МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ВОЛОДИМИРА ДАЛЯ

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни

«Безпека інформаційних систем»

для здобувачів першого (бакалаврського) рівня освіти

за спеціальністю

126 «Інформаційні системи та технології»

(Електронне видання)

ЗАТВЕРДЖЕНО
на засіданні кафедри інформаційних
техногологій та програмування
Протокол № 11 від 17.06 2025р.

Київ 2025

УДК 330.88:338:65.01

Конспект лекцій з дисципліни «Безпека інформаційних систем» для здобувачів першого (бакалаврського) рівня освіти за спеціальністю 126 «Інформаційні системи та технології»(Електронне видання)/ Уклад.: Іванов В.Г. - Київ: Вид–во СНУ ім. В. Даля, 2025. – 152 с.

Укладач: В. Г. Іванов

Рецензент: В.О. Лифар, доц., д.т.н..

ЗМІСТ

Лекція 1. Вступ

Основні поняття інформаційної безпеки

Інформаційна безпека (information security):

1. Стан захищеності деякого об’єкта (інформація, дані, ресурси автоматизованої системи,автоматизована система, інформаційна система підприємства, суспільства, держави тощо)
2. Діяльність , спрямована на забезпечення захищеного стану об’єкту (захист інформації)

Інформаційна система – сукупність технічного, програмного та організаційного забезпечення для задоволення інформаційних потреб в рамках певної предметної області. (іноді включають сюди і персонал). ВК: ІС – софт, хард , дані та лінії зв’язку.

Об’єкт обмежимо як інформація (дані).

Базова модель безпеки інформації

Безпека інформації (даних) (information (data) security) - стан захищеності інформації(даних), при якому забезпечені її (їх) :

- Конфіденційність (confidentiality) - доступ до інформації лише для авторизованихкористувачів.
- Доступність (availability) – постійний доступ до інформації для авторизованихкористувачів.
- Цілісність (integrity) - достовірність і повнота інформації (уникнення несанкціонованоїмодифікації інформації).

Це базова модель безпеки інформації (даних). (Три зазначені стани

(сервіси))Базова модель може бути розширена додаванням

наступних станів (сервісів):

- Невідмовність (апелюємість, non-repudiation) - неможливість відмови від авторства.
- Підзвітність (accountability) - забезпечення ідентифікації суб'єкта доступу і реєстраціїйого дій.
- Надійність (reliability) - відповідність передбаченій поведінці або результату.
- Автентичність (authenticity) - гарантування, що суб'єкт або ресурс ідентичні заявленим.

Системний підхід до опису безпеки

Системний підхід до опису інформаційної безпеки пропонує виділити наступні складовіінформаційної безпеки:

1. Законодавча, нормативно-правова і наукова база:

ЗАКОН УКРАЇНИ - Про Національну систему конфіденційного зв'язкуЗАКОН УКРАЇНИ - Про телекомунікації

ЗАКОН УКРАЇНИ - Про електронні документи та електронний документообігЗАКОН УКРАЇНИ - Про електронний цифровий підпис

КМ - Про затвердження Положення про центральний засвідчувальний орган

КМ - Про деякі питання захисту інформації, охорона якої забезпечуєтьсядержавою, тощо.

2. Організаційно-технічні і режимні заходи і методи (Політика інформаційної безпеки).

3. Програмно-технічні засоби забезпечення інформаційної безпеки. (Soft & Hard)

Політика безпеки (інформації в організації) (Organizational security policy) - сукупність документованих правил, процедур, практичних прийомів або керівних принципів в області безпеки інформації, якими керується організація в своїй діяльності.

Для побудови Політики інформаційної безпеки рекомендується окремо розглядати наступні напрями захисту інформаційної системи:

1. Захист апаратного забезпечення інформаційної системи (харда);
2. Захист процесів, процедур і програм обробки інформації (софта);
3. Захист інформації (даних);
4. Захист каналів зв'язку;
5. Управління системою захисту (Менеджмент безпеки – частина загальної системи менеджменту, яка стосується безпеки. Базується на моделі PDCA (Plan –Do-Check (перевірка відхилення від запланованого) - Act(заходи по запобіганню відхилень від запланованого) і знову Plan- …)).

При цьому, по кожному з перерахованих вище напрямів Політика інформаційної безпеки дати відповідь на наступні запитання:

1. Які об’єкти, що підлягають захисту?;
2. Яка множина потенційних загроз і каналів просочування інформації?;
3. Які уразливості інформації при наявній множині загроз і каналів витоку?;
4. Які вимоги до системи захисту?;
5. Які засоби захисту інформації і їх характеристики?;
6. Як впровадити вибрані засоби захисту?;
7. Як здійснювати менеджмент системою захисту?.

