**МІНІСТЕРСТВО ОСВІТИ І НАУКИ,
МОЛОДІ ТА СПОРТУ УКРАЇНИ
УМАНСЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПАВЛА ТИЧИНИ**

Навчально-методичний посібник до курсу

“*ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ*”

Укладач С. О. Троян

**Умань
2012**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ,
МОЛОДІ ТА СПОРТУ УКРАЇНИ
УМАНСЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПАВЛА ТИЧИНИ**

Навчально-методичний посібник до курсу

“*ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ*”

Укладач С. О. Троян

**Умань
2012**

УДК 004.056(075.8)
ББК. 73.7я73
З-38

Рецензенти: канд. екон. наук, доц. кафедри інформатики КНЕУ В. Д. Дербенцев
(Київський національний економічний університет імені Вадима Гетьмана**)**,
кандидат пед. наук, доц. О. В. Малишевський
(Уманський державний педагогічний університет імені Павла Тичини)

Рекомендовано до друку
Вченою радою факультету
Протокол №___ від _____.2012 р.

З-38 Захист інформаційних ресурсів: навчально-методичний посібник до курсу **“Захист інформаційних ресурсів” / укл. С. О. Троян. – Умань : [б.в.], 2012.-120 с.**

Анотація

У посібнику зроблено спробу подати логічно структурований комплексний виклад теоретичних основ та практичного використання сучасних систем захисту інформаційних ресурсів і технологій згідно із загальними підходами в Україні та світі. Розглядаються поняття, класифікація, сфери застосування, складові і ознаки, різні типи підходів, систем і способі захисту інформаційних ресурсів, а також методи використання інформаційних технологій, їх застосування в різних сферах сучасного життя.

Для фахівців у галузі інформатики, а також студентів, що навчаються за усіма спеціальностями напряму підготовки «Інформатика*» та інш..

УДК 004.056(075.8)
ББК. 73.7я73

ЗМІСТ

Лабораторна робота №1

Тема: Поняття захисту інформації та інформаційної безпеки. Критерії оцінки інформаційної безпеки. Аспекти захисту інформації.

Мета: ознайомитися з базовими поняттями захисту інформації, інформаційної безпеки, властивостями інформації, аспектами захисту інформації та критеріями оцінки інформаційної безпеки.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Захист інформації (англ. Data protection) — сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації. Термін вживається в Україні для опису комплексу заходів по забезпеченню інформаційної безпеки.

Інформаційна безпека (information security) — збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність.

Конфіденційність (англ. confidentiality, privacy) — властивість не підлягати розголосові; довірливість, секретність, суто приватність.

Типологія конфіденційності

Конфіденційність адміністративна [mandatory confidentiality] — послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом адміністративного.

Конфіденційність довірча [discretionary confidentiality] — послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом довірчого.

Конфіденційність інформації [information confidentiality] — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Цілісність (англ. integrity) — внутрішня єдність, пов'язаність усіх частин чого-небудь, єдине ціле. В інформаційній системі — стан даних або інформаційної системи, в якій дані та програми використовуються встановленим чином, що забезпечує:

- стійку роботу системи;
- автоматичне відновлення у випадку виявлення системою потенційної помилки;
- автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

Для інформаційної системи можна розглядати такі поняття як цілісність даних, цілісність інформації, цілісність бази даних, цілісність інформаційної системи і таке інше.

Цілісність даних [data integrity] — в інформаційній системі — стан при якому дані, що зберігаються в системі, в точності відповідають даним у вихідних документах; властивість, що має відношення до набору даних і означає, що дані не можуть бути змінені або зруйновані без санкції на доступ. Цілісність даних вважається збереженою, якщо дані не спотворені і не зруйновані (стерті).

Семантична цілісність даних [semantic data integrity] — стан даних, коли вони зберігають свій інформаційний зміст та однозначність інтерпретації в умовах випадкових впливів.

Цілісність інформації [information integrity] — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і (або процесом). Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення).

Цілісність бази даних [database integrity] — стан бази даних, коли всі значення даних правильні в тому сенсі, що відображають стан реального світу (в межах заданих обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємної не суперечливості. Підтримка цілісності бази даних включає перевірку цілісності і відновлення з будь-якого неправильного стану, який може бути виявлено; це входить у функції адміністратора бази даних.

Цілісність системи [system integrity] — властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

Цілісність адміністративна [mandatory integrity] — послуга безпеки, яка забезпечує цілісність інформації відповідно до принципів адміністративного керування доступом.

Цілісність довірча [discretionary integrity] — послуга безпеки, яка забезпечує цілісність інформації відповідно до принципів керування доступом довірчого.

Цілісність об'єкта [object integrity] — властивість об'єкта доступу, що характеризує його авторизований стан.

Доступність (англ. Availability) — властивість інформаційного ресурсу, яка полягає в тому, що користувач та/або процес, який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу.

Суть властивості полягає в тому, що потрібний інформаційний ресурс знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Апелювання (англ. non-repudiation) — можливість довести, що автором є саме заявлена людина (юридична особа), і ніхто інший.

Підзвітність (англ. accountability) — властивість інформаційної системи, що дозволяє фіксувати діяльність користувачів, використання ними пасивних об‘єктів та однозначно встановлювати авторів певних дій в системі.

Достовірність (англ. reliability)- властивість інформації, яка визначає ступінь об'єктивного, точного відображення подій, фактів, що мали місце.

Автентичність (англ. authenticity) — властивість, яка гарантує, що суб'єкт або ресурс ідентичні заявленим.

Відповідно до властивостей інформації, виділяють такі загрози її безпеці:

- ***загрози цілісності:***
  - знищення;
  - модифікація;
- ***загрози доступності:***
  - блокування;
  - знищення;
- ***загрози конфіденційності:***
  - несанкціонований доступ (НСД);
  - витік;
  - розголошення.

Аспекти захисту інформації

- ***Конфіденційність*** — захист від несанкціонованого ознайомлення з інформацією.
- ***Цілісність*** — захист інформації від несанкціонованої модифікації.
- ***Доступність*** — захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію.

Кожен вид ЗІ забезпечує окремі аспекти ІБ:

Технічний — забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарт-карти тощо):

- попередження витоку по технічним каналам;
- попередження блокування;

Інженерний — попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація).

Криптографічний — попереджує доступ до за допомогою математичних перетворень повідомлення:

- попередження несанкціонованої модифікації ;
- попередження НС розголошення.

Організаційний — попередження доступу на об’єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу).

Інформаційні системи можна розділити на три частини: *програмне забезпечення*, *апаратне забезпечення* та *комунікації* з метою цільового застосування (як механізму захисту і попередження) стандартів інформаційної безпеки. Самі механізми захисту реалізуються на трьох рівнях або шарах: Фізичний, Особистісний, Організаційний. По суті, реалізація політик і процедур безпеки покликана надавати інформацію адміністраторам, користувачам і операторам про те як правильно використовувати готові рішення для підтримки безпеки.

Об'єктивно категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною наявності у людей і їхніх співтовариств інтересів, яким може бути завданий збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує інформаційний обмін між всіма елементами соціуму.

Враховуючи вплив на трансформацію ідей інформаційної безпеки, в розвитку засобів інформаційних комунікацій можна виділити декілька етапів:

I етап — до 1816 року — характеризується використанням природно виникаючих засобів інформаційних комунікацій. В цей період основне завдання інформаційної безпеки полягало в захисті відомостей про події, факти, майно, місцезнаходження і інші дані, що мають для людини особисто або співтовариства, до якого вона належала, життєве значення.

II етап — починаючи з 1816 року — пов'язаний з початком використання штучно створюваних технічних засобів електро- і радіозв'язку. Для забезпечення скритності і перешкодостійкості радіозв'язку необхідно було використовувати досвід першого періоду інформаційної безпеки на вищому технологічному рівні, а саме застосування перешкодостійкого кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу).

III етап — починаючи з 1935 року — пов'язаний з появою засобів радіолокацій і гідроакустики. Основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, направлених на підвищення захищеності засобів радіолокацій від дії на їхні приймальні пристрої активними маскуючими і пасивними імітуючими радіоелектронними перешкодами.

IV етап — починаючи з 1946 року — пов'язаний з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів). Завдання інформаційної безпеки вирішувалися, в основному, методами і способами обмеження фізичного доступу до устаткування засобів добування, переробки і передачі інформації.

V етап — починаючи з 1965 року — обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішувалися, в основному, методами і способами фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних в локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів.

VI етап — починаючи з 1973 року — пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. Загрози інформаційній безпеці стали набагато серйознішими. Для забезпечення інформаційної безпеки в комп'ютерних системах з безпровідними мережами передачі даних потрібно було розробити нові критерії безпеки. Утворилися співтовариства людей — хакерів, що ставлять собі за мету нанесення збитку інформаційній безпеці окремих користувачів, організацій і цілих країн. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки — найважливішою і обов'язковою складовою національної безпеки. Формується інформаційне право — нова галузь міжнародної правової системи.

VII етап — починаючи з 1985 року — пов'язаний із створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення. Можна

припустити що черговий етап розвитку інформаційної безпеки, очевидно, буде пов'язаний з широким використанням надмобільних комунікаційних пристроїв з широким спектром завдань і глобальним охопленням у просторі та часі, забезпечуваним космічними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення макросистеми інформаційної безпеки людства під егідою ведучих міжнародних форумів.

Базові поняття інформаційної безпеки:

Інформаційна безпека держави — стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Інформаційна безпека організації — цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Інформаційна безпеки особистості характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору.

Забезпечення ІБ держави

Згідно з українським законодавством, вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Забезпечення ІБ підприємства/організації

В Україні забезпечення ІБ здійснюється шляхом захисту інформації — у випадку, коли необхідність захисту інформації визначена законодавством в галузі ЗІ. Для реалізації захисту інформації створюється Комплексна система захисту інформації (КСЗІ), або, у випадку, коли суб'єкт ІБ має наміри розробити і реалізувати політику ІБ і може реалізовувати їх без порушення вимог законодавства:

- міжнародними стандартами ISO: ISO/IEC 17799:2005, ISO/IEC 27001:2005 та ін. — для підтримки рішень на основі ITIL та COBIT і виконання вимог англ. Sarbanes-Oxley Act (акту Сербайнза-Оклі про відповідальність акціонерів за обізнаність про стан своїх активів). Тоді на підприємстві створюється Система управління інформаційною безпекою (СУІБ), яка повинна відповідати усім вимогам міжнародних стандартів в галузі ІБ.
- власними розробками.

Забезпечення ІБ особистості

Органи (підрозділи) забезпечення ІБ

1. Міжнародні організації
2. Державні органи

- Відділи спецслужб держави.

- Спеціально уповноважений орган держави з питань захисту інформації (зараз в Україні — це Державна служба спеціального зв'язку та захисту інформації (скор. ДССЗЗІ)

3. Підрозділи підприємства

На підприємстві функцію забезпечення ІБ може виконувати як окремий відділ Служби безпеки підприємства, так і окрема Служба (Служба захисту інформації).

Для контролю за КСЗІ в обов'язковому порядку створюється Служба захисту інформації в інформаційно-телекомунікаційній системі (сама назва «Служба» не є обов'язковою).

Функції з контролю за СУІБ покладаються на певний відділ підприємства.

Законодавчі вимоги і регулювання ІБ

Загальнозаконодавчі вимоги – інформаційне законодавство держави, спеціалізовані нормативні акти (в Україні — це Нормативні документи в галузі технічного захисту інформації (скор. НД ТЗІ).

Галузеві вимоги (галузеві стандарти тощо).

Критерії оцінки інформаційної безпеки (англ. Common Criteria) є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності.

За допомогою критеріїв можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

Для характеристики основних критеріїв інформаційної безпеки застосовують модель тріади CIA.

Ця система передбачає такі основні характеристики інформаційної безпеки як конфіденційність, цілісність, доступність.

Інформаційні системи аналізуються в трьох головних секторах: технічних засобах, програмному забезпеченні і комунікаціях, з метою ідентифікування і застосування промислових стандартів інформаційної безпеки, як механізми захисту і запобігання, на трьох рівнях або шарах: фізичний, особистий і організаційний. По суті, процедури або правила запроваджуються для інформування адміністраторів, користувачів та операторів щодо використовування захисної продукції для гарантування інформаційної безпеки в межах організацій.

В Україні також розробляються і використовуються критерії інформаційної безпеки. Наприклад департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України прийняв нормативний документ технічного захисту інформації 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» який подібний до моделі тріади CIA.

Функціональні критерії

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги відносяться до критеріїв конфіденційності.

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. У випадку, якщо існують вимоги щодо обмеження можливості модифікації інформації, то їх відносяться до критеріїв цілісності.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то їх відносяться до критеріїв доступності.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні функції відносяться до критеріїв спостереженості.

Окрім функціональних критеріїв захищеності існують таки критерії гарантій, що дозволяють оцінити коректність реалізації систем захисту. Ці критерії включають вимоги до архітектури комплексу

засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Запустіть браузер Інтернет (Це може бути Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera чи будь-який інший, що встановлений на вашому комп'ютері).
2. Користуючись однією з пошукових систем (Yahoo!, Google, чи будь-якою іншою) ознайомтеся із законодавчою базою України, що стосується захисту інформації та інформаційної безпеки. Назви основних законів, указів президента, постанов, положень запишіть до звіту (не менше 15).
3. На офіційному сайті Верховної ради «Законодавство України» (http://zakon2.rada.gov.ua/laws) знайдіть Закон України «Про інформацію», ознайомтесь з його основними положеннями та занотуйте до звіту такі відомості:
   - визначення основних термінів;
   - основні види інформації;
   - основні аспекти відповідальності за порушення законодавства про інформацію.
4. На офіційному сайті Верховної ради «Законодавство України» (http://zakon2.rada.gov.ua/laws) знайдіть Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», ознайомтесь з його основними положеннями та занотуйте до звіту такі відомості:
   - визначення основних термінів (не менше 7);
   - об'єкти захисту та суб'єкти відносин;
   - умови обробки державної інформації в системі;
   - повноваження державних органів у сфері захисту інформації в системі;
   - основні аспекти відповідальності за порушення законодавства про захист інформації в системах.
5. Зробіть та запишіть до звіту висновки по роботі.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається інформаційною безпекою?
2. Дайте визначення поняття захисту інформації.
3. Назвіть та охарактеризуйте основні властивості інформації.
4. Назвіть та охарактеризуйте основні аспекти захисту інформації та інформаційної безпеки.
5. Які виділяють загрози безпеки інформації відповідно до її властивостей?
6. Назвіть та дайте визначення базовим поняттям інформаційної безпеки.
7. Охарактеризувати шляхи забезпечення інформаційної безпеки держави, підприємства, особистості.
8. Назвати та охарактеризувати основні критерії інформаційної безпеки.
9. Що являють собою законодавчі вимоги до інформаційної безпеки?
10. Що являє собою модель тріади CIA?

Лабораторна робота №2

Тема: Засоби резервного копіювання та відновлення даних. Пристрої відновлення даних.

Мета: ознайомитися з поняттям резервного копіювання та відновлення даних, засобами їх здійснення; причинами пошкодження інформації та вимогами до систем резервного копіювання інформації.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

В інформаційних технологіях під резервним копіюванням розуміється створення копії файлів даних для того, щоб ці файли можна було відновити у разі їх знищення або втрати. Повне резервне

копіювання в цілях екстреного відновлення означає створення точного образу диска або розділу, який дозволяє повернути систему в повністю робочий стан протягом декількох хвилин, а не годин або навіть днів, включаючи апаратно-незалежне відновлення системи.

Резервне копіювання (англ. backup) — процес створення копії даних на носії (жорсткому диску, дискеті тощо), призначеному для відновлення даних в оригінальному місці їх розташування в разі їх пошкодження або руйнування.

Причини пошкодження та руйнування інформації

Експлуатаційні поломки носіїв інформації (жорстких дисків, дискет, CD / DVD)

Опис: випадкові поломки в межах статистики відмов, пов'язані з необережністю або виробленням ресурсу. Звичайно ж, якщо якась важлива інформація вже втрачена, то можна звернутися в спеціалізовану службу — але надійність цього не стовідсоткова.

Шлях запобігання: зберігати всю інформацію (кожен файл) мінімум у двох примірниках (причому кожен екземпляр на своєму носії даних). Для цього застосовуються:

RAID 1, що забезпечує відновлення найсвіжішої інформації. Файли, розташовані на сервері з RAID, більш захищені від поломок, ніж ті, що зберігаються на локальній машині;

Ручне або автоматичне копіювання на інший носій. Для цього може використовуватися система контролю версій, спеціалізована програма резервного копіювання або підручні засоби на зразок cmd-файлу, які періодично запускається.

Ця причина не найпоширеніша, оскільки сучасні жорсткі диски рідко виходять з ладу.

Сучасний жорсткий диск у режимі постійно включеного комп'ютера (сервера) працює до відмови близько трьох років.

Ризик: якщо організований RAID 1 на двох однакових жорстких дисках, введених в експлуатацію одночасно, то виходити з ладу вони будуть приблизно в один і той же час! Іншими словами, якщо ви виявляєте, що перший диск почав покриватися збійними блоками, велика ймовірність, що збої є і на другому диску. Однак імовірність того, що на обох дисках вийдуть з ладу однакові сектору, порівняно незначна.

Стихійні та техногенні лиха

Опис: шторм, землетрус, крадіжка, пожежа, прорвало водопровід — все це призводить до втрати всіх носіїв даних, розташованих на певній території.

Шлях запобігання: єдиний спосіб захисту від стихійних лих — тримати частину резервних копій в іншому приміщенні.

Шкідливий програмний засіб

Опис: в цю категорію входить випадково занесене ПЗ, яке навмисно псує інформацію — віруси, черв'яки, «троянські коні». Іноді факт зараження виявляється, коли чимала частина інформації перекручена або знищена.

Шлях запобігання:

Встановлення антивірусних програм на робочі станції. Найпростіші антивірусні заходи — відключення автозавантаження, ізоляція локальної мережі від Інтернету, тощо

Забезпечення централізованого поновлення: перша копія антивірусу отримує оновлення прямо з Інтернету, а інші копії налаштовані на папку, де перша завантажує оновлення; також можна налаштувати проксі-сервер таким чином, щоб оновлення кешувати (це всі заходи для зменшення трафіку).

Мати копії в такому місці, до якого вірус не добереться — виділений сервер або знімні носії.

Якщо копіювання йде на сервер: забезпечити захист сервера від вірусів (або встановити антивірус, або використовувати ОС, для якої ймовірність зараження мала). Зберігати версії достатньої давності, щоб існувала копія, яка не контактувала із зараженим комп'ютером.

Якщо копіювання йде на змінні носії: частину носіїв зберігати (без дописування на них) досить довго, щоб існувала копія, що не контактувала із зараженим комп'ютером.

Людський фактор

Опис: навмисне або ненавмисно знищення важливої інформації — людиною, спеціально написаної шкідливою програмою.

Шлях запобігання:

Ретельно розставляються права на всі ресурси, щоб інші користувачі не могли модифіковані чужі файли. Виняток робиться для системного адміністратора, який повинен мати всі права на все, щоб бути здатним виправити помилки користувачів, програм і т. д.

Забезпечити діючу систему резервного копіювання — тобто, систему, якої реально користуються і яка досить стійка до помилок оператора. Якщо користувач не користується системою резервного копіювання, вся відповідальність за збереження лягає на нього.

Зберігати версії достатньою давності, щоб при виявленні зіпсованих даних файл можна було відновити.

Перед встановленням заново ОС слід обов'язково копіювати весь вміст розділу, на якій буде встановлена ОС, на сервер, на інший розділ або на CD / DVD.

Оперативно оновлювати ПЗ, по якому є підозра на втрату даних.

Резервне копіювання необхідно для можливості швидкого і недорогого відновлення інформації (документів, програм, настройок і т. д.) у випадку втрати робочої копії інформації з будь-якої причини. Крім цього вирішуються суміжні проблеми:

- Дублювання даних
- Передача даних і робота з загальними документами.

Вимоги до систем резервного копіювання

Надійність зберігання інформації. Забезпечується застосуванням відмовостійкого обладнання систем зберігання, дублюванням інформації і заміною втраченої копії іншою у разі знищення однієї з копій (в тому числі як частина відмовостійкості) .

Простота в експлуатації — автоматизація (по можливості мінімізувати участь людини: як користувача, так і адміністратора).

Швидке впровадження (просте встановлення та налаштування програм, швидке навчання користувачів).

Види резервного копіювання

- Повне резервування Full Backup
- Диференціальне резервування Differential Backup
- Додаткове резервування Incremental Backup
- Пофайловий метод
- Блочне інкрементальне копіювання Block Level Incremental

Повне резервування – копіювання всієї системи і всіх файлів. Щотижневе, щомісячне та щоквартальне резервне копіювання. Перше щотижневе копіювання повинне бути повним резервуванням, зазвичай виконується по п’ятницям або на вихідних під час якого копіюються всі необхідні файли. Інші копіювання що будуть виконуватися до наступного, можуть бути додатковими або диференційними, головним чином для економії часу та місця на носії.

Диференційне копіювання – кожен файл що було змінено з моменту останнього копіювання копіюється кожен раз заново. Диференційне копіювання пришвидшує процес поновлення.

Додаткове копіювання – копіювання тільки тих фалів які було змінено з тих пір як проводилось останнє повне чи додаткове копіювання. В загальному на додаткові копіювання затрачається менше часу так як копіюється менше файлів. Однак процес поновлення даних займає більше часу так як повинні відновлюватися дані останнього повного резервування плюс всі файли додаткового резервування. При цьому на відміну від диференціального резервування, змінені або нові файли не замінюють старі а додаються на носій незалежно.

Резервування клонуванням – дозволяє скопіювати цілий розділ з усіма файлами і директоріями в інший розділ або на інший носій. Здійснюється у вигляді образу або у режимі реального часу.

Віддалене резервне копіювання – сервіс що надає користувачам систему для резервного копіювання даних. Системи віддаленого резервного копіювання за часту мають вид клієнтської програми яка виконується один раз на день. Ця програма збирає, стикає, шифрує та передає дані серверам розповсюджувачів послуг резервного копіювання.

Для резервного копіювання дуже важливим питанням є вибір схеми ротації носіїв (наприклад, магнітних стрічок). Найчастіше використовують такі схеми:

- Одноразове копіювання;
- Проста ротація;
- «Дід, батько, син»;
- «Ханойська башта»;
- «10 наборів».

Одноразове копіювання (custom) найпростіша схема, не передбачає ротації носіїв. Всі операції проводяться вручну. Перед копіюванням адміністратор задає час початку резервування, перераховує файлові системи або каталоги, які необхідно скопіювати. Цю інформацію можна зберегти в базі, щоб її можна було використовувати знову. При одноразовому копіюванні найчастіше застосовується повне копіювання.

Проста ротація – циклічне використання носіїв для копіювання. (цикл – тиждень: певний носій на певний день тиждня)

«дід, батько, син» - ієрархічна структура використання комплекту з трьох комплектів носіїв. Раз на тиждень – батько (повне резервування), щоденне – син (додаткове або диференційне). Додатково проводиться повне копіювання – дід.

Ханойська вежа – використання комплектів носіїв даних. Кожен комплект має носії що містять місячний, тижневий, денний резерв копій.

«10 наборів» - за кожним носієм закріплюється день в який виконується копіювання при цьому при повторному використанні цей індекс зміщується на одиницю.

Зберігання резервної копії

- Стрічка стримера — запис резервних даних на магнітну стрічку стримера.
- «Хмарний» бекап — запис резервних даних за «хмарною» технологією через онлайн-служби спеціальних провайдерів.
- DVD чи CD — запис резервних даних на компактні диски.
- HDD — запис резервних даних на жорсткий диск комп'ютера.
- LAN — запис резервних даних на будь-яку машину всередині локальної мережі.
- FTP — запис резервних даних на FTP-сервери.
- USB — запис резервних даних на будь-який USB-сумісний пристрій (таких, як флеш-карта або зовнішній жорсткий диск).

Програми для створення резервних копій допомагають полегшити (або повністю автоматизувати) процес створення резервної копії даних.

Одними з найпоширеніших засобів резервного копіювання та відновлення даних є системи резервного копіювання Acronis.

Компанія Acronis є технологічним лідером в розробці системних рішень для корпоративних і домашніх користувачів по роботі з жорсткими дисками, резервному копіюванню даних, управлінню завантаженням операційних систем, редагуванню дисків, надійному знищенню даних, і інших системних засобів. Серед розробок цієї компанії популярні у всьому світі продукти Acronis True Image, Acronis OS Selector, Acronis Privacy Expert, Acronis Migrate Easy, Acronis Disk Editor, Acronis Recovery Expert, а також декілька нових продуктів, які будуть доступні в найближчому майбутньому.

Driver Sweeper — невелика утиліта, призначена для повного видалення з системи різних драйверів, бекапу драйверів та їх відновлення.

Double Driver — безкоштовна програма для аналізу та створення резервних копій драйверів встановлених у вашій системі.

Nero Multimedia Suite — багатофункціональний мультимедійний пакет для роботи з CD і DVD дисками, звуком і відео, що містить безліч інструментів.

Comodo BackUp — потужна програма, що дозволяє користувачам створювати резервні копії даних, для подальшого їх відновлення.

FBackup — безкоштовна програма головним завданням якої є створення резервних копій файлів та відновлення важливих даних.

Cobian Backup — досить проста у використанні безкоштовна програма для бекапа інформації, що відрізняється зручним інтерфейсом користувача.

DriverMax — потужна безкоштовна програма для створення резервної копії драйверів апаратної частини комп'ютера.

Macrium Reflect FREE Edition — швидкодіюча безкоштовна програма для роботи з образами жорсткого диска і бекапу даних.

Handy Backup — проста у використанні програма резервного копіювання даних для захисту особистої інформації і даних співробітників.

Існує значна кількість програмних продуктів, що спеціалізуються виключно на відновлення втрачених даних. Типовим представником таких програм є Recuva.

Recuva - одна з найкращих програм для відновлення файлів випадково видалених або втрачених у результаті програмного збою або помилки.

Деякі основні можливості Recuva: після сканування видає перелік видалених файлів; дозволяє відновлювати файли, видалені з Корзини, MP3-плеєрів, флешок та мобільних пристроїв; активне поле пошуку, в якому можна вказати або ім'я шуканого файлу або його розширення; відновлює всі типи файлів; відновлює файли з карт пам'яті (SmartMedia, Secure Digital, MemoryStick, Digital cameras, Floppy disks, Jaz Disks, Sony Memory Sticks, Compact Flash cards, Smart Media Cards, Secure Digital Cards, та інших); відновлює файли з зовнішніх ZIP приводів, Firewire і USB-дисків; багатомовний інтерфейс (є український і російський переклад).

Інші програми в цій категорії:

Unstoppable copier — потужна програма за допомогою якої можна відновлювати потрібні дані з пошкоджених носіїв.

PC Inspector File Recovery — потужна утиліта яка з легкістю знайде і відновить втрачені з різних причин потрібні файли.

FinalData Standard - швидка і ефективна програма, що вважається однією з кращих для відновлення видалених або пошкоджених даних.

Search and Recover — це потужна програма, що дозволяє швидко і легко знайти на комп'ютері втрачені, видалені, або пошкоджені дані.

Dead Disk Doctor — програма для відновлення файлів з частково пошкоджених оптичних дисків, дискет та інших носіїв інформації.

FreeUndelete сканує жорсткий диск для виявлення втрачених даних, при цьому можна встановити фільтр пошуку, вказавши ім'я і розширення файлу.

DiskInternals Uneraser — програма для відновлення файлів, загублених при очищенні Кошика, видаленні через командний рядок, після форматування і т.д.

Ontrack EasyRecovery Pro Standard — програма, що дозволяє без особливих зусиль відновити дані після їх видалення з кошика, форматування диска або вірусного вторгнення.

Digital ObjectRescue Pro — програма для відновлення втрачених даних з цифрових фотокамер, MP3-плеєрів, диктофонів, цифрових камер, стільникових телефонів.

GetDataBack — програма для відновлення інформації, випадково або в результаті умисних дій видаленої з комп'ютера.

Recover My Files — програма, що є потужним інструментом для відновлення видалених файлів на комп'ютері і портативних носіях.

Відновлення даних с жорстких дисків HDD

Усі несправності накопичувачів HDD можна розділити на 3 основних групи:

- Відновлення даних з фізично несправних HDD
- Відновлення даних у разі логічних руйнувань HDD
- Відновлення даних у разі фізичних і логічних руйнувань HDD.

Під фізично несправними накопичувачами розуміються HDD, ушкодження поверхні або блоку магнітних голівок, що мають, руйнування "службової інформації", що призводять до нестійкого читання і множинних помилок, порушення системи відповідності логічного дискового простору (LBA) з фізичною геометрією HDD (транслятора).

Під логічними руйнуваннями розуміються руйнування логічної структури, що не дозволяють дістати доступ до призначеної для користувача інформації засобами операційної системи. Руйнування можуть бути викликані збоями або несправностями в роботі накопичувача або самої операційної системи, некоректними діями користувача, дією вірусних програм.

Відновлення даних з жорстких дисків це складний процес, що у більшості випадків потребує використання спеціального програмного забезпечення, широкий вибір якого наявний перед сучасним користувачем. Програмний комплекс Data Extractor UDMA - це спеціалізоване програмне забезпечення, що працює спільно з програмно-апаратним комплексом PC, - 3000 for Windows UDMA і призначене для відновлення інформації з будь-яких носіїв (HDD IDE 3.5″, 2.5″, 1.8″, 1.0″; HDD SATA) у разі логічних і деяких фізичних ушкоджень.

При використанні включених до складу комплексу засобів логічного відновлення, дані користувача можуть прочитуватися і копіюватися з несправного накопичувача вибірково. Це дозволяє істотно зменшити об'єм прочитуваних з несправного накопичувача даних і, відповідно, зменшити навантаження на несправний накопичувач, а також зменшити час, потрібний на відновлення даних.

Проблеми, з якими доводиться стикатися в ході відновлення даних, дуже різноманітні. Проте їх можна умовно розділити на три групи випадків. Ці групи випадків відновлення даних і визначають існуючі (на даний момент) типи вирішуваних комплексом завдань :

- Створення копії даних з несправного накопичувача.
- Відновлення даних у разі зруйнованого транслятора.
- Відновлення даних у разі пошкодженої логічної структури.

Перша група об'єднує випадки, коли накопичувач несправний фізично, але виходить в готовність і має справний транслятор. Це можуть бути множинні BAD -сектора, несправність БМГ або каналу читання даних. Основна мета цього завдання - максимально швидко скопіювати з несправного накопичувача максимум призначеної для користувача інформації, використовуючи механізми вичитування даних, режими роботи з логічною структурою різних файлових систем і можливості управління накопичувачем, реалізовані в комплексі Data Extractor. При цьому користувач має можливість істотно зменшити об'єм копійованої інформації за рахунок використання вбудованих в програму інструментів для роботи конкретною файловою системою, контролювати процес створення копії по створюваній в процесі роботи карті результатів і, при необхідності, оперативно міняти параметри роботи з накопичувачем. Усе це може бути дуже корисним у разі "вмираючих" накопичувачів. Істотно прискорює процес відновлення підтримка режимів UDMA33, UDMA66. Для більшості накопичувачів є можливість побудувати і враховувати в ході відновлення карту розподілу секторів накопичувача по головах блоку магнітних голівок.

Друга група - це випадки, коли зруйнована система зіставлення логічного дискового простору LBA з фізичною геометрією HDD, включаючи систему обліку дефектних областей. Це завдання зводиться до відновлення даних, шляхом відновлення транслятора або його програмну імітацію. Перший підхід в окремих випадках можна реалізувати за допомогою програмно-апаратного комплексу

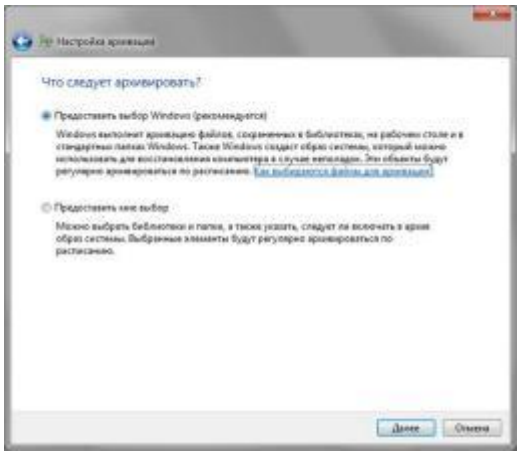
PC - 3000 for Windows UDMA або PC - 3000 for SCSI. У інших випадках можливий тільки другий підхід, який реалізований в комплексі Data Extractor.

Третя група включає усі випадки руйнування логічної структури даних. Для вирішення завдання відновлення даних, до складу комплексу включений ряд спеціалізованих режимів: режим "провідник", призначений для доступу до пошкоджених розділів, каталогів і файлів; режим "чорнове відновлення", призначений для відновлення даних у разі катастрофічних руйнувань структури файлової системи; режим "карта об'єкту", призначений для роботи з фрагментованими структурами і багато інших.

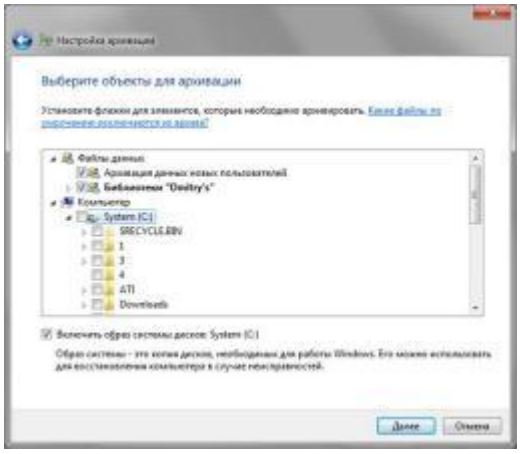
Усі три групи завдань - це досить загальна класифікація і можливі комбінації декількох випадків, але при правильному визначенні завдання можна максимально полегшити роботу по відновленню даних. При цьому методика відновлення інформації індивідуальна для кожного конкретного випадку.

Резервування вбудованими засобами Windows 7

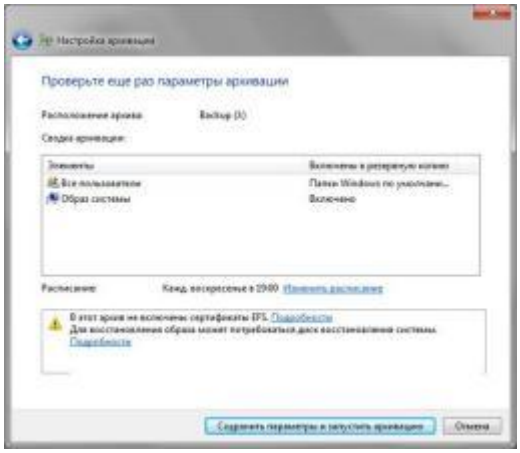
Програма резервного копіювання в Microsoft Windows 7 надає значні поліпшення в порівнянні з Backup and RestoreCenter в Windows Vista. Ви не тільки можете резервувати окремі файли, але і створити образ свого системного розділу і відновити його через завантаження з інсталяційного диска.



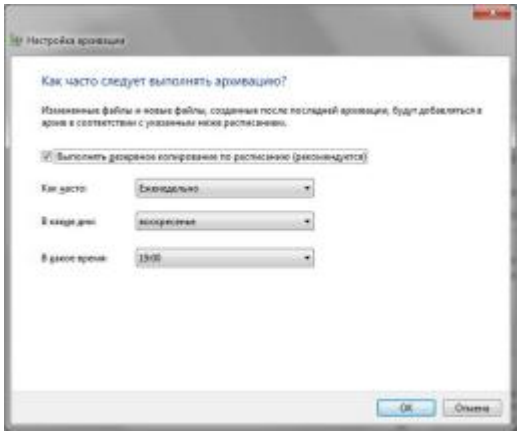
При виборі опції за умовчанням Windows включає в резервну копію всі файли. Сюди входять “Мої файли / My Files” і робочий стіл (“Мій комп’ютер / My Computer”). Дана опція створює також образ системи. Windows навіть подбає про відповідний розкладі.



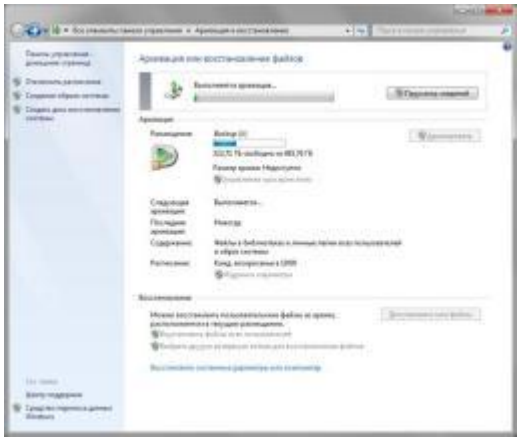
За замовчуванням пропонується резервувати те, що вважається файлами даних користувача. Якщо ви виберете резервування, настроювана користувачем (скріншот вище), то зможете додати в копію більше файлів і дисків.



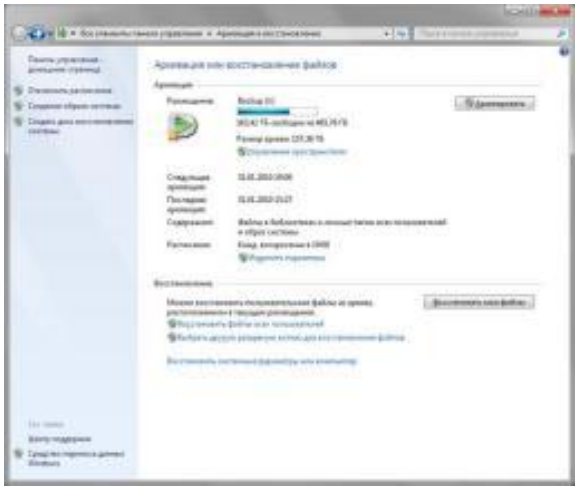
Перш ніж почати діяти, Windows Backup надає звіт про параметри резервування.



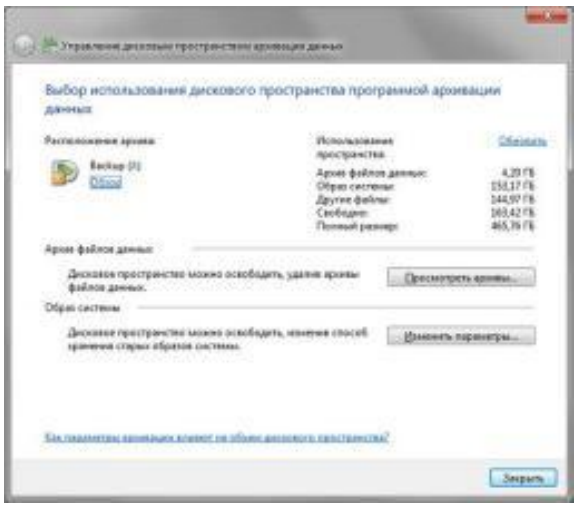
Програма запропонує вам переглянути розклад резервування. Вам не знадобиться диск відновлення системи, якщо у вас є оригінальний інсталяційний диск Windows 7.



У вікні спостереження за ходом процесу ви можете бачити всю необхідну інформацію в стилі Windows Vista / 7. Головне вікно “Архівація та відновлення / Backup and Restore” дозволяє вибрати наявний набір резервування для відновлення.



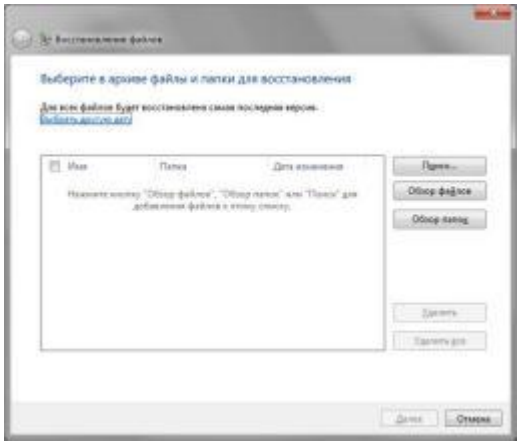
Даний скриншот був зроблений після завершення повного резервування системи на накопичувач Hitachi Portable USB 2.0 Rugged Drive.

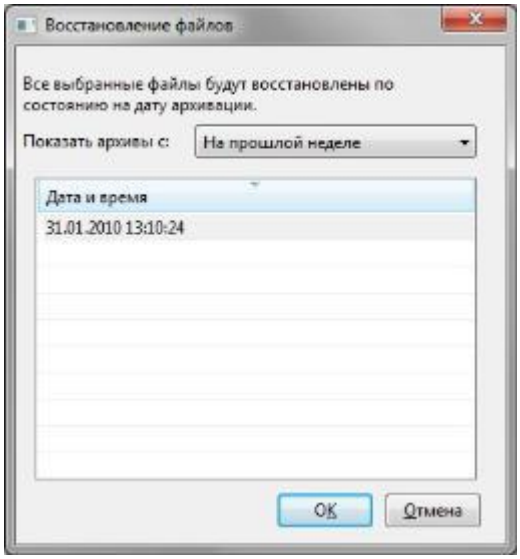


Функція управління дисковим простором буде корисна, якщо у вас закінчується вільне місце. З її допомогою ви зможете видалити старі резервні копії і вказати Windows протягом якого часу зберігати копії.

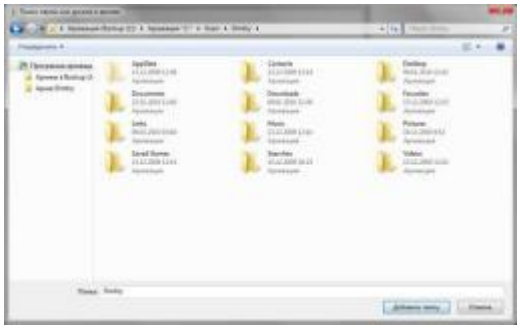
Відновлення

Зрозуміло, ми спробували відновити наші резервні копії, щоб подивитися, як вони працюють.

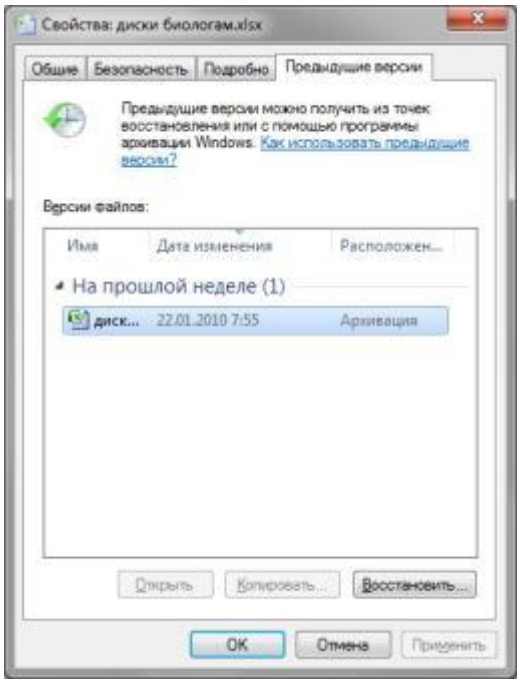




Спочатку потрібно вибрати резервний набір, який ви хочете відновити.



Потім можна всередині цього набору вибирати окремі файли. Можливо, ця функція стане в нагоді вам найчастіше, якщо, скажімо, ви змінили або переписали документ.



Windows автоматично створює і підтримує версії файлів. Їх можна подивитися у властивостях файлу. На нашому скріншоті показана можливість відновлення документа Excel.

Якщо ви хочете відновити систему цілком, доведеться завантажитися з настановного диска Windows 7 або створити диск відновлення системи, який можна використовувати для завантаження в разі відсутності інсталяційного диска.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Запустіть браузер Інтернет (Це може бути Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera чи будь-який інший, що встановлений на вашому комп'ютері)
2. Користуючись однією з пошуковх систем (Yahoo!, Google, чи будь-якою іншою) завантажити програму MiniTool Power Data Recovery Free Edition 6.5.
3. З дозволу викладача встановити даний програмний продукт на ваш робочий комп'ютер.
4. Ознайомитися з інтерфейсом даної програми, до звіту записати її можливості, описати модулі, з яких вона складається, їх призначення, ілюструючи скріншотами.
5. Створити на USB - носієві папку «Відновлення», а в ній – текстовий документ з вашим прізвищем, ім'ям, по-батькові, курсом, групою, факультетом. Видалити повністю дану папку.
6. Користуючись вкладкою ***Undelete Recovery*** програми MiniTool Power Data Recovery відновити дану папку, кожний крок даної процедури описати у звіті, ілюструючи скріншотами.
7. Зробіть та запишіть до звіту висновки по роботі.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що розуміють під резервним копіюванням?
2. Назвіть та охарактеризуйте основні причини пошкодження та руйнування інформації.

3. Які ви знаєте вимоги до систем резервного копіювання? Охарактеризуйте кожну з них.
4. Зробіть аналіз видів резервного копіювання.
5. Які ви знаєте способи зберігання резервних копій?
6. Назвіть та охарактеризуйте програми, призначені для резервного копіювання та відновлення даних.
7. Охарактеризуйте основні моменти відновлення даних с жорстких дисків HDD.
8. Опишіть процес резервування вбудованими засобами Windows 7.
9. Як здійснюється процес відновлення даних вбудованими засобами Windows7?
10. Опишіть можливості та особливості програми

Лабораторна робота №3

Тема: Захист інформації засобами операційних систем. Налаштування власного профілю. Поняття батьківського контролю.

Мета: ознайомитися з способами захисту інформації засобами операційної системи; навчитися налаштовувати власний профіль та користуватися функцією батьківського контролю.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Використання надійного паролю є одним з найбільш важливих факторів захисту комп'ютера від несанкціонованого доступу.

Якщо ввійти в систему з правами адміністратора, то можливо встановити пароль для будь-якого облікового запису.

1. ***Пуск, Панель управления, Учетные записи пользователей***
2. Оберіть команду ***Создать пароль.***
3. Введіть пароль в поле ***Новый пароль***, а потім повторіть введення в поле ***Подтверждение пароля.***
4. Щоб скористатися підказкою паролю введіть її в поле ***Подсказка о пароле.***
5. Оберіть команду ***Создать пароль.***

Для того, щоб змінити існуючий пароль облікового запису, оберіть команду ***Изменение своего пароля.***

Захист файлів за допомогою шифрування дисків BitLocker

Шифрування дисків BitLocker використовується для захисту всіх файлів, що зберігаються на диску з встановленою ОС Windows (диск операційної системи) і на незнімних дисках (наприклад, внутрішніх жорстких дисках). Шифрування BitLocker To Go використовується для захисту всіх файлів, що зберігаються на знімних дисках (наприклад, зовнішніх жорстких дисках або USB флеш-пам'яті). На відміну від шифрованого файлової системи (EFS), що дозволяє зашифровувати окремі файли, BitLocker шифрує диск цілком. Користувач може входити в систему і працювати з файлами як звичайно, а BitLocker буде заважати зловмисникам, які намагаються отримати доступ до системних файлів для пошуку паролів, а також до диску шляхом вилучення його з даного комп'ютера та інсталяції в інший.

