохие слова) в теле письма.

McAfee SpamKiller 2005 6.0

Утилита от известной фирмы разработчика антивирусов, для борьбы со спамом. Поддерживает различные почтовые клиенты, позволяет настроить фильтры и загрузить новые из Интернета.

ESET Internet Security

ESET глобальний бренд з більш ніж 100 мільйонами користувачів у 202 країнах світу. Філософія та цінності залишаються незмінними – допомогти побудувати більш безпечний цифровий світ, де кожен може по-справжньому насолоджуватися технологіями безпеки».

Запобігання зараженню вірусами

Як вже зазначалося, немає й не може бути стовідсоткової гарантії того, що ви ніколи не підхопите в Інтернеті вірус, не зазнаєте вторгнення чи не отримаєте спам, — певний ризик завжди існує. Для запобігання цьому потрібно використовувати відповідні програмні засоби, завжди керуватися здоровим глуздом та дотримуватися правил безпечної поведінки в Інтернеті. Ось деякі з цих правил.

- На комп'ютері завжди має функціонувати антивірусне програмне забезпечення. Стежте за його актуальністю. Настройте програму в такий спосіб, щоб вона автоматично сканувала систему, коли ви не працюєте, скажімо, по неділях чи вночі.
- Не відкривайте файли-вкладення, які надходять разом із повідомленнями електронної пошти, якщо ви не впевнені, що вони містять саме ті дані, на які ви чекаєте.

- Використовуйте лише те програмне забезпечення, яке надійшло з перевірених джерел.
- Своєчасно встановлюйте оновлення операційної системи. Якщо вона не робить це автоматично, відвідуйте сайт оновлень Microsoft за такою адресою:http://www.update.microsoft.com/windowsupdate/v6/default.aspx?ln=ru

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?

Ми вже розповідали про існування певної категорії людей, що здійснюють 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. Проте відомо багато випадків, коли жертвами зловмисників стають приватні особи, особливо якщо вони передають конфіденційну інформацію через Інтернет без належного захисту.

Часом зловмисники намагаються викрасти персональну інформацію для того, щоб від імені іншої людини відкривати рахунки, купувати товари тощо. Найчастіше викрадають дані про банківські картки. Анонімність і величезні розміри Інтернету роблять його «землею обітованою» для шахраїв усіх ґатунків.

Як уберегти персональну інформацію від викрадення?

Незважаючи на всі пов'язані з Інтернетом загрози, ним можна безпечно користуватися за умови дотримання певних правил. Аналогічні правила та надійні й безпечні методи передавання даних Інтернетом розроблені і для персональної інформації.

Захищені сайти та шифрування

Ніколи не надсилайте персональну інформацію незнайомим людям. Це основне правило безпеки. Дітей молодшого віку потрібно вчити, щоб вони ніколи не повідомляли в Інтернеті свої справжні імена, адреси та будь-яку іншу інформацію. Проте ви вже здатні визначити ситуації, коли це робити безпечно, наприклад у разі заповнення форми на сайті навчального закладу, до якого ви маєте намір надіслати документи про вступ. Головне, в кожному випадку треба бути впевненим, що одержувач інформації надійний. Не завадить також переконатися, що сайт захищений і на ньому використовуються технології шифрування.

Захищена веб-сторінка

Зверніть увагу на значок замка у правій частині рядка стану браузера та на URL-сторінки, де як протокол зазначений HTTPS. Значок замка показує, що сайт зашифрований з використанням протоколу SSL (Secure Sockets Layer — рівень захищених сокетів). Він підтримується всіма браузерами та застосовується для безпечного передавання інформації.Відповідно, для передавання веб-сторінок, що належать до захищеної частини сайту, замість протоколу HTTP використовується протокол HTTPS, тобто поєднання протоколів HTTP та SSL.

Правила безпеки, яких слід дотримуватися під час передавання інформації Інтернетом

Коли ви працюєте із захищеними сайтами, дотримуйтесь наведених нижче правил, які стосуються надання вами будь-якої інформації. Це гарантуватиме, що вона не потрапить до чужих рук. Навіть якщо у вас поки немає власної картки чи банківського

рахунку, краще заздалегідь виробити звичку дотримуватись правил, наведених у цьому розділі.