Загроза (threat) - можливість порушення безпеки інформації (конфіденційності, доступності,цілісності).

Уразливість (vulnerability) - недолік в системі, використовуючи який, можна порушити її безпеку (конфіденційність, доступність, цілісність).

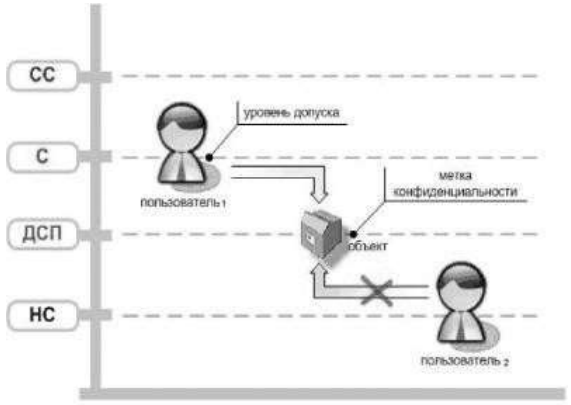
Класифікація засобів захисту інформації

1. Засоби захисту від несанкціонованого доступу (НСД):

Засоби авторизації (authorization) - надання цій особі деяких прав або перевірка їх

наявності;

Мандатне управління доступом (Примусовий контроль доступу, Mandatory access control, MAC) - розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності об'єктам і видачі допусків суб'єктам на звернення до інформації певного рівня конфіденційності.;



СС совершенно секретно (цілком таємно) , С секретно (секретно), ДСП для служебногопользования (для службового користування), НС несекретно (несекретно).

Вибіркове управління доступом (Discretionary access control, DAC, Дискреційне управління доступом, Контрольоване управління доступом і Розмежувальне управління доступом.)- управління доступом суб'єктів до об'єктів на основі списків управління доступом або матриці доступу. Для кожної пари (суб'єкт - об'єкт) має бути задане явне і недвозначне перерахування допустимих типів доступу (читати, писати і т. д.);

Управління доступом на основі ролей (Role Based Access Control, RBAC) - права доступу суб'єктів системи на об'єкти групуються з врахуванням специфіки їх вживання, утворюючи ролі. Оскільки привілеї не призначаються користувачам безпосередньо, і отримуються ними лише через свою роль (або ролі), управління індивідуальними правами користувача по суті зводиться до призначення йому ролей. Це спрощує такі операції, як додавання користувача або зміна підрозділу користувачем. Розвиток вибіркового управління доступом;

Формалізація понять:

S –

суб’єктR

– роль

P – дозвіл

SE – сесія (функція, яка для кожної ролі визначає множину дозволів.

SE:R -> 2P)SA – призначення (задача) суб’єкта (SA $\subset$ S×R)

PA – призначення (задача) дозволу (PA $\subset$ P×R)

RH – частковий порядок на множині ролей (RH $\subset$ R×R)

Ведення журналу (Аудит) - процес запису інформації про події, що відбуваються з якимсь об'єктом (або в рамках якогось процесу), в журнал (наприклад, у файл).

2. Системи моніторингу мереж:

Системи виявлення і запобігання вторгненням (IDS/IPS , Intrusion Detection System) - програмний або апаратний засіб, призначений для виявлення фактів неавторизованого доступу в

комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет.

Системи запобігання витоку конфіденційної інформації (DLP-системы, Data Leak Prevention). DLP-системы будуються на аналізі потоків даних, що перетинають периметр інформаційної системи, що захищається. При детектуванні в цьому потоці конфіденційної інформації спрацьовує активна компонента системи, і передача повідомлення (пакету, потоку, сесії) блокується.

3. Аналізатори протоколів. Аналізатор трафіку, або сніфер (to sniff - нюхати) - мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу мережевого трафіку, призначеного для інших вузлів.

4. Антивірусні засоби.

5. Міжмережеві екрани. Міжмережевий екран або мережевий екран - комплекс апаратних або програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього, на різних рівнях моделі OSI (Open Systems Interconnection) відповідно до заданих правил. Основним завданням мережевого екрану є захист комп'ютерних мереж або окремих вузлів від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, оскільки їх основне завдання - не пропускати (фільтрувати) пакети, не відповідні під критерії, визначені в конфігурації.

6. Криптографічні засоби: (Симетричні криптоалгоритмы, Асиметричні шифри, Хеш- функції)

Шифрування;

Цифровий підпис.