BitLocker автоматично шифрує всі файли, що додаються на зашифрований диск. Файли будуть зашифровані тільки при зберіганні на зашифрованому диску. При їх копіюванні на інший диск або комп'ютер вони будуть розшифровані. При наданні загального доступу до файлів по мережі вони будуть зашифровані на зашифрованому диску, але авторизовані користувачі зможуть отримувати до них доступ звичайним чином.

При шифруванні диска з ОС BitLocker перевіряє комп'ютер при завантаженні на наявність можливих загроз безпеки (наприклад, змін в BIOS або файлах завантаження). При виявленні загрози безпеці BitLocker заблокує диск з ОС. Щоб розблокувати його, потрібно спеціальний ключ відновлення BitLocker. Переконайтеся, що цей ключ створений при першому запуску BitLocker. В іншому випадку доступ до файлів може бути втрачений. Якщо комп'ютер оснащений модуля TPM (TPM), BitLocker

використовує його для запечатування ключів розблокування зашифрованого диска з ОС. При завантаженні комп'ютера BitLocker запитує в модуля TPM ключі для доступу до диска і розблокує його.

Зашифровані диски (незнімні або знімні) можна розблокувати за допомогою пароля або смарт-карти або налаштувати автоматичну розблокування дисків при вході в систему.

BitLocker завжди можна відключити або тимчасово (призупинивши його), або на постійній основі (розшифрувавши диск).

Примітка.

• Можливість шифрувати дані на дисках з використанням шифрування BitLocker доступна не в усіх випусках операційної системи Windows.

Включення BitLocker

1. ***Пуск, Панель управления, Система и безопасность, Шифрование диска BitLocker***
2. Клацніть ***Включить BitLocker***. Відкриється майстер настройки BitLocker. Дотримуйтесь інструкцій майстра. При появі запиту пароля адміністратора або підтвердження, введіть пароль або надайте підтвердження.

Відключення або тимчасове призупинення BitLocker

1. ***Пуск, Панель управления, Система и безопасность, Шифрование диска BitLocker***
2. Виконайте одну з таких дій.

Щоб тимчасово призупинити BitLocker, клацніть ***Приостановить защиту*** і натисніть кнопку ***Да.***

Щоб відключити BitLocker і розшифрувати диск, послідовно клацніть ***Выключить BitLocker*** і ***Расшифровать диск.***

Поняття захисту системи

Захист системи - це компонент, який регулярно створює і зберігає інформацію про системних файлах і параметрах комп'ютера. Захист системи також зберігає попередні версії змінених файлів. Ці файли зберігаються в точках відновлення, які створюються безпосередньо перед значущими системними подіями, такими як установка програми або драйвера пристрою. Вони також створюються автоматично раз на тиждень, якщо за попередній тиждень не було створено інших точок відновлення, проте можна створювати точки відновлення вручну в будь-який час.

Захист системи автоматично включена для диска, на якому встановлена ОС Windows. Захист системи можна включити тільки для дисків, відформатованих з використанням файлової системи NTFS.

Існує два способи скористатися перевагами захисту системи.

• Якщо комп'ютер працює повільно або з помилками, то за допомогою відновлення системи можна відновити стан системних файлів і параметрів комп'ютера на попередній момент часу з використанням точки відновлення.

• Якщо файл або папка були випадково змінені або видалені, можна відновити їх попередню версію, яка зберігається як частина контрольної точки відновлення.

Відновлення системи використовує точки відновлення для повернення системних файлів і параметрів до стану на певний момент часу, не впливаючи на особисті файли. Знімки автоматично створюються щотижня, а також перед значними системними подіями, такими як установка програм або драйверів пристроїв. Точку відновлення також можна створити вручну.

Відновлення системи дозволяє відновити стан системних файлів комп'ютера на попередній моменту часу. Це дозволяє скасувати зміни, внесені в систему комп'ютера, не зачіпаючи особисті файли, такі як електронна пошта, документи або фотографії.

Іноді в результаті установки програми або драйвера виникають несподівані зміни в комп'ютері або спостерігається непередбачувана поведінка ОС Windows. Зазвичай видалення програми або драйвера дозволяє усунути проблему. Але якщо видалення не призвело до усунення проблеми, то можна спробувати відновити стан системи комп'ютера на момент часу в минулому, коли все працювало належним чином.

Зберігаються на жорстких дисках резервні копії образу системи можна використовувати для відновлення системи так само, як і точки відновлення, створені захистом системи.

Відновлення системи не призначене для архівації особистих файлів, тому з його допомогою неможливо відновити видалені або пошкоджені особисті файли. Необхідно регулярно здійснювати архівування своїх особистих файлів і важливих даних за допомогою програми архівування.

Засіб відновлення системи регулярно відстежує зміни в системних файлах комп'ютера і за допомогою функції, званої захист системи, створює точки відновлення. Захист системи включена за замовчуванням на тому диску, де встановлена ОС Windows. Захист системи можна включити і для інших дисків.

Захист системи не можна включити для диска, відформатованого з використанням файлових систем FAT або FAT32.

1***. Пуск, Панель управления, Система и безопасность, Система.***

2. В області ліворуч виберіть ***Защита системы***. При появі запиту пароля адміністратора або підтвердження, введіть пароль або надайте підтвердження.

3. В області ***Параметры защиты*** клацніть диск і виберіть ***Настроить.***

4. Виберіть один із зазначених нижче параметрів.

Щоб забезпечити відновлення параметрів системи і попередніх версій файлів, клацніть ***Восстановить параметры системы и предыдущие версии файлов.***

Щоб забезпечити відновлення тільки попередніх версій файлів, клацніть ***Восстановить только предыдущие версии файлов.***

5. Натисніть кнопку ***ОК***, а потім ***ОК*** ще раз.

При відключенні захисту системи для диска всі точки відновлення цього диска видаляються. Системні дані на диску можна буде відновлювати тільки після повторного включення захисту системи і створення нової точки відновлення. Відключення захисту системи також видаляє всі попередні версії файлів, збережених для цього диска.

Попередні версії - це копії файлів і папок, які ОС Windows, автоматично зберігає з точками відновлення.

1. ***Пуск, Панель управления, Система и безопасность, Система.***
2. В області ліворуч виберіть ***Защита системы***. При появі запиту пароля адміністратора або підтвердження, введіть пароль або надайте підтвердження.
3. В області ***Параметры защиты*** клацніть диск і виберіть ***Настроить.***
4. Клацніть ***Отключить защиту системы***, натисніть кнопку ***ОК***, а потім натисніть кнопку ***ОК*** ще раз.

Захист доступу до мережі (NAP) - це платформа для мережевого адміністратора, що забезпечує безпеку мережі. При підключенні до корпоративної мережі, що використовує NAP, комп'ютер перевіряється на наявність оновлених версій необхідного програмного забезпечення та параметрів. Якщо якийсь з компонентів відсутній або застарілий, він може автоматично оновитися. При цьому доступ до мережі може бути обмежений, але зазвичай це відбувається швидко, після чого повний доступ до мережі поновлюється.

Запобігання виконання даних

DEP - це засіб безпеки, яке допомагає захистити комп'ютер від вірусів та інших загроз безпеці. Компонент DEP призначений для спостереження за програмами, зокрема за тим, як вони використовують системну пам'ять. Якщо програма намагається виконати код, званий виконуваним, з пам'яті невірним способом, засіб DEP закриває програму. Компонент DEP автоматично перевіряє основні програми ОС Windows. При необхідності можна підвищити ступінь захисту, включивши перевірку всіх програм.

Якщо при використанні рекомендованих значень параметрів безпеки антивірусна програма не виявила загрози, комп'ютер, можливо, не піддавався атаці. У цьому випадку програма при включеному засобі DEP може працювати неправильно. Зверніться до виробника програмного забезпечення за

версією програми, сумісної з DEP, або виконайте оновлення програми, перш ніж змінювати параметри DEP.

Програми svchost.exe та explorer.exe є частинами операційної системи Windows. Якщо засіб DEP закриває їх або інші служби Windows, причиною можуть бути невеликі програми, такі як розширення, створені іншими видавцями програмного забезпечення та працюють усередині Windows. Якщо програма встановлена недавно і компонент DEP закриває програми під управлінням ОС Windows, зверніться до виробника програмного забезпечення за оновленою версією, сумісної з DEP, або спробуйте видалити програму.

DEP - це програмний засіб Windows. Деякі процесори також надають апаратний засіб DEP під різними назвами. Ці процесори використовують апаратну технологію заборони програмам виконувати код із захищених областей пам'яті. Якщо процесор не підтримує апаратне засіб DEP, Windows буде використовувати для захисту комп'ютера програмний засіб DEP.

Пароль як засіб захисту окремих файлів

В ОС Windows не можна захистити файл або папку з допомогою пароля. Однак у деяких програмах для ОС Windows, підтримується захист окремих файлів за допомогою пароля.

Існують і інші способи захисту файлів і папок у Windows. Можна зашифрувати файли за допомогою шифрувальної файлової системи (EFS), вручну визначити користувачів, що мають права на доступ до файлів і папок за допомогою дозволів, а можна приховати їх. Можна вибрати метод захисту в залежності від необхідного для файлів і папок рівня безпеки. Шифрування є найбільш безпечним методом захисту, а приховування - найменш безпечним.

Шифрована файлова система (EFS)

Шифрована файлова система (EFS) - це компонент Windows, що дозволяє зберігати відомості на жорсткому диску в зашифрованому форматі. ***Шифрування*** - це найсильніший захист, який надає Windows, для захисту даних.

Деякі ключові властивості EFS:

• Шифрування - проста дія, для його включення досить встановити прапорець у властивостях файлу або папки.

• Можна вказати, кому саме дозволяється читати ці файли.

• Файли шифруються, коли вони закриваються, але при відкритті вони автоматично готові до використання.

• Якщо шифрувати файл більше немає необхідності, зніміть прапорець у властивостях файлу.

Опис захисту, забезпечуваного Захисником Windows, в реальному часі

Функція захисту в реальному часі повідомляє користувача, якщо шпигунська або інша небажана програма намагається встановити або запустити на комп'ютері. В залежності від рівня оповіщення, користувач може застосувати до цієї програми одну з наступних дій.

• *Помістити в карантин.* Переміщує відповідну програму в інше місце на комп'ютері і перешкоджає її запуску, доки вона не буде відновлена або видалена.

• *Видалити.* Остаточно видаляє програму з комп'ютера.

• *Дозволити.* Додає програму в список дозволених програм Захисника Windows, і дозволяє її запуск. Захисник Windows, не буде оповіщати про потенційну загрозу конфіденційності або безпеці комп'ютера, яку може представляти ця програма. Додавайте програму до списку дозволених тільки в тому випадку, якщо довіряєте цій програмі і її видавцеві.

Ви можете вибрати програми і параметри, за якими повинен спостерігати Захисник Windows, проте рекомендується використовувати всі варіанти захисту в реальному часі, які називаються агентами. Призначення кожного з агентів наведено нижче.

Завантажені файли та вкладення. Відстежує файли і програми, призначені для роботи з веб-браузерами. Дані файли можуть завантажуватися, встановлюватися або запускатися самим браузером. До складу цих файлів можуть входити шпигунські та інші небажані програми і встановлюватися без відома користувача.

Програми, що працюють на комп'ютері. Контролює запуск програм і всі виконувані ними операції протягом їх роботи. Шпигунські та інші небажані програми можуть використовувати уразливості встановлених програм для запуску шкідливих та інших небажаних програм без відома користувача. Наприклад, шпигунські програми можуть запускатися у фоновому режимі при відкритті часто використовуваної програми. Захисник Windows, спостерігає за програмами і оповіщає користувача у разі виявлення будь-яких підозрілих дій.

Захист певних файлів і папок від загального доступу в домашній групі

Користувач, який створює домашню групу або приєднується до неї, вибирає бібліотеки, які будуть доступні іншим членам домашньої групи. Загальний доступ до бібліотек спочатку надається з правом доступу ***Чтение***, яке дозволяє переглядати або прослуховувати вміст бібліотеки, але не дозволяє вносити зміни у файли. Рівень доступу пізніше можна налаштувати, а також виключити певні файли і папки із загального доступу.

Виключення бібліотеки із загального доступу (при створенні домашньої групи або приєднання до неї)

1. ***Пуск, Панель управления, Сеть и Интернет, Домашняя группа***
2. Виконайте одну з таких дій.
   - Щоб створити нову домашню групу, клацніть ***Создать домашнюю группу.***
   - Щоб приєднатися до існуючої домашньої групи, клацніть ***Присоединиться.***
3. На наступній сторінці майстра зніміть прапорці для всіх бібліотек, які потрібно виключити з загального доступу.
4. Натисніть кнопку ***Далее***, а потім кнопку ***Готово***.

Виключення бібліотеки із загального доступу (після створення домашньої групи або приєднання до неї)

1. ***Пуск, Панель управления, Сеть и Интернет, Домашняя групп.***
2. Зніміть прапорці для всіх бібліотек, які потрібно виключити із загального доступу, і натисніть кнопку ***Сохранить изменения.***

Виключення певних файлів і папок із загального доступу (після створення домашньої групи або приєднання до неї)

1. Натисніть кнопку ***Пуск***, виберіть ім'я користувача.
2. Перейдіть до файлу або папки, які потрібно виключити із загального доступу, і виберіть файл або папку.
3. Виконайте одну з таких дій.

Щоб виключити файл або папку із загального доступу для всіх, на панелі інструментів натисніть кнопку ***Общий доступ*** для та виберіть пункт ***Никто из пользователей***.

Щоб надати спільний доступ до файлу або папці деяким (але не всім) користувачам, на панелі інструментів натисніть кнопку ***Общий доступ для***, виберіть пункт ***Конкретные пользователи,*** виберіть тих користувачів, яким потрібно надати доступ, і натисніть кнопку ***Добавить***. По завершенні натисніть кнопку ***Доступ***.

Щоб змінити рівень доступу до файлу або папки, на панелі інструментів натисніть кнопку ***Общий доступ для*** та виберіть пункт ***Домашняя группа (чтение)*** або ***Домашняя группа (чтение и запись).***

Пристрій читання відбитків пальців в Windows

Замість пароля для входу в цю версію Windows, можна використовувати пристрій читання відбитків пальців.

Пристрій читання відбитків пальців - це пристрій, призначений для ідентифікації користувачів по відбитках пальців. Це пристрій сканує зображення відбитка пальця користувача та зберігає його копію. Потім для ідентифікації користувача, наприклад, при вході на веб-сайт або в систему для Windows, виконується сканування відбитку пальця і його порівняння із збереженою версією.

Можна використовувати вбудований пристрій читання відбитків пальців, встановлений в деяких моделях ноутбуків, або придбати окремий пристрій і підключити його до комп'ютера.

Якщо у вас кілька пристроїв читання відбитків пальців або потрібно замінити один на інший, то може знадобитися зчитати і зберегти (це часто називається записати) відбитки пальців перед початком використання пристрою читання з Windows. Це необхідно, тому деякі пристрої читання відбитків пальців зберігають відбитки пальців у різних форматах і вони не можуть бути прочитані іншими сканерами.

Безпека і безпечна робота на комп'ютері

Існують різні способи захисту комп'ютера від можливих загроз безпеки.

• Брандмауер. Брандмауер захищає комп'ютер, запобігаючи доступ до нього хакерів і шкідливих програм.

• Центр оновлення Windows. ОС Windows може регулярно перевіряти наявність оновлень для комп'ютера і автоматично їх встановлювати.

• Захист від вірусів. Антивірусне програмне забезпечення допомагає захистити комп'ютер від вірусів, черв'яків і інших погроз безпеці.

• Захист від шпигунських та інших шкідливих програм. Антишпигунське програмне забезпечення допомагає захистити комп'ютер від шпигунських програм та іншого небажаного програмного забезпечення.

Брандмауер. Брандмауер - це програма або пристрій, який перевіряє дані, що надходять з локальної мережі або Інтернету, а потім або відхиляє її, або пропускає в комп'ютер, в залежності від параметрів брандмауера. Таким чином, брандмауер допомагає запобігти доступ хакерів і шкідливих програм до комп'ютера.

Брандмауер Windows, вбудований в Windows, і включається автоматично.

Якщо на комп'ютері використовуються такі програми, як програма передачі миттєвих повідомлень або мережеві ігри, якій потрібно отримувати дані з Інтернету або локальної мережі, брандмауер запитує про блокування або дозволі підключення. Якщо користувач дозволяє підключення, брандмауер Windows, створює виняток, щоб не турбувати користувача запитами, коли в майбутньому цій програмі знадобляться дані.

Захист від вірусів. Віруси, хробаки та троянські коні - це програми, створені хакерами, які використовують Інтернет для зараження комп'ютерів. Віруси та хробаки можуть розмножуватися від комп'ютера до комп'ютера, а троянський кінь потрапляє до комп'ютера, сховавшись у легальних програмах. Деструктивні віруси, хробаки та троянські програми можуть стерти інформацію з жорсткого диска або повністю вивести з ладу. Інші не завдають прямої шкоди, але знижують продуктивність і стабільність комп'ютера.

Антивірусні програми перевіряють електронну пошту та інші файли комп'ютера на наявність вірусів, хробаків і троянських програм. При виявленні антивірусна програма або у карантин (ізолює) або повністю видаляє до нанесення шкоди комп'ютеру та файлам.

ОС Windows не має вбудованої антивірусної програми, але виробник комп'ютера може встановити інші. Якщо антивірусна програма відсутня, відвідайте веб-сайт постачальників програм по забезпеченню безпеки Windows для пошуку антивірусної програми.

Так як нові віруси з'являються щодня, дуже важливо вибрати антивірусну програму з можливістю автоматичного оновлення. При оновленні антивірусне програмне забезпечення додає нові віруси в список перевірки, захищаючи комп'ютер від нових атак. Застарілий комп'ютер стане вразливим до нових загроз. Оновлення зазвичай вимагають щорічної підписки. Підтримуйте підписку для регулярного отримання оновлень.

• Якщо антивірусне програмне забезпечення не використовується, комп'ютер схильний пошкодження шкідливими програмами. Є також ризик заразити вірусами інші комп'ютери.

Захист від шпигунських програм. Шпигунські програми можуть відображати рекламу, збирати особисті відомості та змінювати параметри комп'ютера, зазвичай без отримання на те дозволу.

Наприклад, шпигунські програми можуть встановлювати небажані панелі інструментів, посилання або уподобання в браузер, змінювати домашню сторінку або часто відображати спливаючу рекламу. Деякі шпигунські програми не проявляють видимих симптомів, але таємно збирають важливі відомості, такі як відвідувані сайти або набраний текст. Більшість шпигунських програм інсталюються разом із безплатним програмним забезпеченням, але в деяких випадках спричиняє зараження звичайне відвідування веб-сайту.

Для захисту комп'ютера від шпигунських програм, користуйтеся анти шпигунське програмне забезпечення. Дана версія ОС Windows має вбудовану анти шпигунську програму «Захисник Windows», включену за умовчанням. Захисник Windows, попереджає про шпигунська програма намагається інсталювати себе на комп'ютер. Захисник також може шукати на комп'ютері шпигунські програми та видаляти їх.

Оскільки з'являються нові шпигунські програми кожен день, Windows Defender, повинен регулярно оновлювати, щоб виявляти і захищати комп'ютер від найновіших загроз. Захисник Windows, оновлюється по мірі необхідності разом з оновленням Windows. Для досягнення найвищого рівня захисту увімкніть автоматичне оновлення Windows.

Автоматичне оновлення для Windows. Корпорація Майкрософт регулярно пропонує важливі оновлення Windows, для захисту комп'ютера від нових вірусів та інших загроз безпеці. Для якнайшвидшого отримання оновлень, увімкніть автоматичне оновлення. У цьому випадку не потрібно хвилюватися, що критичні оновлення для Windows можуть бути пропущені.

Оновлення завантажуються у фоновому режимі при підключенні до Інтернету. Оновлення встановлюються в 03:00, якщо не задано інший час. Якщо ви вимикаєте комп'ютер, можна інсталювати перед вимкненням. В іншому випадку ОС Windows інсталює наступного разу при запуску комп'ютера.

Включення автоматичного оновлення

1. ***Пуск, Панель управления, Система и безопасность, «Центр обновления Windows».***

2. Клацніть ***Изменить параметры.***

3. Переконайтеся, що вибрано інсталяція оновлень (рекомендується). ОС Windows буде встановлювати на комп'ютері важливі оновлення по мірі їх появи. Важливі оновлення забезпечують суттєві переваги, наприклад підвищення безпеки і надійності.

4. У групі ***Рекомендуемые обновления*** встановіть прапорець ***Получать рекомендуемые обновления таким же образом, как и важные обновления*** та натисніть кнопку ***ОК***. Рекомендовані оновлення можуть усувати менш істотні проблеми і робити використання комп'ютера більш зручним. При появі запиту пароля адміністратора або підтвердження, введіть пароль або надайте підтвердження.

Стандартна обліковий запис

При вході в систему Windows, призначає користувачеві певний рівень прав, що залежить від типу облікового запису. Є три типи облікових записів користувачів: «стандартна», «адміністратор» та «гість».

Хоча обліковий запис адміністратора надає повний контроль над комп'ютером, використання стандартної облікового запису користувача може сприяти забезпеченню більш високого рівня безпеки комп'ютера. Таким чином, інші люди (або хакери), отримавши доступ до комп'ютера, на якому користувач увійшов в систему зі стандартним обліковим записом, не зможуть зіпсувати параметри безпеки комп'ютера або облікові записи інших користувачів. Увійшовши в систему, користувач може перевірити тип свого облікового запису, виконавши наступні дії.

1. ***Пуск, Панель управления, Учетные записи пользователей и семейная безопасность.***

Тип облікового запису відображається під іменем користувача. Якщо обліковий запис відноситься до типу Адміністратор, то поточний користувач увійшов як адміністратор.

2. Усі облікові записи на комп'ютері можна переглянути, клацнувши ***Управление другой учетной записью***. При появі запиту пароля адміністратора або підтвердження, введіть пароль або надайте підтвердження.

При цьому виводяться всі облікові записи користувачів і їх типи.

Зазвичай за домашніми комп'ютерами працюють кілька членів сім'ї. У тому випадку, якщо користувачем домашнього комп'ютера є тільки його власник, йому не варто хвилюватися про захист файлів і встановлених параметрів операційної системи. Буде достатньо лише встановити безпечний пароль і забути про багато проблем. Але якщо один комп'ютер використовують кілька людей, то варто подумати про прийняття додаткових заходів захисту персональної інформації кожного окремо взятого користувача. Ви можете створити для всіх користувачів окремі облікові записи з обмеженими правами, навіть якщо один або декілька користувачів буде дуже рідко використовувати свій обліковий запис. Також слід видаляти облікові записи тих користувачів, які вже не працюють на цьому комп'ютері. Але як же бути, якщо вашим комп'ютером користується ще й дитина? Для цього був створений компонент, який називається «Батьківський контроль».

За допомогою цього компонента ви можете використовувати рейтинг для того, щоб контролювати, в які ігри може грати ваша дитина, додати тимчасові обмеження, за допомогою яких діти зможуть користуватися комп'ютером тільки в певні години, а також блокувати доступ до деяких програм, які діти не повинні відкривати. Компонент «Батьківський контроль» з'явився ще в операційній системі Windows Vista. У Windows 7 з функціоналу батьківського контролю були виключені компоненти веб-фільтрації та звіту про активність. Тепер їх можна завантажити з веб-сайту Windows Live, встановити і додати в ту службу батьківського контролю, яка вже використовується. Функціонал батьківського контролю доступний у всіх редакціях Windows 7. Далі в цьому керівництві будуть детально описані всі дії, які можна виконувати з «Батьківським контролем», крім функціоналу додаткових компонентів, який завантажується від інших постачальників послуг.

Використання батьківського контролю

Перед тим як встановити батьківський контроль, створіть обліковий запис для вашої дитини. Про способи створення облікових записів я детально розповідав в статті Робота з обліковими записами користувачів в Windows 7 – докладне керівництво (Частина 1). Після того як обліковий запис буде створена, можна приступати до установки обмежень використання комп'ютера для дитини.

Відкриття компонента «Батьківський контроль»

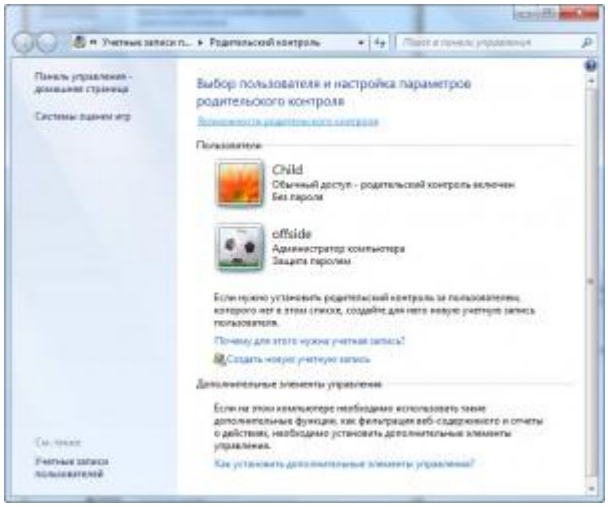
Для початку відкрийте вікно «Батьківський контроль». Це можна зробити наступним чином:

Натисніть на кнопку «Пуск» для відкриття меню, в поле пошуку або введіть Родитель та відкрийте в знайдених результатах;

Скористайтеся комбінацією клавіш + R для відкриття діалогу "Виконати". У діалоговому вікні «Виконати», в полі «Відкрити» введіть %systemroot%\system32\control.exe /name Microsoft.ParentalControls і натисніть на кнопку «ОК»;

Натисніть на кнопку «Пуск» для відкриття меню, відкрийте «Панель управління», зі списку компонентів панелі управління оберіть "Батьківський контроль»;

Вікно «Батьківський контроль» зображено на наступному скріншоті:

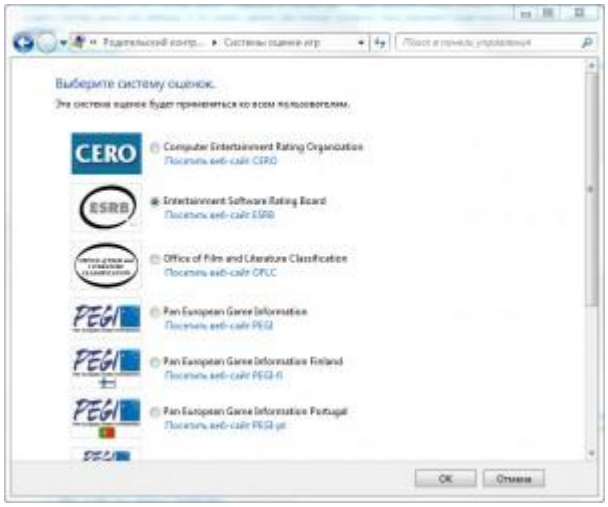


У цьому вікні відображаються всі облікові записи, зроблені на комп'ютері, а також додаткові елементи управління, якщо вони були встановлені. Якщо ви ще не встигли створити обліковий запис

для дитини, то це можна зробити за допомогою основного вікна компонента батьківського контролю. Натисніть на посилання «Створити новий обліковий запис».

Система оцінки ігор

У лівій області вікна «Батьківського контролю» перейдіть за посиланням «Системи оцінки ігор» для того, щоб вибрати ту систему, яка буде застосовуватися до всіх користувачів. Діалог вибору системи оцінювання відображено на наступному скріншоті:



Системи оцінки і категорії для ігор визначаються спеціальними комісіями, які створюють рекомендації по вмісту ігор для різних країн. В основному, у всіх системах присутні вікові категорії для ігор. Перед тим як ігри надходять на прилавки магазинів, ці комісії уважно вивчають вміст ігор і дають свої рецензії.

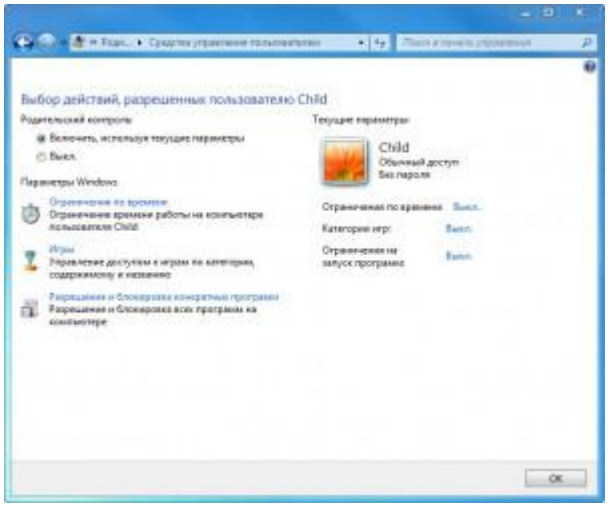
В операційній системі Windows 7 ви можете встановити одну з десяти можливих систем оцінок, а саме:

1. Computer Entertainment Rating Organization;
2. Entertainment Software Rating Organization;
3. Office of Film and Literature Classification;
4. Pan European Game Information;
5. Pan European Game Information Finland;
6. Pan European Game Information Portugal;
7. Pan European Game Information і British Board of Film Classification;
8. Unterhaltungssoftware Selbstkontrolle;
9. Комісія з класифікації програмного забезпечення для комп’ютерів;
10. Комісія з оцінки ігор.

Якщо ви не знаєте, яку систему вам потрібно вибрати, то можете перейти по посиланню, розташованої під назвою системи на веб-сайт цієї комісії, і докладно познайомитися з їх класифікацією та вимогами до ігор. Найбільш поширеними системами оцінки є ESRB і PEGI. Я рекомендую вибрати систему ESRB, тому що в цій системі ви можете вибрати безліч коротких описів, які використовуються для позначення вмісту, який може виявитися небажаним для дітей. На наступному скріншоті ви можете побачити приклади значків різних систем оцінок для однієї і тієї ж гри:

Але, незважаючи на описи до гри, які встановила комісія, найкраще подивіться самі, чи варто забороняти дитині грати в цю гру, оскільки думка фахівців може виявитися упередженим.

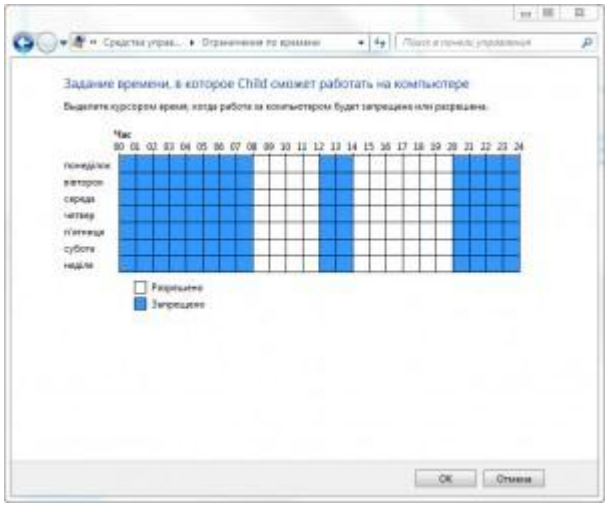
Вибравши систему оцінки ігор, натисніть на кнопку «ОК» для того щоб назад перейти в головне вікно «Батьківського контролю». У головному вікні натисніть на значку облікового запису дитини, для якого будуть застосовуватися обмеження використання комп’ютера. Після вибору облікового запису ви перейдете у вікно «Засоби керування користувачами». Це вікно допоможе вам визначити час роботи комп’ютера, обмежити запуск ігор, а також блокувати запуск програм для вибраного користувача. Вікно засобів управління користувачами відображено нижче:



Для включення батьківського контролю над обліковим записом дитини в області «Батьківський контроль» встановіть перемикач на опції «Включити, використовуючи поточні параметри». Після того як цей пункт буде активовано, ви зможете настроювати параметри батьківського контролю.

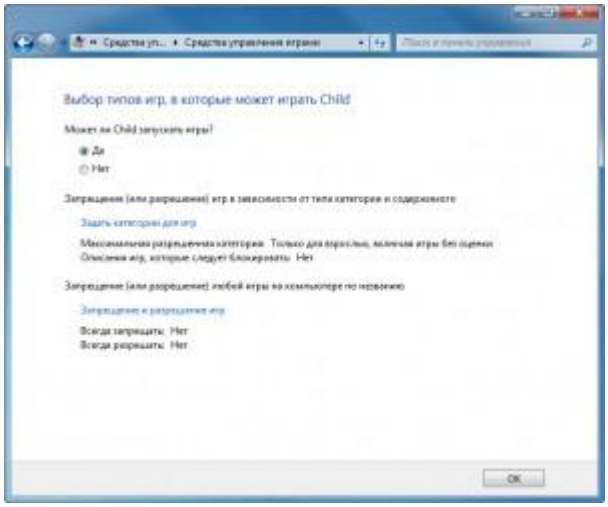
Обмеження за часом

Вікно «Обмеження по часу» призначено для визначення часу, який дозволяється дітям для використання комп'ютера. Тут кожен рядок відповідає за день тижня, а кожен стовпець за годину. Ви можете встановити годинник, які дозволяються для доступу на кожен день тижня, у зв'язку з чим, дитина не зможе ввійти в систему протягом певного періоду часу. Натиснувши лівою кнопкою миші на будь-який з осередків, цю годину буде заблокований. Знизу відображена легенда, де ви можете дізнатися, що означають ті позначки, які ви встановлюєте. Вікно обмеження за часом ви можете побачити нижче:



Обмеження на ігри

За допомогою вікна «Засоби керування іграми» ви можете дозволити або заборонити доступ відразу до всіх ігор, встановленим на комп'ютері, обмежити доступ до ігор на основі вікової оцінки або категорії ігор, а також заблокувати або дозволити доступ до певних ігор. Вікно «Засоби керування іграми» відображує на наступному скріншоті:



Блокування доступу до всіх ігор

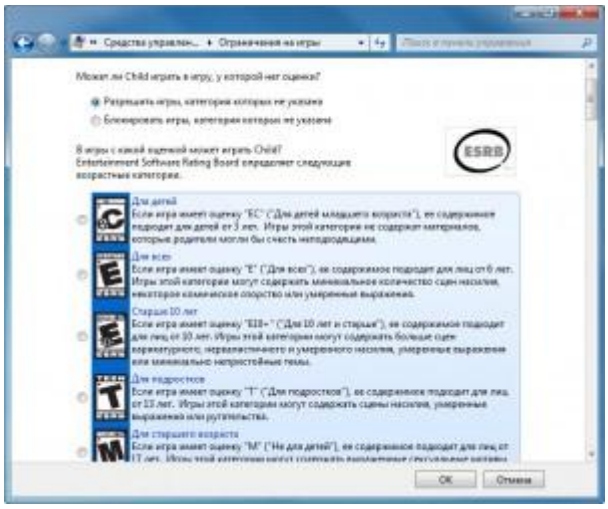
Ви можете повністю відключити для користувача можливість доступу до ігор. Для цього в розділі «Чи може% USERNAME% запускати ігри» встановіть перемикач на опції «Ні». У тому випадку, якщо перемикач встановлений на опцію «Так», користувач зможе запускати ігри, а вам для установки обмежень, потрібно буде налаштувати наступні два розділи, щоб визначити в які саме ігри зможе грати ваша дитина.

Блокування доступу до ігор на підставі категорії та вмісту ігор

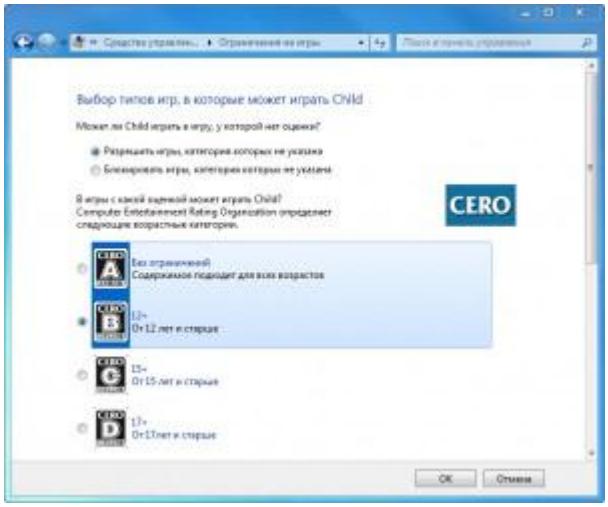
Замість того щоб повністю заблокувати доступ до встановлених на комп'ютер ігор, ви можете дозволити або заборонити дитині відкривати ігри певного типу. Для цього у вікні «Засоби керування іграми» перейдіть по посиланню «Поставити категорії ігор».

У вікні «Обмеження на ігри» ви можете встановити перемикач на опцію «Блокувати ігри, категорія яких не зазначена» для того, щоб дитина не змогла запускати ті ігри, для яких комісія з оцінки ігор категорію не вказала. Трохи нижче, в розділі «В ігри з якою оцінкою може грати% USERNAME%?» Встановіть перемикач напроти тієї категорії, яку хочете зробити максимально допустимої для користувача, якому ви обмежуєте доступ. Наприклад, як показано на наступному скріншоті, якщо встановити перемикач біля категорії «Старше 10 років», даний користувач зможе грати в ігри, тільки з категоріями «Для дітей», «Для всіх», а також «Старше 10 років». У свою чергу, ігри, для яких встановлена категорія «Для підлітків», «Для старшого віку» і «Тільки для дорослих» дитина грати не зможе.

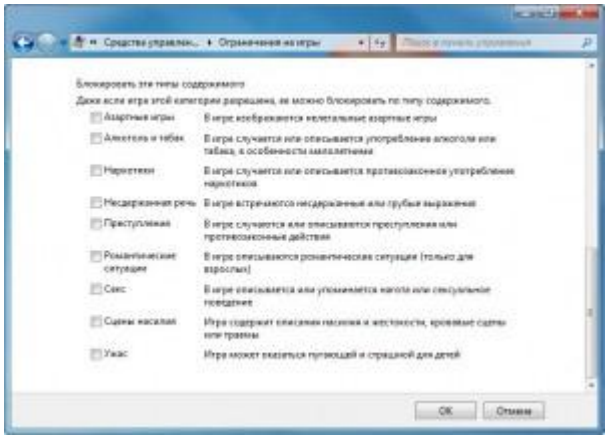
На першому прикладі можна побачити обмеження на ігри для системи оцінки ESRB:



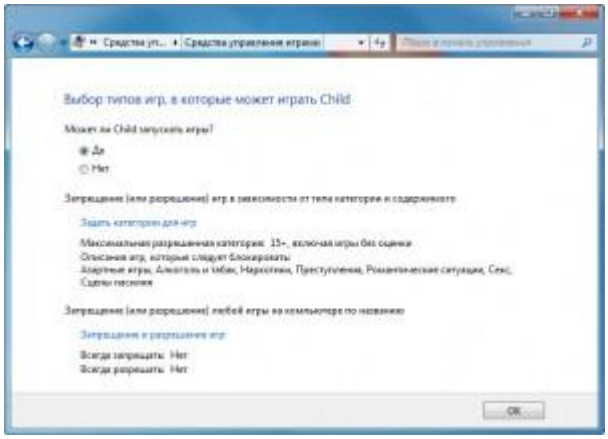
Якщо у вікні «Системи оцінки ігор» ви оберете систему CERO, то в діалозі «Обмеження на ігри» оцінки будуть виглядати наступним чином:



Крім блокування системи ігор, ви також можете заборонити дитині грати в ті ігри, вміст яких не повинно потрапляти йому на очі. Для цього у вікні «Обмеження на ігри» знайдіть розділ «Блокувати ці типи вмісту» і в докладному переліку типів вмісту встановіть прапорці навпроти того типу, який потрібно виключити. Якщо ви не хочете, щоб ваша дитина грав в ігри, в яких присутня будь-якого виду насильства, азартні ігри та нецензурна лексика, установіть відповідні прапорці. У цьому випадку, дитина не зможе запустити гру навіть в тому випадку, якщо вона входить в той склад вікової категорії, яка доступна.



Після натискання на кнопку «ОК», ви повернетеся до вікна «Коштів управління іграми», де ви можете побачити ті настройки, які були вказані у вікні «Обмеження на ігри». У деяких випадках для ігор не вказується вікова категорія і вміст. У такому випадку, ви можете самостійно додати категорію і перелік типів вмісту, про що буде розказано в одній з наступних статей.



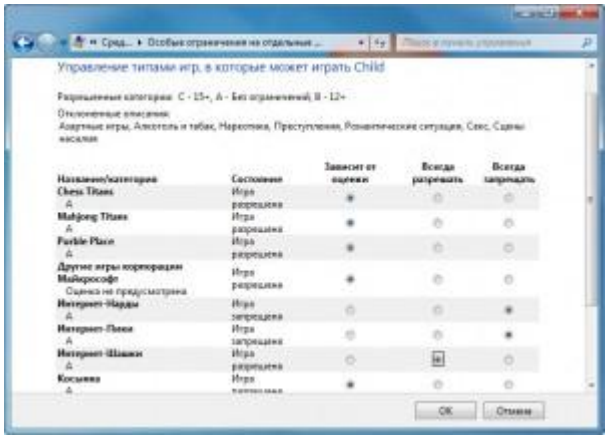
Блокування доступу до певних ігор

Крім способів блокування доступу до ігор зазначених вище, ви можете точно налаштувати управління іграми засобами визначення обмежень для тих ігор, які вже встановлені на вашому комп’ютері. Для цього у вікні «Засоби керування іграми» перейдіть по посиланню «Заборона і дозвіл

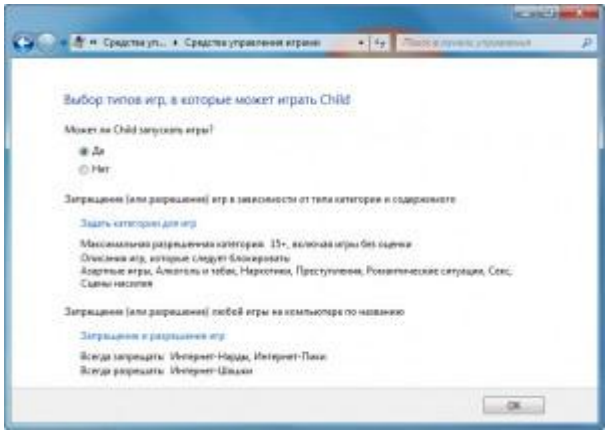
ігор». У вікні «Особливі обмеження на окремі ігри» відобразиться таблиця, в якій міститься така інформація:

- Найменування всіх ігор, встановлених на вашому комп'ютері, а також їх категорії;
- Стан гри, де можна побачити дозволена або заборонена дана гра;
- Три стовпця з перемикачами для вибору дозволів.

Для того щоб дозволити користувачеві запускати певну гру, яка вже встановлена на вашому комп'ютері, установіть перемикач на опції «Завжди дозволяти», а для того щоб заборонити – на опції «Завжди забороняти». Вікно особливих обмежень на окремі ігри відображує на наступному скріншоті:

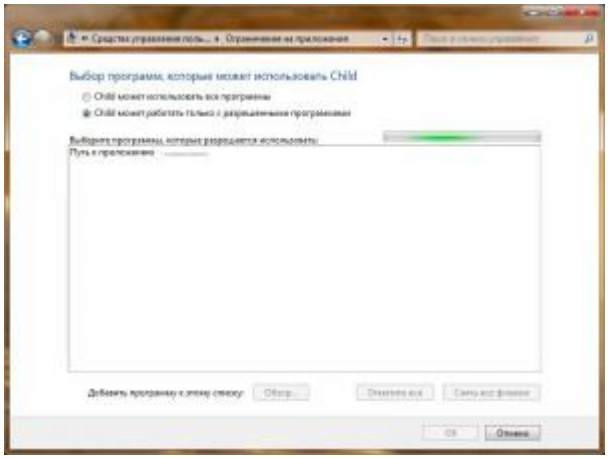


Після того як ви натиснете на кнопку «ОК», у вікні «Засоби керування іграми» ви зможете побачити зведену інформацію про всі обмеження, які були встановлені для даної користувача облікового запису.

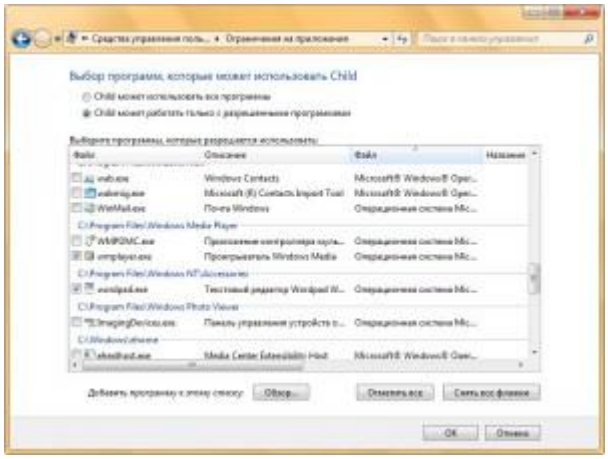


Обмеження на додатки

Крім блокування доступу до ігор та Обмеження користувача за часом, функціонал батьківського контролю операційної системи Windows 7 дозволяє навіть обмежувати доступ користувача до конкретних програм. Тобто ви можете заборонити дитині звертатися до програм, які не повинні його торкатися і бути впевненим в тому, що вам дитина буде відкривати тільки ті програми, які дозволені в списку. Для того щоб обмежити дитині доступ до програм у вікні «Засоби керування користувачем» перейдіть за посиланням «Дозвіл і блокування конкретних програм». Встановивши перемикач на опцію «% USERNAME% може працювати тільки з дозволеними програмами», операційна система сканує комп'ютер на наявність встановлених програм, як показано на наступному скріншоті:

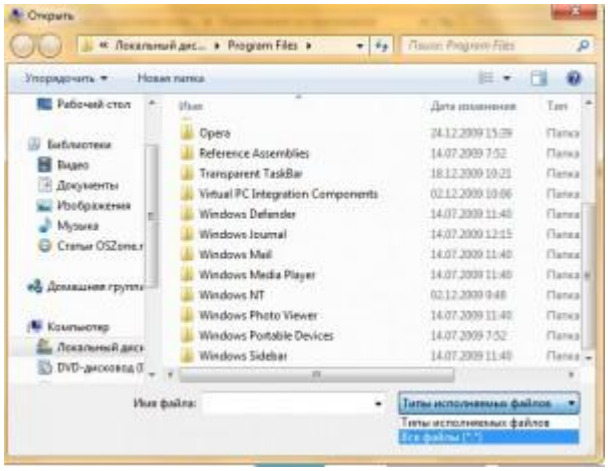


Після того як сканування буде закінчено, у вікні «Обмеження на додатки» ви побачите всі програми, які встановлені на вашому комп'ютері. Для того щоб користувачеві дозволити працювати з певною програмою, встановіть прапорець біля її найменування. Вікно «Обмеження на додатки» можна побачити на наступному скріншоті:

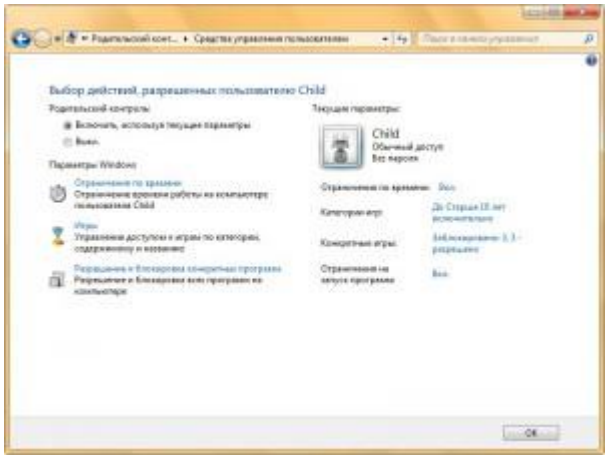


Після того як ви встановите прапорці біля всіх програм, якими може користуватися ваша дитина, до всіх інших програм доступ автоматично буде заблокований. Якщо ви не знайшли в списку якусь програму, то її можна додати до списку за допомогою кнопки «Обзор».