- Не надавайте більше інформації, ніж потрібно.
- Захищені сайти зазвичай вимагають введення імені користувача та пароля. Робіть його довжиною щонайменше вісім символів, комбінуючи букви та числа. І головне, паролем не повинно бути щось очевидне, якісь слова чи дати.

ПРИМІТКА

Зручно мати два пароля: один для так званих розважальних сайтів, тобто ігор, чатів тощо, а інший для більш важливих дій, наприклад для придбання товарів. Тоді зменшиться ймовірність, що ваші важливі дії піддаватимуться ризику. І ніколи не використовуйте для паролів такі дані, як дата народження, номер телефону чи ім'я.

- Користуйтеся останньою версією браузера. У новіших браузерах реалізовані останні досягнення в галузі шифрування та інших технологій захисту й безпеки.
- Уважно читайте правила безпеки сайту. Адже навряд чи вам сподобається, коли інформацію, що ви надасте про себе, організація згодом продасть власникам розсилок.
- Занотовуйте інформацію про дії, пов'язані з купівлею або замовленням товарів через Інтернет.

Як захиститися від людей, які прагнуть завдати мені шкоди?

Коли зловмисник, вкравши ідентифікаційні дані, знімає гроші з чужого рахунку, це дуже неприємно, але значно гірше, коли він отримає персональну інформацію і це стане загрозою безпеці чи життю людини.

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.

Саме чати та системи обміну миттєвими повідомленнями ці особи обирають для налагоджування контактів з молодими людьми, оскільки почуваються там безпечно.

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.
- Візьміть за звичку не надавати свою персональну інформацію в кімнатах чату та системах обміну миттєвими повідомленнями.

ПРИМІТКА

Налаштувати свою програму обміну миттєвими повідомленнями можна так, що «бачити» вас і надсилати вам повідомлення зможуть лише люди зі складеного вами списку знайомих. Можна навіть відкрити кімнату чату зі своїми друзями, але треба уважно стежити, щоб до неї не потрапили сторонні особи.

- Ніколи не погоджуйтеся на зустріч із людиною, з якою ви познайомилися через Інтернет.
- Не надсилайте своє фото інтернет-знайомим.

- Ніколи не давайте незнайомим людям таку інформацію, як повне ім'я, адреса, номер школи, розклад занять або відомості про родину.

ПОРАДИ БАТЬКАМ

Спільною і важливою рисою дитячої безпеки як на вулиці,так і в кіберпросторі є те, що правила поведінки дуже схожі, а тому і розповісти про них буде просто.

1.Не можна розмовляти з чужими на вулиці — не можна відповідати незнайомим в мережі Інернет.Дорослий не має звертатися до дитини з дорослими проблемами. З дорослими проблемами, дорослі повинні звертайтеся до дорослих. Це їх проблеми, тому діти не повинні відчувати себе винними, що відмовили дорослим;

2. Не відчиняємо незнайомим двері — не відкриваємо незнайомі посилання;

3. Тримаємо безпечну для себе дистанцію з незнайомцями, не дозволяючи її порушувати незнайомцям - не додаємо в друзі тих, з ким не знайомі;

4. Не розказуємо всім навколо домашню адресу, персональні контактні дані, місце роботи батьків та будь-яку іншу персональну інформацію — не потрібно заповнювати всі анкети в мережі Інтернет, які вам пропонують;

5.Дорослі завжди повинні знати місцезнаходження їх дитини (садочок, школа, гуртки, друзі і т.д.). Якщо дитина не бажає розповідати куди збирається йти — вона туди НЕ ИДЕ. В мережі дорослі мають знати в яких групах і мережах є їх дитина, або мати доступ до перегляду цих чатів з попередженням про це дитини, інакше є ризик втратити довіру дитини.

6. Головний месседж до дитини — це те, що ви довіряєте йому, але не довіряєте чужим;

7. Про будь-які незрозумілі дії в бік дитини як на вулиці, так і в мережі Інтернет - дитина має вам розповідати. А щоб дитина НІКОЛИ не боялася цього робити — не сваріть її за правду та будьте відкритими до дитячих переживань.

Пам'ятайте, безпека ваших дітей - понад усе!