7. Системи резервного копіювання. Резервне копіювання (backup) - процес створення копії даних на носієві (жорсткому диску, дискеті і т. д.), призначеному для відновлення даних в оригінальному місці їх розташування в разі їх пошкодження або руйнування.

8. Системи безперебійного живлення: Джерела безперебійного живлення; стабілізатори; Генератори напруги.

9. Системи аутентифікації (аутентифікація - це встановлення достовірності особи):

Пароль; Пароль (parole - слово) - це секретне слово або набір символів,

призначений для підтвердження особи або повноважень. Паролі часто використовуються для захисту інформації від несанкціонованого доступу. У більшості обчислювальних систем комбінація «ім'я користувача - пароль» використовується для посвідчення користувача.

Сертифікат; Цифровий сертифікат - випущений засвідчуючим центром електронний або друкарський документ, підтверджуючий приналежність власникові відкритого ключа або яких- небудь атрибутів.

Біометрія.

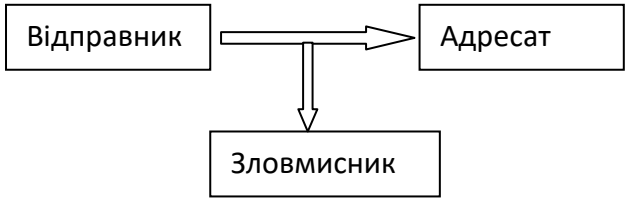
10. Інструментальні засоби аналізу систем захисту

Модель мережевої безпеки

Атака – спроба порушити стан безпеки інформації (даних) (конфіденційність, цілісність,доступність) (ВК).

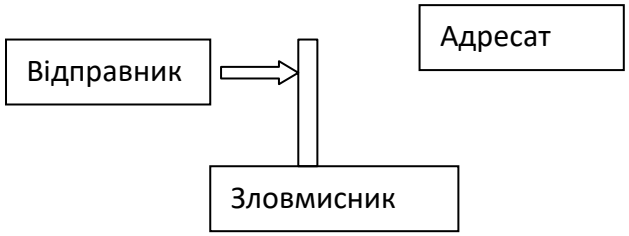
Класифікація атак:

1. Пасивна – порушення конфіденційності.

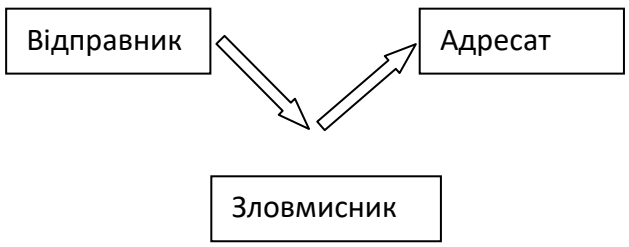


2. Активна – порушення цілісності або доступності.

2.1. Порушення доступності. DoS – атака. (Denial of Service). Зловмисник перехоплює усі повідомлення або створює значний трафік і сервер не може обробити запроси законних користувачів.



2.2. Порушення цілісності. Модифікація потоку. Man in the middle. Змінює вміст повідомлення або порядок повідомлень.



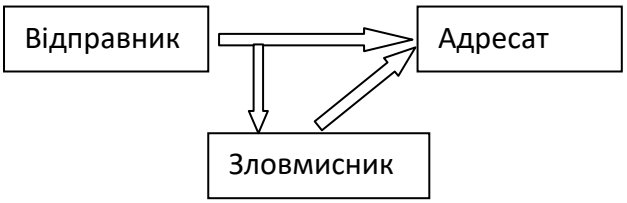
Якщо базова модель безпеки розширена за рахунок, наприклад, автентичності інформації (даних), то атака на автентичність називається фальсифікацією. Це спроба

одного суб’єкту видати себе за іншого.

Зловмисник

Найчастіше мають місце комбінації атак. Наприклад, одна з найбільш розповсюджених атак Replay – атака (повторне використання). Це комбінація пасивної атаки і фальсифікації.

Прослуховуваннятрафіку з наступною пересилкою даних для отриманнянесанкціонованого доступу.



Модель безпеки інформаційної системи

Охоплює ситуації, які не описуються схемою мережевої безпеки.

Засоби безпеки розбивають на дві категорії:

1. Сторожова категорія. (Захисні екрани (Firewalls))
2. Внутрішні монітори, які контролюють доступ і аналізують діяльність користувачів.