У діалоговому вікні «Відкрити», пересуваючись по дереву каталогів, відкрийте папку, яка містить потрібний файл. У діалоговому вікні будуть виведені всі типи виконуваних файлів. Після того, як потрібний файл буде знайдений, виділіть його, клацнувши на ньому лівою кнопкою миші, що помістить його ім'я в рядок для введення імені файлу і натисніть на кнопку «Відкрити».



Після того як ви визначите дозволу для всіх програм, встановлених на вашому комп'ютері, натисніть на кнопку «ОК». Батьківський контроль перемістить вас у вікно «Засоби керування користувачем», де ви зможете побачити коротку інформацію про ті обмеження, які були встановлені.

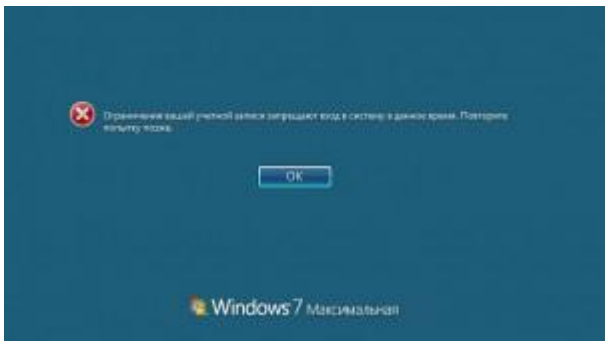


На цьому установка батьківського контролю, використовуючи штатні засоби, закінчується. У наступному розділі ви побачите роботу користувача, для якого були застосовані обмеження, використовуючи батьківський контроль Windows 7.

Робота користувача, на якого застосовується батьківський контроль

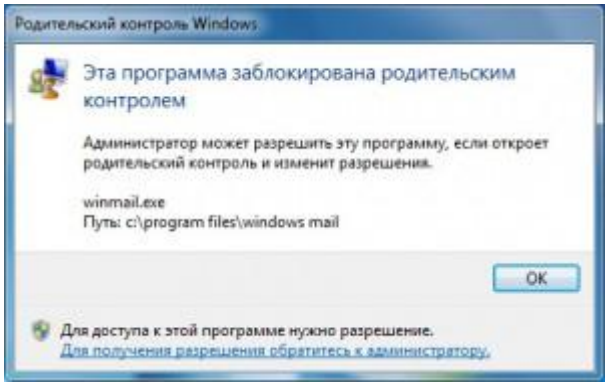
У цьому розділі ви можете побачити приклади всіх обмежень батьківського контролю «в дії», які можна застосувати для облікового запису вашої дитини.

Перш за все, якщо ви обмежили доступ до комп'ютера для дитини, то при спробі входу в свій обліковий запис у заборонений час, дитина побачить наступне попередження:



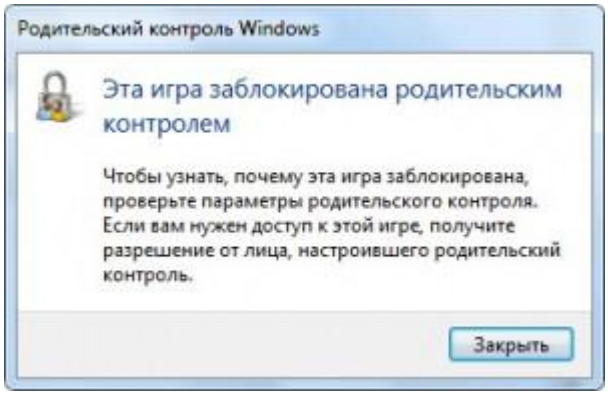
Тепер, як видно на попередньому скріншоті, ви можете бути впевнені, що ваша дитина зможе зайти у свій обліковий запис тільки у вказаний для нього час.

Після того як дитина зможе зайти у свій обліковий запис і спробує відкрити програму, для якого був заблокований доступ, він побачить таке повідомлення:

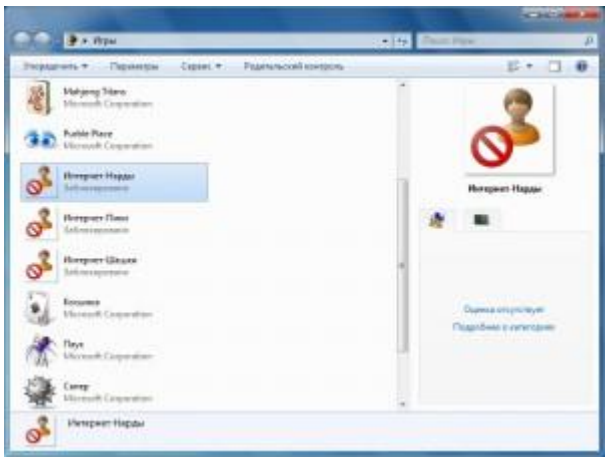


Побачивши це повідомлення, дитина не зможе запустити цю програму до тих пір, поки ви йому не дасте на це свою згоду.

При спробі відкрити гру, вікова категорія якої не входить в список дозволених, якщо вона заблокована по вмісту або якщо ви вручну її заблокували, при запуску з'явиться повідомлення батьківського контролю Windows:



Також, відкривши папку «Ігри», у того облікового запису, для якого застосовується батьківський контроль, на заборонених адміністратором іграх, дитина побачить значок, що свідчить про те, що доступ до цієї гри заблокований.



У цьому керівництві докладно описані всі штатні дії, які можна виконувати компонентом операційної системи Windows 7 – «Батьківським контролем». Існують також і інші програми Батьківського контролю, які можливо встановити на ОС.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

Користуючись інструкціями створити новий обліковий запис та налаштувати для нього батьківський контроль. Хід виконання описати у звіті, ілюструючи скріншотами.

1. З дозволу викладача ввійдіть в систему під обліковим записом «***Адміністратор***».
2. Створіть новий обліковий запис під іменем «***Дитина***».
3. Внесіть до нього зміни, обравши пункт «Установить родительський контроль».
4. Встановіть обмеження для часу роботи: дозвольте працювати на вихідні від 13.00 до 15.00, а в решту днів з 17.00 до 18.30.
5. Задайте категорію ігор «***Для детей***».
6. В пункті «***Запрещение и розрешение игр***» оберіть лише три гри, які дозволяються, до решти доступ закрийте.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Як встановити пароль для облікового захисту?
2. Як здійснюється захист файлів за допомогою шифрування дисків BitLocker?
3. Як здійснюється включення, призупинення роботи та відключення шифрування дисків BitLocker?
4. Що являє собою захист системи?
5. Що ви знаєте про захист доступу до мережі (NAP)?
6. Як реалізується в операційній системі запобігання виконання даних?
7. Опишіть захист, що забезпечується Захисником Windows, в реальному часі.
8. Що являє собою шифрована файлова система (EFS)?
9. Опишіть призначення, можливості, особливості налаштування та використання батьківського контролю, що забезпечується засобами операційної системи.

10. Назвіть та опишіть основні можливості захисту інформації засобами операційної системи.

Лабораторна робота №4

Тема: Захист інформації на мобільних телефонах. Огляд найпоширеніших мобільних вірусів та засобів боротьби з ними.

Мета: ознайомитися з причинами та способами попередження втрати інформації на мобільних телефонах, поняттями мобільного віруса та антивіруса, ознаками прослуховування розмов по мобільному телефоні та способами боротьби з ними.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Невід'ємною частиною нашого життя є мобільні телефони. На сьогоднішній день вони стали не тільки засобом зв'язку, а й отримали ряд додаткових функцій, просто незамінних для сучасної людини в повсякденному житті, що робить їх не тільки корисними, а й вразливими до атак різного роду для отримання інформації.

Особливості роботи з сучасними мобільними телефонами

1. Вхід в систему "Банк-Клієнт тепер здійснюється не тільки з офісного комп'ютера, але і з домашніх ПК і з мобільних пристроїв (найчастіше під ОС Android), на яких, як правило, взагалі немає ніякого антивіруса, а якщо і є - то безкоштовна , сильно обмежена в функціоналі версія.
2. Мобільні телефони можуть величезному ризику втрати / крадіжки. Інформація (включаючи паролі і логіни доступу до корпоративних ресурсів) може потрапити в не завжди доброзичливі руки.
3. Кількість загроз для ОС Android зростає катастрофічними темпами разом із зростанням кількості використовуваних пристроїв.
4. 60% особистих пристроїв не мають ніякого захисту! А значить, люди ніяк не захищені від атак хакерів, використовувані ними додатки можуть мати уразливості.

В більшості сучасних мобільних пристроїв для зберігання інформації (контактів, SMS, нотаток, календарів та інші) використовується Flash пам'ять та носії на її основі – карти пам'яті та/або SSD накопичувачі. Тип носія, формати запису та організації даних в пам'яті не стандартизовано, тому кожний виробник реалізує в своїх гаджетах власні формати та алгоритми збереження інформації.

Тому у випадку втрати інформації на мобільному пристрої відновлення даних представляє собою складну технічну задачу.

Причини втрати інформації на мобільних пристроях:

1. Механічні пошкодження
2. Випадкове чи навмисне видалення інформації
3. Форматування зовнішньої пам'яті
4. Неправильна синхронізація даних
5. Випадкова втрата чи навмисне встановлення паролю доступу до пристрою
6. Вплив вірусів та використання злоякісного ПЗ

Мобільні віруси - це невеликі програми, призначені для втручання в роботу мобільного телефону, смартфона, комунікатора, які записують, пошкоджують або видаляють дані і поширюються на інші пристрої через SMS та Інтернет.

Вперше про мобільних вірусах заговорили ще в 2000 році. Вірусами назвати їх було важко, так як це був набір команд, виконуваний телефоном, який передавався через SMS. Такі повідомлення забивали відповідні комірки пам'яті і при видаленні блокували роботу телефону. Найбільшого поширення набули команди для таких телефонів, як Siemens і Nokia.

У недалекому минулому основною платформою, для якої писали віруси, була Symbian. Однак ситуація на ринку мобільних телефонів складається таким чином, що смартфони на Symbian, хоча і вельми популярні, поступаються чималі частини ринку апаратам інших виробників. Наприклад, пристроям на Windows Mobile, це iPhone та інші платформи.

Тенденція така, що чим функціональніший телефон, тим до більшої кількості загроз він схильний. Будь-які команди, функції та можливості, що дозволяють створювати програми і програми для мобільних телефонів, можуть стати інструментом для створення вірусів. Найбільш перспективною платформою для написання вірусів є Java 2ME, так як переважна більшість сучасних телефонів підтримує дану платформу.

Основною метою мобільних вірусів, як і у випадку з комп'ютерними вірусами, є отримання персональної інформації, яку можна продати або використати в особистих потребах. До такої інформації можуть відноситися особисті дані власника телефону, дані самого пристрою, приватні повідомлення, інколи номери кредитних карт.

Цікава історія віруса Ikee, який був розроблений в кінці 2009 року, та лише поширювався та міняв заставку на телефоні. Автора хробака, австралійця Ешлі Таунс, навіть запросили на роботу в Apple після виходу вірусу. Але на основі Ikee були створені модифікації, які, наприклад, були пристосовані для крадіжки інформації про банківський рахунок власника апарату.

У березні 2011 року власники смартфонів могли безкоштовно закачати з кількох інтернет - серверів таку невеличку гру як «3D Anti-terrorist». Так як же постраждали жертви даної іграшки? Справжні розробники даної гри безкоштовно надавали тільки демо-версію. Однак автор вірусу її зламав і додав код власної програми, потім розмістив на різних серверах мобільних ігор. Ті люди, які вирішили випробувати гру нічого поганого спочатку не відчували, поки не отримали рахунок за телефон від мобільного оператора. Виявилося, що їх улюблений телефон без участі власника сам дзвонив на платні закордонні номери. Після проведеного аналізу було констатовано, що програма цю операцію проробляла з тимчасовим інтервалом у 50 секунд в темний час доби, коли власники смартфонів скоріше за все відпочивали. Причому дзвінки виконувалися на шість платних номерів.

Ще одним прикладом вірусу в стільниковому телефоні може стати, так званий, «MMS Bomber». Даною програмою інфіковані вже багато мільйонів телефонів у всьому світі. Суть даного вірусу полягає в тому, що в телефон потрапляє мила додаткова програмка, після інсталяції, якої починають висилатися мультимедійні повідомлення на всі номери, збережені в записній книжці зараженого телефону. Зміст повідомлення - це посилання на сайт, натиснувши на яку в телефон завантажується новий «MMS Bomber». Причому шкідник може відключити всю систему телефону, що робить деінсталяцію програми абсолютно неможливим.

Існує декілька різних схем і напрямків розвитку вірусів, за якими діють автори мобільних вірусів:

Крадіжка персональної інформації.

В даному випадку віруси збирають різні відомості, наявні в телефоні, наприклад, контакти власника телефону, паролі від програм, параметри облікових записів, таких, як Google Play або AppStore. Вся інформація, отримана вірусом, відправляється на сервер зловмисників, де використовується на їх розсуд. Один з найсерйозніших вірусів такого плану - Android.Geinimi. Потрапляючи в систему, він визначає місце розташування смартфона, завантажує файли з Інтернету, зчитує і записує закладки браузера, отримує доступ до контактів, здійснює дзвінки, відправляє, читає і редагує SMS-повідомлення.

Відправка платних SMS-повідомлень, дзвінки на «партнерський номер» без відома власника.

У даному випадку за відправку повідомлення або за дзвінок списується серйозна сума коштів з особового рахунку власника телефону. Зрозуміло, гроші потрапляють до рук зловмисників. З найвідоміших подібних загроз можна назвати Android.SmsSend, а також давно відомі RedBrowser і Webster для Java-платформи. Вони маскуються під різні корисні програми, викликаючи тим самим довіру у користувача. Також існують віруси і для інших платформ, наприклад Symbian OS, Windows Mobile і інших.

Шахрайство за допомогою використання систем інтернет-банкінгу.

У даному випадку вірус відкриває доступ до мобільного додатком для роботи з банком або відповідному веб-сайту, або перехоплює SMS-повідомлення, що передаються користувачеві від систем інтернет-банкінгу. Небезпека даного типу може підстерігати власників мобільних телефонів, що працюють на різних платформах. Відомий троян Trojan-Spy.SymbOS.Zbot.a, що працює в сукупності з популярним вірусом Zbot для звичайних ПК.

Боротьба з мобільними вірусами

Для того щоб запобігти зараженню мобільним вірусом, слід пам'ятати про заходи безпеки. Способи розповсюдження вірусів досить різні. Наприклад, вірус можна «підчепити» по Bluetooth. А це означає, що Bluetooth не слід тримати постійно включеним, а, беручи що-небудь через «блакитний зуб», потрібно точно знати, що саме Ви приймаєте.

Вірус чи інша шкідлива програма повинна бути встановлена на сотовому перш ніж вона зможе працювати. Творці шкідливого ПЗ широко використовують засоби соціальної інженерії для розповсюдження своїх програм, часом - досить примітивних, які не вміють розмножуватися самостійно, але вміють робити щось інше.

Так, наприклад, зловмисник може написати програму, яка таємно відправляє платні SMS з зараженого телефону. Цю програму можуть безкоштовно пропонувати для скачування з Інтернету та встановлення на мобільний телефон.

Як правило, подібні програми мають вельми привабливі назви. У результаті, встановивши своїми руками на свій же телефон шкідливу програму, власник апарату може позбутися засобів на рахунку, а до усього іншого, втрачати їх регулярно.

Уважно ставтеся до всього, що Ви встановлюєте на телефон. Не завантажуйте підозрілих програм. Пам'ятайте - підозріла (чи занадто вже привабливо названа) програма може бути небезпечною.

Шкідливий код, на жаль, може проникнути на Ваш пристрій абсолютно без Вашого відома. І тут вам може допомогти лише спеціалізоване захисне ПЗ - мобільний антивірус.

Антивірусні компанії вже почали випускати версії своїх програм для захисту мобільних телефонів: Symantec Client Security для смартфонів Nokia, Kaspersky Security для PDA, Kaspersky Anti-Virus для Symbian OS, KAV Mobile, WinMobile і багато інших.

Kaspersky Mobile Security призначений для всебічного захисту смартфона Android – під час перегляду веб-сайтів, скачування файлів, здійснення покупок або спілкування. Крім того, у випадку втрати або крадіжки смартфону Kaspersky Mobile Security допоможе захистити особисті дані і визначити місцезнаходження пристрою - навіть якщо в ньому замінили SIM-карту.

Основні можливості:

1. Виявлення вірусів, шпигунських програм та інших загроз.
2. Блокування переходів по шкідливим і фішингових посиланнях.
3. Фільтрація небажаних дзвінків та SMS.
4. Приховування особистих контактів, дзвінків та SMS-повідомлень.
5. Можливість віддалено заблокувати смартфон, стерти особисті дані та визначити місцезнаходження пристрою в разі втрати або крадіжки.
6. Мінімальне використання ресурсів батареї.

Dr.Web Mobile Security Suite підтримується найсучасними операційними системами: Android OS, S60, Symbian, Windows Mobile. Продукт забезпечує антивірусний захист комунікаторів і КПК від вірусів і інших інтернет-загроз, створених спеціально для інфікування мобільних пристроїв. Сумісний з будь-якими КПК і комунікаторами.

Avira AntiVir Mobile надає надійний захист для кишенькових комп'ютерів і смартфонів на базі операційної системи Windows Mobile.

Avira AntiVir Mobile може виконати сканування всього пристрою на предмет наявності шкідливого ПЗ, в тому числі сканування карт пам'яті і мережевих папок. Оновлення антивірусних баз не викличе складнощів, оскільки його можна виконати декількома шляхами, а сам файл оновлень дуже малий за розміром.

Ключові особливості та функції програми Avira AntiVir Mobile

1. Просте завантаження програми шляхом підключення телефону до комп'ютера або через WLAN, LAN, GPRS.
2. Легке ручне оновлення через LAN, WLAN або Dial-Up GPRS. Підтримується також оновлення через комп'ютер або проксі-сервера.
3. Програма оновлюється через один файл, який дуже малий за розміром. Відкат у разі незавершеного з якихось причин поновлення.
4. Сканування карт пам'яті і мережевих папок.
5. Автоматична або інтерактивна процедура видалення вірусів.
6. Можливість видалення заражених файлів.
7. Надання специфічної інформації по кожному знайденому вірусу.
8. Повноцінне управління програмою кнопками телефону.

Втрата інформації в результаті прослуховування мобільного телефону

Прослуховування мобільного телефону - не така вже і дорога справа, як це може здатися. Для цього досить початкових знань в радіоелектроніці і вміння працювати своїми руками. Інтернет сьогодні сповнений описів самих різних приладів, за допомогою яких можна не тільки прослуховувати мобільні розмови, але і перепрограмувати мобільні телефони так, щоб отримати доступ до записника або навіть безперешкодно прослуховувати розмови, які ведуться в безпосередній близькості від включеного мобільного телефону. Свою майстерність не втомлюються вдосконалювати і спецслужби і шахраї.

Система мобільного зв'язку в тому вигляді, в якому вона склалася і діє сьогодні, - це три основні складові. Перша - це власне ваш мобільний телефон, який, по суті, є портативним радіопередавачем. Друга - це система базових станцій, "сот", від потужності і розташування яких залежить рівень прийому вашого телефону. І основна складова - комунікаційний центр, який керує роботою всієї системи.

У кожного мобільного телефону є персональний електронний серійний номер (MIN). Він кодується виробником в мікрочіпі стільникового телефону. Іноді виробник вказує цей персональний серійний номер в керівництві для користувача, щоб ви могли ідентифікувати свій телефон. Ну, скажімо, у випадку, якщо у вас вкрали ваш стільниковий телефон. Коли ваш апарат підключається до системи стільникового зв'язку, то його мікрочіп зчитує ще й ваш мобільний номер (ESN), який зашифрований в SIM-картці. Тому, якщо ви міняєте, з міркувань безпеки, або будь-яким іншим причинам, вашу SIM-карту, то разом з нею краще викиньте і телефон. Тому що він "повідомить" вашій наступній Sim-карті, який номер на ньому перш стояв. Так само точно "настукає" на вас і ваша нібито секретна Sim-карта, вставлена в інший апарат, тобто по ній можна буде визначити, в якому апараті вона раніше стояла. Цим азам електронної безпеки вчать, при підготовці своїх фахівців всі спецслужби світу.

Телефонний зв'язок здійснюється через найближчу до вас "соту", тобто станцію радіопередачі. Вона пов'язана з базовою станцією, яка вільна приймати і передавати сигнали на великій кількості радіочастот. Ця станція також підключена до звичайної провідної телефонної мережі. Інакше ви б не змогли дзвонити з мобільного телефону на звичайні міські телефони. Для цього базова станція оснащена апаратурою перетворення високочастотного сигналу мобільного телефону в низькочастотний провідного телефону, і навпаки.

Базова станція періодично випромінює службовий сигнал. Пам'ятайте, перші моделі мобільних телефонів моргали нам зеленим вогником: говорячи нам, що зв'язок є. Коли вогник ставав червоним, значить, станція або сигнал від неї загубився. Прийнявши цей сигнал, ваш мобільник навантажує його своїми даними - електронним номером апарату, мобільним номером, місцем розташування "соти" (територіальне знаходження абонента стільникового зв'язку) - і відправляє назад, щоб базова станція змогла ідентифікувати телефон і перевірити стан рахунку власника. Після цього базова станція прив'язує ваш мобільник до певної зоні, де ви в даний момент знаходитеся. Це потрібно для того, щоб у разі вхідного або вихідного дзвінка негайно виділити нам одну з вільних частот цієї зони.

При цьому в комунікаційному центрі, комп'ютер якого управляє всім цим господарством і всіма з'єднаннями в мережі, в базі даних відкладається вся інформація як про місцезнаходження всіх клієнтів, так і про їхні зв'язки з іншими ж мережами. Це необхідно для ідентифікації абонентів та перевірки їх права на доступ в мережу.

У цієї системи як мінімум дві дуже слабких ланки. Перша - сигнал, який йде від вашої трубки до "соти", і другий - передача від "соти" до базової станції. Більшість систем стільникового зв'язку відповідає одному із стандартів аналогового зв'язку. Таких, як AMPS, TAGS, NTS або цифровий - D-AMPS, NTT, GSM і т.п. Найбільш поширені стільникові системи використовують діапазони 450, 800 і 900 МГц. Кожен з цих стандартів докладно описаний у відповідній літературі. А якщо ви знаєте діапазон частот, то завжди зможете підібрати апаратуру з потрібними технічними параметрами. Телефонні переговори з мобільнх телефонів ловили навіть старі автомобільні магнітоли.

Як стверджують фахівці, розмова, що ведеться з стільникового телефону, може бути прослухана за допомогою програмованих сканерів з полосою прийому 30 КГц, здатних здійснювати пошук в діапазоні 860-890 МГц. Для цієї ж мети можна використовувати і звичайні сканери після їх невеликої модифікації, яка детально описана в Інтернеті. І що ще цікаво! Перехопити розмову по мобільному телефону можна навіть шляхом перебудови тюнера в телевізорах старих моделей.

Перепрограмування однієї мікросхеми в телефоні дозволяє отримати доступ комутаційного обладнання телефонних компаній. І тоді рахунки за розмови нікому пред'явити. А клонування ідентифікаційних номерів, яке останнім часом набуває все більшого поширення! Для цього всього-потрібен так званий стільниковий кеш - бокс, який являє собою комбінацію сканера, комп'ютера та стільникового телефону. Він виявляє номера MIN і ESN і автоматично перепрограмує себе на них. Причому після разового використання цього поєднання він стирає їх в пам'яті, і вибирає іншу пару. Що, як ви розумієте, робить виявлення шахрайства практично неможливим.

При всьому при тому прослуховування мобільного зв'язку - справа аж ніяк не така дорога, як це нам намагаються представити. Так, уже сьогодні одночасна прослушка 10 тис. мобільних телефонів може бути здійснена за допомогою одного пристрою вартістю 50 тис. доларів. Будемо вважати, що в місті приблизно 5 млн. мобільних. Це дані експертів. Але розмова одночасно ведеться не більше ніж з 100 тис. з них. Тобто виходить, що для контролю всіх розмов користувачів місцевого зв'язку достатньо 10 таких пристроїв. Це близько півмільйона доларів. Додайте сюди накладні витрати, тобто обробку та зберігання записів, створення алгоритмів пошуку і формування баз даних плюс зарплату фахівців, які всім цим будуть займатися. По самій верхньої цінової планки це не більше 500 тис. на рік. Таким чином, для прослуховування мобільних телефонів всієї Москви протягом року досить одного мільйона доларів. Вражає? І не думайте, що вас врятує один з смартфонів, які використовують набагато складніший тип шифрування розмови, ніж той, що надається операторами стільникового зв'язку. Так, ще кілька років тому пристрій, здатний "розколювати" подібні розмови, коштував понад півмільйона доларів. Крім того, він був здатний відстежувати одночасно не більше 16 абонентів. Але часи змінюються, і можливостям розуму немає меж.

За допомогою мобільного телефону можна легко і безперешкодно прослуховувати розмови, які ведуться в безпосередній близькості від нього. Для цього досить, щоб телефон був зареєстрований в мережі і батарея в нього була не сильно розряджена. Як повідомили деякі ЗМІ, ФБР знайшло спосіб включати практично будь-який мобільний телефон в режим прослуховуючого пристрою без відома його господаря. Здається, що подібною технологією давно вже володіють і наші спецслужби, однак рекламувати це своє досягнення вони якось не кваплятся. Чи потрібно говорити про те, що для цього потрібно повне сприяння оператора стільникового зв'язку. Але отримати таку згоду для спецслужб, як ви розумієте, не проблема.

На думку фахівців, одним зі слабких місць сучасних наворочених телефонів є процедура обробки службових sms. Саме вона дозволяє стороннім отримати контроль над вашим телефоном. Ці sms потрібні оператору для того, щоб, наприклад, модернізувати програмне забезпечення вашого мобільного телефону, подаючи команди за допомогою службових sms повідомлень. Це отримало дуже

велике поширення за кордоном, але все більше використовується і у нас. Телефон зовні ні як не реагує на ці смс і не перевіряє відправника. Цим можна скористатися для того, щоб перепрограмувати його непомітно для власника. Зокрема, таким чином можна отримати доступ до адресної книги власника або прослуховувати розмови завдяки таємній активації конференц-зв'язку.

Для захисту від прослуховування мобільного телефону фахівці рекомендують:

1. Тримати документи з ESN-номером телефону в надійному місці;
2. Щомісяця і ретельно перевіряти рахунки на користування мобільним зв'язком;
3. У випадку крадіжки або пропажі стільникового телефону відразу попередити оператора, який надає вам послуги зв'язку;
4. Тримати телефон вимкненим до того моменту, поки ви не вирішили ним скористатися. Цей спосіб найлегший і найдешевший, але слід пам'ятати, що досить одного виходу на зв'язок, щоб виявити MIN/ESN номера апарату;
5. Регулярно міняти через вашу компанію, що надає вам послуги стільникового зв'язку, MIN-номер вашого апарату;
6. Встановити додатковий чотиризначний PIN-код, що набирається перед розмовою. Цей код ускладнює діяльність шахраїв, так як вони зазвичай перехоплюють тільки MIN і ESN номера, але невелика модифікація апаратури перехоплення дозволяє виявити і його;
7. Під час важливих переговорів, на яких ви обговорюєте конфіденційну інформацію, вимкніть телефон, витягніть з нього батарею і, ще краще, приберіть його подалі від себе;

Ознаки прослуховування мобільних телефонів

Температура батареї. Один із ймовірних індикаторів наявності «прослушки» - це батарея. Якщо ваш телефон у той час, коли ви його не використовуєте буде теплим або навіть гарячим, це означає, що він все ще використовується. Врахуйте, що тепло буває перш за все від надмірного використання. Акумулятор може бути гарячим тільки в тому випадку, якщо телефон використовувався деякий час тому.

Телефон розряджається дуже швидко. Заряджаєте свій мобільний телефон частіше, ніж зазвичай - отримаєте ще один знак потенційної загрози. Якщо ви не використовували гаджет більше, ніж зазвичай, цілком можливо, що ваш телефон використовується кимось без вашого відома. Коли мобільний телефон прослуховують, він втрачає заряд акумулятора набагато швидше. Прослуховуваний мобільний телефон постійно записує розмови в кімнаті, навіть якщо виглядає так, начебто він лежить без діла. Можна використовувати додаток BatteryLife LX, щоб відслідковувати швидкість розрядження батареї.

Примітка: мобільні телефони мають тенденцію втрачати максимальний рівень заряду батареї з плином часу. Якщо вашому телефону більше року, то ємність батареї буде неухильно знижуватися в залежності від інтенсивності використання.

Затримка при вимиканні. Коли ви вимикаєте свій телефон і спостерігаєте велику затримку, підсвічування, палаючу протягом тривалого часу або просто відмову телефону від виключення, то цілком можливо, що ви на гачку. Завжди помічайте нетипову поведінка телефону. Хоча, описані проблеми можуть бути викликані збоями в апаратному або програмному забезпеченні телефону.

Дивна активність. Коли ваш телефон працює, чи буває так, що у нього раптово спалахує підсвічування, самі по собі встановлюються якісь програми, відбувається мимовільне вимикання? Дивна поведінка може бути сигналом до того, що хтось віддалено керує цим пристроєм. До речі, це також може відбуватися через перешкоди при передачі даних.

Фоновий шум. Коли ви розмовляєте, телефон «на прослуховуванні» може створювати перешкоди. Щось на зразок луни, розрядів електрики, клацань - ці звуки можуть бути викликані навколишнім середовищем, перешкодами при з'єднанні... або тим, що хтось вас прослуховує. Якщо чуєте пульсуючий шум зі свого телефону, коли ви його не використовуєте - це може бути серйозною проблемою.

Перешкоди. Якщо ви використовуєте свій телефон в безпосередній близькості до інших електронних пристроїв (на кшталт телевізора) і він створює перешкоди на них, то це може бути наслідком наявності сторонніх пристроїв в корпусі мобільного. У більшості випадків перешкоди - це нормально, але якщо це відбувається в ті моменти, коли ви не використовуєте телефон, то це цілком може значить те, що ви «під ковпаком».

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Запустіть браузер Інтернет (Це може бути Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera чи будь-який інший, що встановлений на вашому комп'ютері)
2. Користуючись однією з пошуковх систем (Yahoo!, Google, чи будь-якою іншою) знайдіть антивірус, що може бути встановлений на ваш мобільний телефон. Запишіть до звіту назву, короткий опис, можливості та особливості даного програмного продукту.
3. Користуючись однією з пошуковх систем знайдіть та запишіть до звіту резонансні випадки втрати інформації через мобільний телефон (не менше 2).
4. Користуючись однією з пошуковх систем знайдіть 5 прикладів вірусів для мобільних телефонів, запишіть до звіту їх назви, особливості, опишіть шкоду, яку вони можуть завдати пристрою.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Назвіть причини втрати інформації на мобільних телефонах.
2. Що називається мобільним вірусом?
3. Що є основною метою створення та розповсюдження мобільних вірусів?
4. Назвіть та опишіть відомі вам схеми роботи мобільних вірусів.
5. Які мобільні антивіруси ви знаєте? Опишіть їх основні можливості.
6. Як здійснюється прослуховування мобільного телефону?
7. Назвіть заходи захисту мобільного телефону від прослуховування.
8. Які ви знаєте ознаки прослуховування розмов по мобільному телефоні?
9. Який антивірус може бути встановлений на ваш мобільний телефон? Які його основні властивості?
10. Які вам відомі вірусні програми, що спрямовані на ураження мобільного телефону?

Лабораторна робота №5

Тема: Інформаційна безпека в соціальних мережах. Захист електронної пошти та власних акаунтів під час роботи в мережі.

Мета: ознайомитися з поняттям служби соціальної мережі та електронної пошти, основними джерелами та шляхами уникнення втрати інформації під час користування послугами соціальної мережі; особливостями захисту особистих даних і таємниці листування в процесі використання електронної пошти.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Однією з най масштабніших мереж загального користування є глобальна мережа Інтернет – система об'єднаних комп'ютерних мереж глобального загальнолюдського суспільства, яка в наш час покриває практично всю поверхню земної кулі. Однак, на базі мережі Інтернет почали з'являтися інші мережі – соціальні. Соціальна мережа — соціальна структура, утворена індивідами або організаціями. Вона відображає розмаїтті зв'язки між ними через різноманітні соціальні взаємовідносини, починаючи з випадкових знайомств і закінчуючи тісними родинними вузами. Вперше термін було запропоновано в 1954році Дж. А. Барнесом (в роботі Class and Committees in a Norwegian Island Parish, «Human Relations»). Максимальний розмір соціальних мереж становить близько 150 осіб, а середній — 123 (Хілл та Данбер, 2002).

Аналіз соціальних мереж (має стосунок із теорія мереж) перетворився на основний метод досліджень в сучасній соціології, антропології, географії, соціальній психології, інформатиці та дослідженні організацій, а також поширену тему для досліджень та дискусій. Дослідження в декількох

академічних сферах показали, що соціальні мережі діють на багатьох рівнях, починаючи від родин, і закінчуючи цілими націями, та відіграють важливу роль в тому, як розв'язуються проблеми, працюють організації, та досягають успіху на шляху до власних цілей індивіди.

Соціальні мережі в Інтернеті

Служба соціальних мереж (англ. *socialnetworkingservice*) — веб-сайт або інша служба у Веб, яка дозволяє користувачам створювати публічну або напівпублічну анкету, складати список користувачів, з якими вони мають зв'язок та переглядати власний список зв'язків і списки інших користувачів. Природа та номенклатура зв'язків може різнитись в залежності від системи.

На відміну від служб соціальних мереж, в *інтернет-спільнотах* користувач не знаходиться в центрі системи; відношення користувача до інших учасників спільноти знаходиться на другому плані. Основна увага інтернет-спільноти зосереджена на внеску користувача в досягнення спільних цілей, цінностей та спілкуванні.

В соціальних мережах користувач знаходиться в центрі системи та може належати до декількох груп водночас.

Ні для кого не секрет, що соціальні мережі вже давно є привабливими платформами для різного роду кібер-злочинів, таких як спаммінг, фішинг, фармінг акаунтів і інших. Причина криється в ряді властивостей, якими володіють всі соціальні мережі і які можуть бути використані зловмисниками в своїх цілях.

Такими властивостями насамперед є:

– Величезна користувача база.

– Виникнення зв'язків довіри як між окремими користувачами так і між групами користувачів.

– Висока розподіл бази користувачів за географічним і тимчасовому параметрам.

– Комп'ютерна неграмотність користувачів соціальної мережі.

Людям знайомим з інформаційною безпекою не треба пояснювати, що при комбінації методів технічних та соціальної інженерії ці властивості дозволяють досягти бажаного результату в короткі терміни при витраті мінімальних зусиль.

Легітимна вразливість

На даний момент надання API для створення сторонніх додатків для соціальних мереж стало фактично стандартом де-факто. У більшості випадків передбачається, що додатки створювані за допомогою даних API не будуть приносити шкоду і звичайно з-за величезної кількості створюваних додатків перевірка кожного з них видається нездійсненним завданням. Відповідно створювані додатки додаються в базу соціальної мережі без належної перевірки на те, чи є вони шкідливим ПЗ. Положення також посилюють згадані раніше зв'язки довіри і насамперед довіра до самої соціальної мережі. Незважаючи на те, що адміністрація всіляко вказує на те, що дані програми є продуктом сторонньої розробки більшість користувачів не звертає на це увагу, вважаючи за краще довіряти будь-якій програмі за умовчанням. Як результат - зловмисники мають можливість додавати і поширювати шкідливі програми засобами, що надається самої соціальною мережею. Велика соціальна мережа Facebook регулярно піддається атакам черв'яків. У побут навіть увійшов спеціальний термін - rogue app. Використовуючи абсолютно легітимні засоби, що надаються API Фейсбук, черв'яки поширюються розсилкою повідомлень друзям зараженого аккаунта. Звичайно основною метою цих черв'яків є поширення іншого шкідливого ПЗ, яке заражає машину користувача, відповідно створюючи ботнет. Подібних атак схильна і вітчизняна мережа ВКонтакте. В даному випадку мали місце і прямі атаки на машину користувача з використанням вразливостей в технології флеш.

Ще одна небезпека, що може трапитися з користувачем соціальної мережі це викрадення аканту. Ціль викрадення може бути різна – наприклад, для подальшої перепродажі спамерам, для розсилки спаму самостійно, для помсти. Основні методи викрадення наведено нище.

1. Взлом через е-мейл. Цей метод діє через функцію відновлення пароля. Як відомо, пароль можна отримати поштою, на яку зареєстрована сторінка. Для цього використовується функція

відновлення пароля. Частенько, зламати поштову скриньку простіше, ніж аккаунт, тому віднесіться уважно до безпеки своєї пошти – вибирайте складний пароль, використовуйте популярні і надійні сервіси. Уважно віднесіться до складання секретного питання. Відповідь на нього повинні знати лише ви. Ваші друзі не повинні зуміти відповісти на секретне питання. Краще всього буде, якщо сама адреса пошти, на яку ви реєструєте свої аккаунти, буде зареєстрована окремо і не буде вашим основним e-mail'ом. Не варто говорити про нього вашим знайомим, зберігайте його, як і пароль – в таємниці. Тоді задача хакера доволі ускладниться, адже не знаючи пошти, на яку зареєстровано аккаунт, незрозуміло яку пошту ламати! Крім того, більшість сервісів дозволяє використовувати підтвердження на мобільний телефон. Користуйтеся цим. Не нехтуйте зайвими мірами захисту – все що ускладнює життя зловмисникові, допомагає вам;

Засоби захисту: Використовуйте завжди складні паролі, використовуйте окрему поштову скриньку для реєстрації, використовуйте підтвердження на мобільний телефон.

2. Брутфорс (підбір пароля) – це досить старий метод і більшість сервісів вимагають від своїх користувачів використовувати надійні паролі, а також не дозволяють більш ніж 3-5 помилок. Після цього на деякий час користувач блокується. Так що цей метод зараз можна не приймати до уваги – звісно, якщо ви дійсно маєте надійні паролі. Також бажано їх час від часу міняти, а також мати різні паролі для різних сервісів;

Засоби захисту: Використовуйте завжди складні паролі.

3. Взлом через cookie. Cookie – це файл на комп'ютері користувача, в якому зберігається його e-mail і зашифрований пароль. Завдяки цим файлам Вам не доводиться кожного разу при вході вводити пароль, адже він збережений в cookie, і ви потрапляєте прямо на сайт. Якщо хакер отримає цей файл cookie, то взнає ваш e-mail і пароль (правда в зашифрованому вигляді). Розшифрувати пароль не складно, якщо він короткий і простий, але якщо пароль складений відповідно до пункту 2 – задача крадія буде дуже ускладнена. Крадуть cookie різними способами, але, щоб цього уникнути, слідуйте наступними порадам: не вводьте в рядок браузера незнайомі скрипти, адже вони можуть зберігати cookies; не встановлюйте жодні доповнення для соціальних мереж з сумнівних джерел; на жодних сайтах не залишайте значення своїх cookies (зараз дуже популярні безкоштовні дарунки в однокласниках, безкоштовний рейтинг в контакті і так далі); не залишайте своїх знайомих за вашим комп'ютером одних, якщо не довіряєте їм, вкрасти cookies займе 5-10 сек, якщо підійти із знанням справи;

Засоби захисту: не вводьте в рядок браузера незнайомі скрипти, не встановлюйте жодні доповнення для соціальних мереж з сумнівних джерел, на жодних сайтах не залишайте значення своїх cookies, не залишайте своїх знайомих за вашим комп'ютером одних.

4. Використовування фейків – фейк (від англійської fake – підробний, фальшивий) – це спеціальна сторінка, яка цілком виглядає так, як оригінальна для вводу логіну та пароля в соціальній мережі. Ціль зловмисників – заставити вас ввести ваші логін та пароль – після чого вони будуть переслані їм. Після вводу вас перенаправлять на оригінальній сайт. Фейки зараз дуже популярні – їх легко зробити, та легко використовувати. Більшість користувачів не дивляться на адресу сторінки, де вони знаходяться. Дуже часто фейкові сторінки пропонують у вигляді спаму з уже зломаних аккаунтів. Будьте уважні – не переходьте на посилання тільки тому, що воно прийшло від знайомого, особливо якщо до цього він ніколи вам подібного нічого не присилав. Не переходьте за посиланням якщо вам пропонують щось "бесплатно"– пам'ятайте де буває безплатний сир.

Засоби захисту: не переходьте на посилання тільки тому, що воно прийшло від знайомого, не переходьте за посиланнями, якщо вам пропонують щось "бесплатно" та "безвозмездно", будьте уважні.

5. Взлом через програми – це дуже популярний спосіб злому – особливо для таких мереж як ВКонтакте. Пам'ятайте – використовувати треба тільки ті програми, які ви отримали із надійного джерела. Надійними джерелами є тільки ті, що рекомендує безпосередньо адміністрація цієї мережі. Всі інші – ви використовуєте на свій страх та ризк. До речі – аргументація типа – "Друг Вася використовує і нічого …" – це не дуже розумно. Якщо вже вам так необхідні "примочки" – шукайте тільки ті, що

розповсюджуються з відкритим вихідним кодом. Якщо програма розповсюджується задарма, але розробник не відкриває її код, подумайте ще раз – де буває той дешевий сир.

Засоби захисту: не використовуйте програми з ненадійних джерел.

Що не варто писати в соціальних мережах

Явки і паролі. Першими під заборону потрапили логіни і паролі. Виявилося, що соціальні мережі використовуються не тільки для спілкування, але й для зберігання та обміну секретними даними. Причому деякі користувачі можуть "виставити на загальний огляд" пароль і від самої соціальної мережі. Тому особливо наївним радять відразу ж змінити пароль, після того, як він потрапив у чий-небудь чужий ящик.

Дівоче прізвище. Продовжуючи тему безпеки в мережі, не можна не згадати і про кодових словах, які використовуються для відновлення забутого пароля. Ні для кого не секрет, що найпопулярнішими з кодових питань є або дівоче прізвище матері, або номер школи. Саме з цієї причини користувачів, що бажають надати про себе якомога більше інформації, застерігають від афішування прізвищ родичів і номерів навчальних закладів.

"Стіна" ганьби. Наступними в списку заборонених дій в соціальних мережах виявилися публікації повідомлень особистого характеру на так званій "стіні". Не треба забувати про те, що шедеври на "стіні" бачить не лише одержувач, але й інші користувачі. Тому перед тим, як відправити чергове повідомлення провокаційного змісту, задумайтеся, чи не зашкодить воно адресату.

Принада для шахраїв. Контактні дані, зокрема адресу та телефон, також не варто залишати у відкритому доступі. Пам'ятайте, що зловмисники в будь-який момент можуть використовувати цю інформацію в незаконних цілях, особливо якщо знають, о котрій годині вас не буває вдома.

Плани на вечір. Для обговорення планів на вечір або вихідні краще використовувати особисту переписку або створювати закриті групи. Інакше інформація про барвистий вікенд може бути використана проти вас же самих (дивіться попередній пункт).

Бережіть свій гаманець. Інформація про ваше фінансове становище є, мабуть, однією з найбільш секретних. Ні в якому разі не можна повідомляти про розмір вашої заробітної плати та про те, де ви її отримуєте і зберігайте.

Ви і ваша робота. Під грифом секретності повинна залишитися і інформація про вашу організацію. Так, компанія Sophos, що займається питаннями інформаційної безпеки, провела дослідження і з'ясувала, що близько 63% організацій побоюються зайвої балакучості своїх співробітників, які не замислюючись про наслідки можуть опублікувати цінну інформацію. Одним з найяскравіших прикладів подібного випадку є історія з компанією Microsoft. Через профілі співробітників "комп'ютерного гіганта" у соціальній мережі Linkedin журналістам неодноразово вдавалося отримувати дані про які-небудь новинки чи плани компанії за кілька місяців до їх офіційного оприлюднення.

Дитячі фотографії. Нешкідливі на перший погляд фотографії дітей насправді можуть зіграти злий жарт із їхнім власником. По-перше, не можна забувати про людей, хворих педофілією, а, по-друге, інформація про те, що дитина може залишитися вдома одна, що може призвести до наслідків, описаним у пункті 4.

Мисливці за компроматом. Інформація з вашого профілю також може бути використана іншими сервісами і в підсумку спрямована проти вас. Існує чимало курйозних випадків, коли людина, відпросившись з роботи з причини поганого самопочуття, замість кабінету стоматолога проводила час на якій-небудь вечірці, а роботодавець випадково отримував фотографії "важко хворого співробітника", танцюючого і щасливого.

Сам собі ворог. Довірливо публікувати інформацію про себе, сподіваючись лише тільки на те, що навряд чи хтось побачить її крім самих близьких людей, - помилка багатьох користувачів. Пам'ятайте, що велика частина додатків соціальних мереж призначена для доступу до конфіденційної інформації.

Електронна пошта - традиційні засоби зв'язку, що дозволяють обмінюватися інформацією, принаймні, двом абонентам.

Основні протоколи передачі пошти (SMTP, POP3, IMAP4), як правило, не здійснюють надійної автентифікації, що дозволяє легко створити листи з фальшивими адресами. Жоден із цих протоколів не використовує криптографію, яка могла б гарантувати конфіденційність електронних листів. Хоча існують розширення цих протоколів, рішення про їх використання повинне бути прийняте як складова частина політики адміністрації поштового сервера. Деякі такі розширення використовують уже наявні засоби автентифікації, а інші дозволяють клієнтові й серверові погодити тип автентифікації, який використовуватиметься в цьому з'єднанні.

Адресі відправника в електронній пошті Інтернету не можна довіряти, тому що відправник може вказати фальшиву зворотну адресу, або заголовок може бути модифікований у ході передачі листа, або відправник може сам з'єднатися з SMTP-портом на машині, від імені якої він хоче відправити лист, і ввести текст листа.

Заголовки й вміст електронних листів передаються в чистому вигляді. У результаті зміст повідомлення може бути прочитаний або змінений у процесі передачі його через Інтернет. Заголовок може бути модифікований, щоб приховати або змінити відправника, або для того, щоб перенаправляти повідомлення.