Лекція 2. Безпека мережевої інфраструктури

Дана лекція присвячена способам розгортання мережевої інфраструктури на основі ОС Windows 2003/XP. Автоматичне розгортання ОС і клієнтських робочих місць є важливим завданням для забезпечення безпеки мережевої інфраструктури будь-якої організації.

Далі будемо розглядати комп'ютерну мережу, сервери якої управляються операційними системами Windows Server 2003, а робочі станції - Windows XP (SP2), іншими словами, мережеву інфраструктуру на основі ОС Windows 2003/XP.

На цьому занятті розглянемо способи розгортання такої мережевої інфраструктури. Термін "розгортання" (англ. deployment) не слід плутати з "установкою" (англ. install) операційних систем. Розгортання увазі автоматизацію процесу установки ОС на комп'ютер. Можливі механізми розгортання операційних систем Microsoft, коли цей процес стає повністю автоматичним.

Чому важливо вміти забезпечувати швидке розгортання мережевої інфраструктури? Будь- яка комп'ютерна система організації не застрахована від серйозних аварій, викликаних природними причинами (діями зловмисників, халатністю або некомпетентністю співробітників). У той же час, у кожній організації є функції, які керівництво вважає критично важливими, і вони повинні виконуватися незважаючи ні на що. Мережева інфраструктура для більшості сучасних організацій є базисом для виконання бізнес-процесів. Тому дуже важливо вміти відновлювати (розгортати) мережеву інфраструктуру в короткі терміни і з мінімальними витратами.

Розглянемо два основних механізми розгортання, які застосовуються для ОС Microsoft:

- метод дублювання дисків з використанням утиліти Sysprep;
- метод віддаленої установки з використанням сервера віддаленого встановлення (RIS).

На практиці дуже рідко вдаються до автоматичної установки серверної ОС. Для невеликих і середніх організацій найбільш важливим завданням може бути розгортання ОС для робочих станцій з необхідним прикладним ПЗ. Тому на лабораторних роботах розглянемо зазначені вище методи на прикладі ОС Windows XP Professional.

Перш за все

Для вивчення матеріалів цієї глави необхідні наступні ресурси:

- Комп'ютер під управлінням операційної системи Windows XP Professional з параметрами зазамовчуванням, об'ємом оперативної пам'яті не менше 1 Гб і мережевою картою.
- Вільне місце на жорсткому диску не менше 6 Гб.
- Завантажувальний компакт-диск з дистрибутивом Windows XP Professional.

• Завантажувальний компакт-диск з дистрибутивом Windows Server 2003.

Метод дублювання дисків з використанням утиліти Sysprep

Ідея методу полягає в тому, що якщо необхідно встановити ОС Windows XP Professional відразу на кілька комп'ютерів з однаковою конфігурацією обладнання, то на одному з комп'ютерів створюється образ диска, на який встановлюють ОС з необхідним прикладним ПЗ. Потім цей образ копіюється на інші комп'ютери.

Перевага методу над звичайною установкою полягає, насамперед, в економії часу. Інший плюс полягає в тому, що, створивши один раз образ диска, ви отримуєте базову точку розгортання робочого місця користувача, до якої завжди можна повернутися, якщо на якомусь з комп'ютерів виникнуть проблеми.

Головну роль в реалізації методу грає утиліта "Підготовка системи" - Sysprep (System Preparation). Вона запобігає проблему, з якою можна зіткнутися при копіюванні образу диска, пов'язану з унікальним кодом безпеки (SID, Security Identifier). Кожен комп'ютер в мережі повинен мати унікальний код безпеки. Якщо просто копіювати образ диска, то кожен кінцевий комп'ютер буде мати той же код безпеки, що й основний комп'ютер. Через конфлікти SID мережа не буде працювати. Утиліта Sysprep допомагає вирішити цю проблему, видаляючи унікальний код безпеки на основному комп'ютері перед копіюванням образу диска. При запуску копії системи на кінцевому комп'ютері Sysprep генерує новий унікальний код безпеки.

Для використання утиліти Sysprep в процесі дублювання дисків повинні виконуватися наступні вимоги:

• основний і кінцеві комп'ютери повинні мати сумісні файли рівня апаратних абстракцій (HAL, Hardware Abstraction Layer);

• контролери жорстких дисків на основному і кінцевих комп'ютерах повинні бути однаковими;

• пристрої Plug and Play, такі як модеми, звукові карти, мережні карти, відеокарти і т. д., можуть бути різними. Тим не менш, всі драйвери пристроїв, не включені в файл Drivers.cab, повинні бути перенесені в основний комп'ютер перед запуском Sysprep. Слід переконатися, що драйвери доступні на кінцевому комп'ютері при першому запуску, щоб технологія Plug and Play могла виявити і встановити пристрої;

• обсяг жорсткого диска на кінцевому комп'ютері повинен бути не менше об'єму жорсткого диска на основному комп'ютері;

• якщо версією BIOS (Basic Input-Output System - базова система введення-виведення) на основному і кінцевих комп'ютерах розрізняються, рекомендується заздалегідь протестувати процес установки.