Поштова бомба — це атака за допомогою електронної пошти. Система, що атакується, переповнюється листами доти, поки вона не вийде з ладу. Як це може спричинитися, залежить від типу поштового сервера і того, як він сконфігурований.

Деякі провайдери Інтернету дають тимчасові логіни кожному для тестування підключення до Інтернету, і ці логіни можуть бути використані для початку подібних атак.

Типові варіанти виходу поштового сервера з ладу:

1. Поштові повідомлення приймаються доти, поки диск, де вони розміщаються, не переповниться. Наступні листи не приймаються. Якщо цей диск є також основним системним диском, то вся система може аварійно вимкнутися.
2. Вхідна черга переповнюється повідомленнями, які потрібно обробити й передати далі, доти, поки не буде досягнутий граничний розмір черги. Наступні повідомлення не потраплять до черги.
3. У деяких поштових систем можна встановити максимальну кількість поштових повідомлень або максимальний загальний розмір повідомлень, які користувач може прийняти за один раз. Наступні повідомлення будуть відкинуті або знищені.
4. Може бути перевищена квота диска для цього користувача. Не буде можливості прийняти наступні листи або виконувати інші дії. Відновлення може виявитися важким для користувача, тому що йому може знадобитися додатковий дисковий простір для видалення листів.
5. Великий розмір поштової скриньки може утруднити для системного адміністратора одержання системних попереджень і повідомлень про помилки.
6. Посилка поштових бомб у список розсилання може призвести до того, що його члени можуть відписатися від списку.

У минулому, коли Інтернет був дослідницькою мережею, його комерційне використання було заборонене. Крім того, занадто мало компаній і людей мали доступ до Інтернет-пошти, тому було недоцільно використовувати її з комерційною метою. Зараз Інтернет розширився й дозволяється використовувати його в комерційних цілях, тому компанії почали підтримувати списки розсилання для обміну інформацією зі своїми клієнтами. Як правило, клієнти повинні надіслати запит для того, щоб потрапити в список розсилання. Коли великі онлайнові сервіси почали шлюзувати листи в Інтернет, несподівано виявилося, що в такий спосіб можна передати інформацію набагато більшій аудиторії. Так народився маркетинг в Інтернеті за допомогою посилання окремих поштових повідомлень.

Через те що будь-яка людина у світі може послати вам лист, не так просто змусити її припинити посилати їх вам. Люди можуть розпізнати вашу адресу зі списку адрес організації, списку осіб, що підписалися на список розсилання, або листів у Usenet. Якщо ви вказали вашу поштову адресу на

якому-небудь веб-сайті, то він може продати вашу адресу «поштовим сміттярам». Деякі веб-браузери самі вказують вашу поштову адресу, коли ви відвідуєте вебсайт, тому ви можете навіть не знати, що ви її дали. Багато поштових систем мають можливості фільтрації пошти, тобто пошуку зазначених слів або словосполучень у заголовку листа або його тілі, і наступного вміщення його в певну поштову скриньку або видалення. Але більшість користувачів не знає, як використовувати механізм фільтрації. Крім того, фільтрація в клієнта відбувається після того, як лист вже отриманий або завантажений, тому утруднюється видалення великих обсягів листів.

Для безпечної атаки може використовуватися анонімний ремайлер. Коли хтось хоче послати образливий або загрозливий лист і при цьому приховати свою особу, він може скористатися анонімним ремейлером. Якщо людина хоче послати електронний лист, не розкриваючи свою домашню адресу тим, хто може загрожу-вати їй, вона може теж використовувати анонімний ремейлер. Якщо вона почне раптом одержувати небажані листи на свою поточну адресу, вона може відмовитися від неї і взяти нову.

Одним із поширених засобів захисту, до якого часто вдаються деякі користувачі Usenet, є конфігурація своїх клієнтів для читання новин у такий спосіб, що в полі Reply-To (зворотна адреса) листа, який посилається ними в групу новин, міститься фальшива адреса, а реальна адреса міститься в сигнатурі або в тілі повідомлення. Тому робота програм збирання поштових адрес, які збирають адреси з поля Reply-To, виявиться марною.

У конгресі США було подано кілька біллів про обмеження на роботу таких програм-сміттярів. В одному пропонувалося створити списки стоп-слів і поміщати слово «реклама» у рядок теми листа. В іншому пропонувалося вважати їх просто незаконними.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Зайдіть під власним акаунтом на одну з соціальних мереж, в якій зареєстровані.
2. Проаналізуйте анкету, яку заповнює кожен учасник даної соціальної мережі.
3. Запишіть до звіту назви полів, з яких складається дана анкета, опишіть які з них можливо приховувати, можливі варіанти доступу до них інших учасників, оцініть степінь безпечності розголошення даної інформації по 5-бальній шкалі. Зробіть в звіті аналіз можливих небезпек в результаті доступу до інформації, яку розміщує учасник даної соціальної мережі.
4. Зробіть аналіз власної анкети з точки зору роботодавця. Яка інформація буде для вас цікавою? Що може вплинути на ваше рішення взяти цю людину до себе на роботу? Висновки запишіть до звіту.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Дайте визначення поняття служби соціальних мереж.
2. Назвіть основні властивості служби соціальних мереж.
3. Охарактеризуйте основні методи викрадення аканту користувача соціальної мережі та засоби захисту від них.
4. Що не варто писати в соціальних мережах?
5. Що таке електронна пошта? Назвіть основні способи втрати інформації під час роботи з даним сервісом.
6. Що називається поштовою бомбою?
7. Назвіть та опишіть типові варіанти виходу поштового сервера з ладу.
8. Опишіть способи боротьби із втратою інформації під час роботи з електронною поштою.
9. Сформулюйте правила під час спілкування в соціальній мережі.
10. Сформулюйте основні правила для користувача електронною поштою.

Лабораторна робота №6

Тема: Управління паролями. Засоби збереження та доступу до паролів. Правила роботи з паролями.

Мета: ознайомитися з поняттям паролю, основними засобами збереження та доступу до паролів, правилами роботи з паролями.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Паролі - це ключі, які відкривають доступ до особистих даних, що зберігаються на комп'ютері та в облікових записах в Інтернеті.

Якщо зловмисники вкрадуть ці дані, вони можуть скористатися ними для відкриття нових рахунків кредитних карт, отримання кредиту або виконання через Інтернет інших дій від вашого імені. Дуже часто ви можете не підозрювати про такі дії до тих пір, поки не стане занадто пізно.

З величезною кількістю системних паролів та сайтів, доступ до яких надається лише зареєстрованим користувачам, неможливо запам'ятати всі пари «ім'я користувача / пароль», якщо тільки ви не використовуєте одні й ті самі ім'я та пароль для всіх облікових записів або не записуєте їх. Обидва ці методи мають зниженим рівнем безпеки.

Той, хто використовує одні й ті ж ім'я користувача та пароль, починаючи електронною поштою і закінчуючи особистими банківськими рахунками, надають повний доступ до власного життя кожному, хто зможе зламати один з використовуваних акаунтів, так як таким чином, зловмисники зможуть використовувати отримані дані для будь-яких інших облікових записів. Отримати доступ до важливої інформації можна через файли cookie, які зберігаються на комп'ютері (це залежить від ступеня уразливості використовуваного браузера), і за допомогою сайтів, які не можуть використовувати протокол http або технологію SSL (відкритий стандарт для створення безпечних каналів підключення, які запобігають витік важливих конфіденційних відомостей, таких як номери кредитних карт). В даному випадку, ваші ім'я користувача та пароль виявляються у відкритому доступі в Інтернеті і можуть бути отримані будь-якою кількістю комп'ютерів.

При записуванні ім'я користувача та пароль на папір завжди існує можливість втратити цей листок, або хто-небудь може знайти його і отримати доступ до ваших акаунтів. Ймовірність такої загрози значно зростає, якщо ви залишаєте листок з даними під клавіатурою, приклеюєте його на монітор, ноутбук або просто залишаєте його на столі. Пароль використовується для забезпечення безпеки комп'ютерних програм, і тому, записуючи його на папір, ви просто видаляєте всяку безпеку. З іншого боку, ім'я користувача та пароль можуть бути легко викрадені, якщо вони надсилаються через Інтернет відкритим текстом, але зазвичай ті користувачі, які записують дані на папір для різних акаунтів, використовують різні паролі. Тому при втраті листка з паролем вони не втратять контроль над усіма обліковими записами.

Одним з кращих способів забезпечити безпеку при відкритті акаунтів є використання різних ім'я користувача та пароль при кожній реєстрації. Запам'ятати їх буває дуже складно (тому часто використовуються методи, описані вище). Все ж існує кращий спосіб збереження паролів - використання інструменту управління паролями. Таким чином, значно спрощується збереження паролів для кожного облікового запису. Іншою важливою перевагою використання менеджера паролів є те, що можна використовувати безпечніші паролі і не боятися забути їх.

Існує безліч менеджерів паролів, доступних в Інтернеті, - деякі платні, інші безкоштовні. Вибір типу програм залежить від користувача.

Менеджер паролів - програмне забезпечення, яке допомагає користувачеві працювати з паролями і PIN-кодами. У подібного програмного забезпечення зазвичай є в наявності місцева база даних або файли, які містять зашифровані дані пароля. Багато менеджерів паролів також працюють як заповнювач форми, тобто вони заповнюють поле користувач і дані пароля автоматично в формах. Зазвичай вони реалізовані як розширення браузера.

Менеджери паролів діляться на три основні категорії:

Десктоп - зберігають паролі до програмного забезпечення, встановленого на жорсткому диску комп'ютера.

Портативні - зберігають паролі до програмного забезпечення на мобільних пристроях, таких як КПК, смартфон або до портативних додатків на USB флеш-накопичувачі.

Мережеві - менеджери паролів онлайн, де паролі збережені на веб-сайтах провайдерів.

Менеджери паролів можуть також використовуватися як захист від фішингу. На відміну від людей, програма менеджер паролів може звертатися з автоматизованим скриптом логіна не сприйнятливі до візуальних імітацій, які схожі на веб-сайти. З цією вбудованою перевагою використання менеджера паролів вигідно, навіть якщо у користувача є всього кілька паролів, які він пам'ятає. Однак не всі менеджери паролів можуть автоматично звертатися з більш складними процедурами ідентифікації, накладеними багатьма банківськими веб-сайтами.

Менеджери паролів зазвичай використовують вибраний користувачем основний пароль, або секретну фразу (passphrase), щоб сформувати ключ, використовуваний для зашифровки збережених паролів. Цей основний пароль повинен бути досить складним, щоб встояти при атаках зловмисників (наприклад повний перебір).

Якщо основний пароль буде зламаний, то будуть розкриті всі збережені в базі даних програми паролі. Це демонструє зворотний зв'язок між зручністю використання і безпекою: єдиний пароль може бути більш зручний, але якщо він буде зламаний, то поставить під загрозу всі збережені паролі.

Основний пароль може також бути атакований і виявлений при використанні кейлоггера або акустичного криптоаналізу (acoustic cryptanalysis). Така загроза може бути знижена шляхом використання віртуальної клавіатури, як, наприклад, в KeePass.

Деякі менеджери паролів включають генератор паролів. Згенеровані паролі можуть бути відгадувати, якщо менеджер пароля не використовує криптографічно безпечний генератор випадкових чисел.

Онлайн менеджер паролів - веб-сайт, який надійно зберігає дані логіна. Таким чином це мережева версія звичайного десктоп-менеджера паролів.

Переваги онлайн менеджерів паролів над десктоп-версіями - це мобільність (вони можуть використовуватися на будь-якому комп'ютері з web-браузером і інтернет-з'єднанням, без необхідності встановлювати програмне забезпечення) і менший ризик втрати паролів через злодійство або пошкодження PC. Ризик пошкодження може бути в значній мірі знижений, якщо заздалегідь будуть створені резервні копії.

Головний недолік онлайн менеджерів паролів - необхідна довіра хостингу сайту. Неодноразові зломи і втрати централізовано збереженої інформації на сервері не вселяють довіри.

Існують змішані рішення. Ряд ресурсів, таких як FortNotes або МоіПаролі, що надають послуги онлайн-зберігання паролів та інших секретних даних, поширюють вихідні коди цих систем. Можливість провести аудит коду та встановити таку систему на захищений фаєрволом сервер або на сервер, що не має прямий вихід в Інтернет, дозволяє вирішити проблему з можливою компрометацією даних.

Використання мережевого менеджера паролів - альтернатива технології єдиного входу (Single Sign On), такий як OpenID або Microsoft's Windows Live ID, і може використовуватися як тимчасова міра, поки не буде прийнятий кращий метод.

Також існує менеджери паролів з бар'єрним захистом. У цьому випадку захищається інтернет-аккаунт користувача в цілому. Периметр захисту будується починаючи від протидії клавіатурним і екранним шпигунам, і закінчуючи захистом від підміни ip-адреси мережевого ресурсу. Прикладом є Keepy Internet Password Security. Для мережевого захисту використовується Google Public DNS, а протидія шпигунам забезпечується автоматичною підстановкою авторизаційних даних в web-форми.

Правила роботи з паролями.

Для зловмисника най надійний пароль виглядає як випадковий набір знаків. Наступні критерії допоможуть в виборі пароля.

Використовуйте якомога більше символів. Кожен додатковий знак збільшує ступінь захисту пароля. Пароль повинен містити не менш 8 знаків; 14 знаків і більше є ідеальним варіантом.

Так як багато систем дозволяють використовувати знак пробілу при створенні пароля, можна скласти пароль з декількох слів - парольний фразу. Такі фрази легше запам'ятати і важче підібрати.

Використовуйте комбінацію з літер, цифр та інших символів. Чим більше різних знаків містить пароль, тим важче його підібрати. Інші важливі відомості:

Чим менше різних символів ви використовуєте, тим довше повинен бути ваш пароль. Пароль з 15 випадково вибраних літер і цифр приблизно в 33 тисячі разів надійніше, ніж пароль з 8 знаків, що містить різні типи наявних на клавіатурі знаків. Якщо немає можливості включити в пароль символи, слід зробити його значно довше, щоб забезпечити ту ж ступінь захисту. Ідеальний пароль поєднує в собі довжину і різноманітність знаків.

Використовуйте всі символи клавіатури, А не тільки часто використовувані. Цифри і символи, що вводяться за допомогою клавіші Shift, також часто використовуються при створенні паролів. Пароль буде надійніше, якщо ви використовуєте всі наявні на клавіатурі символи, включаючи знаки пунктуації, розташовані не в верхньому ряду клавіатури, і символи, характерні тільки для вашої мови.

Використовуйте слова і фрази, легкі для запам'ятовування, але не очевидні для зловмисників. Найпростіше запам'ятати паролі і парольні фрази, записавши їх. Всупереч загальноприйнятій думці, немає нічого страшного в записі пароля, якщо дані при цьому захищені належним чином.

Паролі, записані на папері, звичайно важче зламати через Інтернет, ніж паролі, що зберігаються в диспетчері паролів, на веб-сайті або в іншій програмі для зберігання даних.

Шість етапів створення надійного пароля що легко запам’ятовується

1. Придумайте речення, яке точно не забудете, Ця пропозиція і буде основою для надійного пароля або парольного фрази. Пропозиція повинна бути незабутнім (наприклад, "Моєму синові Павлу три роки").
2. Переконайтеся, що обрана вами система перевірки пароля допускає використання ідентифікаційних фраз. Якщо є можливість використовувати парольну фрази (з пробілами між знаками), скористайтеся нею.
3. Якщо використання ідентифікаційних фраз недопустимо в даній системі, скористайтеся звичайним паролем. Складіть нове безглузде слово з перших букв усіх слів, що входять до створеного пропозицію. У нашому прикладі вийде: "мсптг".
4. Ускладните комбінацію, Використовуючи великі літери, малі літери і цифри. Можна поміняти місцями букви в слові або навмисно допустити орфографічні помилки. Наприклад, в парольного фразі, наведеній вище, можна допустити помилку в імені або замінити слово "три" на цифру 3. Є безліч можливих підстановок, і чим довше пропозицію, тим більш надійним буде пароль. Наш приклад можна перетворити так: "Моєму синові Па8лУ 3 року". Якщо комп'ютер або система не підтримують парольні фрази, той же метод можна застосувати і до простого паролю. Наприклад, "мСп3Г".
5. Нарешті, замініть окремі символи. Можна використовувати знаки, схожі на літери, об'єднувати слова (видаляючи пробіл між ними) і т. п. Дотримуючись нашого прикладу, ми отримуємо: "Моєму $ иНуП @ в8лУ 3 року" або "м $ п3Г!".
6. Перевірте свій новий пароль за допомогою програми перевірки паролів. Програма перевірки паролів на цьому веб-сайті визначить надійність вибраного пароля, як тільки ви його введете і не збережете при цьому.

Методи створення пароля, які не слід використовувати.

Вище ми розглянули як створити надійний пароль. Тепер розглянемо те, що не потрібно робити при підборі надійних паролів. Існують загальноприйняті методи, про які можуть знати і зловмисники. Щоб уникнути створення ненадійного пароля: не використовуйте послідовні комбінації і повторювані символи. Такі поєднання (наприклад, "12345678", "222222", "abcdefg" або поєднання сусідніх букв на клавіатурі) не є надійними паролями.

Уникайте використання тільки замін схожих цифр і символів. Злочинців та інших зловмисників, що володіють достатніми знаннями для підбору і злому пароля, не вдасться ввести в оману подібними замінами, наприклад "і" на "1" або "а" на "@" в словах "M1cr0 $ 0ft" або "П @ р0ль ". Однак не варто нехтувати такими замінами в поєднанні з іншими методами підвищення надійності пароля, такими як збільшення довжини, неправильне написання, використання великих і малих букв.

Не застосовуйте своє ім'я користувача в якості пароля. Уникайте також використання інших особистих даних (своїх або своїх близьких), таких як ім'я, дата народження, код соціального страхування і т. д. Ці відомості використовуються зловмисниками в першу чергу.

Уникайте словникових слів на будь-якій мові. Зловмисники володіють досконалими засобами, що дозволяють швидко підібрати паролі, в основі яких лежать слова з різних мов; слова, написані задом наперед; поширені орфографічні помилки і заміни, а також всі види лайки та інших слів, які не вимовляють при дітях.

Використовуйте кілька паролів. При зломі одного комп'ютера або системи, де використовується певний пароль, небезпеки піддаються всі інші дані, захищені тим же паролем. Настійно рекомендується використовувати різні паролі для різних систем.

Не зберігайте пароль в Інтернеті. Зловмисник, який отримав доступ до вашого паролю в Інтернеті або в комп'ютерній мережі, отримує доступ до всіх даних.

Використання порожнього пароля

Порожній пароль (відсутність пароля) більш ефективний, ніж ненадійний, такий як, наприклад, "1234". Простий пароль легко розгадати, але на комп'ютерах з Windows XP до облікового запису, не захищеної паролем, не можна отримати доступ через локальну мережу або Інтернет (недоступна в ОС Microsoft Windows 2000, Windows Me і в більш ранніх версіях). Порожній пароль для облікового запису на комп'ютері можна використовувати, якщо виконані перераховані нижче вимоги.

У вас один або кілька комп'ютерів, але вам не потрібен доступ з одного комп'ютера на інший.

Ваш комп'ютер фізично захищений (ви довіряєте всім, хто має доступ до вашого комп'ютера).

Не завжди рекомендується використовувати порожній пароль. Наприклад, переносний комп'ютер швидше за все фізично не захищений, і на ньому краще використовувати самий надійний пароль.

Облікові записи в Інтернеті

Веб-сайти мають різні політики, що регулюють доступ до облікового запису і зміна пароля. На домашній сторінці веб-сайту знайдіть посилання (наприклад "Рахунок"), що служить для переходу на сторінку веб-сайту, де виконується управління паролем і обліковим записом.

Паролі на комп'ютері

Відомості про створення і зміну облікових записів, захищених паролями, а також про доступ до них і про те, як встановити захист паролем при завантаженні комп'ютера, зазвичай маються на файлах довідки операційної системи. Можна також спробувати знайти ці відомості на веб-сайті виробника програмного забезпечення. Наприклад, в ОС Microsoft Windows XP відомості про управлінні паролями, їх зміну і т. д. можна знайти в системі інтерактивної довідки.

Зберігання паролів в секреті

Ставтеся до паролів та парольним фразам так само серйозно, як до даних, які вони захищають.

Нікому не повідомляйте пароль. Тримайте пароль в секреті від своїх близьких (особливо від дітей) та друзів, які можуть повідомити його кому-небудь ще. Винятком є паролі, які необхідно знати вашим близьким, наприклад пароль до вашого банківського рахунку в Інтернеті, який можна повідомити дружині або чоловікові.

Ніколи не пересилайте пароль по електронній пошті. Будь-яке повідомлення електронної пошти, що містить запит пароля або вимагає перейти на веб-сайт для підтвердження пароля, майже напевно є шахрайським. Це відноситься і до повідомлень такого типу, отриманим від надійної компанії або людини. Повідомлення електронної пошти може бути перехоплено, а відправник запиту може бути зовсім не тим, за кого себе видає. В фішинг-аферах використовуються шахрайські повідомлення

електронної пошти, обманним шляхом змушують розкрити ім'я користувача та пароль і дозволяють зловмисникам заволодіти ідентифікаційними даними і т. п. Додаткові відомості про фішинг-аферах і про захист від шахрайства в Інтернеті.

Регулярно змінюйте паролі. Це допоможе ввести зловмисників в оману. Чим надійніше пароль, тим довше можна його використовувати.

Пароль з 8 знаків-менш можна застосовувати протягом тижня, у той час як поєднання з 14 і більше знаків може служити кілька років, якщо воно складено за всіма правилами, наведеними вище.

Не вводьте паролі на чужих комп'ютерах. Комп'ютери в інтернет-кафе і лабораторіях, системи загального доступу, інтерактивні термінали, а також комп'ютери на конференціях і в залах очікування аеропортів не можуть вважатися безпечними і підходять тільки анонімного виходу в Інтернет. Не користуйтеся такими комп'ютерами для перевірки електронної пошти, банківського рахунку, доступу в віртуальні кімнати для розмов і доступу до інших облікових записів, де запитується ім'я користувача та пароль. Зловмисники застосовують недорогі і швидко встановлюються пристрої, що записують послідовність натиснень на клавіші. Такі пристрої дозволяють шахраям отримувати через Інтернет всі дані, введені в комп'ютер. Пам'ятайте, що ваші паролі і парольні фрази так само важливі, як і дані, які вони захищають.

Дії у разі викрадення пароля

Відстежуйте всі дані, захищені паролями: фінансові звіти за місяць, звіти про кредитні операції, дані про покупки через Інтернет і т. д. Надійні, легко запам'ятовуються паролі допомагають захиститися від шахрайства і розкрадання ідентифікаційних даних, але не є абсолютною гарантією захисту. Незалежно від того, наскільки надійним є пароль, якщо шахраям вдасться зламати систему, де він зберігається, вони його дізнаються. Якщо ви помітили підозрілі дії, які можуть означати, що хтось отримав доступ до ваших даних, як можна швидше повідомте про це у відповідні органи. Додаткові відомості про діях в разі викрадення ідентифікаційних даних або подібного шахрайства.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

(*Всі кроки виконання занотуйте до звіту у вигляді скріншотів*)

Завдання 1.

1. Запустіть браузер Інтернет (Це може бути Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera чи будь-який інший, що встановлений на вашому комп’ютері).
2. Відвідайте ресурс http://fortnotes.com/.
3. Створіть власний акаунт.
4. Проаналізуйте можливості даної служби.
5. Створіть кілька паролів електронної пошти, бази даних, сайтів.
6. Перегляньте створені записи.

Завдання 2.

1. Запустіть браузер Інтернет (Це може бути Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera чи будь-який інший, що встановлений на вашому комп’ютері).
2. Відвідайте ресурс http://websecurity.com.ua/password/
3. Ознайомтесь з можливостями та призначенням ресурсу.
4. Введіть власні паролі в поле для діагностики рівня їх надійності. Запишіть в звіт результати.
5. Створіть 10 нових паролів (не користуючись відповідним сервісом) з різним рівнем надійності. Запишіть їх та висновки до звіту.
6. Скористуйтеся сервісом створення паролю. Створіть таким чином та запишіть до звіту 7 паролів.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається паролем?
2. Яке програмне забезпечення називається менеджером паролів?
3. На які категорії діляться менеджери паролів.
4. Який принцип роботи менеджерів паролів?

5. Що називається онлайн менеджером паролів?
6. Назвіть основні переваги та недоліки онлайн менеджерів паролів.
7. Що являють собою менеджери паролів з бар’єрним захистом?
8. Назвіть правила створення та користування паролями.
9. Назвіть етапи створення надійного паролю.
10. Які програми управління паролями ви знаєте? Опишіть їх основні можливості.

Лабораторна робота №7

Тема: Поняття шкідливого програмного забезпечення. Основні типи та загальний огляд сучасних комп’ютерних вірусів.

Мета: отримати навички виявлення на комп'ютері шкідливих програм, вивчити основні методи по усуненню наслідків вірусних атак без використання антивірусного програмного забезпечення.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Вірус - програма, здатна створювати свої копії (необов'язково співпадаючі з оригіналом) і впроваджувати їх у файли, системні області комп'ютера, комп'ютерних мереж, а також здійснювати інші деструктивні дії. При цьому копії зберігають здатність подальшого поширення. Комп'ютерний вірус відноситься до шкідливим програмам.

Ще одна проблема, пов'язана з визначенням комп'ютерного вірусу криється в тому, що сьогодні під вірусом найчастіше розуміється не "традиційний" вірус, а практично будь-яка шкідлива програма. Це призводить до плутанини в термінології, ускладненої ще й тим, що сьогодні практично будь антивірус здатний виявляти всі типи шкідливих програм, таким чином асоціація "шкідлива програма-вірус" стає все більш стійкою.

Шкідлива програма - комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в комп'ютерній системі (КС), або для прихованого нецільового використання ресурсів КС, або іншого впливу, що перешкоджає нормальному функціонуванню КС. До шкідливим програмам ставляться комп'ютерні віруси, трояни, мережні хробаки і інші.

Віруси

До вірусів відносяться:

– ***Завантажувальні віруси*** - віруси, що заражають завантажувальні сектори постійних і змінних носіїв;

– ***Файлові віруси*** - віруси, що заражають файли;

– ***Макровіруси*** - віруси, написані мовою макрокоманд і виконують у середовищі якого-небудь додатка. У переважній більшості випадків мова йде про макроси в документах Microsoft Office;

– ***Скрипт-віруси*** - віруси, що виконуються у середовищі певної командної оболонки: раніше - bat-файли в командній оболонці DOS, зараз частіше VBS-і Java-скрипти в командній оболонці Windows Scripting Host (WSH);

Окремо варто сказати пару слів про макровіруси. Більшість електронних документів створюються й обробляються у форматі MS Office, інструмент VBA (Visual Basic for Application), який можна використовувати для створення макровірусів поставляється разом з додатком MS Office. Такий стан речей призводить до того, що на сьогоднішній день макровіруси - найбільш розповсюджений тип вірусів. Однак боротьба з ними не викликає особливих проблем і зводиться до вивчення тіла шкідливого макросу за допомогою того ж VBA на предмет виконуваних операцій, контролю стартових макросів AutoOpen, AutoClose, AutoSave, глобальних макросів FileOpen, FileSaveAs, FileSave, FileClose і ряду стандартних операцій, таких як виклик API-функцій, виконання команд Shell і т. д. Процедура лікування макровірусів зводиться до видалення тіла макросу з документів і шаблонів MS Office.

Мережеві черв'яки

Черв'як (мережний черв'як) - тип шкідливих програм, що поширюються по мережних каналах, здатних до автономного подолання систем захисту автоматизованих і комп'ютерних систем, а також до створення й подальшого поширення своїх копій,

У залежності від шляхів проникнення в операційну систему чирви діляться на:

– *Поштові черв'яки* (Mail-Worm) - черв'яки, що поширюються у форматі повідомлень електронної пошти;

– *IM черв'яки* (IM-Worm) - черв'яки, що використовують Інтернет-пейджери;

– *P2P черв'яки* (P2P-Worm) - черв'яки, що розповсюджується за допомогою пірінгових (peer-to-peer) файлообмінних мереж;

– *Мережеві черв'яки* (Net-Worm) - інші мережеві черв'яки, серед яких має сенс додатково виділити Інтернет-хробаки і LAN-черв'яки.

Інтернет черв'яки - черв'яки, що використовують для поширення протоколи Інтернет. Переважно цей тип черв'яків поширюється з використанням неправильної обробки деякими додатками базових пакетів стека протоколів TCP / IP.

LAN черв'яки - черв'яки, що поширюються по протоколах локальних мереж.

Трояни

– ***Троян*** (троянський кінь) - тип шкідливих програм, основною метою яких є шкідливий вплив стосовно комп'ютерної системи. Трояни відрізняються відсутністю механізму створення власних копій.

– Деякі трояни здатні до автономного подолання систем захисту КС, з метою проникнення й зараження системи. У загальному випадку, троян попадає в систему разом з вірусом або хробаком, у результаті необачних дій користувача або ж активних дій зловмисника. Найбільш поширені наступні види троянів:

– ***Клавіатурні шпигуни*** (Trojan-SPY) - трояни, що постійно перебувають у пам'яті і зберігають всі дані, що надходять від клавіатури з метою наступної передачі цих даних зловмисникові. Зазвичай в такий спосіб зловмисник намагається довідатися паролі або іншу конфіденційну інформацію.

– ***Викрадачі паролів*** (Trojan-PSW) - трояни, також призначені для одержання паролів, але не використають спостереження за клавіатурою. Зазвичай в таких троянах реалізовані способи добування паролів з файлів, в яких ці паролі зберігаються різними додатками.

– ***Утиліти віддаленого керування*** (Backdoor) - трояни, що забезпечують повний віддалений контроль над комп'ютером користувача. Існують легальні утиліти такої ж властивості, але вони відрізняються тим, що повідомляють про своє призначення при установці або ж постачаються з документацією, у якій описані їхні функції. Троянські утиліти вилученого керування ніяк не видають свого реального призначення, так що користувач і не підозрює про те, що його комп'ютер підконтрольний зловмисникові. Найбільш популярна утиліта віддаленого управління - Back Orifice.

– ***Анонімні smtp-сервери й проксі*** (Trojan-Proxy) - трояни, що виконують функції поштових серверів або проксі й, що використаються в першому випадку для спам-розсилок, а в другому для замітання слідів хакерами.

– ***Модифікатори настроювань браузера*** (Trojan-Cliker) - трояни, які міняють стартову сторінку в браузері, сторінку пошуку або ще які-небудь настроювання, для організації несанкціонованих звертань до Інтернет-ресурсів.

– ***Інсталятори інших шкідливих програм*** (Trojan-Dropper) - трояни, що представляють можливість зловмисникові здійснювати приховану установку інших програм.

– ***Завантажувачі шкідливих програм*** (Trojan Downloader) - трояни, призначені для завантаження на комп'ютер-жертву нових версій шкідливих програм, або рекламних систем.

– ***Повідомлювачі про успішну атаку*** (Trojan-Notifier) - трояни даного типу призначені для повідомлення своєму "господарю" про зараження комп'ютеру.

– ***"Бомби" в архівах*** (ARCBomb) - трояни, що представляють собою архіви, спеціально оформлені таким чином, щоб викликати нештатну поведінку архіваторів при спробі розархівувати дані - зависання або істотне уповільнення роботи комп'ютера, заповнення диска великою кількістю "порожніх" даних.

– ***Логічні бомби*** - частіше не стільки трояни, скільки троянські складові черв'яків і вірусів, суть роботи яких полягає в тому, щоб за певних умов (дата, час доби, дії користувача, команда ззовні) зробити певну дію: наприклад, знищення даних.

– ***Утиліти дозвону*** - порівняно новий тип троянів, що представляє собою утиліти dial-up доступу в Інтернет через платні поштові служби. Такі трояни прописуються в системі як утиліти дозвону за замовчуванням і спричиняють за собою великі рахунки за користування Інтернетом.

Життєвий цикл шкідливих програм

Процес розмноження вірусів може бути умовно розділений на кілька стадій:

- Активація вірусу.
- Пошук об'єктів для зараження.
- Підготовка вірусних копій.
- Впровадження вірусних копій.

Так само як для вірусів, життєвий цикл хробаків можна розділити на певні стадії:

- Проникнення в систему.
- Активація.
- Пошук "жертв".
- Підготовка копій.
- Поширення копій.

У троянів внаслідок відсутності функцій розмноження й поширення, їхній життєвий цикл менше ніж у вірусів - усього три стадії:

- Проникнення на комп'ютер.
- Активація.
- Виконання закладених функцій.

Це, само собою, не означає малого часу життя троянів. Навпаки, троян може непомітно перебувати в пам'яті комп'ютера тривалий час, ніяк не видаючи своєї присутності, до тих пір, поки не виконає свою шкідливу функцію.

Основні шляхи проникнення в систему і активації

Існує твердження - будь-яку шкідливу програму користувач може перемогти самостійно, тобто не вдаючись до використання антивірусних програм. Це дійсно так, за успішними діями будь-якої антивірусної програми стоїть праця вірусних аналітиків, які вручну розбираються з алгоритмами роботи нових вірусів, виділяють сигнатури, описують алгоритм роботи вірусу.

Сигнатура вірусу - в широкому сенсі, інформація, що дозволяє однозначно визначити наявність даного вірусу у файлі або іншому коді.

Прикладами сигнатур є: унікальна послідовність байт, присутня в даному вірусі і не зустрічається в інших програмах; контрольна сума такої послідовності

Таким чином, антивірусну програму можна розглядати як засіб автоматизації боротьби з вірусами. Слід зауважити, що аналіз вірусів потребує від користувача володіння більшим обсягом специфічних знань в області програмування, роботи операційних систем і т.д. Сучасні шкідливі програми використовують складні технології маскування і захисту своїх копій, які обумовлюють необхідність застосування спеціальних засобів для їх аналізу.

Процес підготовки шкідливою програмою своїх копій для поширення може істотно відрізнятися від простого копіювання. Автори найбільш складних у технологічному плані вірусів

намагаються зробити різні копії максимально несхожими для ускладнення їх виявлення антивірусними засобами. Як наслідок, складання сигнатури для такого вірусу вкрай ускладнено.

При створенні копій для маскування можуть застосовуватися наступні технології:

Шифрування - вірус складається із двох функціональних блоків: власне вірусу і шифратора. Кожна копія вірусу складається із шифратора, випадкового ключа й вірусного блоку, зашифрованого цим ключем

Метаморфізм - створення різних копій вірусу шляхом заміни груп команд на еквівалентні, перестановки місцями блоків коду, вставки між значущими шматками коду "сміттєвих" команд, які практично нічого не роблять.

Поєднання цих двох технологій приводить до появи наступних типів вірусів.

Шифрований вірус - вірус, що використає просте шифрування з випадковим ключем і незмінний шифратор. Такі віруси легко виявляються по сигнатурі шифратора.

Метаморфний вірус - вірус, що застосовує метаморфізм до всього свого тіла для створення нових копій.

Поліморфний вірус - вірус, що використає метаморфний шифратор для шифрування основного тіла вірусу з випадковим ключем. При цьому частина інформації, використовуваної для одержання нових копій шифратора також може бути зашифрована. Наприклад, вірус може реалізовувати кілька алгоритмів шифрування і при створенні нової копії міняти не тільки команди шифратора, але і сам алгоритм

Розглядаючи сучасні вірусні загрози необхідно відзначити, що більше 90% відсотків вірусних погроз останнім часом пов'язані з хробаками. Найбільш численну групу в цьому класі шкідливих програм становлять поштові черв'яки. Інтернет-черв'яки також є помітним явищем, але не стільки через кількість, скільки через якість: епідемії, викликані Інтернет-хробаками найчастіше відрізняються високою швидкістю розповсюдження і великими масштабами. IRC і P2P черв'яки зустрічаються досить рідко, частіше IRC та P2P служать альтернативними каналами поширення для поштових і Інтернет-черв'яків. Поширення через LAN також використовується переважно як додатковий спосіб поширення.

Крім того, на етапі активації хробаків можна розділити на дві великі групи, що відрізняються як за технологіями активації, так і по тривалістю життя:

Для активації необхідно активна участь користувача.

Для активації участь користувача не потрібна зовсім або досить лише пасивної участі.

Активація мережного хробака без участі користувача завжди означає, що хробак використовує пролом в безпеці програмного забезпеченні комп'ютера. Це призводить до дуже швидкого поширення хробака у середині корпоративної мережі з більшим числом станцій, істотно збільшує завантаження каналів зв'язку і може повністю паралізувати мережу. Саме цей метод активації використали черв'яки Lovesan і Sasser. Під пасивною участю користувача розуміється, наприклад, перегляд листів у поштовому клієнті, при якому користувач не відкриває вкладені файли, але його комп'ютер тим не менше виявляється зараженим.

Активна участь користувача в активації хробака означає, що користувач був уведений в оману методами соціальної інженерії. У більшості випадків основним фактором служить форма подачі інфікованого повідомлення: воно може імітувати лист від знайомої людини (включаючи електронну адресу, якщо знайомий уже заражений), службове повідомлення від поштової системи або ж що-небудь подібне, настільки ж часто зустрічається в потоці звичайної кореспонденції.

При зараженні комп'ютера хробаки зазвичай виробляють наступні дії:

Створюють виконуваний файл з розширенням .exe з довільним ім'ям або ім'ям дуже схожим на ім'я системних файлів Windows. У деяких черв'яках можуть використовуватися технології притаманні вірусам, в такому випадку черв'яки інфікують вже існуючий файл програми (наприклад WSOCK32.DLL) або замінюють його на свій файл (наприклад I-Worm.MTX записує одну зі своїх процедур в файл WSOCK32.DLL таким чином, що вона перехоплює відсилання даних в Інтернет

(процедура send). Внаслідок черв'як в зараженій бібліотеці WSOCK32.DLL отримував управління кожен раз, коли дані відправляються в Інтернет).

Крім цього, разом з додаванням в систему виконуваних файлів, в ряді випадків черв'яки поміщають в систему файли бібліотек, які зазвичай виконують функції Backdoor компонентів (наприклад один з клонів хробака MyDoom - I-Worm.Mydoom.aa створював системному каталозі Windows файл tcp5424.dll , що є Backdoor-компонентом і реєстрував його в системному реєстрі: HKCR \ CLSID \ {E6FB5E20-DE35-11CF-9C87-00AA005127ED} \ InProcServer32 {Default} = "% SysDir% \ tcp5424.dll").

Шкідлива програма може вносити зміни в системні файли win.ini і system.ini. Наприклад Email-Worm.Win32.Toil при установці в заражаємо системі копіює себе в папку Windows з випадковим ім'ям і записує у файл system.ini наступні значення:

[Boot]

shell = Explorer.exe% ім'я хробака%

що забезпечує йому автозапуск при кожному перезавантаженні Windows (але тільки під Win9x/Me).

Email-Worm.Win32.Atak.h в процесі інсталяції копіює себе з ім'ям dec25.exe в системний каталог Windows і модифікує файл win.ini для свого подальшого запуску - додає повний шлях до файлу dec25.exe в ключ run секції [windows]:

[Windows]

run =% SystemDir% \ dec25.exe)

Слід так само відзначити, що у файлі system.ini крім секції [boot] шкідливі програми можуть використовувати секцію [Drivers].

Шкідливі програми можуть вносити зміни в наступні гілки реєстру:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion в ключі Run, RunOnce, RunOnceEx, RunServices, RunServicesOnce - для того щоб система запускала створені хробаком файли.

HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion в ключ Run.

Наприклад, Email-Worm.Win32.Bagle.ax після запуску копіює себе в системний каталог Windows, після чого реєструє в реєстрі скопійований файл: HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Run "Sysformat" = "% System% \ sysformat. exe

HKEY_CLASSES_ROOT \ exefile \ shell \ open \ command

Крім вище перерахованих гілок і ключів реєстру шкідливі програми можуть вносити зміни і в інші гілки і ключі реєстру, наприклад:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ WOW \ boot

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Drivers32

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows NT \ CurrentVersion \ WinLogon

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Active Setup \ Installed Components

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ AeDebug.

Усунення наслідків зараження

У зв'язку з тим що, що черв'яки практично не використовують технології шифрування і метаморфізму для маскування своїх копій, боротьба з ним вручну дещо спрощується і зводиться до наступного алгоритму дій:

1. Аналіз і виявлення за допомогою Диспетчера завдань Windows підозрілих процесів;
2. Аналіз відкритих портів за допомогою команди Netstat;
3. Вивантаження підозрілих процесів;
4. Аналіз реєстру за допомогою утиліти Regedit.exe в вище перерахованих гілках і ключах;

5. Відновлення та правка ключів реєстру;
6. Пошук інфікованих файлів по імені на основі даних аналізу процесів операційної системи і даних аналізу реєстру;
7. Видалення або заміна інфікованих файлів;
8. Перевантаження системи;
9. Контрольний аналіз процесів, ключів реєстру, відкритих портів.

Якщо підозрілих процесів не виявлено, ключі реєстру не змінилися, значить, процедуру дезинфекції комп'ютера можна вважати успішною, в іншому випадку алгоритм доведеться повторити.

Тим не менше, враховуючи той факт, що сучасні хробаки можуть використовувати технології притаманні вірусам, встановлювати backdoor-компоненти, ускладнюючи тим самим, процедуру аналізу та виявлення своїх файлів, для повної впевненості комп'ютер після дезінфекції вручну настійно рекомендується здійснити перевірку антивірусним засобом. Слід також зазначити, що боротися вручну з шкідливими програмами можна тільки постфактум - після того, як вони вразили комп'ютер, в той же час використання антивірусного програмного забезпечення в переважній більшості випадків не допустить активації шкідливої програми на комп'ютері

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Запустіть Диспетчер завдань Windows і проаналізуйте список запущених процесів, навантаження, яку вони надають на ЦП. Запишіть в звіт лабораторної роботи назву підозрілих процесів. Поясніть, на підставі чого були зроблені такі висновки.
2. Використовуючи Диспетчер завдань Windows вивантажити підозрілі процеси.
3. Запустіть інтерфейс командного рядка Windows. Ознайомтеся з ключами команди netstat. Отримайте статистку поточних мережевих підключень Вашого комп'ютера з параметрами відображення всіх підключень і чекаючих портів, відображення послідовності компонентів, що беруть участь у створенні підключення, відображення виконуваного файлу, який бере участь у створенні кожного підключення. Збережіть статистику в файл з назвою netstat.log. Запишіть протокол лабораторної роботи формат команди для цієї дії. Проаналізує дані netstat.log. Запишіть в протокол лабораторної роботи підозрілі відкриті порти і програми що їх використовують. Поясніть, на підставі чого були зроблені такі висновки.
4. Запустіть утиліту роботи з реєстром Windows. Проаналізуйте вміст перерахованих в теоретичній частині гілок і ключів реєстру.
5. При необхідності внесіть зміни в параметри ключів з метою видалення підозрілих записів, створені шкідливою програмою. Запишіть в протокол лабораторної роботи всі внесені зміни.
6. Проаналізуйте зміст файлу win.ini на предмет підозрілих записів. При необхідності внесіть корективи в файл win.ini. Запишіть в протокол лабораторної роботи внесені коректування.
7. Проаналізуйте файл system.ini на предмет підозрілих записів. При необхідності внесіть корективи в файл system.ini. Запишіть в протокол лабораторної роботи внесені коректування.
8. Використовуючи стандартні засоби пошуку, знайдіть файли, які породжували підозрілі процеси і видаліть їх. Запишіть в протокол лабораторної роботи імена цих файлів.
9. Перезавантажте комп'ютер, виконайте пункти 1-6, щоб переконатися, що видалення шкідливої програми пройшло успішно, в оперативній пам'яті немає підозрілих процесів, ключі реєстру не змінилися, на комп'ютері відсутні підозріло відкриті порти.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається комп’ютерним вірусом?
2. Які існують основні групи вірусів?
3. Опишіть основні типи мережевих черв’яків.
4. Опишіть основні типи троянів.
5. Зробіть аналіз життєвого циклу шкідливих програм.
6. Які існують способи проникнення шкідливої програми на персональний комп’ютер?

7. Назвіть основні ознаки враження вірусом.

8. Поясніть у чому різниця між шифрованим і поліморфним вірусом?

9. Чи достатньо для захисту від зараження шкідливою програмою встановити файлам дозвіл тільки для читання? Обґрунтуйте відповідь.

10. Поясніть у чому відмінність понять вірус і шкідлива програма.

Лабораторна робота №8

Тема: Поняття антивірусної програми. Огляд найпоширеніших антивірусних програм та їх класифікація.

Мета: ознайомитися з поняттям антивірусної програми, розглянути методи антивірусного захисту, зробити огляд найпоширеніших антивірусних програм, їх структури та основних функцій.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Антивірусна програма (антивірус) — програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом.

Перші, найпростіші антивірусні програми з'явилися майже одразу після появи вірусів. Зараз розробкою антивірусів займаються великі компанії. Як і в творців вірусів, у цій сфері також сформувались оригінальні засоби — але вже для пошуку і боротьби з вірусами. Сучасні антивірусні програми можуть знаходити десятки тисяч вірусів.

Антивірусне програмне забезпечення складається з комп'ютерних програм, які намагаються знайти, запобігти розмноженню і видалити комп'ютерні віруси та інші шкідливі програми.

З усіх методів антивірусного захисту можна виділити дві основні групи:

- ***Сигнатурні методи*** - точні методи виявлення вірусів, засновані на порівнянні файлу з відомими зразками вірусів
- ***Евристичні методи*** - приблизні методи виявлення, які дозволяють з певною вірогідністю припустити, що файл заражений.

Слово сигнатура в даному випадку є калькою на англійське signature, що означає "підпис" або ж у переносному розумінні "характерна межа, щось ідентифікуюча". Власне, цим все сказано. Сигнатурний аналіз полягає у виявленні характерних ідентифікуючих рис кожного вірусу і пошуку вірусів шляхом порівняння файлів з виявленими рисами.

Сигнатурою вірусу вважатиметься сукупність рис, що дозволяють однозначно ідентифікувати наявність вірусу у файлі (включаючи випадки, коли файл цілком є вірусом). Всі разом сигнатури відомих вірусів складають антивірусну базу.

Задачу виділення сигнатур, як правило, вирішують люди - експерти в області комп'ютерної вірусології, здатні виділити код вірусу з коду програми і сформулювати його характерні риси у формі, найбільш зручній для пошуку. Як правило - тому що в найбільш простих випадках можуть застосовуватися спеціальні автоматизовані засоби виділення сигнатур. Наприклад, у разі нескладних по структурі троянів або черв'яків, які не заражають інші програми, а цілком є шкідливими програмами.

Практично в кожній компанії, що випускає антивіруси, є своя група експертів, що виконує аналіз нових вірусів і поповнює антивірусну базу новими сигнатурами. З цієї причини антивірусні бази в різних антивірусах відрізняються. Проте, між антивірусними компаніями існує домовленість про обмін зразками вірусів, а значить рано чи пізно сигнатура нового вірусу потрапляє в антивірусні бази практично всіх антивірусів. Кращим же антивірусом буде той, для якого сигнатура нового вірусу була випущена раніше всіх.

Одна з поширених помилок щодо сигнатур полягає в тому,що кожна сигнатура відповідає рівно одному вірусу або шкідливій програмі. І як наслідок, антивірусна база з великою кількістю сигнатур дозволяє виявляти більше вірусів. Насправді це не так. Дуже часто для виявлення сімейства схожих вірусів використовується одна сигнатура, і тому вважати, що кількість сигнатур рівна кількості вірусів, що виявляються, вже не можна.

Співвідношення кількості сигнатур і кількості відомих вірусів для кожної антивірусної бази своє і цілком може опинитися, що база з меншою кількістю сигнатур насправді містить інформацію про більшу кількість вірусів. Якщо ж пригадати, що антивірусні компанії обмінюються зразками вірусів, можна з високою часткою упевненості вважати, що антивірусні бази найбільш відомих антивірусів еквівалентні.

Важлива додаткова властивість сигнатур - точне і гарантоване визначення типу вірусу. Ця властивість дозволяє занести в базу не тільки самі сигнатури, але і способи лікування вірусу. Якби сигнатурний аналіз давав тільки відповідь на питання, є вірус чи ні, але не давав би відповіді, що це за вірус, очевидно, лікування було б не можливе - дуже великим був би ризик зробити не ті дії і замість лікування отримати додаткові втрати інформації.

Інша важлива, але вже негативна властивість - для отримання сигнатури необхідно мати зразок вірусу. Отже, сигнатурний метод непридатний для захисту від нових вірусів, оскільки до тих пір, поки вірус не потрапив на аналіз до експертів, створити його сигнатуру неможливо. Саме тому всі найбільш крупні епідемії викликаються новими вірусами. З моменту появи вірусу в мережі Інтернет до випуску перших сигнатур зазвичай проходить декілька годин, і весь цей час вірус здатний заражати комп'ютери майже безперешкодно. Майже - тому що в захисті від нових вірусів допомагають додаткові засоби захисту, розглянуті раніше, а також евристичні методи, використовувані в антивірусних програмах.

Якщо сигнатурний метод заснований на виділенні характерних ознак вірусу і пошуку цих ознак у файлах, що перевіряються, то евристичний аналіз ґрунтується на (вельми правдоподібному) припущенні, що нові віруси часто виявляються схожі на які-небудь з вже відомих. Постфактум таке припущення виправдовується наявністю в антивірусних базах сигнатур для визначення не одного, а відразу декількох вірусів. Заснований на такому припущенні евристичний метод полягає в пошуку файлів, які не повністю, але дуже близько відповідають сигнатурам відомих вірусів.

Позитивним ефектом від використання цього методу є можливість виявити нові віруси ще до того, як для них будуть виділені сигнатури. Негативні сторони:

- Вірогідність помилково визначити наявність у файлі вірусу, коли насправді файл чистий - такі події називаються помилковими спрацьовуваннями.
- Неможливість лікування - і через можливі помилкові спрацьовування, і через можливе неточне визначення типу вірусу, спроба лікування може привести до більших втрат інформації, чим сам вірус, а це неприпустимо.
- Низька ефективність - проти дійсно новаторських вірусів, що викликають найбільш масштабні епідемії, цей вид евристичного аналізу малопридатний.

Інший метод, заснований на евристиці, виходить з припущення, що шкідливі програми так чи інакше прагнуть завдати шкоди комп'ютеру. Метод заснований на виділенні основних шкідливих дій, таких як, наприклад:

- Видалення файлу
- Запис у файл
- Запис в певні області системного реєстру
- Відкриття порту на прослуховування
- Перехоплення даних що вводяться з клавіатури
- Розсилка листів та ін.

Зрозуміло, що виконання кожної такої дії окремо не є приводом рахувати програму шкідливою. Але якщо програма послідовно виконує декілька таких дій, наприклад, записує запуск себе ж в ключ автозапуску системного реєстру, перехоплює дані, що вводяться з клавіатури і з певною частотою пересилає ці дані на якусь адресу в Інтернет, означає, що ця програма щонайменше підозріла. Заснований на цьому принципі евристичний аналізатор повинен постійно стежити за діями, які виконують програми.

Перевагою описаного методу є можливість виявляти невідомі раніше шкідливі програми, навіть якщо вони не дуже схожі на вже відомі. Наприклад, нова шкідлива програма може використовувати для

проникнення на комп'ютер нову вразливість, але після цього починає виконувати вже звичні шкідливі дії. Таку програму може пропустити евристичний аналізатор першого типу, але цілком може виявити аналізатор другого типу.

Негативні риси ті ж, що і раніше:

- Помилкові спрацьовування.
- Неможливість лікування.
- Невисока ефективність.

В першу чергу, кожен антивірус повинен містити ***модуль оновлення***. Це пов'язано з тим, що основним методом виявлення вірусів сьогодні є сигнатурний аналіз, який покладається на використання антивірусної бази. Для того, щоб сигнатурний аналіз ефективно справлявся з найостаннішими вірусами, антивірусні експерти постійно аналізують зразки нових вірусів і випускають для них сигнатури.

Другий важливий допоміжний модуль - це ***модуль планування***. Існує ряд дій, які антивірус повинен виконувати регулярно,зокрема: перевіряти ваш комп'ютер на наявність вірусів і оновлювати антивірусну базу. Модуль оновлення якраз і дозволяє набудувати періодичність виконання цих дій.

У міру збільшення кількості модулів в антивірусі виникає необхідність в додатковому ***модулі для управління і настройки***. У простому випадку - це ***загальний інтерфейсний модуль***, за допомогою якого можна в зручній формі дістати доступ до найбільш важливих функцій:

- Настройки параметрів антивірусних модулів.
- Настройки оновлень.
- Настройки періодичного запуску оновлення і перевірки.
- Запуску модулів вручну, на вимогу користувача.
- Звітам про перевірку.
- Іншим функціям, залежно від конкретного антивіруса.

Серед інших допоміжних засобів в багатьох антивірусах є спеціальні технології, які захищають від можливої втрати даних в результаті дій антивіруса. Таким засобом є карантин, в який антивірус розміщує файл, що не вдалося вилікувати, тоді якщо опиниться, що файл був видалений помилково або була втрачена важлива інформація, завжди можна буде виконати відновлення з резервної копії.

Загальний огляд сучасних антивірусних програм

Avira AntiVir — серія антивірусних програм від німецької компанії Avira GmbH. Всі продукти серії засновані на антивірусному двигуні Luke Filewalker, який було вперше представлено у 1988 році. 17 жовтня 2008 було випущено значно покращену версію продукту, завдяки чому швидкість сканування збільшилась на 20%. Це було досягнуто завдяки «прибиранню» з вірусної бази старих версій вірусних сигнатур. AntiVir може постійно стежити за файлами і архівами, які можуть бути потенційними переносниками вірусів. Відшукуються також і макроси, які упроваджуються в офісні документи.

NOD32 — антивірусний пакет, що випускається словацькою фірмою ESET. Перша версія була випущена в кінці 1987 році. Назва спочатку розшифровувалася як Nemocnica na Okraji Disku («Лікарня на краю диска», перифраз назви популярного тоді в Чехословаччині телесеріалу «Лікарня на околиці міста»).

NOD32 — це комплексне антивірусне рішення для захисту в реальному часі. ESET NOD32 забезпечує захист від вірусів, а також від інших загроз, включаючи троянські програми, черв'яки, spyware, adware, фішинг-атаки. В ESET NOD32 використовується патентована технологія ThreatSense, призначена для виявлення нових загроз, які виникають в реальному часі, шляхом аналізу виконуваних програм на наявність шкідливого коду, що дозволяє попереджати дії авторів шкідливих програм.

При оновленні баз використовується ряд серверів-дзеркал, при цьому також можливе створення внутрішньомережевого дзеркала оновлень, що призводить до зниження навантаження на інтернет-канал. Для отримання оновлень з офіційних серверів необхідні ім'я користувача і пароль, які можна отримати, активувавши свій номер продукту на сторінці реєстрації регіонального сайту.

Нарівні з базами вірусів NOD32 використовує евристичні методи, що забезпечує краще виявлення ще невідомих вірусів.

Велика частина коду антивірусу написана на мові асемблера, тому для нього характерне мале використання системних ресурсів і висока швидкість перевірки з налаштуваннями за замовчуванням.

AVG — антивірусне програмне забезпечення розроблене чеською компанією AVG Technologies (раніше відома під назвою Grisoft). Антивірус має сканер файлів, має змогу перевіряти електронну пошту, та моніторинг системи. Програма містить пошуковий механізм Virus Stalker, яких сертифікований незалежними дослідницькими лабораторіями.

AVG Antivirus існує у двох версіях:

AVG Antivirus Free Edition

AVG Antivirus Pro Edition

Антивірус Касперського (раніше відомий як Antiviral Toolkit Pro; коротко називається KAV — від англ. Kaspersky Antivirus) — антивірусне програмне забезпечення, що розробляється Лабораторією Касперського. Надає користувачеві захист від вірусів, троянських програм, шпигунських програм, руткітів, adware, а також невідомих погроз за допомогою проактивного захисту, що включає компонент HIPS.

Базовий захист

- Перевірка файлів, веб-сторінок, поштових і ICQ-повідомлень
- Блокування посилань на заражених і фішингові веб-сайти
- Проактивний захист від невідомих погроз, заснований на аналізі поведінки програм
- Самозахист антивірусу від спроб виключення з боку шкідливого ПО
- Регулярні і екстрені оновлення — завжди актуальний захист комп'ютера
- Віртуальна клавіатура для безпечного введення логінів, паролів і номерів кредитних карт на веб-сторінках
- Спеціальний Ігровий профіль для тимчасового відключення оновлень, перевірки за розкладом і повідомлень
- Перевірка операційної системи і встановлених програм на наявність уразливостей
- Налаштування операційної системи і інтернет-браузера для безпечної роботи в інтернеті
- Відновлення працездатності системи після вірусної атаки
- Інструменти створення Диска аварійного відновлення системи
- Видалення тимчасових файлів інтернет-браузера

Kaspersky Internet Security 2010

Базовий захист та:

- Контроль роботи програм і обмеження їх доступу до важливих областей ОС і особистих даних користувача
- Доступ до паролів, логінів і інших особистих даних — лише для довірених програм
- Захист від спаму і фішингу в поштових програмах
- Блокування банерної реклами на веб-сторінках
- Батьківський контроль (обмеження використання інтернету дітьми)
- Аналіз мережевої активності в режимі реального часу за допомогою інструменту Моніторинг мережі
- Запуск підозрілих файлів і веб-сайтів в Безпечному середовищі
- Захищена область для тек і файлів з важливими даними, доступна лише для довірених програм
- Налаштування правил доступу програм до системних і онлайну-ресурсам
- Навчання модуля Анти-спам на прикладі вже наявних листів для ефективнішої фільтрації спаму-повідомлень

Avast! Professional Edition увібрав в себе всі високопродуктивні технології для забезпечення однієї мети: надати вам найвищий рівень захисту від комп'ютерних вірусів. Даний продукт є ідеальне рішення для робочих станцій на базі Windows. Нова версія ядра антивируса avast! забезпечує високий рівень виявлення укупі з високою ефективністю, що гарантує 100%-е виявлення вірусів "In-the-Wild" і

високий рівень виявлення троянів з мінімальним числом помилкових спрацьовувань. Механізм антивірусного ядра сертифікований ICSA, постійно бере участь в тестах VirusBulletin і отримує нагороди VB100%. Зовнішній вигляд призначеного для користувача інтерфейсу відображається за допомогою так званих скінів, тому у вас є можливість набудувати зовнішній вигляд панелі продуктів avast! по-своєму бажанню.

Вдосконалений призначений для користувача інтерфейс (тільки у версії Professional).

На додаток до простого, призначеного для користувача інтерфейсу Professional Edition представляє вдосконалений, призначений для користувача інтерфейс, забезпечуючи вас можливістю розширеного сканування.

На відміну від простого інтерфейсу, сканування проводиться за допомогою так званих "завдань". Спочатку ви визначаєте завдання, включаючи різні параметри - області сканування, що сканувати, як сканувати і т.д. Визначивши завдання, ви можете його запустити на виконання. Кожне завдання генерує список результатів, з яким ви можете працювати пізніше.

Інша важлива особливість, тісно пов'язана із завданнями, - сканування за розкладом. Воно дає вам можливість задавати час для запуску завдання на виконання, одноразово або періодично.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. З’ясувати, яке антивірусне програмне забезпечення встановлене на Вашому робочому комп’ютері.
2. Ознайомитись з інтерфейсом даної антивірусної програми, режимами роботи, модулями, основними можливостями, способами оновлення бази вірусних сигнатур.
3. Всі отримані результати занотуйте до звіту, використовуючи скріншоти для ілюстрації.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається антивірусною програмою?
2. Назвіть дві основні групи методів антивірусного захисту.
3. Опишіть принципи роботи, переваги та недоліки сигнатурного та евристичного методів антивірусного захисту.
4. З яких основних модулів складається сучасне антивірусне програмне забезпечення?
5. Що таке карантин?
6. Які ви знаєте сучасні найпоширеніші антивірусні програми?
7. Охарактеризуйте можливості більшості сучасних антивірусних програм.
8. Який антивірус встановлений на вашому робочому комп’ютері? Охарактеризуйте його основні можливості.

Лабораторна робота №9

Тема: Криптографічний вид захисту інформації. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування інформації.

Мета: ознайомитися з поняттям криптографії, способами шифрування файлів, папок, повідомлень та криптографічними методами захисту інформації, розглянути основні засоби здійснення криптографічного захисту інформації.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Криптографія — наука про методи перетворення (шифрування) інформації з метою її захисту від зловмисників.

Криптографічні методи захисту інформації - це методи захисту даних із використанням шифрування.

Шифрування — процес застосування шифру і інформації, що захищається, тобто перетворення інформації, що захищається, в шифроване повідомлення за допомогою певних правил, що містяться в шифрі.

Всі відомі способи шифрування розбиті на п'ять груп: підстановка (заміна), перестановка, аналітичне перетворення, гаммування і комбіноване шифрування. Кожен з цих способів може мати декілька різновидів.

Під ***кодуванням*** розуміється такий вид криптографічного закриття, коли деякі елементи даних (не обов'язково окремі символи), що захищаються, замінюються заздалегідь вибраними кодами (цифровими, буквеними, буквено-цифровими поєднаннями і так далі). Цей метод має два різновиди: смислове і символьне кодування. При смисловому кодуванні кодовані елементи мають цілком певний сенс (слова, пропозиції, групи пропозицій). При символьному кодуванні кодується кожен символ тексту, що захищається. Символьне кодування по суті співпадає з підстановлювальним шифруванням.

До окремих видів криптографії відносяться ***методи розтину і стиснення даних***. Розтин полягає в тому, що масив даних, що захищаються, ділиться (розтинається) на такі елементи, кожен з яких окремо не дозволяє розкрити зміст інформації, що захищається. Виділені таким чином елементи даних розносяться по різних зонах пам'яті або розташовуються на різних носіях. Стиснення даних є заміною однакових рядків даних або послідовностей однакових символів, що часто зустрічаються, деякими заздалегідь вибраними символами.

Розтин шифру — процес отримання інформації (відкритого тексту), що захищається, з шифрованого повідомлення (шифртекста) без знання застосованого шифру.

Дешифрування — процес, зворотний шифруванню, що полягає в перетворенні шифрованого повідомлення в інформацію, що захищається, за допомогою певних правил, що містяться в шифрі.

Під ***ключем*** в криптографії розуміють змінний елемент шифру, який застосовують для шифрування конкретних повідомлень.

Одне з центральних місць в понятійному апараті криптографії займає таке поняття, як стійкість шифру. Під ***стійкістю шифру*** розуміють здатність шифру протистояти всіляким методам розтину.

Для того, щоб криптографічні методи перетворення забезпечили ефективний захист інформації, вони повинні задовольняти ряду вимог. У стислому вигляді їх можна сформулювати таким чином:

- складність і стійкість криптографічного захисту повинні вибиратися залежно від об'єму і ступеня секретності даних;
- надійність захисту повинна бути такою, щоб секретність не порушувалася у тому випадку, коли зловмисникові стає відомий метод захисту;
- метод захисту, набір використовуваних ключів і механізм їх розподілу не можуть бути дуже складними;
- виконання процедур прямого і зворотного перетворень повинне бути формалізованим. Ці процедури не повинні залежати від довжини повідомлень;
- помилки, що виникають в процесі виконання перетворення, не повинні розповсюджуватися на текст повною мірою і по системі;
- надмірність, що вноситься процедурами захисту повинна бути мінімальною.

Головна мета шифрування (кодування) інформації - її захист від несанкціонованого читання. Системи криптографічного захисту (системи шифрування інформації) можна поділити за різними ознаками:

• за принципами використання криптографічного захисту (вбудований у систему або додатковий механізм, що може бути відключений);

• за способом реалізації (апаратний, програмний, програмно-аларатний);

• за криптографічними алгоритмами, які використовуються (загальні, спеціальні);

• за цілями захисту (забезпечення конфіденційності інформації (шифрування) та захисту повідомлень і даних від модифікації, регулювання доступу та привілеїв користувачи);

• за методом розподілу криптографічних ключів (базових/сеансових ключів, відкритих ключів) тощо.

Додаткові механізми криптозахисту - це додаткові програмні або апаратні засоби, які не входять до складу системи. Така реалізація механізмів криптозахисту має значну гнучкість і можливість

швидкої заміни. Для більшої ефективності доцільно використовувати комбінацію додаткових і вбудованих механізмів криптографічного захисту.

За способом реалізації криптографічний захист можна здійснювати різними способами: апаратним, програмним або програмно-апаратним. Апаратна реалізація криптографічного захисту - найбільш надійний спосіб, але й найдорожчий. Інформація для апаратних засобів передається в електронній формі через порт обчислювальної машини всередину апаратури, де виконується шифрування інформації. Перехоплення та підробка інформації під час її передачі в апаратуру може бути виконана за допомогою спеціально розроблених програм типу "вірус".

Програмна реалізація криптографічного захисту значно дешевша та гнучкіша в реалізації. Але виникають питання щодо захисту криптографічних ключів від перехоплення під час роботи програми та після її завершення. Тому, крім захисту від "вірусних" атак, потрібно вжити заходів для забезпечення повного звільнення пам'яті від криптографічних ключів, що використовувались під час роботи програм "збирання сміття".

Крім того, можна використовувати комбінацію апаратних і програмних механізмів криптографічного захисту. Найчастіше використовують програмну реалізацію криптоалгоритмів з апаратним зберіганням ключів. Такий спосіб криптозахисту є досить надійним і не надто дорогим. Але, вибираючи апаратні засоби для зберігання криптографічних ключів, треба пам'ятати про забезпечення захисту від перехоплення ключів під час їх зчитування з носія та використання в програмі.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

Криптографічний алгоритм - це математична функція, яка комбінує відповідний текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримання незв’язаного (шифрованого) тексту.

Усі криптографічні алгоритми можна поділити на дві групи: загальні і спеціальні.

Спеціальні криптоалгоритми мають таємний алгоритм шифрування, а ***загальні*** криптоалгоритми характерні повністю відкритим алгоритмом, і їх криптостійкість визначається ключами шифрування. Спеціальні алгоритми найчастіше використовують в апаратних засобах криптозахисту.

Загальні криптографічні алгоритми часто стають стандартами шифрування, якщо їхня висока криптостійкість доведена. Ці алгоритми оприлюднюють для обговорення, при цьому навіть визначається премію за успішну спробу його "злому". Криптостійкість загальних алгоритмів визначається ключем шифрування, який генерується методом випадкових чисел і не може бути повторений протягом певного часу. Криптостійкість таких алгоритмів буде вищою відповідно до збільшення довжини ключа.

Є дві великі групи загальних криптоа лгоритмі в: ***симетричні і асиметричні***. До ***симетричних криптографічних алгоритмів*** належать такі алгоритми, для яких шифрування і розшифрування виконується однаковим ключем, тобто і відправник, і отримувач повідомлення мають користуватися тим самим ключем. Такі алгоритми мають досить велику швидкість обробки як для апаратної, так і для програмної реалізації. Основним їх недоліком є труднощі, пов'язані з дотриманням безпечного розподілу ключів між абонентами системи. Для ***асиметричних криптоалгоритмів шифрування*** і розшифрування виконують за допомогою різних ключів, тобто, маючи один із ключів, не можна визначити парний для нього ключ. Такі алгоритми часто потребують значно довшого часу для обчислення, але не створюють труднощів під час розподілу ключів, оскільки відкритий розподіл одного з ключів не зменшує криптостійкості алгоритму і не дає можливості відновлення парного йому ключа.

Усі криптографічні алгоритми можна використовувати з різними цілями, зокрема:

• для шифрування інформації, тобто приховування змісту повідомлень і даних;

• для забезпечення захисту даних і повідомлень від модифікації.

З найпоширеніших методів шифрування можна виділити американський алгоритм шифрування ***DES*** (Data Encryption Standart, розроблений фахівцями фірми IBM і затверджений урядом США 1977 року) із довжиною ключа, що може змінюватися, та алгоритм ГОСТ 28147-89, який був розроблений та

набув широкого застосування в колишньому СРСР і має ключ постійної довжини. Ці алгоритми належать до симетричних алгоритмів шифрування.

Алгоритм Потрійний DES був запропонований як альтернатива DES і призначений для триразового шифрування даних трьома різними закритими ключами для підвищення ступеня захисту.

RC2, RC4, RC5 - шифри зі змінною довжиною ключа для дуже швидкого шифрування великих обсягів інформації. Здатні підвищувати ступінь захисту через вибір довшого ключа.

IDEA (International Data Encryption Algoritm) призначений для швидкої роботи в програмній реалізації.

Для приховування інформації можна використовувати деякі асиметричні алгоритми, наприклад, алгоритм RSA. Алгоритм підтримує змінну довжину ключа та змінний розмір блоку тексту, що шифрується.

Алгоритм RSA дозволяє виконувати шифрування в різних режимах:

• за допомогою таємного ключа відправника. Тоді всі, хто має його відкритий ключ, можуть розшифрувати це повідомлення;

• за допомогою відкритого ключа отримувача, тоді тільки власник таємного ключа, який є парним до цього відкритого, може розшифрувати таке повідомлення;

• за допомогою таємного ключа відправника і відкритого ключа отримувача повідомлення. Тоді тільки цей отримувач може розшифрувати таке повідомлення.

Але не всі асиметричні алгоритми дозволяють виконувати шифрування даних у таких режимах. Це визначається математичними функціями, які закладені в основу алгоритмів.

Другою метою використання криптографічних методів є захист інформації від модифікації, викривлення або підробки. Цього можна досягнути без шифрування повідомлень, тобто повідомлення залишається відкритим, незашифрованим, але до нього додається інформацію, перевірка якої за допомогою спеціальних алгоритмів може однозначно довести, що ця інформація не була змінена. Для симетричних алгоритмів шифрування така додаткова інформація - це код автентифікації, який формується за наявності ключа шифрування за допомогою криптографічних алгоритмів.

Для асиметричних криптографічних алгоритмів формують додаткову інформацію, яка має назву електронний цифровий підпис. Формуючи електронний цифровий підпис, виконують такі операції:

• за допомогою односторонньої хеш-функції обчислюють прообраз цифрового підпису, аналог контрольної суми повідомлення;

• отримане значення хеш-функції шифрується: а) таємним або відкритим; б) таємним і відкритим ключами відправника і отримувача повідомлення - для алгоритму RSA

• використовуючи значення хеш-функції і таємного ключа, за допомогою спеціального алгоритму обчислюють значення цифрового підпису, - наприклад, для російського стандарту Р.31-10.

Для того, щоб перевірити цифровий підпис, потрібно:

• виходячи із значення цифрового підпису та використовуючи відповідні ключі, обчислити значення хеш-функції;

• обчислити хеш-функцію з тексту повідомлення;

• порівняти ці значення. Якщо вони збігаються, то повідомлення не було модифікованим і відправлене саме цим відправником.

Ефективність захисту систем за допомогою будь-яких криптографічних алгоритмів значною мірою залежить від безпечного розподілу ключів. Тут можна виділити такі основні методи розподілу ключів між учасниками системи.

1. Метод базових/сеансових ключів. Такий метод описаний у стандарті ISO 8532 і використовується для розподілу ключів симетричних алгоритмів шифрування. Для розподілу ключів вводиться ієрархія ключів: головний ключ (так званий майстер-ключ, або ключ шифрування ключів) і ключ шифрування даних (тобто сеансовий ключ). Ієрархія може бути і дворівневою: ключ шифрування ключів/ключ шифрування даних. Старший ключ у цій ієрархії треба розповсюджувати неелектронним

способом, який виключає можливість його компрометації. Використання такої схеми розподілу ключів потребує значного часу і значних затрат.

2. Метод відкритих ключів. Такий метод описаний у стандарті ISO 11166 і може бути використаний для розподілу ключів як для симетричного, так і для асиметричного шифрування. За його допомогою можна також забезпечити надійне функціонування центрів сертифікації ключів для електронного цифрового підпису на базі асиметричних алгоритмів та розподіл сертифікатів відкритих ключів учасників інформаційних систем. Крім того, використання методу відкритих ключів дає можливість кожне повідомлення шифрувати окремим ключем симетричного алгоритму та передавати цей ключ із самим повідомленням у зашифрованій асиметричним алгоритмом формі.

Вибір того чи іншого методу залежить від структури системи і технології обробки даних. Жоден із цих методів не забезпечує "абсолютного" захисту інформації, але гарантує, що вартість "злому" у кілька разів перевищує вартість зашифрованої інформації.

Щоб використовувати систему криптографії з відкритим ключем, потрібно генерувати відкритий і особистий ключі. Після генерування ключової пари слід розповсюдити відкритий ключ респондентам. Найнадійніший спосіб розповсюдження відкритих ключів - через сертифікаційні центри, що призначені для зберігання цифрових сертифікатів.

Цифровий сертифікат - це електронний ідентифікатор, що підтверджує справжність особи користувача, містить певну інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Сертифікаційні центри несуть відповідальність за перевірку особистості користувача, надання цифрових сертифікатів та перевірку їхньої справжності.

Розкриття зашифрованих текстів (в першу чергу знаходження ключа) здійснюється за допомогою методів криптоаналізу. Основними методами криптоаналізу є:

– ***статистичн***і, при яких знаючи статистичні властивості відкритого тексту намагаються досліджувати статистичні закономірності шифротексту і на підставі виявлених закономірностей розкрити текст;

– ***метод вірогідних слів***, в якому при зіставленні деякої невеликої частини шифротекста з відомим фрагментом відкритого тексту намагаються знайти ключ і з його допомогою розшифрувати весь текст. Необхідний фрагмент відкритого тексту можна знайти за допомогою статистичних методів або просто вгадати, виходячи з передбачуваного змісту або структури відкритого тексту.

Оскільки криптографічні методи застосовуються давно, то вже сформульовані основні вимоги до них.

1. Метод повинен бути надійним, тобто відновлення відкритого тексту при володінні тільки шифротекстом, але не ключем повинно бути практично нездійсненним завданням

2. Через труднощі запам'ятовування об'єм ключа не повинен бути великим.

3. Через труднощі, пов'язані з складними перетвореннями, процеси шифрування повинні бути простими.

4. Через можливості появи помилок передачі дешифровка шифротексту, що містить окремі помилки, не повинна привести до нескінченного збільшення помилок в отриманому передбачуваному відкритому тексті.

5. Через труднощі передачі об'єм шифротексту не повинен бути значно більше відкритого тексту.

Криптографічні перетворення забезпечують вирішення двох головних проблем захисту інформації: проблеми секретності (позбавлення супротивника можливості витягувати інформацію з каналу зв'язку) і проблеми імітостійкості (позбавлення супротивника можливості ввести помилкову інформацію.

Сучасний криптографічний захист інформації здійснюється за допомогою спеціалізованого програмного забезпечення, що дає змогу використовувати складні методи шифрування з мінімальною затратою часу. Ще одним позитивним моментом такого застосування є доступність можливостей

зашифрувати важливу інформацію, в тому числі повідомлення, окремі файли і папки звичайним користувачам, адже більшість таких програм доступні для розповсюдження та мають нескладний інтерфейс, звільняють користувача від необхідності знання способів та методів шифрування. Звичайно, якщо йде мова про криптографічний захист банківських систем, інформації стратегічного чи державного значення, то використовують спеціальні криптографічні системи, що складаються з програмних засобів, доступних вузькому колу користувачів, а частіше всього, оригінальними, спеціально створеними засобами.

Програмний комплекс криптографічного захисту інформації «Криптосервер»

Комплекс є сукупністю засобів криптографічного захисту інформації з функціями шифрування інформації, формування та зберігання ключової інформації, а також надання послуг встановлення автентичності даних, які надходять, зберігаються та обробляються в комп'ютеризованих системах оброблення інформації.

Комплекс реалізує наступні функції:

Захист даних - забезпечує захист інформації, яка передається по загальнодоступним мережам, від несанкціонованого ознайомлення й/або модифікації.

Керування - забезпечує конфігурування та налаштування параметрів компонентів Комплексу, необхідних для їх функціонування.

Аудит - дозволяє проводити аналіз записів у файлах протоколів.

Ідентифікація й автентифікація - блокує доступ до можливостей керування Комплексом осіб, що не мають відповідних повноважень.

Захист функціонування - підтримує функціонування Комплексу при спробах порушити цілісність програмного забезпечення або конфігураційної інформації.

Комплекс складається з наступних компонентів:

Центр генерації ключів (ЦГК) - програмний модуль, призначений для генерації закритих і відкритих ключів, а також для запису ключових носіїв для всіх компонентів Комплексу. Центр генерації ключів встановлюється на комп'ютері, що не має мережевих з'єднань.

Центр розподілу ключів (ЦРК) - програмний модуль, призначений для зберігання та видачі мережевими каналами довіреним компонентам Комплексу сертифікатів відкритих ключів, інформації про контур безпеки, що визначає учасників захищеної мережі, та іншої службової інформації.

Модуль шифрування (МШ) - програмний модуль, призначений для побудови захищеної мережі (шлюз ЗМ), який встановлюється на границі ЗМ або границі сегмента ЗМ, що функціонує в інтересах одного, декількох або всіх суб'єктів (об'єктів) даної ЗМ (сегмента ЗМ), що забезпечує створення захищених з'єднань із іншими довіреними модулями шифрування.

Модуль керування (МК) - програмний модуль, призначений для дистанційного керування компонентами Комплексу, такими як ЦРК, МШ.

Компоненти Комплексу обмінюються ідентифікаційною інформацією й виконують процедури автентифікації з використанням сертифікатів відкритих ключів, які запитуються у ЦРК. Захищене з'єднання може бути встановлено тільки після виконання процедур взаємної автентифікації компонентів Комплексу.

На сьогодні існує велика кількість алгоритмів і протоколів шифрування. Серед алгоритмів симетричного криптографії, яких безліч, можна згадати RC4, RC5, CAST, DES, AES і т.д. Оптимальна довжина ключів шифрування для цих алгоритмів - 128 розрядів. Що стосується асиметричного шифрування, то тут в основному використовуються алгоритми RSA, Diffie-Hellman і El-Gamal, при цьому довжина ключів шифрування звичайно становить 2048 розрядів. Найбільш широко для криптографічного захисту переданих по каналах зв'язку даних, включаючи листи електронної пошти, застосовується протокол SSL, у якому для шифрування даних використовуються ключі RSA.

Популярним пакетом програм для шифрування листування по електронній пошті і будь-яких даних, що зберігаються на жорсткому диску є PGP (Pretty Good Privacy).

В безкоштовному варіанті PGP Desktop Email 9.6 (призначений тільки для приватного некомерційного використання) включені функції шифрування файлів і папок, в платному варіанті опцій значно більше - від шифрованого листування (включаючи через інтернет-пейджери) і створення зашифрованих дисків на локальному комп'ютері до розгортання захищеної локальної мережі.

Переваги:

• Простота і зручність у використанні.

• Вичерпна безпека електронної кореспонденції на шляху від відправника до одержувачу - 100% захист від несанкціонованого доступу і зміни даних.

• Автоматичний пошук відкритих ключів одержувача в інтернет-каталозі PGP Global Directory.

• Загальна інфраструктура ключів для шифрування електронної пошти, миттєвих повідомлень, файлів.

• Створення зашифрованих архівів PGP Zip на одну дію.

• Політики захисту інформації для автоматичного шифрування/дешифрування та цифрового підпису електронних листів з урахуванням адреси одержувача і відправника, а також вмісту і теми листа.

• Шифрування миттєвих повідомлень і пересилаються файлів.

• Перевірені технології.

• Криптозахист даних з використанням перевірених часів технологій, які отримали широке галузеве визнання.

• Підтримка галузевих стандартів і 100% сумісність з рішеннями OpenPGP і S/MIME.

• Програма PGP Desktop Email можна захищати за допомогою ключа PGP або сертифікату X.509. Воно також підтримує існуючі інфраструктури з ключами. • Підтримка смарт-карт/маркеров забезпечує багатофакторну аутентифікацію адміністраторів і користувачів.

• Інтеграція з популярними клієнтами електронної пошти, включаючи MS Outlook, Outlook Express, Eudora, Entourage і Apple Mail.

• Оновлення ПЗ PGP Desktop Email 9.6.

Програма STCLite 3.3 призначена для забезпечення захищеного і шифрованого пересилання поштових повідомлень по мережі Інтернет, а також для шифрованого та безпечного зберігання інформації на знімних носіях і жорстких дисках. Легко та витончено, ви можете зашифрувати вміст вашого листа, переконатися в цьому на власні очі (тому що шифрування виконується не на льоту, коли вже нічого змінити неможливо, а до відправки повідомлення) і спокійно відправити його своєму кореспонденту. При цьому ви можете бути впевнені, що жодних слідів не залишилося у вашому комп'ютері, тому що вся обробка повідомлення ведеться тільки в оперативної пам'яті комп'ютера, без запису інформації на жорсткий диск.

Програма STCLite 3.3 складається з модуля шифрування тексту, модуля шифрування файлів і папок, модуля стеганографії.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Шифр Цезаря — симетричний алгоритм шифрування підстановками. Використовувався римським імператором Юлієм Цезарем для приватного листування. Принцип дії полягає в тому, щоб циклічно зсунути алфавіт, а ключ — це кількість літер, на які робиться зсув. Користуючись алфавітом АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ та використовуючи в якості ключа власний номер в журналі зашифрувати повідомлення та записати даний шифр в звіт

«Шифр Цезаря має замало ключів — на одиницю менше, ніж літер в абетці. Тому перебрати усі ключі не складає особливої роботи. Дешифрування з одним з ключів дасть нам вірний відкритий текст.»

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Дайте визначення поняттям «криптографія», «криптографічні методи захисту інформації», «шифрування».

2. Назвіть основні групи шифрування.
3. Що таке кодування? Які типи кодування ви знаєте?
4. В чому суть методів розтину та стиснення даних?
5. Що розуміють під стійкістю шрифту?
6. Сформулюйте основні вимоги до методів криптографічного перетворення.
7. Яка головна мета шифрування (кодування) інформації?
8. Охарактеризуйте способи реалізації криптографічного захисту.
9. Що таке криптографічні алгоритми? На які групи вони поділяються, охарактеризуйте їх.
10. Сформулюйте вимоги до криптографічних методів.
11. Охарактеризуйте програмний комплекс криптографічного захисту інформації «Криптосервер».

Лабораторна робота №10

Тема: Інформаційна безпека держави. Потенційні загрози, засоби їх попередження та ліквідації.

Мета: ознайомитися з поняттям інформаційної безпеки держави та інформаційної війни, основними інтересами України та потенційними небезпеками у сфері інформаційної безпеки, елементами інформаційної боротьби; законодавством України, що стосується інформаційної безпеки держави.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Інтереси держави в інформаційній сфері в основному зводяться до гармонійного розвитку інформаційної структури держави.

Інформаційна безпека держави – це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає істотної шкоди національним інтересам.

Ще дотепер вважається, що загрози інтересам держави можуть проявлятися тільки у вигляді отримання зловмисниками протиправного доступу до відомостей, що становлять державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести збитки державі. Також вважається, що найбільш небезпечними джерелами загроз інтересам держави в інформаційному суспільстві є неконтрольоване розповсюдження інформаційної зброї, спроби релізації концепції ведення інформаційних війн.

Відповідно до законодавства України, поняття "інформаційна безпека" має таке визначення: "стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди державі через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації".

Виокремлюють три рівня забезпечення інформаційної безпеки:

1. ***рівень особи*** (формування раціонального, критичного мислення на основі принципів свободи вибору);
2. ***суспільний рівень*** (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам);
3. ***державний рівень*** (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту

інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам).

Національні інтереси України в інформаційній сфері вирізняють такі життєво важливі інтереси:

– недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері;

– побудова та розвиток інформаційного суспільства;

– забезпечення економічного та науково-технологічного розвитку України;

– формування позитивного іміджу України; інтеграція України у світовий інформаційний простір.

Принципи забезпечення інформаційної безпеки України зводяться до такого:

- свобода збирання, зберігання, використання та поширення інформації;
- достовірність, повнота та неупередженість інформації;
- обмеження доступу до інформації виключно на підставі закону;
- гармонізація особистих, суспільних і державних інтересів;
- запобігання правопорушенням в інформаційній сфері;
- економічна доцільність;
- гармонізація українського законодавства в інформаційній сфері з міжнародним;
- пріоритетність національної інформаційної продукції.

Вперше термін "інформаційна війна" з'явився наприкінці 80-х років XX століття. Він став результатом плідної праці теоретиків збройних сил США, почав широко використовуватися після вдало проведеної роботи зі знищення СРСР. На сьогодні саме інформаційні війни становлять найбільшу небезпеку нормальному функціонуванню системи органів державного управління.

Відомі два трактування поняття "інформаційні війни": гуманітарне і технічне. У гуманітарному розумінні інформаційна війна представляє собою активні методи перетворювання інформаційного простору, тобто нав'язування громадянам України таких моделей суспільства, які забезпечують бажані типи поведінки, а також породжують інформаційні процеси міркувань.

Інформаційна війна при використанні інформації як зброї ведення бойових дій у будь-якій сфері життєдіяльності містить такі складові:

- здійснення впливу на інфраструктуру систем життєзабезпечення – телекомунікації, транспортні мережі, електростанції тощо;
- промисловий шпіонаж – порушення прав інтелектуальної власності, розкрадання патентованої інформації, викривлення або знищення важливих даних, проведення конкурентної розвідки;
- хакінг – зламування та використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо.

Існує декілька підвидів інформаційних воєн:

- ***кібервійна*** – комп'ютерне протистояння у просторі мережі Інтернет, спрямоване на дестабілізацію комп'ютерних систем державних установ, фінансових і ділових центрів, створення безладу та хаосу в житті країни;
- ***мережева війна*** – форма ведення конфліктів, коли її учасники застосовують мережеві стратегії та технології, пристосовані до сучасної інформаційної доби. Учасниками таких воєн можуть бути терористи, кримінальні угруповання, громадські організації та соціальні рухи, які використовують децентралізацію комп'ютерних систем;
- ***електронна війна*** – використання та управління інформацією з метою набуття переваги конкурента над супротивником, здійснює збирання тактичної інформації, забезпечує безпеку

власних інформаційних ресурсів, поширює неправдиву інформацію про ворога і населення, перешкоджає збиранню інформації супротивником;

- ***психологічна війна*** – сукупність різних форм, методів і засобів впливу на людину з метою зміни в бажаному напрямку її психологічних характеристик, групових норм поведінки, масових настроїв, суспільної свідомості загалом;
- ***радіоелектронна боротьба*** – сукупність узгоджених за цілями, задачами, місцем і часом заходів і дій військ, спрямованих на здобування інформації про місцезнаходження радіоелектронних засобів, систем управління військами і зброї суперника, їх знищення всіма видами зброї, а також радіоелектронному подавленню сигналів передачі інформації.

Отже, поняття ***інформаційна війна*** – це дії, що здійснюються для досягнення інформаційної переваги власної воєнної стратегії через вплив на інформацію та комунікаційні системи суперника при одночасному забезпеченні безпеки власних інформаційних ресурсів. Одним з прикладів є вказівка спецслужб США відстежувати телефонні розмови, що виходять за її межі. За допомогою відповідної програми усі телефонні дзвінки записуються, а потім пропускаються через спеціальну апаратуру, яка за допомогою пошукових систем за ключовими словами виявляє та ідентифікує важливу інформацію.

Основна мета сучасної інформаційної війни полягає не у фізичному знищенні суперника та ліквідації його збройних сил, а у широкомасштабному порушенні роботи фінансових, транспортних і комунікаційних мереж і систем, у руйнуванні економічної інфраструктури і підкоренні населення країни, що зазнала атаки, волі країни-переможця.

Основним інструментом ведення інформаційної війни є інформаційна зброя, тобто пристрої та засоби, які призначені для нанесення протидіючій стороні максимальної шкоди в ході інформаційної боротьби.

Основними елементами інформаційної боротьби є:

- засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, не зважаючи на систему захисту, обмеження доступу до цієї інформації законних користувачів;
- інформаційно-психологічні засоби, які дезорганізують інформаційні системи шляхом дезінформації, формування помилкових логічних інформаційних концепцій, інтерпретацій та ін., впливаючи таким чином на суспільну думку, на життя суспільства, держави або групи держав загалом.

Інформаційна зброя є інструментом встановлення контролю над інформаційними ресурсами потенційного суперника, тому вона втручається в роботу систем управління та інформаційних систем, систем зв'язку, з метою порушення їх працездатності аж до цілковитого виведення їх з ладу, вилучення, перекручення даних, які в них містяться, або цілеспрямованого введення спеціальної інформації. Здебільшого інформаційна зброя розповсюджує дезінформацію в системі формування суспільної свідомості й прийняття рішень.

Особливу небезпеку в цьому випадку становлять дані, що надходять для органів державної влади, оскільки від їх достовірності залежить здатність цих органів приймати правильні рішення та вживати своєчасні заходи з управління державою.

Інформаційна зброя враховує різні варіанти протидії, тому чим більше таких варіантів ураховано, тим більша ймовірність успіху в тій чи іншій інформаційній агресії.

Інформаційне протиборство – форма боротьби сторін в інформаційному просторі з використанням політичних, економічних, дипломатичних, військових та інших методів, способів та засобів для впливу на інформаційне поле суперника та захисту власного інформаційного поля в інтересах досягнення поставлених цілей. На сьогодні відомі такі сфери протиборства: світоглядна, політична, дипломатична, воєнна, науково-технологічна, соціальна та гуманітарна, ідеологічна, екологічна тощо.

Інформаційна війна має наступальні та оборонні складові, починаючи з цільового проектування та розроблення своєї структури командування, управління, комунікацій комп'ютерів і розвідки. Вона

може бути спрямована проти трьох елементів інфраструктури: комп'ютерів; програмного забезпечення; людини. Однією з головних цілей та завдань інформаційної війни є придушення в людині морального творчого початку, зміна власного світогляду. На міжнародній арені інформаційні війни ведуться:

- між державами та блоками держав;
- між міжнародними корпораціями, транснаціональними компаніями і міжнароними фінансовими групами з державами;
- між терористичними організаціями та державами;
- між злочинними організаціями;
- між злочинними організаціями та державами.

Загалом сучасні інформаційні технології певною мірою зрівняли індустріальні, постіндустріальні та доіндустріальні країни: всі вони мають доступ до інструментарію, необхідного для ведення інформаційної війни, а отже виступають як суб'єкти, так і об'єкти інформаційної війни і, як наслідок, забезпечення внутрішньої інформаційної безпеки.

Таким чином, інформаційна війна використовує переваги технологічних вдосконалень, вона вже настільки близько підійшла до практичної реалізації, що подальше нехтування цим питанням просто недопустиме. Зброєю в цьому напрямку боротьби є пристрої та технології, які використовуються для широкомасштабного, цілеспрямованого, швидкого та таємного впливу на цивільні та військові інформаційні системи суперника.

Види джерел загроз інформаційній безпеці України.

Однією з основних загроз інформаційній безпеці Закон України "Про основи національної безпеки" називає "намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації". До інших загроз віднесено:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави.

В "Доктрині інформаційної безпеки України", підписаній Президентом в липні 25.05.2009 р., серед всього виділено такі загрози інформаційній безпеці країни:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;
- зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;
- деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності України;
- прояви сепаратизму в засобах масової інформації, а також у мережі Інтернет, за етнічною, мовною, релігійною та іншими ознаками.

Таким чином, поняття "загроза інформаційній безпеці" визначається:

1) відсутністю єдиного підходу до дослідження основних понять інформаційної безпеки;

2) недостатньою розробленістю початкового поняття "загроза" і питань його відмежування від інших споріднених понять, таких як "небезпека", "виклик", "ризик", і відповідно видового "інформаційна загроза" і його відмежування від таких понять, як "інформаційна війна", "інформаційне протиборство", "інформаційний тероризм";

3) наявністю невирішеної проблеми формування категорійно-понятійного апарату теорії інформаційної безпеки;

4) можливістю на підставі теоретичних розробок цього апарату формувати адекватну систему моніторингу та управління джерелами загроз та рівнем їх небезпеки в інформаційній сфері.

Загрози інформаційним ресурсам держави можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, що зберігається в ній. Виникнення загрози, тобто виявлення джерел актуалізації певних подій у реалізації загрози інформаційним ресурсам характеризується таким елементом як уразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація джерел загроз і небезпек.

Згідно з Законом України "Про основи національної безпеки України", до джерел загроз і небезпек національним інтересам і національній безпеці в інформаційній сфері належать:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу таємницю, передбачену законом, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів особи, суспільства та держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

До джерел загроз і небезпек інформаційній безпеці системі управління національною безпекою належать: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання.

Отож, як інформаційні війни, так і інформаційне протиборство й інформаційна боротьба є проявами одного більш широкого поняття – загрози національним інтересам і національній безпеці в інформаційній сфері.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Запустіть браузер Інтернет (Це може бути Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera чи будь-який інший, що встановлений на вашому комп’ютері)
2. Користуючись однією з пошуковх систем (Yahoo!, Google, чи будь-якою іншою) ознайомтеся із законодавчою базою України, що стосується інформаційної безпеки держави. Назви основних законів, указів президента, постанов, положень запишість до звіту (не менше 15).
3. На офіційному сайті Верховної ради «Законодавство України» (http://zakon2.rada.gov.ua/laws) знайдіть Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», ознайомтесь з його основними положеннями та занотуйте до звіту такі відомості:
   - основні стратегічні цілі розвитку інформаційного суспільства в Україні;
   - основні напрямки розвитку інформаційного суспільства в Україні;
   - законодавче забезпечення розвитку інформаційного суспільства;
   - інформаційна безпека в інформаційному суспільстві.
4. Користуючись однією з пошукових систем (Yahoo!, Google, чи будь-якою іншою) знайдіть текст Доктрини інформаційної безпеки України, ознайомтесь з основними положеннями та занотуйте до звіту такі відомості:
   - основні напрями забезпечення державою національного інформаційного суверенітету;
   - принципи забезпечення інформаційної безпеки України;
   - основні реальні та потенційні загрози інформаційній безпеці України у сфері державної безпеки;
   - основні засади державної політики забезпечення інформаційної безпеки України
5. Зробіть та запишіть до звіту висновки по роботі.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що розуміють під інформаційною безпекою держави?