Далі розглянемо основні кроки виконання методу дублювання дисків з використанням утиліти Sysprep.

Крок 1. Встановіть і налаштуйте Windows XP Professional на тестовому комп'ютері (якщо необхідно, то встановіть драйвери устаткування, не включені в файл Drivers.cab). Встановіть необхідне прикладне ПЗ (архіватори, антивіруси, офісні пакети і т. д.), включаючи пакети оновлень.

Крок 2. Створіть файл відповідей Sysprep.inf для того, щоб процес розгортання був автоматичним. Даний крок не є обов'язковим. Якщо файл відповідей не створювати, то після копіювання образу диску на цільовий комп'ютер при їх подальшому включенні запуститься майстер міні-установки (Mini-Setup Wizard), який буде запитувати введення різних параметрів (пароль адміністратора, ім'я комп'ютера і т.д.).

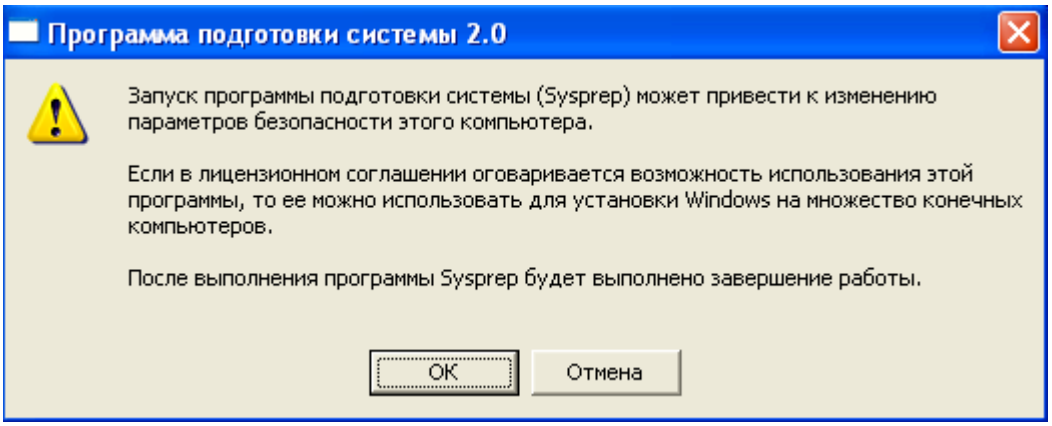
Sysprep.inf - це текстовий файл, у якому наведено відповідей, що вводяться в

діалогових вікнах графічного інтерфейсу користувача при установці Windows XP Professional. Для створення файлу відповідей Sysprep.inf, який потім буде використовуватися утилітою Sysprep, можна використати текстовий редактор або диспетчером установки.

Файл Sysprep.inf повинен зберігатися в папці Sysprep в кореневому каталозі диска, на якому встановлена ОС Windows XP Professional, або на гнучкому диску. Програма установки не може використовувати папки з іншими назвами. Параметра для зазначення файлу відповідей майстра міні- інсталяції.

Крок 3. Запустіть на тестовому комп'ютері утиліту Sysprep, файли якої знаходяться в архіві \ Support \ Tools \ Deploy.cab на установчому диску Windows XP Professional. На екрані з'явиться діалогове вікно "Програма підготовки системи 2.0", попереджувала, що запуск програми Sysprep

може призвести до зміни деяких параметрів безпеки. Після натискання кнопки "ОК"утиліта Sysprep продовжить роботу.



Крок 4. Скопіюйте образ диска на цільові комп'ютери. Для цього буде потрібно спеціальне ПЗ для клонування дисків, що надається сторонніми фірмами. Найбільш популярними є утиліти Ghost фірми Symantec, Drive Image Pro фірми PowerQuest та ін.. Всі перераховані утиліти працюють приблизно однаково. Комп'ютер завантажується в режимі DOS, потім запускається програма формування образу диска. Можна отримати образ всього диска або єдиного розділу і зберегти його на іншому розділі, диску або загальному мережному накопичувачі. Згодом збережений образ можна відновити на іншому диску. Жорсткі диски не обов'язково повинні мати однакову ємність, але завантажуваний образ не повинен бути більше цільового диска.