2. Назвіть найбільш небезпечні джерела загроз інтересам держави в інформаційному суспільстві.
3. Назвіть та охарактеризуйте рівні забезпечення інформаційної безпеки.
4. Охарактеризуйте основні національні інтереси України в інформаційній сфері.
5. Назвіть принципи забезпечення інформаційної безпеки України.
6. Що ви розумієте під поняттям «інформаційна війна»?
7. Назвіть складові інформаційної війни.
8. Охарактеризуйте основні елементи інформаційної боротьби.
9. Які ви знаєте види джерел загроз інформаційній безпеці України?
10. Чим визначається поняття "загроза інформаційній безпеці"?

Лабораторна робота №11

Тема: Захист комп'ютерних мереж та персональних комп'ютерів за допомогою брандмауера (Firewall).

Мета: ознайомитися з основним типами, призначенням, базовими функціями брандмауера, зробити загальний огляд вбудованого брандмауера операційної системи Windows.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Брандмауер (Firewall) – це захисна стіна, що стоїть між мережним адаптером та операційною системою. Будь-який IP-пакет, перш ніж потрапити на обробку операційної системи (наприклад, для маршрутизації або передачі його web-серверу) проходить через суворий контроль. Будь-який вихідний пакет також натрапляє на цю стіну, і може бути пропущений, відкинутий, підрахований або змінений. Якщо пакет проходить через операційну систему наскрізь (маршрутизується), то його перевірка відбувається як на вході, так і на виході. При складній обробці пакету він може проходити через брандмауер і більшу кількість разів.

Поза комп'ютерної сфери брандмауером (або firewall) називають стіну, зроблену з негорючих матеріалів і перешкоджає поширенню пожежі. У сфері комп'ютерних мереж міжмережевий екран є бар'єр, що захищає від фігуральні пожежі - спроб зловмисників вторгнутися у внутрішню мережу для того, щоб скопіювати, змінити або стерти інформацію або скористатися пам'яттю чи обчислювальною потужністю працюючих у цій мережі комп'ютерів. Міжмережевий екран покликаний забезпечити безпечний доступ до зовнішньої мережі та обмежити доступ зовнішніх користувачів до внутрішньої мережі.

Брандмауери можуть бути виконані у вигляді як апаратного, так і програмного комплексу, записаного в комутуючий пристрій або сервер доступу (сервер-шлюз, просто сервер, хост-комп'ютер і т.д.), вбудованого в операційну систему або представляти собою програму, що працює під її управлінням.

Робота брандмауера полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і в залежності від результатів аналізу пропуску пакетів у внутрішню мережу (сегмент мережі) або повному їх фільтруванні. Ефективність роботи міжмережевого екрану, що працює під управлінням Windows, обумовлена тим, що він повністю заміщає реалізований стек протоколів TCP \ IP, і тому порушувати його роботу з допомогою спотворення протоколів зовнішньої мережі (що часто робиться хакерами) неможливо.

Міжмережеві екрани зазвичай виконують такі функції:

- фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі (внутрішньої підмережі) від зовнішніх каналів зв'язку;
- багатоетапну ідентифікацію запитів, що надходять в мережу (ідентифікація серверів, вузлів зв'язку про інших компонентів зовнішньої мережі);
- перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;
- реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні;

– контроль цілісності програмного забезпечення і даних;

– економію адресного простору мережі (у внутрішній підмережі може використовуватися локальна система адресації серверів);

– приховування IP адрес внутрішніх серверів з метою захисту від хакерів.

Брандмауери можуть працювати на різних рівнях протоколів моделі OSI.

На мережевому рівні виконується фільтрація пакетів, заснована на IP адресах (наприклад, не пропускати пакети з Інтернету, направлені на ті сервери, доступ до яких зовні заборонено; не пропускати пакети з фальшивими зворотними адресами або IP адресами, занесеними до «чорного списку», і т.д.). На транспортному рівні фільтрація припустима ще й за номерами портів TCP і прапорів, що містяться в пакетах (наприклад, запитів на встановлення з'єднання). На прикладному рівні може виконуватися аналіз прикладних протоколів (FTP, HTTP, SMTP і т.д.) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь-яких типів файлів: рекламної інформації або виконуваних програмних модулів).

Можливо в брандмауері створювати експертну систему, яка, аналізуючи трафік, діагностує події, що можуть становити загрозу безпеки внутрішньої мережі, та інформує про це адміністратора. Експертна система здатна також у разі небезпеки (спам, наприклад) автоматично посилювати умови фільтрації і т.д.

Брандмауери бувають апаратними або програмними.

Апаратний брандмауер представляє собою пристрій, фізично підключається до мережі. Це пристрій відслідковує всі аспекти вхідного і вихідного обміну даними, а також перевіряє адреси джерела і призначення кожного оброблюваного повідомлення. Це забезпечує безпеку, допомагаючи запобігти небажаним проникнення в мережу або на комп'ютер.

Програмний брандмауер виконує ті ж функції, використовуючи не зовнішній пристрій, а встановлену на комп'ютері програму.

На одному і тому ж комп'ютері можуть використовуватися як апаратні, так і програмні брандмауери.

Брандмауер представляє собою захисну кордон між комп'ютером (або комп'ютерною мережею) і зовнішнім середовищем, користувачі або програми якої можуть намагатися отримати несанкціонований доступ до комп'ютера. Зазвичай зломщики використовують спеціальні програми для пошуку в Інтернеті незахищених підключень. Така програма відправляє на комп'ютер дуже маленьке повідомлення. За відсутності брандмауера комп'ютер автоматично відповідає на повідомлення, виявляючи свою незахищеність. Встановлений брандмауер отримує такі повідомлення, але не відповідає на них; таким чином, зломщики навіть не підозрюють про існування даного комп'ютера.

Існує кілька шляхів звести нанівець або піддати ризику захист братмауерів. Виходячи з того, що основною метою встановлення більшості брандмауерів є блокування доступу, очевидно, що виявлення будь-ким лазівки, що дозволяє проникнути в систему, веде до повного краху всієї захисту даної системи. Якщо ж несанкціонованому користувачеві вдалося проникнути в брандмауер і переконфігурувати його, ситуація може прийняти ще більш загрозливого характеру. З метою розмежування термінології приймемо, що в першому випадку ми маємо справу зі зломом захисту Firewall, а в другому - з повним її руйнуванням. Ступінь впливу, який може спричинити за собою руйнування захисту братмауера, визначити неймовірно складно. Найбільш повні відомості про надійність такого захисту може дати тільки інформація про діяльність, спробі злому, зібрана цим брандмауером. Найгірше відбувається із системою захисту саме тоді, коли при повному руйнуванні брандмауера не залишається жодних слідів, що вказують на те, як це відбувалося. У кращому ж випадку брандмауер сам виявляє спробу злому і ввічливо інформує про це адміністратора. Спроба при цьому приречена на провал.

Один зі способів визначити результат спроби злому захисту Firewall - перевірити стан речей в так званих зонах ризику. Якщо мережа підключена до Internet без брандмауера, об'єктом нападу стане вся мережа. Така ситуація сама по собі не передбачає, що мережа стає вразливою для кожної спроби

злому. Однак якщо вона приєднується до загальної незахищеної мережі, адміністраторові доведеться забезпечувати безпеку кожного вузла окремо. У разі утворення проломів в брандмауері зона ризику розширюється і охоплює всю захищену мережу. Зломщик, що отримав доступ до входу в брандмауер, може вдатися до методу "захоплення островів" і, користуючись брандмауером як базою, охопити всю локальну мережу. Подібна ситуація все ж дасть слабку надію, бо порушник може залишити сліди в брандмауері, і його можна буде викрити. Якщо ж брандмауер повністю виведений з ладу, локальна мережа стає відкритою для нападу з будь-якої зовнішньої системи, і визначення характеру цього нападу стає практично неможливим.

Загалом, цілком можливо розглядати брандмауер як засіб звуження зони ризику до однієї точки пошкодження. Однак практикою підтверджено, що будь-яка досить велика мережа включає, щонайменше, декілька вузлів, уразливих при спробі злому навіть не дуже досвідченим порушником, якщо у нього достатньо для цього часу. Багато великих компаній мають на озброєнні організаційну політику забезпечення безпеки вузлів, розроблену з урахуванням цих недоліків. Однак було б не надто розумним цілком покладатися виключно на правила. Саме за допомогою брандмауера можна підвищити надійність вузлів, направляючи порушника в такий вузький тунель, що з'являється реальний шанс виявити і вистежити його, до того як він завдасть шкоди.

Зазвичай міжмережеві екрани захищають внутрішню мережу підприємства від "вторгнень" з глобальної мережі Internet, однак вони можуть використовуватися і для захисту від "нападів" з корпоративної мережі, до якої підключена локальна мережа підприємства. Жоден міжмережевий екран не може гарантувати повного захисту внутрішньої мережі при всіх можливих обставин. Однак для більшості комерційних організацій установка міжмережевого екрану є необхідною умовою забезпечення безпеки внутрішньої мережі. Головний аргумент на користь застосування міжмережевого екрану полягає в тому, що без нього системи внутрішньої мережі наражаються на небезпеку з боку слабо захищених служб мережі Internet, а також зондування і атакам з будь-яких інших хост - комп'ютерів зовнішньої мережі.

Проблеми недостатньої інформаційної безпеки є "вродженими" практично для всіх протоколів і служб Internet. Велика частина цих проблем пов'язана з історичною залежністю Internet від операційної системи UNIX. Відомо, що мережа Arpanet (прабатько Internet) будувалася як мережа, що зв'язує дослідні центри, наукові, військові та урядові установи, великі університети США. Ці структури використовували операційну систему UNIX в якості платформи для комунікацій і вирішення власних завдань. Тому особливості методології програмування в середовищі UNIX та її архітектури наклали відбиток на реалізацію протоколів обміну і політики безпеки в мережі. Через відкритості та поширеності система UNIX стала улюбленою здобиччю хакерів. Тому зовсім не дивно, що набір протоколів TCP / IP, який забезпечує комунікації в глобальній мережі Internet, має "вроджені" недоліки захисту. Те ж саме можна сказати і про ряд служб Internet.

Набір протоколів управління передачею повідомлень в Internet (Transmission Control Protocol / Internet Protocol - TCP / IP) використовується для організації комунікацій в неоднорідному мережевому середовищі, забезпечуючи сумісність між комп'ютерами різних типів. Сумісність - одна з основних переваг TCP / IP, тому більшість локальних комп'ютерних мереж підтримує ці протоколи. Крім того, протоколи TCP / IP надають доступ до ресурсів глобальної мережі Internet. Оскільки TCP / IP підтримує маршрутизацію пакетів, він зазвичай використовується в якості міжмережевого протоколу. Завдяки своїй популярності TCP / IP став стандартом де фактора для міжмережевої взаємодії.

У заголовках пакетів TCP / IP зазначається інформація, яка може піддатися нападам хакерів. Зокрема, хакер може підмінити адресу відправника у своїх "шкідливих" пакетах, після чого вони будуть виглядати, як пакети, що передаються авторизованим клієнтом.

Функціональні вимоги до міжмережевих екранів включають:

- вимоги до фільтрації на мережевому рівні;
- вимоги до фільтрації на прикладному рівні;
- вимоги по налаштуванню правил фільтрації та адміністрування;

- вимоги до засобів мережевої аутентифікації;
- вимоги щодо впровадження журналів та обліку.

Більшість компонентів міжмережевих екранів можна віднести до однієї з трьох категорій:

- фільтруючі маршрутизатори;
- шлюзи мережевого рівня;
- шлюзи прикладного рівня.

Ці категорії можна розглядати як базові компоненти реальних міжмережевих екранів. Лише деякі міжмережеві екрани включають тільки одну з перерахованих категорій. Тим не менше, ці категорії відображають ключові можливості, що відрізняють міжмережеві екрани один від одного.

Фільтруючий маршрутизатор являє собою маршрутизатор або працюючий на сервері програму, сконфігуровану таким чином, щоб фільтрувати вхідні і вихідні пакети. Фільтрація пакетів здійснюється на основі інформації, що міститься в TCP-і IP-заголовках пакетів.

Фільтруючі маршрутизатори звичайно мають можливості фільтрувати IP-пакет на основі групи наступних полів заголовка пакету:

- IP-адреса відправника (адреса системи, яка послала пакет);
- IP-адресу одержувача (адреса системи, яка приймає пакет);
- порт відправника (порт з'єднання в системі відправника);
- порт одержувача (порт з'єднання в системі одержувача);

Порт - це програмне поняття, яке використовується клієнтом або сервером для здійснення та отримання повідомлень; порт ідентифікується 16 - бітовим числом.

В даний час не всі фільтруючі маршрутизатори фільтрують пакети по TCP / UDP - порт відправника, однак багато виробників маршрутизаторів почали забезпечувати таку можливість. Деякі маршрутизатори перевіряють, з якого мережевого інтерфейсу маршрутизатора прийшов пакет, і потім використовують цю інформацію як додатковий критерій фільтрації.

Фільтрація може бути реалізована в різний спосіб для блокування сполук з певними хост - комп'ютерами або портами. Наприклад, можна блокувати з'єднання, що надходять від конкретних адрес тих хост-комп'ютерів і мереж, які вважаються ворожими або ненадійними.

Додавання фільтрації по портах TCP і UDP до фільтрації по IP-адресам забезпечує більшу гнучкість. Відомо, що такі сервери, як домен TELNET, зазвичай пов'язані з конкретними портами (наприклад, порт 23 протоколу TELNET). Якщо міжмережевий екран може блокувати з'єднання TCP або UDP з певними портами або від них, то можна реалізувати політику безпеки, при якій деякі види з'єднань встановлюються лише з конкретними хост - комп'ютерами.

До позитивних якостей фільтруючих маршрутизаторів слід віднести:

- порівняно невисоку вартість;
- гнучкість у визначенні правил фільтрації;
- невелику затримку при проходженні пакетів.

Недоліками фільтруючих маршрутизаторів є:

- правила фільтрації пакетів важкі в описі і вимагають дуже хороших знань технологій TCP і UDP;
- при порушенні працездатності брандмауера з фільтрацією пакетів всі комп'ютери за ним стають повністю незахищеними або недоступними;
- аутентифікацію з використанням IP-адреси можна обдурити шляхом підміни IP-адреси (атакуюча система видає себе за іншу, використовуючи її IP-адресу);
- відсутня аутентифікація на рівні користувача.

Шлюзи мережевого рівня

Шлюз мережевого рівня іноді називають системою трансляції мережевих адрес або шлюзом сеансового рівня моделі OSI. Такий шлюз виключає, пряма взаємодія між авторизованим клієнтом і зовнішнім хост-комп'ютером. Шлюз мережевого рівня приймає запит довіреного клієнта на конкретні

послуги, і після перевірки допустимості запитаного сеансу встановлює з'єднання із зовнішнім хост - комп'ютером. Після цього шлюз копіює пакети в обох напрямках, не здійснюючи їх фільтрації.

Шлюз стежить за підтвердженням зв'язку між авторизованим клієнтом і зовнішнім хост - комп'ютером, визначаючи, чи є запитуваний сеанс зв'язку допустимим.

Фактично більшість шлюзів мережевого рівня не є самостійними продуктами, а поставляються в комплекті зі шлюзами прикладного рівня. Прикладами таких шлюзів є Gauntlet Internet Firewall компанії Trusted Information Systems, Alta Vista Firewall компанії DEC і ANS Interlock компанії ANS. Наприклад, Alta Vista Firewall використовує канальні посередники прикладного рівня для кожної з шести служб TCP / IP, до яких належать, зокрема, FTP, HTTP (Hyper Text Transport Protocol) і Telnet. Крім того, міжмережевий екран компанії DEC забезпечує шлюз мережевого рівня, що підтримує інші загальнодоступні служби TCP / IP, такі як Gopher і SMTP, для яких міжмережевий екран не надає посередників прикладного рівня.

Шлюз мережевого рівня виконує ще одну важливу функцію захисту: він використовується в якості сервера-посередника. Цей сервер-посередник виконує процедуру трансляції адрес, при якій відбувається перетворення внутрішніх IP-адрес в одну "надійну" IP-адресу. Ця адреса асоціюється з міжмережевим екраном, з якого передаються всі вихідні пакети. У результаті в мережі зі шлюзом мережевого рівня всі вихідні пакети виявляються відправленими з цього шлюзу, що виключає прямий контакт між внутрішньою (авторизованої) мережею і потенційно небезпечною зовнішньою мережею. IP-адреса шлюзу мережевого рівня стає єдино активною IP-адресою, яка потрапляє в зовнішню мережу. Таким чином, шлюз мережевого рівня та інші сервери-посередники захищають внутрішні мережі від нападів типу підміни адрес.

Шлюзи прикладного рівня

Для усунення ряду недоліків, властивих фільтруючим маршрутизаторам, міжмережеві екрани повинні використовувати додаткові програмні засоби для фільтрації повідомлень сервісів типу TELNET і FTP. Такі програмні засоби називаються повноважними серверами (серверами-посередниками), а хост-комп'ютер, на якому вони виконуються, - шлюзом прикладного рівня.

Шлюз прикладного рівня виключає пряму взаємодію між авторизованим клієнтом і зовнішнім хост - комп'ютером. Шлюз фільтрує всі вхідні і вихідні пакети на прикладному рівні. Пов'язані з додатком сервери - посередники перенаправляють через шлюз інформацію, що генерується конкретними серверами.

Для досягнення більш високого рівня безпеки та гнучкості шлюзи прикладного рівня і фільтруючі маршрутизатори можуть бути об'єднані в одному міжмережному екрані. Як приклад розглянемо мережу, в якій за допомогою фільтруючого маршрутизатора блокуються вхідні з'єднання TELNET і FTP. Цей маршрутизатор допускає проходження пакетів TELNET або FTP тільки до одного хост - комп'ютера - шлюзу прикладного рівня TELNET / FTP. Зовнішній користувач, який хоче з'єднатися з деякою системою в мережі, повинен спочатку з'єднатися зі шлюзом прикладного рівня, а потім вже з потрібним внутрішнім хост-комп'ютером.

На додаток до фільтрації пакетів багато шлюзи прикладного рівня реєструють всі виконувані сервером дії і, що особливо важливо, попереджають мережевого адміністратора про можливі порушення захисту. Наприклад, при спробах проникнення в мережу ззовні BorderWare Firewall Server компанії Secure Computing дозволяє фіксувати адреси відправника і одержувача пакетів, час, в який ці спроби були зроблені, і використовуваний протокол. Міжмережевий екран Black Hole компанії Milkyway Networks реєструє всі дії сервера і попереджає адміністратора про можливі порушення, посилаючи йому повідомлення по електронній пошті або на пейджер. Аналогічні функції виконують і ряд інших шлюзів прикладного рівня.

Шлюзи прикладного рівня дозволяють забезпечити найбільш високий рівень захисту, оскільки взаємодія із зовнішнім світом реалізується через мало прикладних повноважних програм-посередників, повністю контролюють весь вхідний і вихідний трафік.

Шлюзи прикладного рівня мають ряд переваг у порівнянні зі звичайним режимом, при якому прикладної трафік пропускається безпосередньо до внутрішніх хост - комп'ютерів. Розглянемо ці переваги.

– Невидимість структури мережі, що захищається з глобальної мережі Internet. Імена внутрішніх систем можна не повідомляти зовнішнім системам через DNS, оскільки шлюз прикладного рівня може бути єдиним хост - комп'ютером, ім'я якого повинно бути відомо зовнішнім системам.

– Надійна аутентифікація та реєстрація. Прикладної трафік може бути аутентифікований, перш ніж він досягне внутрішніх хост-комп'ютерів, і може бути зареєстрований більш ефективно, ніж за допомогою стандартної реєстрації.

– Оптимальне співвідношення між ціною і ефективністю. Додаткові або апаратні засоби для аутентифікації або реєстрації потрібно встановлювати тільки на шлюзі прикладного рівня.

– Прості правила фільтрації. Правила на фільтруючому маршрутизаторі виявляються менш складними, ніж вони були б, якщо б маршрутизатор сам фільтрував прикладний трафік і відправляв його великому числу внутрішніх систем. Маршрутизатор повинен пропускати прикладної трафік, призначений тільки для шлюзу прикладного рівня, і блокувати весь інший трафік.

– Можливість організації великого числа перевірок. Захист на рівні додатків дозволяє здійснювати велику кількість додаткових перевірок, що знижує ймовірність злому з використанням "дірок" у програмному забезпеченні.

До недоліків шлюзів прикладного рівня відносяться:

– більш низька продуктивність у порівнянні з фільтруючими маршрутизаторами; зокрема, при використанні клієнт-серверних протоколів, таких як TELNET, потрібно двокрокова процедура для вхідних та вихідних з'єднань;

– більш висока вартість у порівнянні з фільтруючим маршрутизатором.

Крім TELNET і FTP шлюзи прикладного рівня зазвичай використовуються для електронної пошти, Windows і деяких інших служб.

Одним з важливих компонентів концепції міжмережевих екранів є автентифікація (перевірка дійсності користувача). Перш ніж користувачеві буде надано право скористатися тим чи іншим сервісом, необхідно переконатися, що він дійсно той, за кого себе видає.

Одним із способів аутентифікації є використання стандартних UNIX-паролів. Однак ця схема найбільш вразливе з точки зору безпеки - пароль може бути перехоплений і використаний іншою особою. Багато інцидентів в мережі Internet відбулися через уразливість традиційних паролів. Зловмисники можуть спостерігати за каналами в мережі Internet і перехоплювати що передаються в них відкритим текстом паролі, тому схему аутентифікації з традиційними паролями слід визнати застарілою.

Для подолання цього недоліку розроблено ряд засобів посиленою аутентифікації: смарт-карти, персональні жетони, біометричні механізми і т.п. Хоча в них задіяні різні механізми аутентифікації, загальним для них є те, що паролі, які генеруються цими пристроями, не можуть бути повторно використані порушником, що спостерігає за встановленням зв'язку. Оскільки проблема з паролями в мережі Internet є постійною, міжмережевий екран для з'єднання з Internet, не має в своєму розпорядженні засобів посилення аутентифікації або не використовує їх, втрачає всякий сенс.

Ряд найбільш популярних засобів посиленою аутентифікації, що застосовуються в даний час, називаються системами з одноразовими паролями. Наприклад, смарт-карти або жетони аутентифікації генерують інформацію, яку хост-комп'ютер використовує замість традиційного пароля. Результатом є одноразовий пароль, який, навіть якщо він буде перехоплений, не може бути використаний зловмисником під виглядом користувача для встановлення сеансу з хост - комп'ютером.

Так як міжмережеві екрани можуть централізувати управління доступом в мережі, вони є підходящим місцем для установки програм або пристроїв посиленою аутентифікації. Хоча кошти посиленою аутентифікації можуть використовуватися на кожному хост - комп'ютері, більш практично їх розміщення на межсетевом екрані. Якщо хост - комп'ютери не застосовують заходів посиленої

аутентифікації, зловмисник може спробувати зламати паролі або перехопити мережевий трафік з метою знайти в ньому сеанси, в ході яких передаються паролі.

У цьому випадку сеанси TELNET або FTP, що встановлюються з боку мережі Internet з системами мережі, повинні проходити перевірку за допомогою засобів посиленою аутентифікації, перш ніж вони будуть дозволені, Системи мережі можуть запитувати для дозволу доступу і статичні паролі, але ці паролі, навіть якщо вони будуть перехоплені зловмисником, не можна буде використовувати, тому що кошти посиленою аутентифікації та інші компоненти міжмережевого екрану запобігають проникнення зловмисника або обхід ними міжмережевого екрану.

Основні схеми мережевого захисту на базі міжмережевих екранів

При підключенні корпоративної або локальної мережі до глобальних мереж адміністратор мережевої безпеки має вирішувати такі завдання:

- захист корпоративної або локальної мережі від несанкціонованого доступу з боку глобальної мережі;
- приховування інформації про структуру мережі та її компонентів від користувачів глобальної мережі,
- розмежування доступу в мережу, що захищається з глобальної мережі і з мережі, що захищається в глобальну мережу.

Необхідність роботи з віддаленими користувачами вимагає встановлення жорстких обмежень доступу до інформаційних ресурсів мережі, що захищається. При цьому часто виникає потреба в організації у складі корпоративної мережі декількох сегментів з різними рівнями безпеки:

- вільно доступні сегменти (наприклад, рекламний WWW-сервер),
- сегмент з обмеженим доступом (наприклад, для доступу співробітникам організації з віддалених вузлів),
- закриті сегменти (наприклад, локальна фінансова мережа організації).

Для захисту корпоративної або локальної мережі застосовуються такі основні схеми організації міжмережевих екранів:

- міжмережевий екран - фільтруючий маршрутизатор;
- міжмережевий екран на основі двопортового шлюзу;
- міжмережевий екран на основі екранованого шлюзу;
- міжмережевий екран - екранована підмережа.

Міжмережевий екран, заснований на фільтрації пакетів, є поширеним і найбільш простим в реалізації. Він складається з фільтруючого маршрутизатора, розташованого між що захищається мережею і мережею Internet. Фільтруючий маршрутизатор налаштований для блокування або фільтрації вхідних і вихідних пакетів на основі аналізу їх адрес і портів. Комп'ютери, що знаходяться в мережі, що захищається, мають прямий доступ в мережу Internet, в той час як більша частина доступу до них з Internet блокується. Часто блокуються такі небезпечні служби, як X Windows, NIS і NFS.

Міжмережевий екран на базі двопортового прикладного шлюзу включає дводомний хост-комп'ютер з двома мережевими інтерфейсами. При передачі інформації між цими інтерфейсами і здійснюється основна фільтрація. Для забезпечення додаткового захисту між прикладним шлюзом та мережею Internet зазвичай розміщують фільтруючий маршрутизатор. У результаті між прикладним шлюзом та маршрутизатором утворюється внутрішня екранована підмережа. Цю підмережу можна використовувати для розміщення доступних ззовні інформаційних серверів.

Міжмережевий екран на основі екранованого шлюзу об'єднує фільтруючий маршрутизатор і прикладної шлюз, дозволяються з боку внутрішньої мережі. Прикладної шлюз реалізується на хост - комп'ютері і має тільки один мережевий інтерфейс.

Міжмережевий екран, що складається з екранованої підмережі, являє собою розвиток схеми міжмережевого екрану на основі екранованого шлюзу. Для створення екранованої підмережі використовуються два екрануючих маршрутизатора. Зовнішній маршрутизатор розташовується між мережею Internet і під мережею, що екранується, а внутрішній - між підмережею, що екранується і

захищається внутрішньою мережею. Ця підмережа містить прикладної шлюз, а також може включати інформаційні сервери та інші системи, що вимагають контрольованого доступу. Ця схема міжмережевого екрану забезпечує хорошу безпеку завдяки організації екранованої підмережі, яка ще краще ізолює внутрішню мережу, що захищається від Internet.

Можливості брандмауер Windows

- Блокувати комп'ютерним вірусам і «черв'якам» доступ на комп'ютер.
- Здійснити запит до користувача про вибір блокування або дозволу для певних запитів на підключення.
- Вести облік (журнал безпеки) - за бажанням користувача - записуючи дозволені та заблоковані спроби підключення до комп'ютера. Цей журнал може виявитися корисним для діагностики помилок.

Відсутні можливості брандмауер Windows

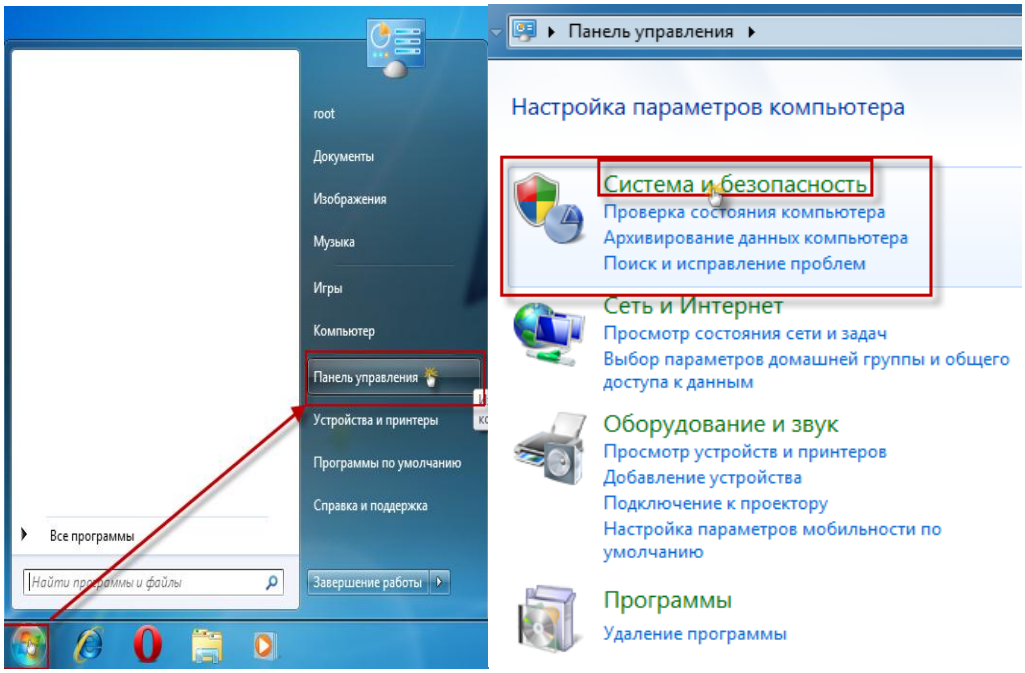
– Виявити або знешкодити комп'ютерні віруси, якщо вони вже потрапили на комп'ютер. З цієї причини необхідно також встановити антивірусне програмне забезпечення та своєчасно оновлювати його, щоб запобігти пошкодження комп'ютера вірусами, «черв'яками» та іншими небезпечними об'єктами, а також не допустити використання даного комп'ютера для поширення на інші комп'ютери.

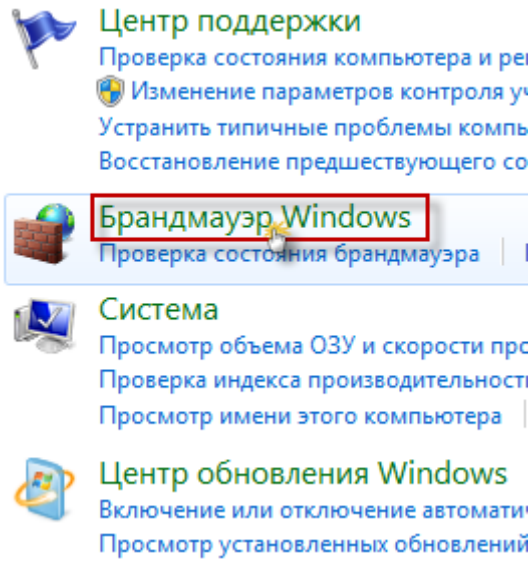
– Заборонити користувачеві відкривати повідомлення електронної пошти з небезпечними вкладеннями. Не відкривайте вкладення в повідомленнях електронної пошти від незнайомих відправників. Слід проявляти обережність, навіть якщо джерело повідомлення електронної пошти відоме і заслуговує довіри. При отриманні від знайомого користувача електронного листа з вкладенням уважно прочитайте тему повідомлення перед тим, як відкрити його. Якщо тема повідомлення являє собою безладний набір знаків або не має сенсу, не відкривайте лист, поки не зв'яжетеся з відправником для отримання підтвердження.

– Блокувати спам або несанкціоновані поштові розсилки, щоб вони не надходили в папку вхідних повідомлень. Однак деякі програми електронної пошти здатні робити це.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

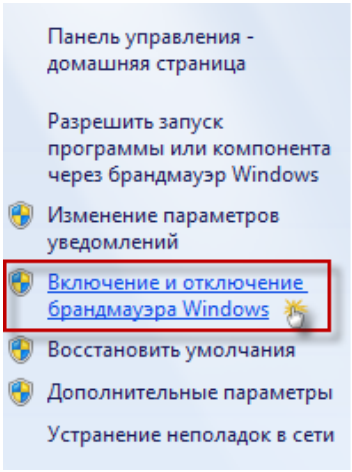
1. Виконати послідовність дій ***Пуск, Панель управления, Система и безопасность, Братмауэр Windows***.





2. З’ясуйте стан підключення брандмауера. Якщо він відключений – включіть його.

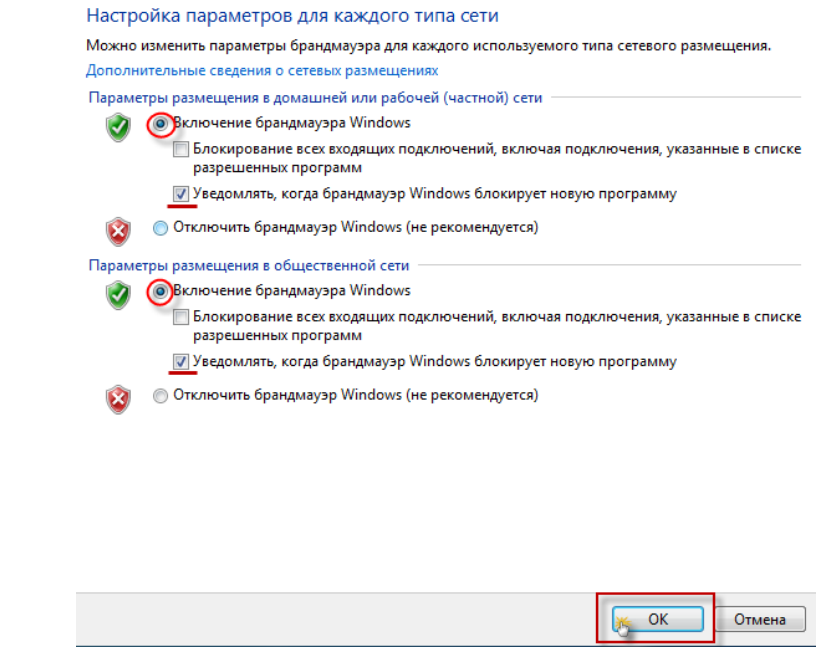
Налаштування брандмауера Windows відбувається, в першу чергу, шляхом вказівки "Винятків".



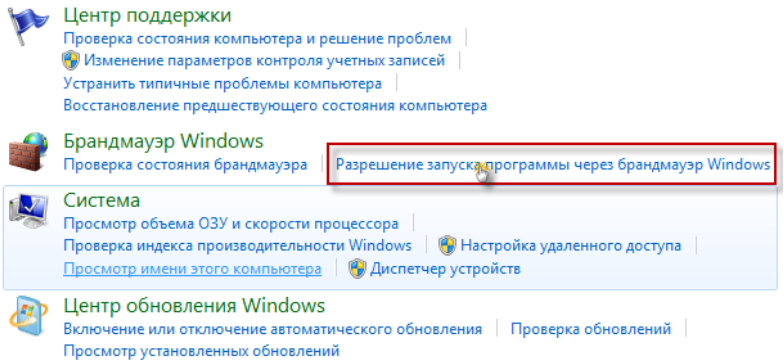
3. Створіть виняток для програми, яка повинна приймати вихідні підключення з мережі.

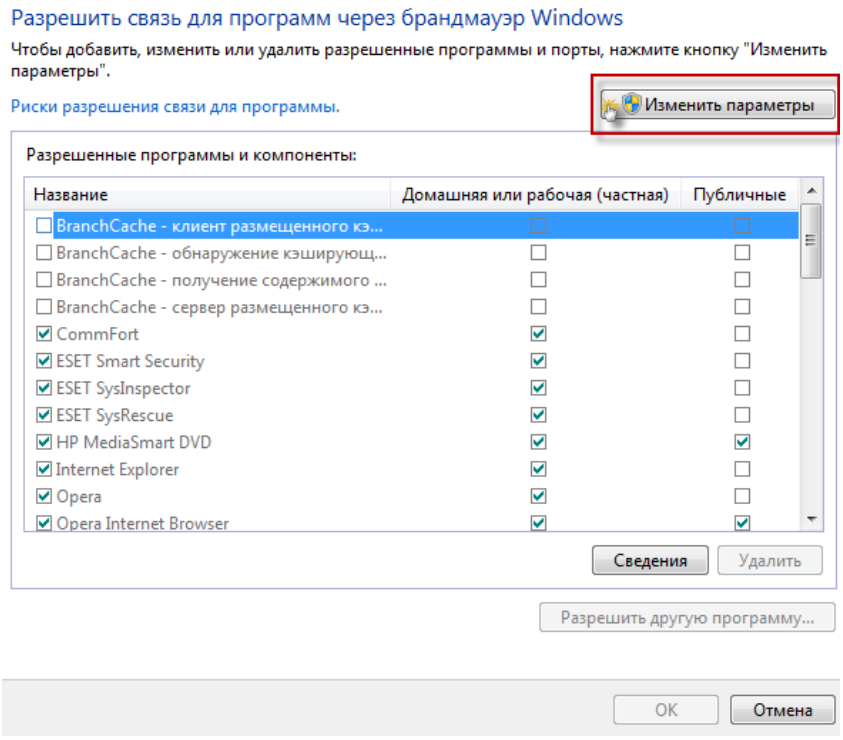
- Щоб створити виняток потрібно натиснути кнопку "Додати програму ...." відкриється вікно, приклад якого показаний нижче.

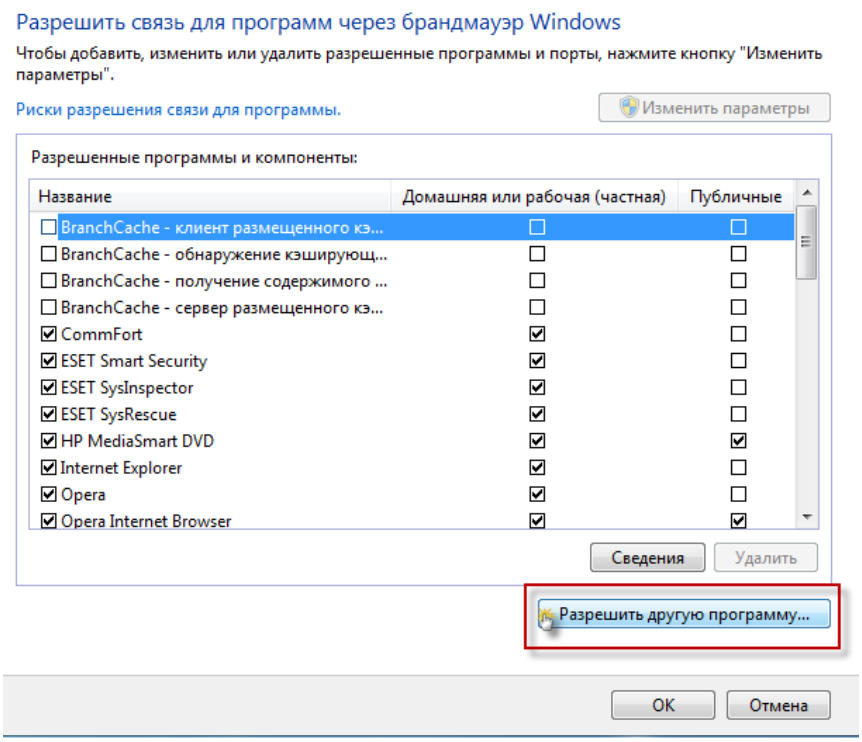
У цьому вікні в списку програм перераховані ті з них, які встановлені на комп'ютері. Якщо програма, якою необхідно дозволити приймати вхідні підключення, відсутній у списку, то за допомогою кнопки Огляд можна вказати шлях до неї. Після натискання кнопки OK виключення буде створено і додано до списку, де буде зазначено прапорцем, який говорить про те, що дане правило дозволяє зазначеним Додатком відкривати порти і чекати підключення з мережі. Якщо необхідно заборонити додатком відкривати порти, то прапорець слід зняти.

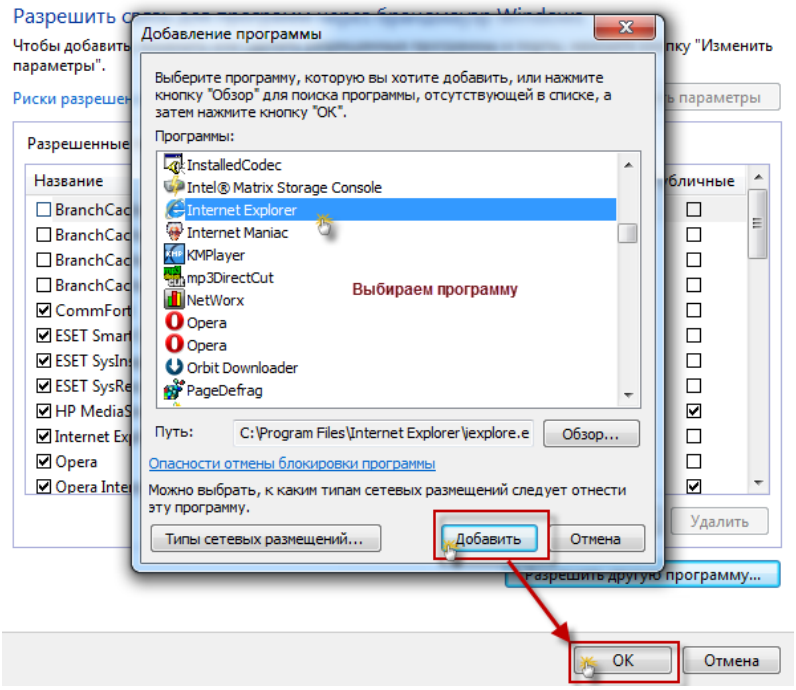

Настройка параметров для каждого типа сети
Можно изменить параметры брандмауэра для каждого используемого типа сетевого размещения.
Дополнительные сведения о сетевых размещениях
Параметры размещения в домашней или рабочей (частной) сети
Включение брандмауэра Windows
Блокирование всех входящих подключений, включая подключения, указанные в списке разрешенных программ
Уведомлять, когда брандмауэр Windows блокирует новую программу
Отключить брандмауэр Windows (не рекомендуется)
Параметры размещения в общественной сети
Включение брандмауэра Windows
Блокирование всех входящих подключений, включая подключения, указанные в списке разрешенных программ
Уведомлять, когда брандмауэр Windows блокирует новую программу
Отключить брандмауэр Windows (не рекомендуется)

OK
Отмена


Центр поддержки
Проверка состояния компьютера и решение проблем
Изменение параметров контроля учетных записей
Устранить типичные проблемы компьютера
Восстановление предшествующего состояния компьютера
Брандмауэр Windows
Проверка состояния брандмауэра
Разрешение запуска программы через брандмауэр Windows
Система
Просмотр объема ОЗУ и скорости процессора
Проверка индекса производительности Windows
Настройка удаленного доступа
Просмотр имени этого компьютера
Диспетчер устройств
Центр обновления Windows
Включение или отключение автоматического обновления
Проверка обновлений
Просмотр установленных обновлений


Разрешить связь для программ через брандмауэр Windows
Чтобы добавить, изменить или удалить разрешенные программы и порты, нажмите кнопку "Изменить параметры".
Риски разрешения связи для программы.
Изменить параметры
Разрешенные программы и компоненты:
Название
Домашняя или рабочая (частная)
Публичные
BranchCache - клиент размещенного кэ...
BranchCache - обнаружение кэширующ...
BranchCache - получение содержимого ...
BranchCache - сервер размещенного кэ...
CommFort
ESET Smart Security
ESET SysInspector
ESET SysRescue
HP MediaSmart DVD
Internet Explorer
Opera
Opera Internet Browser
Сведения
Удалить
Разрешить другую программу...
OK
Отмена





3. Процес створення винятку опишіть у звіті з використанням власних скріншотів.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається брандмауером?
2. Які основні функції брандмауера?
3. Дайте визначення апаратному та програмному міжмережевим екранам.
4. Що включають в себе функціональні вимоги до міжмережевих екранів?
5. Назвіть основні категорії компонентів між мережевих екранів.
6. Дайте визначення фільтруючому маршрутизаторі.
7. Назвіть переваги та недоліки фільтруючих маршрутизаторів.
8. Охарактеризуйте шлюзи мережевого рівня.
9. Дайте визначення шлюзам прикладного рівня.
10. Які ви знаєте основні схеми мережевого захисту на базі міжмережевих екранів.

11. Назвіть можливості брандмауер Windows.

Лабораторна робота №12

Тема: Основи безпеки інформації в комп'ютерних мережах.

Мета: ознайомитися з основами безпеки інформації в комп'ютерній мережі, найпоширенішими ризиками та способами попередження втрати інформації; навчитися забезпечувати надійний захист інформації під час роботи в мережі.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Мережева атака (Network Attacks) або віддалена атака (Remote Attacks) - атака на розподілену обчислювальну систему, що здійснюють програмні засоби каналами зв'язку. Така атака може бути здійснена на протоколи і мережні служби, а також на операційні системи та прикладні програми вузлів мережі.

Типові небезпеки

- угадування паролів, або атаки за словником;
- реєстрація та маніпуляції з мережним трафіком;
- імпорт фальшивих пакетів даних;
- експлуатація відомих уразливостей програмного забезпечення (мови макросів, помилки в ОС, служби віддаленого доступу тощо).

З-поміж типових віддалених атак виокремлюють такі:

- аналіз мережного трафіку;
- підміна довіреного об'єкта в розподіленій системі;
- упровадження в розподілену систему фальшивого об'єкта через нав'язування фальшивого маршруту;
- упровадження в розподілену систему фальшивого об'єкта шляхом використання недоліків алгоритмів віддаленого пошуку;
- відмова в обслуговуванні.

Сервіси безпеки

- автентифікація;
- керування доступом;
- конфіденційність даних;
- цілісність даних;
- унеможливлення відмови від авторства.

Автентифікація. Цей сервіс забезпечує автентифікацію сторін, що спілкуються (Communicating peer Entity), і автентифікацію джерела даних.

Автентифікацію сторін здійснюють у момент встановлення з'єднання та іноді під час передавання даних з метою підтвердження автентичності сутностей з'єднання. Завдяки використанню цього сервісу можна бути впевненим, що суб'єкт не влаштує «маскарад» і не використає повторно попередній несанкціонований сеанс зв'язку. Застосовують різні схеми автентифікації, які забезпечують різний ступінь захисту.

Автентифікація джерела даних — це підтвердження автентичності джерела блоку даних. Сервіс, який реалізують засобами певного рівня моделі OSI та надають для сутностей вищого рівня, підтверджує автентичність сутності цього ж таки рівня. Слід зауважити, що сервіс не забезпечує захист від повторення або пошкодження даних.

Керування доступом. Цей сервіс забезпечує захист від несанкціонованого використання ресурсів, доступних через взаємодію відкритих систем. Керування доступом може застосовуватися до різних типів доступу до ресурсу (наприклад, використання комунікаційного ресурсу, читання, записування або видалення інформаційного ресурсу, виконання ресурсу оброблення).

Конфіденційність даних. Цей сервіс забезпечує захист даних від їх несанкціонованого розкриття. Розрізняють кілька сервісів конфіденційності даних:

– конфіденційність даних під час обміну зі встановленням з'єднання — цей сервіс захищає всю інформацію користувачів, окрім даних щодо запиту на встановлення з'єднання (це залежатиме від рівня моделі OSI);

– конфіденційність даних під час обміну без встановлення з'єднання — цей сервіс захищає всю інформацію користувачів;

– конфіденційність окремих полів даних — цей сервіс забезпечує захист інформації в окремих обраних полях даних у сеансі зі встановленням з'єднання або без нього;

– конфіденційність трафіку — цей сервіс забезпечує захист інформації, яку отримують під час здійснення аналізу трафіку.

Цілісність даних. Цей сервіс спрямований на протидію активним загрозам. Розрізняють такі сервіси цілісності даних:

– цілісність даних під час обміну зі встановленням з'єднання з відновленням — цей сервіс забезпечує цілісність усіх даних користувача шляхом виявлення будь-якої модифікації даних (додавання, видалення та повторення) і здійснює спробу відновити дані;

– цілісність даних під час обміну зі встановленням з'єднання без відновлення — так само, як і попередній сервіс, забезпечує цілісність усіх даних, але без спроби їхнього відновлення;

– цілісність окремих полів даних під час обміну зі встановленням з'єднання — цей сервіс забезпечує цілісність окремих обраних полів даних у сеансі зі встановленням з'єднання і визначає, чи не було ці поля модифіковано (додано, видалено та повторено);

– цілісність даних під час обміну без встановлення з'єднання — цей сервіс на відміну від попередніх у разі його реалізації на певному рівні моделі OSI забезпечує цілісність даних за запитом сутності вищого рівня; сервіс забезпечує цілісність окремого блоку даних, що передається без встановлення з'єднання, і може визначати, чи було блок даних модифіковано, крім того він може виявляти дані, що повторюються;

– цілісність окремих полів даних під час обміну без встановлення з'єднання — цей сервіс забезпечує цілісність окремих обраних полів в окремому блоці даних, що передається без встановлення з'єднання, і визначає, чи було модифіковано обрані поля.

Унеможливлений відмови від авторства. Унеможливлений відмови від авторства включає:

– унеможливлення відмови від авторства з підтвердженням справжності джерела даних — цей сервіс захищає одержувача даних від будь-якої спроби відправника відмовитися від факту відправлення ним даних чи справжності їхнього вмісту;

– унеможливлення відмови від авторства з підтвердженням про отримання — цей сервіс сповіщає відправнику даних про їх отримання, що не дає одержувачу відмовитися від факту отримання даних або викривити їх.

Специфічні механізми безпеки. Реалізувати сервіси безпеки можна, впровадивши на певному рівні моделі OSI такі механізми:

- шифрування;
- цифровий підпис;
- керування доступом;
- контроль цілісності даних;
- автентифікаційний обмін;
- заповнення трафіку;
- керування маршрутом;
- нотаризація.

Шифрування. Цей механізм, який захищає окремі дані або потік даних (шифрування трафіку), може бути використаний іншими механізмами або може замінити деякі з них.

Застосовують симетричні й асиметричні алгоритми шифрування. Використання алгоритму шифрування майже завжди передбачає впровадження механізму керування ключами.

Цифровий підпис. Механізм цифрового підпису складається із двох процедур:

- підписання блоку даних;
- перевірки підписаного блоку даних.

Процедура підписування блоку даних полягає у шифруванні блоку даних або обчисленні криптографічної контрольної суми з використанням приватної (унікальної та конфіденційної) інформації користувача, що здійснює підпис.

Для перевірки підписаного блоку даних використовують процедури та інформацію, що є загальнодоступними, але з яких неможливо здобути приватну інформацію про того, хто підписує. Ця процедура, фактично, дає змогу перевірити, чи справді цифровий підпис було зроблено з використанням приватної інформації того, хто підписав блок даних.

Керування доступом. Ці механізми використовують ідентифікацію сутності або деяку інформацію про сутність (як належність до певної відомої множини сутностей), а також посвідчення, надане сутністю для визначення і встановлення її прав доступу. Якщо сутність намагається здійснити неавторизований (несанкціонований) доступ (використати неавторизований ресурс або недозволений метод доступу до авторизованого ресурсу), функція керування доступом перешкодить цьому і, можливо, згенерує повідомлення про інцидент (для ініціювання протидії або з метою аудита).

Механізми керування доступом можуть використовувати один чи кілька із зазначених нижче видів та джерел інформації:

- бази даних керування доступом, в яких зберігаються права доступу сутностей; ці бази підтримуються централізовано або на кінцевих системах; права доступу зберігаються у вигляді списків керування доступом або матриці ієрархічної чи розподіленої структури (використання бази даних керування доступом передбачає, що сутності перед цим було автентифіковано);
- інформація автентифікації, володіння якою і надання якої є доказом авторизації (наприклад, паролі);
- посвідчення, володіння якими і подання яких є доказом дозволу доступу до сутності або ресурсу, вказаних у посвідченні;
- мітки безпеки, асоційовані із сутностями (суб'єктами та об'єктами доступу), які використовують для надання або заборони доступу, як правило, на основі політики безпеки;
- момент часу, коли було здійснено спробу доступу;
- маршрут спроби доступу;
- тривалість спроби доступу.

Механізми керування доступом можуть бути задіяні на будь-якій із сторін, що здійснюють зв'язок, а також у проміжній точці. Механізми, задіяні у точці, яка ініціює доступ, і у проміжних точках, мають перевіряти, чи відправник авторизований для зв'язку з одержувачем та (або) для використання комунікаційних ресурсів. Якщо зв'язок було здійснено без встановлення з'єднання, вимоги механізму, реалізованого у кінцевій точці, мають бути відомими у точці, що ініціює доступ, апріорі.

Контроль цілісності даних

- цілісність окремого блоку даних або поля інформації;
- цілісність потоку блоків даних або полів інформації.

Для забезпечення цих двох видів сервісу цілісності у загальному випадку можуть бути задіяні різні механізми, але контроль цілісності потоку без контролю окремих блоків даних (полів) не є практичним.

Контроль цілісності окремого блоку даних (поля) здійснюють як на стороні, що передає дані, так і на стороні, що їх приймає. На стороні, що передає, до блоку даних додається інформація, яка є функцією від цих даних (циклічна або криптографічна контрольна сума, яка також може бути

зашифрованою). На стороні, що приймає, генерується аналогічна контрольна сума, яка в подальшому порівнюється з отриманою. Зауважте, цей механізм не здатний захистити від повторення блоків даних.

Перевірка цілісності потоку блоків даних (тобто захист від втрати даних, їх перевпорядкування, дублювання, вставляння та модифікації) вимагає додаткового впровадження порядкових номерів, часових штампів або криптографічного зв'язування (коли результат шифрування чергового блоку залежить від попереднього). Під час здійснення зв'язку без встановлення з'єднання використання часових штампів надає обмежений захист від дублювання блоків даних.

Автентифікаційний обмін. Механізми автентифікаційного обміну впроваджуються на певному рівні моделі OSI для підтвердження автентичності сутності. Якщо механізм не підтверджує автентичність сутності, з'єднання забороняється або закривається вже встановлене з'єднання, при цьому може бути згенероване повідомлення про інцидент (для ініціювання протидії або з метою аудита). Автентифікаційний обмін здійснюють у кілька способів:

–використовуючи автентифікаційну інформацію (на кшталт паролів), яку надає відправник і перевіряє одержувач;

–із застосуванням криптографічних методів;

–демонструючи характеристики або можливості сутності.

Щоб уникнути повторення даних, криптографічні методи іноді використовують разом із процедурами «рукостискання» (Handshaking) — обміну з квитируванням, підтвердження зв'язку.

Методи автентифікаційного обміну інколи (залежно від обставин) використовують разом із:

- часовими штампами і синхронізацією годинників;
- двох- і трьохетапними процедурами «рукостискання» (відповідно для одно-та двохсторонньої автентифікації);
- сервісами унеможливлення відмови від авторства, що досягається використанням механізмів цифрового підпису та (або) нотаризації.

Заповнення трафіку. Механізми заповнення трафіку застосовують для забезпечення захисту від аналізування трафіку. Ці механізми ефективні лише в поєднанні із засобами забезпечення конфіденційності.

Керування маршрутом. Маршрути можна обирати динамічно або статично таким чином, щоб використовувати лише фізично безпечні підмережі, вузли комутації та канали. Кінцеві системи у разі виявлення неодноразових атак на маршруті мають можливість звернутися до провайдера мережних послуг для встановлення з'єднання за іншим маршрутом.

Передавання даних, що мають мітки безпеки, через певні підмережі, вузли комутації та канали може бути заборонено політикою безпеки. Ініціатор з'єднання, або відправник даних, які передаються без встановлення з'єднання, має можливість обмежити маршрут таким чином, щоб оминути певні підмережі, вузли комутації та канали.

Нотаризація. За допомогою механізму нотаризації завіряються характеристики даних, що передаються між двома (або більше) сутностями (їх цілісність, джерело, час передавання і пункт призначення). Достовірність таких даних стверджує третя сторона, якій довіряють сутності, що взаємодіють, і яка володіє достатньою для цього інформацію. Кожна сутність, що взаємодіє із застосуванням механізму нотаризації, використовує цифровий підпис, шифрування і контроль цілісності.

Захист мережі за допомогою міжсіткового екрану

Міжсітковий екран – це напівпроникна мембрана, що розташовується між що внутрішньої мережею (що захищається) і зовнішнім середовищем (зовнішніми мережами чи іншими сегментами корпоративної мережі) і контролює всі інформаційні потоки у внутрішню мережу і з неї. Контроль інформаційних потоків складається в їхній фільтрації, тобто у вибірковому пропущенні через екран, можливо, з виконанням деяких перетворень і повідомленням відправника про те, що його даним у пропуску відмовлено. Фільтрація здійснюється на основі набору правил, попередньо завантажених в екран і сіткові аспекти, що є вираженням, політики безпеки організації.

Доцільно розділити випадки, коли екран установлюється на границі з зовнішньої (звичайно загальнодоступної) чи мережею на границі між сегментами однієї корпоративної мережі. Відповідно, ми буде говорити про зовнішній і внутрішній міжсітковий екрани.

Як правило, при спілкуванні з зовнішніми мережами використовується виняткове сімейство протоколів TCP/IP. Тому зовнішній міжсітковий екран повинен враховувати специфіку цих протоколів. Для внутрішніх екранів ситуація складніше, тут варто брати до уваги крім TCP/IP принаймні протоколи SPX/IPX, застосовувані в мережах Novell NetWare. Іншими словами, від внутрішніх екранів нерідко потрібна багатопротокольність.

При розгляді будь-якого питання, що стосується мережних технологій, основою служить семирівнева еталонна модель ISO/OSI. Міжсіткові екрани також доцільно класифікувати по тому, на якому рівні виробляється фільтрація - канальному, мережному, транспортному чи прикладному. Відповідно, можна говорити про концентратори, що екранують, (рівень 2), маршрутизаторах (рівень 3), про транспортне екранування (рівень 4) і про прикладні екрани (рівень 7). Існують також комплексні екрани, що аналізують інформацію на декількох рівнях.

Приведена конфігурація що екранує називається підсіткою. Як правило, сервіси, що організація надає для зовнішнього застосування (наприклад “представницький” Web-сервер), доцільно виносити саме в підсітку що екранує.

Крім виразних можливостей і припустимої кількості правил якість міжсіткового екрана визначається ще двома дуже важливими характеристиками - простотою застосування і власною захищеністю. У плані простоти використання першорядне значення мають наочний інтерфейс при завданні правил фільтрації і можливість централізованого адміністрування складних конфігурацій. У свою чергу, в останньому аспекті хотілося б виділити кошти централізованого завантаження правил фільтрації і перевірки набору правил на несуперечність. Важливий і централізований збір і аналіз реєстраційної інформації, а також одержання сигналів про спроби виконання дій, заборонених політикою безпеки.

Власна захищеність міжсіткового екрана забезпечується тими ж засобами, що і захищеність універсальних систем. При виконанні централізованого адміністрування варто ще подбати про захист інформації від пасивного й активного прослуховування мережі, тобто забезпечити її (інформації) цілісність і конфіденційність.

Хотілося б підкреслити, що природа екранування (фільтрації), як механізму безпеки, дуже глибока. Крім блокування потоків даних, що порушують політику безпеки, міжсітковий екран може ховати інформацію про мережу, що захищається, тим самим утрудняючи дії потенційних зловмисників. Так, прикладний екран може здійснювати дії від імені суб'єктів внутрішньої мережі, у результаті чого з зовнішньої мережі здається, що має місце взаємодія виняткова з міжсітковим екраном. При такому підході топологія внутрішньої мережі схована від зовнішніх користувачів, тому задача зловмисника істотно ускладнюється.

Більш загальним методом приховання інформації про топологію мережі, що захищається, є трансляція “внутрішніх” мережних адрес, що попутно вирішує проблему розширення адресного простору, виділеного організації.

Обмежуючий інтерфейс також можна розглядати як різновид екранування. На невидимий об'єкт важко нападати, особливо за допомогою фіксованого набору засобів. У цьому змісті Web-інтерфейс має природний захист, особливо в тому випадку, коли гіпертекстові документи формуються динамічно. Кожний бачить лише те, що йому покладене.

Роль Web-сервісу, що екранує, наочно виявляється і тоді, коли цей сервіс здійснює посередницькі (точніше, що інтегрують) функції при доступі до інших ресурсів, зокрема таблицям бази даних. Тут не тільки контролюються потоки запитів, але і ховається реальна організація баз даних.

Безпека програмного середовища

Ідея мереж з так називаними активними агентами, коли між комп'ютерами передаються не тільки пасивні, але й активні виконувані дані (тобто програми), зрозуміло, не нова. Спочатку ціль

полягала в тому, щоб зменшити сітковий трафік, виконуючи основну частину обробки там, де розташовуються дані (наближення програм до даних). На практиці це означало переміщення програм на сервери. Класичний приклад реалізації подібного підходу - це збережені процедури в реляційних СУБД.

Для Web-серверів аналогом збережених процедур є програми, що обслуговують загальний шлюзовий інтерфейс (Common Gateway Interface - CGI).

CGI-процедури розташовуються на серверах і звичайно використовуються для динамічного породження HTML-документів. Політика безпеки організації і процедурних мір повинні визначати, хто має право поміщати на сервер CGI-процедури. Жорсткий контроль тут необхідний, оскільки виконання сервером некоректної програми може привести до яких завгодно важких наслідків. Розумна міра технічного характеру складається в мінімізації привілеїв користувача, від імені якого виконується Web-сервер.

У технології Intranet, якщо піклуватися про якість і виразну силу користувальницького інтерфейсу, виникає нестаток у переміщенні програм з Web-серверів на клієнтські комп'ютери - для створення анімації, виконання семантичного контролю при введенні даних і т.д. Узагалі, активні агенти - невід'ємна частина технології Intranet.

У якому би напрямку не переміщалися програми по мережі, ці дії становлять підвищену небезпеку, тому що програма, отримана з ненадійного джерела, може містити ненавмисно внесені помилки чи цілеспрямовано створений шкідливий код. Така програма потенційно загрожує всім основним аспектам інформаційної безпеки:

- приступності (програма може поглинути всі наявні ресурси);
- цілісності (програма може знищити чи пошкодити дані);
- конфіденційності (програма може прочитати дані і передати їх по мережі).

Проблему ненадійних програм усвідомлювали давно, але, мабуть, тільки в рамках системи програмування Java уперше запропонована цілісна концепція її рішення.

Java пропонує три оборонних рубежі:

- надійність мови;
- контроль при одержанні програм;
- контроль при виконанні програм.

Утім, існує ще одне, дуже важливий засіб забезпечення інформаційної безпеки - безпрецедентна відкритість Java-системи. Вихідні тексти Java-компілятора й інтерпретатора доступні для перевірки, тому велика імовірність, що помилки і недоліки першими будуть виявляти чесні фахівці, а не зловмисники.

У концептуальному плані найбільших труднощів представляє контрольоване виконання програм, завантажених по мережі. Насамперед, необхідно визначити, які дії вважаються для таких програм припустимими. Якщо виходити з того, що Java – це мова для написання клієнтських частин додатків, одним з основних вимог до яких є мобільність, завантажена програма може обслуговувати тільки користувальницький інтерфейс і здійснювати мережну взаємодію із сервером. Програма не може працювати з файлами хоча б тому, що на Java-терміналі їхній, можливо, не буде. Більш змістовні дії повинні вироблятися на серверній стороні чи здійснюватися програмами, локальними для клієнтської системи.

Цікавий підхід пропонують фахівці компанії Sun Microsystems для забезпечення безпечного виконання командних файлів. Мова йде про середовище Safe-TCL (Tool Command Language, інструментальна командна мова). Sun запропонувала так називану коміркову модель інтерпретації командних файлів. Існує головний інтерпретатор, якому доступні всі можливості мови.

Якщо в процесі роботи задачі необхідно виконати сумнівний командний файл, породжується підлеглий командний інтерпретатор, що володіє обмеженою функціональністю (наприклад, з нього можуть бути вилучені засоби роботи з файлами і сіткові можливості). У результаті потенційно небезпечні програми виявляються ув'язненими в осередки, що захищають користувальницькі системи від ворожих дій. Для виконання дій, що вважаються привілейованими, підлеглий інтерпретатор може

звертатися з запитами до головного. Тут, мабуть, проглядається аналогія з поділом адресних просторів операційної системи і користувальницьких процесів і використанням останніми системних викликів. Подібна модель уже близько 30 років є стандартної для багатокористувацьких ОС.

Захист web-серверів

У Web-серверах об'єктами доступу виступають універсальні локатори ресурсів (URL - Uniform (Universal) Resource Locator). За цими локаторами можуть стояти різні сутності - HTML-файли, CGI-процедури і т.п.

Як правило, суб'єкти доступу ідентифікуються по IP-адресах і/чи іменам комп'ютерів і областей керування. Крім того, може використовуватися парольна аутентифікація чи користувачів більш складні схеми, засновані на криптографічних технологіях.

У більшості Web-серверів права розмежовуються з точністю до каталогів (директорій) із застосуванням довільного керування доступом. Можуть надаватися права на читання HTML-файлів, виконання CGI-процедур і т.д.

Для раннього виявлення спроб нелегального проникнення в Web-сервер важливий регулярний аналіз реєстраційної інформації.

Зрозуміло, захист системи, на якій функціонує Web-сервер, повинна випливати універсальним рекомендаціям, головне з яких є максимальне спрощення. Усі непотрібні сервіси, файли, пристрої повинні бути вилучені. Число користувачів, що мають прямий доступ до сервера, повинне бути зведене до мінімуму, а їхні привілеї - упорядковані у відповідності зі службовими обов'язками.

Ще один загальний принцип полягає в тому, щоб мінімізувати обсяг інформації про сервер, що можуть одержати користувачі. Багато серверів у випадку звертання по імені каталогу і відсутності файлу index.HTML у ньому, видають HTML-варіант змісту каталогу. У цьому змісті можуть зустрітися імена файлів з вихідними текстами чи CGI-процедур з іншою конфіденційною інформацією. Такого роду “додаткові можливості” доцільно відключати, оскільки зайве знання (зловмисника) множить суму (власника сервера).

Аутентифікація у відкритих мережах

Методи, застосовувані у відкритих мережах для підтвердження і перевірки дійсності суб'єктів, повинні бути стійкі до пасивного й активного прослуховування мережі. Суть їх зводиться до наступного.

- Суб'єкт демонструє знання секретного ключа, при цьому ключ або взагалі не передається по мережі, або передається в зашифрованому виді.
- Суб'єкт демонструє володіння програмним чи апаратним засобом генерації одноразових чи паролів засобом, що працює в режимі “запит-відповідь”. Неважко помітити, що перехоплення і наступне відтворення одноразового чи пароля відповіді на запит нічого не дає зловмиснику.
- Суб'єкт демонструє дійсність свого місця розташування, при цьому використовується система навігаційних супутників.

Віртуальні приватні мережі

Однієї з найважливіших задач є захист потоків корпоративних даних,переданих по відкритих мережах. Відкриті канали можуть бути надійно захищені лише одним методом - криптографічним.

Відзначимо, що так називані виділені лінії не мають особливі переваги перед лініями загального користування в плані інформаційної безпеки. Виділені лінії хоча б частково будуть розташовуватися в неконтрольованій зоні, де їх можуть чи зашкодити здійснити до них несанкціоноване підключення. Єдина реальна перевага - це гарантована пропускна здатність виділених ліній, а зовсім не якась підвищена захищеність. Утім, сучасні оптоволоконні канали здатні задовольнити потреби багатьох абонентів, тому і зазначена перевага не завжди умісна в реальній формі.

Цікаво, що в мирний час 95% трафіка Міністерства оборони США передається через мережі загального користування (зокрема через Internet). У воєнний час ця частка повинна складати “лише” 70%. Можна припустити, що Пентагон - не сама бідна організація. Американські військові

покладаються на мережі загального користування тому, що розвивати власну інфраструктуру в умовах швидких технологічних змін - заняття дуже дороге і безперспективне, виправдане навіть для критично важливих національних організацій тільки у виняткових випадках.

Представляється природним покласти на межсітковий екран задачу шифрування і дешифрування корпоративного трафіка на шляху в зовнішню мережу і з неї. Щоб таке шифрування/дешифрування стало можливим, повинне відбутися початковий розподіл ключів. Сучасні криптографічні технології пропонують для цього цілий ряд методів.

Після того як міжсіткові екрани здійснили криптографічне закриття корпоративних потоків даних, територіальна разнесеність сегментів мережі виявляється лише в різній швидкості обміну з різними сегментами. В іншому вся мережа виглядає як єдине ціле, а від абонентів не потрібно залучення яких-небудь додаткових захисних засобів.

Простота й однорідність архітектури

Найважливішим аспектом інформаційної безпеки є керованість системи. Керованість - це і підтримка високої приступності системи за рахунок раннього виявлення і ліквідації проблем, і можливість зміни апаратної і програмної конфігурації відповідно до умов, що змінилися, чи потребами, і оповіщення про спроби порушення інформаційної безпеки практично в реальному часі, і зниження числа помилок адміністрування, і багато, багато чого іншого.

Найбільше гостро проблема керованості встає на клієнтських робочих місцях і на стику клієнтської і серверної частин інформаційної системи. Причина проста - клієнтських місць набагато більше, ніж серверних, вони, як правило, розкидані по значно більшій площі, їх використовують люди з різною кваліфікацією і звичками. Обслуговування й адміністрування клієнтських робочих місць – заняття надзвичайне складне, дороге і чревате помилками. Технологія Intranet за рахунок простоти й однорідності архітектури дозволяє зробити вартість адміністрування клієнтського робочого місця практично нульової. Важливо і те, що заміна і повторне введення в експлуатацію клієнтського комп'ютера можуть бути здійснені дуже швидко, оскільки це “клієнти без стану”, у них немає нічого, що вимагало б тривалого чи відновлення конфігурування.

На стику клієнтської і серверної частин Intranet-системи знаходиться Web-сервер. Це дозволяє мати єдиний механізм реєстрації користувачів і наділення їх правами доступу з наступним централізованим адмініструванням. Взаємодія з численними різнорідними сервісами виявляється схованим не тільки від користувачів, але й у значній мірі від системного адміністратора.

Задача забезпечення інформаційної безпеки в Intranet виявляється більш простій, чим у випадку довільних розподілених систем, побудованих в архітектурі клієнт/сервер. Причина тому - однорідність і простота архітектури Intranet. Якщо розроблювачі прикладних систем зуміють повною мірою скористатися цією перевагою, то на програмно-технічному рівні їм буде досить декількох недорогих і простих в освоєнні продуктів. Правда, до цього необхідно додати продуману політику безпеки і цілісний набір мір процедурного рівня.

Реалізації політики безпеки – вживання різних програмних і апаратно-технічних засобів в процесі побудови системи безпеки.

Використовування міжмережевого екрану.

Міжмережевий екран (firewall) - це засіб розмежування доступу клієнтів з однієї безлічі мережі до серверів з іншої безлічі мережі. Екран виконує свої функції, контролюючи всі інформаційні потоки між двома безліччю систем.

Вимоги до реальної системи, що здійснює міжмережеве екранування. В більшості випадків екрануюча система повинна:

- Забезпечувати безпеку внутрішньої (що захищається) мережі і повний контроль над зовнішніми підключеннями і сеансами зв'язку;
- Володіти могутніми і гнучкими засобами управління для повного і, наскільки можливо, простого втілення в життя політики безпеки організації;

- Працювати непомітно для користувачів локальної мережі і не утрудняти виконання ними легальних дій;
- Працювати достатньо ефективно і встигати обробляти весь вхідний і витікаючий трафік;
- Володіти властивостями самозахисту від будь-яких несанкціонованих дій, оскільки міжмережевий екран є ключем до конфіденційної інформації в організації;
- Якщо у організації є декілька зовнішніх підключень, у тому числі і у видалених філіалах, система управління екранами повинна мати нагоду централізований забезпечувати для них проведення єдиної політики безпеки;
- Мати засобу авторизації доступу користувачів через зовнішні підключення.

Екранування дозволяє підтримувати доступність сервісів усередині інформаційної системи, зменшуючи або взагалі ліквідовуючи навантаження, ініційоване зовнішньою активністю.

Екранування дає можливість контролювати інформаційні потоки, направлені в зовнішню область, забезпечуючи режим конфіденційності.

Шифрування інформації

TCP/IP володіє високою сумісністю як з різними по фізичній природі і швидкісним характеристикам каналами, так і з широким довкола апаратних платформ, сукупність цих характеристик робить протокол TCP/IP унікальним засобом для інтеграції великих розподілених гетерогенних інформаційних систем.

Технології інформаційної безпеки протоколу TCP/IP дозволяють з регульованим ступенем надійності захищати трафік всіх без виключення користувачів і прикладних систем при повній прозорості (невидимості для додатків) засобів захисту.

Такі засоби захисту включають:

Протокол, що управляє шифруванням трафіку SKIP (Simple Key management for Internet Protocol) і створений на його основі ряд продуктів захисту інформації (ряд програмних реалізацій протоколу SKIP для базових апаратно-програмних платформ, пристрій колективного захисту локальної мережі SKIPBridge, пристрій забезпечення регульованої політики безпеки SunScreen).

SKIP (Simple Key mamagement for Internet Protocol - Простий протокол управління криптоключами в інтермережі) розроблений компанією Sun Microsystems в 1994 році і запропонований як стандарт Internet.

У основі SKIP лежить криптографія відкритих ключів Діффі-Хеллмана.

SKIP має, в порівнянні з існуючими системами шифрування трафіку ряд унікальних особливостей:

- SKIP універсальний: він шифрує IP-пакети, не знаючи нічого про додатки, користувачів або процеси, їх формуючих; він обробляє весь трафік, не накладаючи ніяких обмежень ні на вищерозміщене програмне забезпечення, ні на фізичні канали, на яких він використовується;
- SKIP сеансонезалежний: для організації захищеної взаємодії не вимагається додаткового інформаційного обміну;
- SKIP незалежний від системи шифрування - користувач може вибирати будь-який з пропонованих постачальником або використовувати свій алгоритм шифрування інформації.

Пристрій SKIPBridge забезпечує захист (шифрування) трафіку, спрямовуваного з внутрішньої мережі в зовнішню на основі протоколу SKIP, а також фільтрацію і дешифрування трафіку, що поступає із зовнішньої мережі у внутрішню.

IP-пакеты, що приймаються із зовнішньої мережі, обробляються протоколом SKIP. Пакети, що пройшли фільтрацію SKIP, за допомогою протоколу IP передаються програмному забезпеченню SKIPBridge, вирішальному задачі адміністративної безпеки (забезпечуючому пакетну фільтрацію), і потім - операційній системі.

SunScreen - це спеціалізована система захисту, розроблена компанією Sun Microsystems, вирішальна задачі фільтрації пакетів, аутентифікації і забезпечення конфіденційності трафіку. Пристрій SunScreen виконаний на основі апаратного модуля SPF-100. SPF-100 містить SPARC-процессор, що

працює під управлінням ОС Solaris. SunScreen не має IP-адреса, тому він "невидимий" із зовнішньої мережі і несхильний до атаки.

Пристрій SunScreen, містить п'ять Ethernet-адаптеров, до яких можуть під'єднуватися чотири незалежні сегменти локальної мережі і комунікаційний провайдер. Для кожного сегменту забезпечується настройка індивідуальної політики безпеки шляхом завдання складного набору правил фільтрації пакетів.

Захист інформації в мережі WiFi

Звичайний користувач може буквально за декілька хвилин налаштувати домашню мережу, але, не маючи базових знань про ці технології та забезпечення безпеки в локальній мережі, він стає легкою мішенню для того, хто хоче проникнути в його мережу. Дехто може сказати, що йому нема чого приховувати на своєму комп‘ютері, то він не усвідомлює того факту, що хакер може використати його комп‘ютер для здійснення своїх атак, і після цього до нашого користувача можуть завітати представники державних органів, яким він буде довго пояснювати, що уявлення не має про те, що сталось.

Отже, в важливості цього питання ми переконались. Розглянемо основні маніпуляції з точкою доступу, що задовольняють мінімальні вимоги до безпеки WiFi мереж.

- перш за все необхідно змінити заводський пароль точки доступу;
- якщо ви не провайдер, то можна відключити трансляцію ID мережі, це допоможе приховати вашу мережу і виявити її зможе тільки людина, яка знає її назву. Але це не означає, що ваша мережа тепер недоступна для посторонніх людей: тому, хто хоч трохи знайомий з технологіями WiFi, знадобиться близько 2-10 хв., щоб виявити приховану мережу;
- при можливості, необхідно включати фільтрацію по MAC-адресі. Але насправді і цей захід безпеки не створить проблем для проникнення в вашу мережу. Все що потрібно хакеру, для того, щоб обійти цю перепону, це – перехопити пакет одного з користувачів цієї мережі, визначити його MAC-адресу і призначити своєму адаптеру цю MAC-адресу, і точка доступу буде вважати, що це авторизований користувач;
- використовувати надійне шифрування даних.

Перші три правила не створюють серйозних проблем для хакерів - вони швидше спрямовані для боротьби з людьми, які прочитали декілька статей в Інтернеті і випробовують свої сили на погано захищених, а то і взагалі на незахищених мережах. Шифрування – більш надійний спосіб захистити мережу, але і тут не все так просто.

Розглянемо методи шифрування, що використовуються на сьогоднішній день.

WEP (Wired Equivalent Privacy) – технологія, розроблена спеціально для шифрування потоку даних в локальній мережі. Це застаріла технологія, але до 2003 року вона було єдиною.

В ній використовується не самий стійкий алгоритм RC4 на статичному ключі. Для підвищення захисту, частина ключа – статична, а друга – динамічна (вектор ініціалізації), яка змінюється в процесі роботи мережі. Цей вектор 24-бітний. Основний недолік WEP полягає в тому, що вектор ініціалізації повторюється через деякі проміжки часу. Для того, щоб зламати це шифрування необхідно лише зібрати ці повтори і за секунди отримати іншу частину ключа. Для того, щоб зібрати ці повтори (їх необхідно близько мільйона) потрібно 5-10 хв.

WPA (WiFi Protected Access) – більш стійкий алгоритм шифрування, ніж WEP. Високий рівень безпеки досягається за рахунок використання протоколів TKIP і MIC.

MIC – технологія перевірки цілісності повідомлень – захищає від перехвату пакетів і їх перенаправлення. Стандарт TKIP використовує автоматично підібрані 128-бітні ключі, які створюються непередбачуваним способом і їх загальна варіація сягає 500 млрд. Складна ієрархічна система алгоритму підбору ключів і їх динамічна зміна через кожні 10 КБ роблять систему максимально захищеною. MIC використовує складний математичний алгоритм, який дозволяє звіряти відправлені в одній і отримані в другій точці дані. Якщо помічені зміни і результати порівняння не сходяться, то такі

дані вважаються недостовірними і ігноруються. WPA вважається надійним методом шифрування, але японські учені з інституту Хіросіми заявляють, що знайшли спосіб його злому за 1 хв.

WPA2 – створенийна основі попередньої версії, WPA. Враховуючи деякі зміни і доповнення в цьому методі шифрування, вважають, що він зможе ще більше підвищити безпеку мереж.

WPA2 не містить недоліків (відомихна сьогоднішній день), а тому єдиний спосіб проникнення в мережу – прямий підбір пароля. І тут уже все залежить від якості пароля.

Використання технологій приватних віртуальних тунелів (VPN) вважають найкращим методом захисту в WiFi мережах. І хоч ця технологія розроблялась для захищеного підключення до Інтернету через загальнодоступні канали, вона непогано зарекомендувала себе і в бездротових локальних мережах. Суть цієї технології полягає в тому, що створюються «безпечні» канали від клієнта до заданого вузла.

Для шифрування трафіка в VPN використовується протокол IPSec, рідше – PPTP чи L2TP. При цьому можуть використовуватись такі алгоритми, як DES, Triple DES, AES і MD5. На сьогоднішній день не зафіксовано випадків злому VPN-мереж. Застосування цієї технології рекомендується в корпоративних мережах, тому що для домашнього користування встановлення і налаштування може виявитись важким і громіздким. Крім того, при використанні цієї технології доведеться пожертвувати близько 35% пропускної здатності каналу.

В корпоративних мережах є доцільним використання RADIUS-сервера для авторизації користувачів. Це на порядок підвищує захищеність мережі.

Алгоритм шифрування MD5 – є одним із найпоширеніших алгоритмів шифрування, тому на його прикладі продемонструємо, що, знаючи хеш MD5-функції, на сьогоднішній день не є великою проблемою отримати початкові дані.

Є три методи злому хеша:

- перебір варіантів за словником (задані можливі варіанти вихідної фрази і їх хеш порівнюється з хешом, що зламується);
- brute-force метод (перебираються всі можливі комбінації заданих вихідних символів і хеш кожної комбінації порівнюється з хешом функції, що зламується);
- rainbow crack (він оснований на генерації великої кількості хешів із набору символів і по отримані базі ведеться пошук заданого хеша. Хоч генерація хешів займає багато часу, проте наступні зломи виконуються набагато швидше).

На сьогоднішній день в Інтенеті існує багато он-лайн сервісів, що дозволяють за декілька секунд переглянути MD5-хеш вашого виразу і навпаки із заданого MD5-хеша відновити початковий вираз.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

Зробити та записати до звіту аналіз ризику безпеки мережі, що функціонує в університеті, користуючись даним планом.

1. Опис складу системи: апаратних засобів, процес забезпечення, даних, документації, персоналу.
2. Наявність доступу до мережі Інтернет.
3. Визначити:
   - тип мережі (однорангова, з виділеним сервером);
   - кількість і функціональне призначення сервера мережі;
   - вказати тип мережевої операційної системи (сервера, робочої станції);
   - визначити топологію комп' ютерної мережі;
   - визначити тип обладнання, що використовується (тип кабелю, мережевий адаптер).
4. Засоби захисту комп’ютерної мережі що використовуються.
5. Визначення слабких місць - виявляються слабкі місця по кожному елементу оцінкою можливих джерел загроз.
6. Оцінка імовірності реалізації загроз.
7. Оцінка очікуваних розмірів втрат.

8. Аналіз можливих методів і засобів захисту.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Дайте визначення поняттю «мережева атака».
2. Назвіть основні небезпеки втрати інформації під час роботи в мережі.
3. Охарактеризуйте основні сервіси безпеки.
4. Зробіть аналіз специфічних механізмів безпеки.
5. Опишіть механізм захисту мережі за допомогою міжсіткового екрану.
6. Як уникнути втрату інформації під час роботи з командними файлами в мережі?
7. Як здійснюється захист веб-серверів?
8. Дайте аналіз процесу аутентифікації у відкритих мережах.
9. Як здійснюється захист потоків корпоративних даних, що передаються по відкритих мережах?
10. Проаналізуйте особливості захисту інформації в мережах WiFi.

Лабораторна робота №13

Тема: Поняття особистої безпеки користувача персонального комп'ютеру.

Мета: ознайомитися з основним правилами роботи з персональним комп'ютером для запобігання втрати інформацією та навчитися їх використовувати на практиці.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Якщо ви підключаєтеся до Інтернету, дозволяєте комусь користуватися своїм комп'ютером або спільно з іншими використовуєте файли, то слід вжити заходів для захисту комп'ютера від потенційної шкоди. Тому, що існують комп'ютерні злочинці (іноді їх називають хакерами або зломщиками), які атакують комп'ютери інших людей. Ці люди можуть атакувати безпосередньо, проникнувши до комп'ютера через Інтернет і викравши особисту інформацію, або опосередковано за допомогою програм, створених зловмисниками (зловмисних програм) для того, щоб уразити ваш комп'ютер.

На щастя, ви можете захиститися, вживши кілька простих запобіжних заходів.

Перевірка статусу безпеки комп'ютера в Центрі безпеки Windows

Центр безпеки Windows — це штаб-квартира захисту комп'ютера. Тут відображено поточний стан безпеки комп'ютера та наведено рекомендації щодо дій для підвищення рівня безпеки. Щоб його відкрити:

Відкрийте ***Центр безпеки***. Для цього натисніть кнопку ***Пуск***, виберіть пункт ***Панель керування***, потім відкрийте розділ ***Безпека*** і виберіть пункт ***Центр безпеки***.

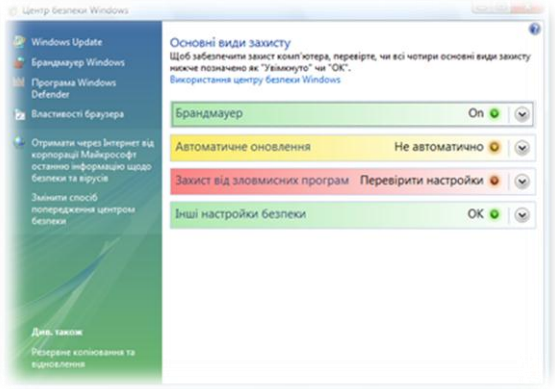
Центр безпеки контролює три головні компоненти системи безпеки комп'ютера:

Брандмауер. Брандмауер допомагає захистити комп'ютер, не дозволяючи хакерам або зловмисним програмам отримати до нього доступ.

Автоматичне оновлення. Windows може постійно стежити за наявністю оновлень для вашого комп'ютера, а також автоматично інсталювати їх.

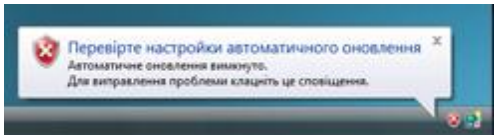
Захист від зловмисних програм. Антивірусне програмне забезпечення допомагає захистити комп'ютер від вірусів, хробаків та інших небезпек. Антишпигунські програми допомагають захищати комп'ютер від шпигунських та інших потенційно небажаних програм.

Інші параметри безпеки. Центр безпеки перевіряє відповідні параметри безпеки Інтернету та ввімкнення керування обліковими записами користувачів.



Якщо будь-які об’єкти безпеки відображено на червоному або жовтому тлі, комп’ютер може бути вразливий до загроз безпеки. Щоб усунути проблему, клацніть об’єкт, щоб відкрити його, і дотримуйтесь інструкцій.

Попередження системи безпеки



Якщо Windows виявить, що систему безпеки комп’ютера потрібно зміцнити в будь-якій із трьох областей безпеки (брандмауер, захист від вірусів або автоматичне оновлення), на екрані буде відображатися сповіщення після кожного входу до системи, поки проблему не буде усунуто. Сповіщення відображаються в області сповіщень на панелі завдань.

Клацніть сповіщення, щоб відкрити центр безпеки, в якому ви зможете навчитися вирішувати проблему.

Щоб вимкнути сповіщення безпеки або приховати піктограму Центру безпеки в області сповіщень, відкрийте ***Центр безпеки***, клацніть пункт ***Змінити спосіб попередження Центром безпеки*** та задайте відповідні параметри. Навіть якщо сповіщення вимкнуто, Центр безпеки продовжуватиме перевіряти та відображати стан безпеки.

Використання брандмауера

Брандмауер — це програма або пристрій, який перевіряє дані, що надходять з Інтернету або мережі, та на основі поточних параметрів приймає рішення, потрібно їх пропускати чи ні. Таким чином, брандмауер запобігає доступу до вашого комп’ютера хакерів і зловмисних програм.

Брандмауер Windows вбудований у систему Windows та вмикається автоматично.

Якщо використовується така програма, як служба обміну миттєвими повідомленнями або мережна гра для багатьох користувачів, якій потрібно отримувати дані з Інтернету або мережі, брандмауер запитує, чи потрібно заблокувати або розблокувати (дозволити) підключення. Якщо дозволити з’єднання, брандмауер Windows створить виняток і не буде відображати запит стосовно цієї програми в майбутньому, коли їй буде потрібно отримати дані з мережі.

Використання захисту від вірусів

Віруси, хробаки та троянські коні — це програми, створені хакерами, які використовують Інтернет для зараження комп'ютерів. Віруси та хробаки можуть самостійно переписуватись із комп'ютера на комп'ютер, а троянський кінь потрапляє до комп'ютера, сховавшись у звичайній на перший погляд програмі, такій як заставка. Деструктивні віруси, хробаки та троянські коні можуть стерти інформацію з жорсткого диска або повністю вивести з ладу комп'ютер. Інші не завдають прямої шкоди, але знижують продуктивність і стабільність комп'ютера.

Антивірусне програмне забезпечення перевіряє електронну пошту та інші файли комп'ютера на наявність вірусів, хробаків і троянських коней. Якщо такі будуть знайдені, антивірусна програма переміщує їх у карантин (ізолює) або повністю видаляє до того, як буде заподіяно шкоду комп'ютеру та файлам.

Оскільки нові віруси з'являються щодня, важливо обрати антивірусну програму з можливістю автоматичного оновлення. Під час оновлення антивірусного програмного забезпечення до списку вірусів завантажуються дані про нові віруси, що убезпечує комп'ютер від нових атак. Якщо ж база антивірусного програмного забезпечення застаріє, комп'ютер стане вразливим до нових загроз. Оновлення зазвичай вимагають щорічної плати за підписку. Подовжуйте підписку, щоб отримувати регулярні оновлення.

Якщо не використовувати антивірусне програмне забезпечення, комп'ютеру загрожує вплив зловмисних програм. Також існує ризик розповсюдити віруси на інші комп'ютери.

Використання захисту від шпигунських програм

Шпигунськими називають програми, які можуть відображати рекламні повідомлення, збирати інформацію про вас або змінювати параметри на комп'ютері, зазвичай, без вашого відома. Наприклад, шпигунські програми можуть встановлювати небажані панелі інструментів, посилання або уподобання у браузері, змінювати домашню сторінку за замовчуванням або часто відображати спливаючі рекламні оголошення. Деякі шпигунські програми не відображають помітних симптомів, але приховано збирають приватну інформацію, наприклад, про відвідані веб-сайти або введений текст. Більшість шпигунських програм інсталюються разом із безплатним програмним забезпеченням, завантаженим вами, проте подеколи навіть просте відвідування веб-сайту спричиняє зараження шпигунською програмою.

Щоб захистити свій комп'ютер від шпигунських програм, користуйтеся антишпигунською програмою. Windows має вбудовану антишпигунську програму Windows Defender, яка вмикається за замовчуванням. Windows Defender попереджає вас, коли шпигунська програма намагається інсталювати себе на комп'ютер. Також ця програма може шукати на комп'ютері наявні шпигунські програми та видаляти їх.

Оскільки щодня з'являються нові шпигунські програми, Windows Defender потрібно регулярно оновлювати, щоб виявляти найновіші шпигунські загрози та захищатись від них. Windows Defender оновлюється належним чином під час оновлення Windows. Для досягнення найвищого рівня захисту ввімкніть у системі Windows автоматичне інсталювання оновлень.

Автоматичне оновлення Windows

Корпорація Майкрософт регулярно пропонує необхідні оновлення Windows, які можуть допомогти захистити ваш комп'ютер від нових вірусів та інших загроз. Щоб забезпечити якнайшвидше отримання цих оновлень, увімкніть автоматичне оновлення. Таким чином вам не доведеться перейматися тим, що критичні виправлення в роботі Windows будуть відсутні на вашому комп'ютері.

Оновлення завантажуються приховано, коли ви підключені до Інтернету. Оновлення інсталюються о 3:00, проте ви можете встановити інший час для цього. Якщо ви вимикаєте комп'ютер до цього часу, оновлення можна інсталювати перед вимкненням. Інакше, Windows інсталює їх після наступного ввімкнення комп'ютера.

Щоб увімкнути автоматичне оновлення

Відкрийте службу Windows Update. Для цього натисніть кнопку ***Пуск***, виберіть пункт ***Усі програми*** і виберіть пункт ***Windows Update***.

Переконайтеся, що вибрано пункт ***Автоматична інсталяція оновлень*** (рекомендовано). Потрібні для вашого комп'ютера оновлення буде інстальовано Windows, щойно вони стануть доступні. Важливі оновлення забезпечують значне покращення захисту і надійності роботи комп'ютера.

Переконайтеся, що у розділі Рекомендовані оновлення установлено прапорець поруч із пунктом ***Включати рекомендовані оновлення під час завантаження, інсталяції або сповіщення про оновлення для комп'ютера***, і натисніть кнопку ***ОК***. Рекомендовані оновлення можуть стосуватися некритичних неполадок і покращувати роботу комп'ютера. Якщо потрібно, введіть пароль адміністратора або надайте підтвердження.

Використання стандартного облікового запису користувача

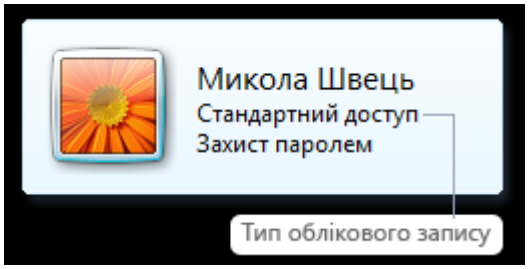
Під час входу до системи Windows надає вам певний рівень прав і привілеїв, залежно від типу вашого облікового запису користувача. Існує три типи облікових записів користувачів: стандартний, адміністратор і гість.

Хоча обліковий запис адміністратора надає повний контроль над комп'ютером, використання стандартного запису може допомогти убезпечити ваш комп'ютер. Таким чином, якщо інші люди (або хакери) отримають доступ до вашого комп'ютера, коли ви увійшли до системи, вони не зможуть змінювати настройки безпеки комп'ютера або облікові записи інших користувачів.

Щоб визначити тип свого облікового запису

Відкрийте діалогове вікно «***Облікові записи користувачів***». Для цього натисніть кнопку ***Пуск,*** виберіть пункт ***Панель керування***, потім виберіть розділ ***Облікові записи користувачів і безпека сім'ї*** (або розділ Облікові записи користувачів, якщо комп'ютер підключено до мережного домену) і виберіть пункт Облікові записи користувачів.

Під вашим іменем з'явиться тип облікового запису.