Крок 5. Включіть цільові комп'ютери після того, як завершиться копіювання образу диску з тестового комп'ютера. Якщо утиліта Sysprep виявила файл відповідей Sysprep.inf, то з'явиться вікно "Установка Windows XP" і через деякий час завантажиться ОС Windows XP Professional. В іншому випадку запуститься майстер міні-установки.

Якщо додаток Sysprep.exe запускалося з папки% systemdrive% \ Sysprep, після завершення установки Windows XP Professional ця папка і її вміст автоматично видаляються!

Метод віддаленої установки

Найбільш ефективним методом розгортання ОС Windows XP Professional є віддалена установка. Її можна проводити, якщо мережева інфраструктура заснована на ОС Windows Server 2003, а клієнтські комп'ютери підтримують віддалене завантаження.

Віддалена установка (remote installation) - це процес встановлення з'єднання з сервером, на якому запущена служба RIS (Remote Installation Services), і наступного запуску автоматичної установки клієнтської ОС, наприклад Windows XP Professional, на цільовий комп'ютер, підключений до мережі.

Попередні вимоги для проведення методу

Для виконання віддаленої установки клієнтський комп'ютер повинен мати BIOS і мережевий адаптер, що підтримують технологію предзагрузочной середовища виконання - PXE (Pre-boot execution Environment). Технологія PXE застосовується для встановлення з'єднання з сервером RIS. Переконайтеся, що на всіх клієнтських комп'ютерах в BIOS є можливість встановити в якості завантажувального пристрою мережевий адаптер. Якщо така можливість відсутня, то необхідно створити завантажувальну дискету віддаленої установки за допомогою утиліти "Генератор дисків віддаленого завантаження" - rbfg.exe (Remote Boot Disc Generator). Файл rbfg.exe розташований в папці \ RemoteInstall \ Admin \ i386 на сервері віддаленого встановлення RIS.

Для функціонування сервера RIS в мережевій інфраструктурі необхідна наявність наступних мережевих служб:

- Служба DNS. Потрібно для пошуку в мережі серверів RIS. Клієнт RIS запитує у сервера DNS ім'я і IP-адресу сервера RIS.
- Служба DHCP. Для установки мережевого з'єднання клієнт RIS повинен мати IP-адресу. Але так як на клієнтському комп'ютері ще немає операційної системи, призначити статичний IP-адресу неможливо, тому необхідно використовувати динамічну адресацію. Для цього в мережі повинен працювати сервер DHCP.
- Служба Active Directory. RIS використовує групову політику Active Directory для визначення дозволів облікових записів користувачів і комп'ютерів. Облікового запису користувача, яка буде використовуватися для проведення віддаленої установки, має бути призначене право "Вхід у якості пакетного завдання" ("Log On as a Batch Job") і дозвіл на створення облікових записів в домені. Перш ніж сервер RIS зможе обслуговувати запити клієнтських комп'ютерів, він повинен бути авторизований в Active Directory. Також Active Directory застосовується для того, щоб визначити, який сервер RIS повинен використовуватися для віддаленої установки, якщо таких серверів в мережі декілька.

Перераховані мережеві служби не обов'язково повинні бути встановлені на тому ж сервері, що і RIS, але вони повинні бути доступні в мережевій інфраструктурі.

Метод віддаленої установки вимагає, щоб RIS був встановлений на тому, до якого дозволений загальний доступ через мережу. Загальний тому повинен відповідати наступним вимогам:

- він не є тим же самим диском, з якого запускається Windows Server 2003;
- на ньому є достатньо вільного місця для зберігання програмного забезпечення RIS і різних образів Windows XP Professional;
- він відформатований з використанням файлової системи NTFS версії 5 або вище.

Встановлення та налаштування RIS

Розгортання сервера віддаленого встановлення у вашій мережевій інфраструктурі виконується в два етапи:

- установка RIS-сервера;
- настройка RIS-сервера.

При установці ОС Windows Server 2003 на сервер служба RIS за замовчуванням не встановлюється.

За допомогою компонента панелі керування "Установка й видалення програм" в розділі "Установка компонентів Windows" необхідно додати "Служби віддаленої установки". Після цього в розділі "Адміністрування" з'являється компонент "Установка служб віддаленого встановлення", що дозволяє запустити майстер підготовки сервера RIS. При першому запуску майстра установки служб віддаленої установки вибирається диск для розміщення RIS, папка для зберігання інсталяційних

файлів, створюється образ для віддаленої установки клієнтської ОС. Після завершення процесу установки служби RIS з'явиться вікно, представлене на рис..