Незалежно від операційної системи та набору програмного забезпечення, які ми використовуємо на своєму настільному комп'ютері або ноутбуці, для забезпечення приватності та збереження даних нам потрібно дотримуватись основних принципів при експлуатації персональної обчислювальної техніки:

1. Встановлювати та використовувати тільки ліцензійне програмне забезпечення

На сьогоднішній день це загальне правило оскільки майже все контрафактне програмне забезпечення, яке можна вільно скачати в мережі, вже має в собі сторонній програмний код, який зловмисники розмістили всередині контрафактного програмного забезпечення для використання зараженої системи в майбутньому.

2. Регулярно оновлювати всі компоненти системи

Всі сучасні операційні системи та більшість програм, що масово використовуються в наш час, мають в собі автоматичні системи оновлення, які слід використовувати. Зазвичай дана опція активована за замовченням або зводиться до активації цієї функції після першого запуску програми.

3. Використовувати фаєрвол

Кожна сучасна операційна система має за замовчанням вбудований фаєрвол та вбудовані системи сповіщення про стан його роботи. Базові налаштування зазвичай достатні для забезпечення захисту системи і їх використання є мінімальним необхідним рівнем захисту.

4. Використовувати антивірусне програмне забезпечення

Сьогодні на Україні легально доступні десятки різних систем від провідних розробників систем захисту (як окремих програм-антивірусів, так і комплексів, що мають в собі ще й фаєрвол,

“батьківський контроль” тощо). Ці системи є платні, а також такі, що дозволені для використання в некомерційних (домашніх) цілях безкоштовно, наприклад AVG Anti-virus Free Edition.

5. Виконувати регулярне резервне копіювання критичних даних

В усіх сучасних операційних системах є вбудовані засоби резервного копіювання, які варто використовувати для створення резервних копій ваших критичних даних. В якості сховищ для резервних копій можна використовувати доступні сьогодні зовнішні дискові масиви NAS, накшталт D-Link DNS-323.

6. Використовувати стійкі паролі

Паролі – це сьогодні основна складова частина захисту як приватної, так корпоративної інформації. Деякі основні рекомендації з цього приводу наведено в статті, що присвячено вибору правильного паролю.

7. “Обмеження” в правах

Коли користувач в будь-якій операційній системі має права “Адміністратора” і не користується ними, це зовсім не означає, що й зловмисник не може ними скористатися. Віруси та трояни, коли попадають в таку систему можуть без перешкоди виконувати свої дії і не бути поміченими користувачами

Поради з безпечної роботи з електронною поштою та Інтернетом

• Будьте уважні при відкритті вкладення електронної пошти. Вкладення електронної пошти (файли, вкладені в повідомлення електронної пошти) - це основне джерело зараження вірусами. Не відкривайте вкладення від невідомих осіб. Знаючи відправника, але не очікуючи вкладення, переконайтеся, не відкриваючи, що його дійсно послав відправник.

• Ретельно оберігайте особисту інформацію. Якщо веб-сайт запитує номер кредитної картки, банківські дані або інші особисті відомості, переконайтеся, що цьому веб-сайту можна довіряти і його система транзакцій захищена.

• Будьте обережні, відкриваючи гіперпосилання в повідомленнях електронної пошти. Гіперпосилання (посилання, що відкривають веб-сайти по клацанню) часто використовуються як частина фішингових і афер і як засіб передачі вірусів. Відкривайте гіперпосилання лише в повідомленнях електронної пошти.

• Встановлюйте компоненти лише з веб-сайтів. Надбудови браузера дозволяють веб-сторінкам відображати панелі інструментів, біжучі рядки Stock Ticker, відео та анімацію. Однак компоненти також можуть інсталювати шпигунські програми та інші шкідливі програми. Якщо веб-сайт пропонує встановити надбудову, перевірте, чи можна йому довіряти.

Захист USB носія

Найчастіше віруси потрапляють на комп'ютер з чужих USB носіїв або і з власних, які побували в чужих ПК (друзі, знайомі, комп'ютерні клуби...) Як же захистити свою флешку від вірусів? Звичайно, що існує безліч програм, які дозволяють сканувати флеш карту на предмет інфекції, але по-перше — не всі програми однаково ефективні, по-друге — наша задача вберегти саме флешку від вірусів, а не комп’ютер від інфікованої флеш карти (тут все зрозуміло: вставив флешку, просканував антивірусом і видалив чи вилікував).

Давайте розглянемо, як працює вірус на флешці і як він туди потрапляє. Зараження флешки не обов'язково відбувається тільки тоді, коли Ви щось переписали чи зберегли на носій. Тут все зрозуміло — якщо файл інфікований, то визначити можливо його тільки антивірусом вже у себе вдома. Але є такі флеш-віруси, які записуються на наш USB носій просто під час під’єднання його до зараженого комп’ютера.

Існують, так звані, autorun віруси, які і полюбляють найчастіше флеш-карти. Принцип роботи його дуже простий. На флешці створюється файл autorun.inf і при активації USB носія на будь-якому ПК запускається автоматично (autorun — автозапуск) та стимулює виконання процесу, шкідливого коду в тілі чи активації прихованого файлу. Це троян, макро-вірус, мережевний черв'як та інші види шкідливих програм.

Існує дуже цікавий спосіб захисту USB носія від autorun.inf.

Відкриваємо звичайний Блокнот, AkelPad чи інший текстовий редактор, не важливо, який є в будь-якій версії операційної системи Windows, вибираємо ***Файл — Сохранить как...***

Далі зберігаємо в будь-яке місце ПК (наприклад, на робочий стіл) порожній файл під назвою autorun.

В результаті ми повинні отримати на робочому столі файл autorun.txt — звичайний текстовий файл.

Тепер, нам необхідно з файлу autorun.txt зробити файл autorun.inf. Для цього клацаємо правою кнопочкою мишки по autorun.txt і вибираємо «Свойства». Якщо Ви користуєтесь Total Commander, то розширення файлу можна змінити і там.

У віконечку, що з'являється, змінюємо розширення .txt на .inf і тиснемо ОК. Система видасть нам попередження про те, що змінений файл буде недоступним, але для нас це не є важливо. Тиснемо «***Да***».

Тепер на робочому столі замість файлу autorun.txt з'явився файл autorun.inf

Так як вірус створює на флешці шкідливий файл autorun.inf з вірусним кодом чи функцією запуску шкідливого процесу, ми створили такий же файл, але порожній, тобто без всіляких кодів. Тепер, просто переписуємо його на флешку.

У випадку, коли вірус спробує створити на флешці файл autorun.inf з вірусним кодом всередині, то отримає меседж про те, що такий файл уже є.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

Записати до звіту наступну інформацію:

1. Аналіз налаштувань захисту персонального комп’ютера, на якому працюєте, відповідь на запитання: Чи включений брандмауер? Чи налаштоване оновлення операційної системи? Скільки облікових записів є на вашому робочому комп’ютері? Які з них захищені паролем? Який тип вашого облікового захисту?
2. Аналіз встановленого антивірусного програмного забезпечення на вашому робочому комп’ютері. Яка його назва? Як здійснюється оновлення даної антивірусної програми? Які вона має можливості, особливості інтерфейсу?
3. Аналіз загроз втрати інформації користувача вашого комп’ютера. Які засоби захисту потрібно посилити?
4. Складені вами рекомендації користувача даного комп’ютера для зменшення ризиків втрати інформації.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається центром безпеки Windows?
2. Які головні компоненти системи безпеки комп’ютера контролює центр безпеки?
3. Як здійснюється сповіщення про стан системи безпеки на комп’ютері?
4. Опишіть процес налаштування автоматичного оновлення Windows.
5. Які основні небезпеки втрати інформації під час роботи з персональним комп’ютером?
6. Опишіть основні заходи безпеки під час роботи з персональним комп’ютером.
7. Сформулюйте основні поради безпечної роботи з електронною поштою та Інтернетом.
8. Як забезпечити захист USB носія?

Лабораторна робота №14

Тема: Поняття авторського права. Захист авторських прав. Поняття комп'ютерного піратства.

Мета: ознайомитися з поняттями авторського права та комп'ютерного піратства, способами захисту від порушення авторських прав; розглянути законодавство України в галузі захисту авторських прав.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Інтелектуальна власність — це поняття, яке охоплює результати творчої діяльності у сфері науки, техніки, літератури, мистецтва, дизайну та створення товарних знаків.

Відповідно до чинного законодавства України, **правом інтелектуальної власності** є право особи на результат інтелектуальної, творчої діяльності або на інший об'єкт права інтелектуальної власності, визначений Цивільним кодексом України або іншим законом.

Авторське право (англ. — copyright) являє собою особисті немайнові та майнові права авторів і їх правонаступників, пов'язані зі створенням і використанням творів науки, літератури та мистецтва.

Серед багатьох об'єктів авторського права одним із найбільш складних є **комп'ютерна програма**, тобто набір інструкцій у вигляді слів, цифр, кодів, схем, символів, які виражені у формі, придатній для зчитування комп'ютером, та приводять його в дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладні програми, виражені у вихідному або об'єктному коді).

Згідно з положеннями Бернської конвенції про охорону літературних і художніх творів, до якої Україна приєдналася 25 жовтня 1995 року, **комп'ютерні програми охороняються як літературні твори** незалежно від способу або форми їх вираження.

Авторське право на комп'ютерну програму виникає в силу факту її створення.

Згода на використання творів, що охороняються авторським правом, оформлюється авторськими договорами або ліцензійними угодами (ліцензіями), які визначають обсяг переданих прав на твори, включаючи право на використання, виготовлення та розповсюдження копій.

Авторське право на саму програму зберігається за автором (правовласником), а у власність покупця переходять лише матеріальні носії, на яких вона розповсюджується (наприклад, диски). По суті, під час купівлі ліцензійного програмного продукту придбавається право (дозвіл) на його використання, яке включає в себе також право на відтворення програми в пам'яті комп'ютера.

Одним із порушень прав автора на комп'ютерну програму є **піратство** — опублікування, відтворення, ввіз на митну територію України, вивіз із митної території України та розповсюдження контрафактних (виготовлених без згоди правовласника) екземплярів творів (зокрема, комп'ютерних програм і баз даних). Комп'ютерне піратство є несанкціонованим правовласником копіюванням, використанням і розповсюдженням програмного забезпечення.

Найбільш типовими формами комп'ютерного піратства є:

а) виготовлення та розповсюдження контрафактних носіїв (дисків) із копіями програмних продуктів;

б) продаж комп'ютерної техніки з програмним забезпеченням, попередньо встановленим із порушенням ліцензійних угод;

в) встановлення неліцензійного програмного забезпечення на замовлення користувача;

г) відтворення неліцензійного ПЗ на персональних комп'ютерах кінцевими користувачами, включаючи випадки встановлення більшої кількості копій, ніж це передбачено умовами ліцензійної угоди;

д) інтернет-піратство — надання доступу до нелегальних копій програмних продуктів із використанням Інтернету.

Використання програмних продуктів без дозволу правовласника порушує майнові й особисті не майнові права на інтелектуальну власність, а, отже, є правопорушенням.

Розуміння юридичних засад захисту авторських прав дає змогу встановлювати правила і процедури, що запобігають відтворенню та розповсюдженню нелегальних копій комп'ютерних програм і таким чином сприяють зниженню ризиків юридичного переслідування.

Форми захисту авторських прав

Захист особистих немайнових і майнових прав суб'єктів авторського права здійснюється в порядку, встановленому адміністративним, цивільним та кримінальним законодавством України.

Розглядаються дві основні форми захисту авторських прав:

Не юрисдикційна — передбачає дії юридичних і фізичних осіб із захисту своїх авторських прав на твір, які здійснюються ними самостійно, без звертання в державні або інші компетентні органи. При цьому маються на увазі лише законі способи захисту, наприклад сповіщення порушника про існування авторських прав і пропозицію вирішити спір шляхом переговорів.

Юрисдикційна — передбачає діяльність уповноважених державою органів стосовно захисту прав, які порушені. Суть такої форми захисту полягає в тому, що особа, права якої порушені неправомірними діями, може звернутися за захистом своїх прав у спеціально вповноважені державні органи.

Юрисдикційна форма захисту прав автора може здійснюватися з використанням таких процедур.

Цивільно-правова. Найбільш розповсюджена процедура вирішення спорів щодо прав автора на твір. Головна мета — не покарання порушника, а відновлення прав і компенсація збитків. У зв'язку з цим законодавство України встановило достатньо широкий спектр способів такого захисту:

а) визнання виняткового права;

б) припинення дій, які порушують право;

в) відновлення положення, що існувало до порушення права;

г) компенсація збитків;

д) компенсація моральної (нематеріальної) шкоди;

е) визнання незаконним рішення державного органу.

Підставою для притягнення порушника до цивільно-правової відповідальності є звернення власника авторських прав із позовом до суду.

Адміністративно-правова. Відповідно до статті 51-2 (порушення прав на об'єкт права інтелектуальної власності) Кодексу України про адміністративні правопорушення, незаконне використання об'єкта прав інтелектуальної власності (зокрема, комп'ютерної програми), привласнення авторства на такий об'єкт або інше умисне порушення прав на об'єкт права інтелектуальної власності, що охороняється законом, тягне за собою накладання штрафу в сумі від десяти до двохсот неоподатковуваних мінімальних доходів громадян із конфіскацією незаконно виготовленої продукції та обладнання і матеріалів, які призначені для її виготовлення.

Кримінально-правова. **Статтею 176** (порушення авторського права і суміжних прав) Кримінального кодексу України передбачена кримінальна відповідальність за незаконне відтворення, розповсюдження комп'ютерних програм, їх тиражування на носіях інформації або інше умисне порушення авторського права, якщо це завдало матеріальної шкоди у значному розмірі. Здійснення таких дій карається штрафом від двохсот до тисячі неоподатковуваних мінімальних доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, а також обладнання і матеріалів, які спеціально використовувались для їх виготовлення.

Дії, передбачені частиною першої статті, якщо вони вчинені повторно, або за попередньою змовою групою осіб або завдали матеріальної шкоди у великому розмірі, караються штрафом від тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк від двох до п'яти років, з конфіскацією та знищенням всіх

примірників матеріальних носіїв комп'ютерних програм та обладнання і матеріалів, які спеціально використовувались для їх виготовлення.

Дії, передбачені частинами першою або другою цієї статті, вчинені службовою особою з використанням службового становища або організованою групою, або якщо вони завдали матеріальної шкоди в особливо великому розмірі, караються штрафом від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до шести років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або з конфіскацією і знищенням всіх примірників матеріальних носіїв комп'ютерних програм та обладнання і матеріалів, які спеціально використовувалися для їх виготовлення.

Статтею 203-1 (незаконний обіг дисків для лазерних систем зчитування, матриць, обладнання та сировини для їх виробництва) Кримінального кодексу України передбачена кримінальна відповідальність за незаконне виробництво, експорт, імпорт, зберігання, реалізацію та переміщення дисків для лазерних систем зчитування, матриць, обладнання та сировини для їх виробництва, якщо ці дії вчинені у значних розмірах. Такі дії караються штрафом від одної до п'яти тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк із конфіскацією та знищенням дисків для лазерних систем зчитування, матриць, обладнання чи сировини для їх виробництва.

Ті самі дії, якщо вони вчинені повторно або за попередньою змовою групою осіб, або вчинені у великих розмірах, караються позбавленням волі на строк від двох до п'яти років з конфіскацією та знищенням дисків для лазерних систем зчитування, матриць, обладнання чи сировини для їх виробництва.

Типові ситуації, що призводять до порушення авторських прав на комп'ютерні програми

Використання програмних продуктів здійснюється на підставі договору із правовласниками (виробниками програмного продукту), в якому правовласник встановлює певні умови та процедури використання й розповсюдження відповідних програмних продуктів.

Можна виділити такі типові ситуації, що призводять до порушення авторських прав на програмні продукти компаніями, які здійснюють складання і/або продаж комп'ютерної техніки споживачам:

Під час продажу ПК працівник компанії встановлює на його жорсткий диск копію програмного продукту (можливо, з оригінального дистрибутива за допомогою ОПК), але в момент продажу не передає покупцю OEM-комплект, який включає носій продукту, сертифікат справжності (наклейку з ключем продукту), ліцензійну угоду (може надаватися лише в електронному вигляді), посібник користувача (якщо він входить до комплекту поставки продукту) та інші матеріали. Встановлення продукту виконується з носія, який є в розпорядженні продавця, безоплатно або за винагороду. Покупець отримує неліцензійну копію ПЗ, причому він може бути, а може й не бути проінформований щодо факту встановлення неліцензійної копії ПЗ на комп'ютер, який ним купується.

Відсутність повного комплекту, який продавець має передати покупцю, є порушенням.

Під час продажу ПК продавець здійснює встановлення ПЗ із неліцензійного носія, власником якого є сам покупець. Продавець встановлює ПЗ і виконує конфігурування безоплатно або за винагороду.

Встановлюючи ПЗ із контрафактного носія (незалежно від того, кому належить такий носій), продавець здійснює неправомірне розповсюдження програмного продукту.

Перед продажем ПК продавець встановлює на нього програму з оригінального дистрибутива та виконує її настроювання з метою демонстрації працездатності ПК, не наклеюючи сертифікат справжності на корпус.

Такі дії є порушенням авторського права, оскільки попереднє встановлення ПЗ має здійснюватись за допомогою ОРК та супроводжуватись наклеюванням сертифіката справжності(СОА) на корпус ПК.

Продавець встановлює на ПК перед його продажем неліцензійні копії знятих із виробництва версій програм.

Майнові авторські права на комп'ютерні програми охороняються протягом всього передбаченого законом терміну. За наявності офіційних каналів постачання попередніх версій Windows® і MS-DOS® їх розповсюдження відбувається за загальними принципами. Якщо певний продукт виключено зі списку продуктів, що постачаються, то продавати його споживачам уже не можна, однак авторські права на нього зберігаються.

Продавець встановлює на ПК перед його продажем неліцензійні копії командних файлів (наприклад, файлу command.com) або «урізаної» версії MS-DOS.

У кожному виконуваному (.EXE) і командному (*.COM) файлі є так звана сигнатура (підпис), яка вказує на ім'я правовласника цього файлу. Розповсюдження навіть окремих файлів, що входять до складу операційної системи, не може здійснюватися без згоди правовласника.*

OEM-версії програмних продуктів, призначені для постачання кінцевим користувачам лише у складі повністю забраної комп'ютерної системи, реалізуються окремо від них.

Реалізація OEM-версій програмних продуктів кінцевим користувачам окремо від повністю зібраної комп'ютерної системи) є порушенням умов ліцензійної угоди.

Рекомендації щодо попередження порушень авторських прав на комп'ютерні програми

Щоб мінімізувати ризики застосування юридичних санкцій стосовно керівництва компанії або її персоналу, рекомендується:

- Здійснювати реалізацію техніки або з ліцензійними копіями програм і видачею на руки покупцю OEM-комплектів у повному складі, або з видаленням встановленого ПЗ у випадку, якщо споживач не зацікавлений у придбанні ПК із ліцензійних ПЗ.
- Пам'ятати про те, що попереднє встановлення ПЗ має здійснюватись за допомогою ОРК та супроводжуватись наклеюванням сертифіката справжності (СОА) на корпус ПК. Лише в цьому випадку дозволяється демонстрація працездатності ПК.
- Вносити в гарантійні зобов'язання на техніку інформацію про те, що фірма-продавець не несе відповідальності за відмови в роботі персонального комп'ютера, пов'язані з функціонуванням ПЗ, якщо комп'ютер постачався без ПЗ, а також у випадку звернення покупця в сервісну службу, якщо він не зможе пред'явити документи, що підтверджують його право на використання ПЗ, встановленого ним самостійно після купівлі комп'ютера.
- Не зберігати в офісах і торгових залах контрафактні носії з установочними копіями програм, а також OEM-версії продуктів без документів, які підтверджують їх правомірне введення у цивільний обіг.

Конкретні заходи

а) Перевірити, чи є ліцензійним програмне забезпечення, що використовується на підприємстві, в установі або організації .

Підроблені копії програмних продуктів іноді досить складно відрізнити від справжніх. Тому дуже важливим є надання користувачу інформації про те, за якими ознаками можна відрізнити оригінальну продукцію від підробленої. З цією метою корпорація Майкрософт вбудовує у свої продукти низку елементів захисту від піратського копіювання. Ці елементи призначені для підвищення захищеності користувача, який за їх допомогою може переконатися в справжності продукту перед купівлею.

б) Регулярно проводити інвентаризацію використовуваних комп'ютерних програм та зіставлення їх з наявними ліцензіями.

Є два способи інвентаризації програмного забезпечення:

Простий. Ви можете провести інвентаризацію вручну, переглянувши жорсткі диски всіх комп'ютерів й зафіксувавши всю інформацію у вигляді звіту.

Автоматизований. Для автоматичної інвентаризації ПЗ на комп'ютерах і серверах підприємства слід використовувати спеціальні програми, наприклад Microsoft Software Inventory Analyzer, (http://www.microsoft.com/resources/sam/msia.mspx).

в) У разі виявлення нестачі ліцензій негайно закупити необхідну їх кількість (дуже важливо вести базу придбаних ліцензій).

г) Зберігати всю ліцензійну документацію в надійному місці.

Документи, що підтверджують легальність придбання і використання ПЗ:

Ліцензійні угоди або їх копії, завірені печаткою організації.

Сертифікат справжності — наклейка, яка дає змогу відрізнити справжнє програмне забезпечення.

Якщо сертифікат справжності відсутній, то ви не маєте законної ліцензії на використання програмного забезпечення. Сертифікат справжності не є ліцензією на програмне забезпечення, це наочний засіб, що допомагає встановити справжність програмного забезпечення, яке використовується. Сертифікат справжності не може бути придбаним окремо від програмного забезпечення, справжність якого він засвідчує. Наклейка сертифіката справжності має бути розміщена на корпусі комп'ютера (у разі придбання OEM-версій операційних систем).

Документи, що підтверджують оплату ПЗ (рахунки, акти, рахунки-фактури).

Рахунки, що підтверджують взяття ПЗ на баланс (у випадку OEM-версій ПЗ міститься у складі ПК).

У разі купівлі ПЗ на виплат — документи, що підтверджують намір придбати ПЗ для всього парку комп'ютерів.

У разі придбання ПЗ через Інтернет — роздруківка сторінок, що підтверджують закупівлю.

д) Запровадити політику використання ліцензійного ПЗ і повідомити всім співробітникам про ризики, пов'язані з нелегальними комп'ютерними програмами, а також про неприпустимість їх використання в компанії.

Рекомендації для IT-менеджера

У разі виявлення нестачі ліцензій необхідно:

- оцінити бюджет;
- проінформувати керівника підприємства в письмовому вигляді;
- зберегти матеріали, що підтверджують поінформованість керівництва підприємства про існуючу проблему.

IT-менеджеру слід завжди пам'ятати, що, відповідно до чинного законодавства України, він як особа, що має спеціальні знання в галузі інформаційних технологій та функціонально відповідає за IT-інфраструктуру підприємства, може бути суб'єктом притягнення до встановленої законом відповідальності.

Радимо вам скористатися рекомендаціями BSA (Business Software Alliance — Асоціація виробників програмного забезпечення). На допомогу IT-спеціалістам створено спеціалізований розділ «Юридична консультація від представника BSA», що містить витяги із законодавства України, опис ситуацій, у яких несе відповідальність IT-спе-ціаліст, а також інформацію про те, що потрібно знати IT-спеціалісту, щоб убезпечити себе перед перевірками компетентних органів.

Адреса ресурсу: http://www.bsa.org/country/Anti-Piracy/antipiracy2008.aspx.

Не юридичні ризики використання неліцензійного ПЗ

Правоохоронні та контролюючі органи докладають все більше зусиль для виявлення та припинення порушень у сфері використання підприємствами, установами та організаціями неліцензійного ПЗ, тому сьогодні більшість фірм усвідомлює існуючі юридичні ризики. Разом із тим досить часто їх керівництво не бере до уваги економічні, технічні та іміджеві фактори ризику, а також недооцінює фактичні витрати, що виникають у зв'язку з цим.

За результатами дослідження міжнародної аналітичної компанії IDC, суб'єкти господарювання з високим рівнем використання неліцензійного ПЗ стикаються з ризиковими ситуаціями **у два рази**

частіше, ніж підприємства з низьким рівнем цього показника. Критичні збої інформаційних систем на підприємствах із високим рівнем використання неліцензійного ПЗ виникають у три рази частіше, ніж на підприємствах із низьким рівнем. У разі виникнення проблем компанії з **високим рівнем неліцензійного ПЗ зазнають більш значних втрат, ніж аналогічні компанії з низьким рівнем**, оскільки відновлення систем вимагає більше часу та людських ресурсів.

Частота критичних і дрібних збоїв систем, кількість втрат або пошкоджень даних, а також непередбачуваних витрат на ПЗ виявляються значно вищими, ніж здається на перший погляд IT-менеджерам та бізнес-керівникам. **Більше того, частота виникнення таких ситуацій прямо пропорційна частці неліцензійного ПЗ у компанії.** Отже, чим більше неліцензійного ПЗ використовує компанія, тим вищим економічним ризикам вона піддається.

IDC провела оцінку фінансових збитків, спричинених трьома найрозповсюдженішими проблемами, пов'язаними з використанням неліцензійного ПЗ, — **критичні збої систем, дрібні збої систем і непередбачувані витрати на програмне забезпечення**. Виявилося, що компанії з високим рівнем використання неліцензійного ПЗ не лише частіше стикаються з різними технічними проблемами, але й ціна таких проблем для них є значно вищою, ніж для компаній із низьким рівнем використання неліцензійного ПЗ.

Цілком очевидно, що керівники бізнес-структур дуже недооцінюють витрати на навчання, оновлення та підтримку для неліцензійного ПЗ і уявляють собі високими ці витрати для ліцензійного ПЗ. Водночас IT-менеджери, які значно краще інформовані про загальну вартість володіння для IT-систем, чітко розуміють, що витрати на придбання ПЗ складають лише невелику частку сукупної вартості володіння програмними продуктами.

Крім того, будь-яка можлива економія, отримана внаслідок відмови від придбання ліцензійного ПЗ, призводить до більш високого рівня витрат на обслуговування й технічну підтримку інформаційних систем.

Ключові недоліки неліцензійного ПЗ порівняно з ліцензійним

1. Відсутність надійності та безпеки
2. Відсутність сервісів й технічної підтримки
3. Обмеження в отриманні оновлень
4. Висока ймовірність зараження ПК вірусами
5. Витік персональної (конфіденційної) інформації
6. Втрачені можливості в наслідок використання неліцензійного ПЗ (наприклад, недоотримання прибутку, недооцінка вартості підприємства, неможливість пройти сертифікацію на відповідність стандартам ISO 9000, а також неможливість інтегруватися у міжнародний бізнес, систему кредитування тощо).
7. Значні фінансові збитки
8. Встановлена Законом відповідальність за порушення авторських прав.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Запустіть браузер Інтернет (Це може бути Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera чи будь-який інший, що встановлений на вашому комп'ютері)
2. На офіційному сайті Верховної ради «Законодавство України» (http://zakon2.rada.gov.ua/laws) знайдіть Закон України «Про авторське право і суміжні права», ознайомтесь з його основними положеннями та занотуйте до звіту такі відомості:
   - визначення термінів «автор», «база даних», «ім'я автора», «комп'ютерна програма», «технічні засоби захисту», «державна система правової охорони інтелектуальної власності».
   - об'єкти та суб'єкти авторського права;
   - основні аспекти Статі 23. Вільне відтворення примірників твору для навчання;
   - основні аспекти Статті24. Вільне копіювання, модифікація і декомпіляція комп'ютерних програм;

- поняття суміжного права;
- основні способи цивільно-правового захисту авторського права і суміжних прав.

3. Зробіть та запишіть до звіту висновки по роботі.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що охоплює поняття інтелектуальної власності?
2. Що являє собою авторське право?
3. Що називається піратством? А комп'ютерним піратством?
4. Охарактеризуйте найбільш типові форми комп'ютерного піратства.
5. Дайте аналіз основним формам захисту авторських прав.
6. Охарактеризуйте типові ситуації, що призводять до порушення авторських прав на комп'ютерні програми.
7. Назвіть рекомендації щодо попередження порушень авторських прав на комп'ютерні програми.
8. Охарактеризуйте не юридичні ризики використання неліцензійного ПЗ.
9. Перерахуйте ключові недоліки неліцензійного ПЗ порівняно з ліцензійним.

Лабораторна робота №15

Тема: Поняття плагіату. Загальний огляд програмного забезпечення призначеного для виявлення плагіату.

Мета: ознайомитися з поняттям плагіату, його основними типами, розглянути найпоширеніші програми, призначені для виявлення плагіату.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

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.

Єдиного, вичерпного та загальноприйнятого визначення плагіату не існує. Приміром, автори одного з найбільших англомовних ресурсів для виявлення плагіату "Turnitin"(http://www.turnitin.com/) дають такі визначення цього поняття:

- вкрасти ідею або слова іншої людини і видати їх за власні;
- використати результати роботи іншої людини без зазначення джерела, звідки вони були взяті;
- повністю або частково вкрасти мистецький, науковий або інший твір чи роботу та видати їх за свою;
- представити вже існуючу ідею або продукт як новий та оригінальний.

Крім того, в різних сферах і галузях діяльності плагіат може мати більш персоніфіковані відносно специфіки цієї діяльності визначення. Так, в навчальних закладах він може розглядатися як:

- офіційно не підтверджена домовленість між щонайменше двома студентами наслідком якої є виконання однакових, або майже однакових робіт;
- фальсифікація — зміст завдань, наприклад, статистичні показники, були вигадані або невірно вказані як результат власної роботи;
- реплікація — коли студент здає однакову, або майже однакову роботу кілька раз для підняття власного академічного рейтингу;
- використання не дозволених допоміжних матеріалів під час іспитів;
- отримання недозволеної копії екзаменаційних завдань;
- спілкування з іншими студентами під час іспитів для розв'язання завдань;
- представлення себе під іменем іншого студента на іспитах.

Таким чином, плагіат в будь-якому разі розглядається як шахрайство, суть якого — у крадіжці чужої роботи або її частини і представленні її як власної. Загалом, можна поділити на три основні типи плагіату:

- Копіювання чужої роботи (як без, так і з відома) та оприлюднення її під своїм іменем.
- Представлення суміші власних та запозичених в інших аргументів без належного цитування джерел.
- Перефразування чужої роботи без належно оформленого посилання на оригінального автора або видавця.

Подібну, але більш розгорнуту класифікацію пропонують автори вже згаданого ресурсу «Turnitin»:

- Видання виконаної іншим автором роботи за свою без внесення в неї жодних змін.
- Копіювання значної частини чужої роботи в свою без внесення в запозичене жодних змін.
- Копіювання інформації з кількох різних джерел без внесення в неї правок. «Маскування плагіату» самостійним написанням перехідних речень між скопійованими частинами.
- Внесення незначних правок у скопійований матеріал (переформулювання речень, зміна порядку слів в них тощо).
- Повне запозичення текстів з інших джерел, але цілковите їх перефразування;
- Видання власної колись вже написаної роботи за нову (переважно стосується студентів).

Найочевиднішими є перші типи. Їх найлегше виявити. Натомість, перефразування чужої роботи та порушення правил цитування, що також є плагіатом, виявити значно важче. Тому цим часто зловживають.

Наслідками плагіату є зубожіння інформаційного простору, порушення законів, матеріальні та моральні збитки авторів, видавництв.

Для боротьби з плагіатом існує спеціальне програмне забезпечення, а не рідко цілі організації, працівники яких спеціалізуються на виявленні плагіату в науковій чи художній літературі в результаті багаторівневого всебічного аналізу тексту.

Найпоширеніші програми для виявлення плагіату

- IN-SPIRE™ Visual Document Analysis для опрацювання текстових даних науково-технічної літератури;
- VantagePoint для глибинного аналізу тексту.
- Histcite – програмний продукт, призначений для формалізованого аналізу результатів пошуку в БД.
- Web of Science, що містить ключові слова, авторів і процитованих авторів, журнали, країни й організації, від яких автори публікують свої статті.

Російські програмісти розробили спеціальну систему для виявлення плагіату. Замовником чудо-програми виступив ректор одного з російських ВНЗ. Свій винахід винахідники назвали просто – "Антиплагіат" (AntiPlagiat.ru).

Працює програма досить просто: потрібно всього лише відкрити сайт програми та завантажити необхідний документ, наприклад, дипломну роботу або ж дисертацію. Комп'ютер шукає в мережі схожі тексти, і через 5 секунд видає, наприклад, вердикт: текст на 40% запозичений з Інтернету. Тут же даються посилання на справжнього автора.

Творці системи ставлять за мету підвищення якості російської освіти, переважно в тих її складових, де від студента потрібне застосування творчих зусиль при написанні рефератів, дипломних робіт або творів. Однак, чим обернеться "програма викриттів" насправді, поки що сказати важко.

На даний момент сервіс працює в тестовому режимі, при цьому творці системи відзначають стабільну роботу механізму пошуку збігів. Система працює з форматами HTML, RTF, PDF, .txt, .doc. Аналіз тексту обсягом 5 тисяч знаків здійснюється за кілька секунд. На сьогоднішній день AntiPlagiat.ru

проводить аналіз тексту більш ніж за 4 мільйонами джерел. В майбутньому розроблювачі планують значно поповнити базу.

Більшість програмних продуктів такого типу для виявлення плагіату використовують такі процедури:

- Створення частотних масивів слів.
- Визначення тематичного напряму тексту.
- Динамічне визначення частотного словника певного тематичного напряму корпусу та дослідного тексту (статті) (вилучення стоп-слів, нормалізація тексту).
- Визначення масивів слів: - всі слова статті; всі слова корпусу; слова, які є в обох масивах; унікальні слова статті; унікальні слова корпусу.
- Підрахунок косинусної міри.

Правила цитування

Цитування має використовуватися у всіх випадках, коли в роботі використовуються дані, взяті зі сторонніх джерел, а не отримані або створені безпосередньо автором. Порушення вказаних нижче правил і їх недотримання має розцінюватися як плагіат:

- якщо думка автора наводиться дослівно, то її слід взяти в лапки;
- якщо цитується великий уривок тексту, то він може не братися в лапки, натомість — виділяється або відбивається від решти тексту певним способом (набирається іншим кеглем, шрифтом, накресленням, відбивається від основного тексту більшими абзацними відступами тощо);
- допускається скорочення цитати, яке не веде до викривлення думки автора. Місце скорочення має бути відзначене в цитаті квадратними дужками з трикрапкою всередині;
- допускається перефразування цитати, зміна словоформ чи відмінків певних слів. В такому разі, цитата в лапки не береться, але в квадратних дужках обов'язково ставиться посилання на джерело (його порядковий номер зі списку використаної літератури, який додається до роботи);
- в списку використаної літератури завжди слід вказувати навіть ті джерела, які використовувалися під час підготовки роботи і вивчення теми, навіть якщо прямих посилань чи цитувань цих джерел в роботі нема.

З розвитком програмування набув поширення ще один вид плагіату – видання програмного коду, написаного іншою людиною за власний.

Розглянемо основні детектори такого плагіату: MOSS, JPlag, SIM, Sherlock (BOSS), PMD(CMD), CodeMatch.

MOSS – автоматична безкоштовна система пошуку плагіату, яка має дуже простий інтерфейс і працює он-лайн. Для використання програми, користувачеві необхідно лише вказати список файлів, які необхідно перевірити. У відповідь на запит сервер MOSS створює HTML сторінки з перерахуванням пар програм зі схожими частинами коду, які виділені підкресленням. Результати сканування коду можуть бути доступними для перегляду протягом 14 днів. Користувач може ввімкнути функцію автоматичного видалення коду, що був автоматично згенерований або код бібліотек, щоб бачити яку кількість коду програміст написав самостійно.

Детектор плагіату MOSS здатен аналізувати код, що написаний на мовах: C, C++, Java, C#, Python, Visual Basic, JavaScript, FORTRAN, ML, Haskell, Lisp, Scheme, Pascal, Modula-2, Ada, Perl, TCL, Matlab, VHDL, Verilog, Spice, MIPS та HCL2. Така велика кількість підтримуваних мов програмування є значною перевагою у порівнянні з іншими детекторами плагіату. Для того, щоб розпочати користування даною системою, необхідно відправити свої контактні дані на офіційну електронну пошту сервісу.

Але, незважаючи на всі переваги, система є закритою, що не дозволяє переглядати алгоритми, що використовуються у програмі, а відповідно не дозволяє дізнатись, які техніки плагіату може знайти дана система, а також забороняє додати можливість пошуку коду на інших мовах, що не підтримує на даний момент MOSS.

JPlag – є найбільш популярним безкоштовним детектором плагіату, який дозволяє порівнювати код програми з існуючою базою вже написаних програм.

JPlag підтримує невелику кількість існуючих мов програмування: Java, C#, C, C++, Scheme, але має декілька переваг. Серед них можливість пошуку плагіату серед текстів написаних природною мовою та використання для нових та універсальних алгоритмів пошуку плагіату.

Для початку користування програмою необхідно зареєструватися на офіційному сайті. Результати сканування коду програм доступні доти, доки користувач не видалить історію пошуків. Інтерфейс програми є зрозумілим і дозволяє не тільки знайти і підкреслити частини коду, в яких помічено плагіат, але й надає гістограми, на яких показано кількість та частота випадків копіювання. Система не є відкритою, але незважаючи на це розробники надали інформацію по використовуваних алгоритмах, методиках пошуку та видах технік плагіату, які може виявити система JPlag.

SIM - детектор плагіату, який перевіряє код за допомогою вимірювання лексичної схожості текстів, написаних на мовах C, Java, Pascal, Modula-2, Miranda. Також дана система дозволяє перевіряти тексти написані природною мовою. Детектор плагіату SIM працює локально, не вимагаючи підключення до Інтернет. Головною перевагою даної системи є те, що вона є однією з небагатьох безкоштовних та відкритих детекторів коду та знаходиться в постійній розробці та вдосконалюється.

Одним з недоліків даної системи є незручний інтерфейс та відсутність графічного та достатнього статистичного представлення результатів по виконаному пошуку.

Sherlock (BOSS) - це частина системи BOSS, яка може працювати як окремий додаток . Даний детектор плагіату порівнює вихідний код і тексти, написані природною мовою. Система Sherlock є відкритою та безкоштовною, але, незважаючи на це, підтримка користувачів з боку розробників відсутня та можливості до модифікації програми власноруч з метою додавання нових мов немає.

Головним недоліком даної системи є підтримка невеликої кількості мов програмування: Java, C та C++.

Детектор плагіату аналізує код програм на найпопулярніші техніки плагіату: додавання (видалення) пробілів, додавання (видалення) коментарів, перестановка частин коду у тексті та перейменування змінних, але не зважаючи на це Sherlock використовує застарілі версії алгоритмів, що не дозволяє говорити про якісні результати пошуку плагіату.

Інтерфейс програми є достатньо зрозумілим, а статистичної інформації вистачає для того, щоб виявити плагіат (графіки, таблиці зі статистикою та можливість явно передивитися виділені кольором частини в коді, які були скопійовані).

PMD (CMD) – відкрита та безкоштовна система виявлення плагіату, яка не була задумана, як інструмент пошуку плагіату коду в сфері навчання, але зараз добре працює і в цій сфері. Дозволяє знаходити плагіат в коді програм, написаних на мовах Java, JSP, C, C++, PHP і FORTAN. Головною з переваг даної системи є існування можливості та інструкцій для додавання нової мови програмування, для аналізу коду, написаного на ній.

Результати аналізу коду програма повертає у файл з кодом програми, який аналізується. Це є незручним, адже наочно не можна побачити, які частини коду скопійовані, недостатньо статистики і робота з програмою ведеться з командного рядка.

PMD сканує код на виявлення наступних основних технології плагіату:

- змінні, що не використовуються;
- перейменовані змінні;
- копіювання приватних методів;
- додавання (видалення) коментарів;
- дублювання коду;
- завантаження з Інтернет.

PMD інтегрований з такими середовищами розробки, як JDeveloper, Eclipse, Jedit, JBuilder, BlueJ, CodeGuide, IntelliJ IDEA, TextPad, Maven, Ant, JCreator, і Emacs.

CodeMatch – це комерційна програма-детектор плагіату, що має дуже широкі можливості для аналізу коду програм. CodeMatch в даний час підтримує наступні мови програмування: Basic, C, C++,

C#, Delphi, Flash ActionScript, Java, JavaScript, MASM, Pascal, Perl, PHP, PowerBuilder, Ruby, SQL, Verilog, VHDL [4].

В пакеті з CodeMatch можуть бути додаткові програми перевірки на плагіат (BitMatch та CodeDiff). Детектор CodeMatch порівнює тільки вихідний код, на відміну від BitMatch, який корисний у тому випадку, якщо є тільки доступ до виконуваних файлів, а не до вихідного коду. CodeDiff корисний у випадку, якщо вже точно відомо, що існує плагіат у файлах, що будуть перевірятися. CodeDiff надає більш детальну інформацію про те, що і яким чином було скопійовано та перероблено.

CodeMatch порівнює кожен файл із вказаних директорій, включаючи всі підкаталоги, якщо потрібно. CodeMatch створює бази даних з перевірених програм. Інформація, про виконання пошуку відображається на HTML-сторінках, як звіт. Ви маєте можливість обрати, наскільки докладний звіт буде вам наданий.

CodeMatch в даний час підтримуються наступні мови програмування: ABAP, ASM-m68k, BASIC, C++, C#, Delphi, Flash, ActionScript, Fortran, FoxPro, Java, JavaScript, LISP, MASM, MATLAB, Pascal, Perl, PHP, PL/M PowerBuilder, Python, REALbasic, SQL, Verilog, VHDL, Visual Basic тощо. Підтримка нових мов є простою та швидкою. Якщо користувачеві необхідно проаналізувати код на мові, якої в переліку немає, то розробники додадуть дану мову протягом декількох днів.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Запустіть браузер Інтернет (Це може бути Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera чи будь-який інший, що встановлений на вашому комп’ютері).
2. Відвідайте ресурс http://www.antiplagiat.ru.
3. Користуючись інформацією, що знаходиться на даному сайті запишіть до звіту:

– Набір послуг, що надає даний сервіс, їх ціна, наявність тарифів;

– Опис технологій, які використовуються для виявлення плагіату;

4. Перевірте будь-який фрагмент тексту на оригінальність. Результати запишіть до звіту.
5. Зробіть та запишіть до звіту висновки, в яких зробіть аналіз даного сервісу, висвітліть переваги та недоліки.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що охоплює поняття плагіату? Назвіть різні варіанту тлумачення даного терміну.
2. Назвіть та охарактеризуйте найпоширеніші програми для виявлення плагіату.
3. Зробіть аналіз програми, призначеної для виявлення плагіату "Антиплагіат".
4. Які процедури використовують у своїй роботі програми для виявлення плагіату?
5. Назвіть основні правила цитування.
6. Охарактеризуйте програми для виявлення плагіату в програмному коді які ви знаєте.
7. Яку шкоду несе в собі явище плагіату?
8. Як законодавством України карається плагіат?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богуш В. М., Юдін О. К. «Інформаційна безпека держави». — К.: «МК-Прес», 2005. — 432с., іл.
2. Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. — Київ. 2004. — 508 с.
3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, введений в дію Наказом ДСТСЗІ від 28.04.1999 р. № 22
4. Сідак В. С., Артемов В. Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник. — К.: КНТ, 2007.
5. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: Автореф. дис. д-ра юрид. наук: 12.00.07. — Х.: НХУ України, 2004.
6. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. - К.: Кондор, 2004. - 384 с.
7. Харченко В. С. Інформаційна безпека. Глосарій. — К.: КНТ, 2005.
8. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права // Кормич Б. А.
9. Організаційно-правові основи політики інформаційної безпеки України: Автореф. дис. д-ра юрид. наук: 12.00.07. — Х.: НХУ України, 2004.
10. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. - К.: Кондор, 2004. - 384 с.
11. Харченко В. С. Інформаційна безпека. Глосарій. — К.: КНТ, 2005.
12. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — К.: НТУУ «КПІ», 2001. — № 4.
13. Петров А.А. Построение комплексной системы защиты информации в сетях общего пользования. / Петров А.А. // Вісник СНУ ім. В.Даля. – 2009. - №136. – С. 135-143.
14. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996. — 336с.
15. Вербицький О.В. Вступ до криптології. — Львів: Видавництво науково-технічної літератури, 1998. — 248 с.
16. Вєртузаев М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник/За ред.
17. С.Г. Лаптєва. — К.: Видавництво Європейського університету, 2001. — 201 с.
18. Герасименко В.А., Малюк А.А. Основы защиты информации. — М.: МГИФИ, 1997. — 538 с.
19. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. — М.: ТЕИС, 1994. — 69 с.
20. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996. — 336с.
21. Организация и современные методы защиты информации/Под общ. ред. С.А. Диева, А.Г. Шаваева. — М.: Коцерн "Банковский Деловой Центр", 1998. — 472 с.
22. Полмар Н., Аллен Т.Б. Энциклопедия шпионажа/Пер. сангл. В. Смирнова. — М.: КРОН-ПРЕСС, 1999. — 816 с.
23. Росоловський В.М., Анкудович Г.Г., Катерноза К.О., Шевченко М.Ю. Основи інформаційної безпеки автоматизованої інформаційної системи державної податкової служби України: Навч. посібник/За ред. М.Я. Азарова. — Ірпінь: Академія ДПС України, 2003. — 466 с.
24. Хорев А.А. Способы и средства защиты информации. — М.: МО РФ, 2000. — 316 с.
25. Барабаш А.В., Шанкин г.п. История криптографии. Ч.l. — М.: Гелиос АРВ, 2002. — 240 с.
26. Болдырев А.И., Василевский И.В., Сталенков С.Е. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. Практическое пособие. — М.: НЕЛК, 2001. — 138 с.
27. Попов М.О. До забезпечення воєнної безпеки в умовах загрози інформаційної війни /

28. М.О. Попов, А.Г. Лук'янець // Наука і оборона : наук.-теорет. та наук.-практ. журнал. – 1999. – № 2. – С. 37-43.
29. Сідак В.С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник / В.С. Сідак, В.Ю. Артемов. – К. : Вид-во КНТ, 2007. – 21-24 с.
30. Харченко В.С. Інформаційна безпека : глосарій / В.С. Харченко. – К. : Вид-во КНТ, 2005. – 13-18 с.
31. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : Вид-во НТУ України "КПІ", 2001. – № 4. – С. 43-48.
32. http://uk.wikipedia.org/wiki/Інформаційна_безпека_України
33. Постанова Верховної Ради України "Про прийняття за основу проекту Закону України про Концепцію державної інформаційної політики". [Електронний ресурс]. – Доступний з http://zakon1.rada.gov.ua/cgibin/laws/main.cgi?nreg=2897-17.
34. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" // Відомості Верховної Ради України (ВВР), 2007 р., № 12, ст. 102.

Місце для нотатків

НАВЧАЛЬНЕ ВИДАННЯ

Навчально-методичний посібник до курсу

“*ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ*”

Укладач С. О. Троян