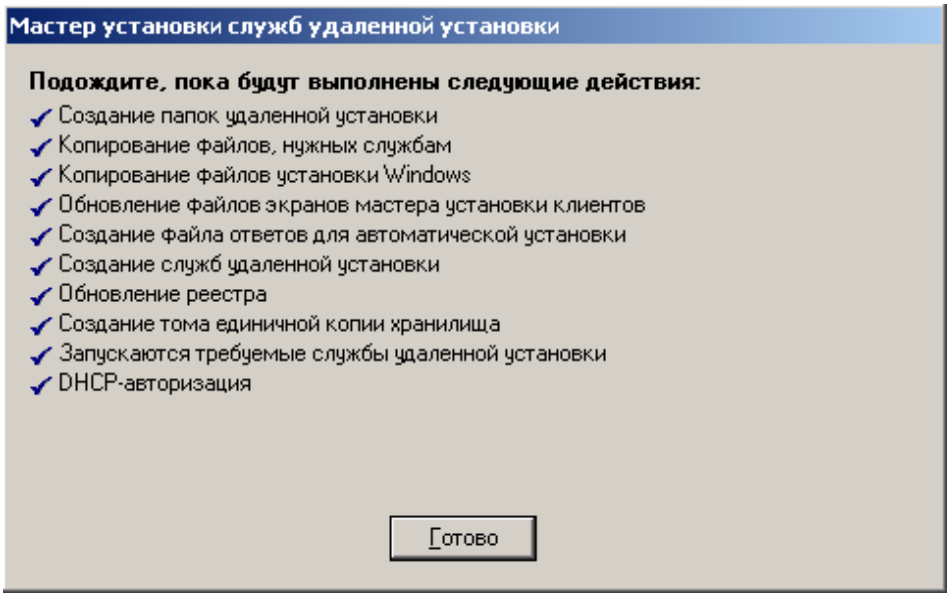


Рис. Завершення установки служби RIS

Важливо, щоб сервер RIS пройшов авторизацію в Active Directory, про це сигналізує останній прапорець "DHCP-авторизація". Якщо не авторизувати сервер RIS, то він не зможе відповідати на запити клієнтських комп'ютерів для мережевої завантаження служби.

Необхідно також створити в Active Directory обліковий запис користувача, якою буде дозволено створювати облікові записи комп'ютерів у домені. Процес віддаленого встановлення ОС на клієнтському комп'ютері починається з введення імені і пароля користувача, у якого є такі дозволи.

Важливим аспектом виконання методу віддаленої установки є підготовка образів ОС, які зберігаються на окремому томі сервера RIS. Використовуючи файл відповідей для віддаленої установки, можна налаштувати декілька варіантів автоматичної установки, які будуть пов'язані з одним чином ОС, що зберігаються на сервері RIS. Для цього необхідно створити відповідні файли відповідей, в яких можна налаштувати параметри ОС, що конфігуруються під час її установки. Файли відповідей для віддаленої установки мають розширення *. Sif і можуть бути створені за допомогою диспетчера установки Windows.

Якщо на сервері RIS зберігається більше одного образу, то при запуску майстра установки клієнтів завантажиться екран вибору образів ОС. Якщо доступний тільки один образ ОС, то майстер установки клієнтів просто попросить користувача підтвердити установку. Коли один з образів ОС обраний, з'являється повідомлення про те, що на даний комп'ютер буде встановлена ОС, існуючі розділи будуть видалені, а жорсткий диск буде відформатований, і всі дані, що знаходяться на диску, будуть стерті.

Як бачимо з усього перерахованого вище, виконання методу віддаленої установки має багато нюансів і вимагає великої підготовки для його реалізації. Однак, виконавши установку і настройку сервера RIS один раз і провівши його апробацію на тестовому клієнтському комп'ютері, ваша мережева інфраструктура придбає незамінний і дуже корисний сервіс. Процес віддаленої установки клієнтських ОС Windows XP Professional за допомогою сервера RIS вимагає мінімум участі користувача.

Створення файлів відповідей для автоматизації процесів розгортання

Для того щоб методи розгортання, описані вище, виконувалися успішно, важливо правильно скласти файли відповідей. Нижче представлений список використовуваних файлів відповідей для різних методів автоматичної установки ОС Windows XP Professional.

Unattend.txt - Для виконання сценарію автоматичної установки ОС Windows XP Professional (%systemdrive% \ Deploy)

Winnt.sif - Для виконання сценарію автоматичної установки ОС Windows XP Professional с компакт- диска. Створюється перейменуванням файлу Unattend.txt, в який додається секція [Data] з відповідними розділами (Флоппі-диск A: \)

Sysprep.inf - Для використання утилітою Sysprep (% systemdrive% \ Sysprep)

Winbom.ini - Якщо утиліта Sysprep використовується з параметром-factory, то вона працює з даним файлом відповідей (% systemdrive% \ Sysprep)

*. Sif - Для віддаленої установки з використанням сервера RIS. Кожен плоский образ ОС, розміщений на сервері RIS, буде містити папку \ Templates, в якій повинні знаходитися пов'язані з образом файли відповідей автоматичної установки *. Sif

Використання диспетчера установки Windows

Диспетчер установки Windows (Windows Setup Manager) спрощує створення файлів відповідей і виключає в них виникнення синтаксичних помилок. Диспетчер установки Windows входить до складу компакт-диска з ОС Windows XP Professional (архів \ Support \ Tools \ Deploy.cab), а також до складу пакета Microsoft Windows XP Resource Kit.

Коли ви запускаєте диспетчер установки Windows, на екран виводиться перша сторінка майстра диспетчера установки Windows.

Клацніть кнопку "Далі", щоб перейти до наступної сторінки, на якій слід зробити вибір:

- створити новий файл відповідей;
- змінити існуючий файл відповідей.

Якщо виберете пункт "Створити новий файл відповідей", то далі необхідно вибрати типстворюваного файлу відповідей. Диспетчер установки Windows може створювати файли відповідей всіх типів:

- Для автоматичної установки Windows;
- Для установки Sysprep;
- Для служб віддаленої установки.

Лекція 3. Безпека зберігання даних в ОС Microsoft

Розглянемо один з ключових моментів інформаційної безпеки будь-якої організації - забезпечення збереження даних. Під даними будемо розуміти різні користувальницькі файли, які постійно створюються, редагуються і видаляються в процесі функціонування організації. У цих файлах може зберігатися інформація будь важливості: від несуттєвою, втрата якої ніяк не позначиться на бізнес-процесах, до критичною, втративши яку компанія ризикує закінчити своє існування.

В рамках цього заняття не будемо торкатися питання класифікації даних за ступенем їх важливості. З цієї тематики є багато літератури з області теорії інформаційної безпеки, управління ризиками і т. п. Мета цього заняття - ознайомитися з наданими можливостями ОС Microsoft Windows 2003/XP щодо забезпечення безпеки зберігання даних в цілому, незважаючи на їх ступінь значимості.

З теорії інформаційної безпеки відомо, що забезпечення схоронності інформації досягається різними рішеннями: починаючи з тиражування інформаційних ресурсів (програм і даних) і закінчуючи резервуванням пристроїв зберігання даних . Тому на даному занятті розглянемо цікаві та корисні рішення, надані ОС Microsoft Windows 2003/XP в цьому діапазоні:

- технологія тіньового копіювання даних;
- архівація даних;
- створення відмовостійких томів для

зберігання даних.Перш за все

Для вивчення матеріалу необхідні наступні ресурси:

- Комп'ютер під управлінням операційної системи Windows XP Professional з параметрами зазамовчуванням, об'ємом оперативної пам'яті не менше 1 Гб і мережевою картою.
- Вільне місце на жорсткому диску не менше 8 Гб.

Технологія тіньового копіювання даних

Суть цієї технології полягає у створенні копій вибраних файлів через певні проміжки часу. Реалізована технологія у вигляді окремої служби тіньового копіювання тому (VSS). Вона використовується для управління даними на дисках і може взаємодіяти з різними додатками. Наприклад, в програмах резервного копіювання ця служба забезпечує копіювання файлів, зайнятих під час архівації іншими додатками.

Важливою практичною функцією технології тіньового копіювання є можливість відновлення останніх версій випадково видалених або пошкоджених файлів. В ОС Microsoft Windows 2003/XP надається можливість користувачам клієнтських комп'ютерів відновлювати файли з тіньової копії самостійно без втручання системних адміністраторів, що, безумовно, дуже зручно з точки зору

економії часу.

Обмеження тіньового копіювання томів

Тіньові копії файлів на заданих томах доступні тільки на серверах під управлінням ОС Windows Server 2003. На сервері в каталозі% Systemroot% \ System32 \ Clients \ Twclient \ x86 \ мається клієнтське ПЗ для інсталяції на комп'ютери під управлінням Windows XP Professional, встановивши яке, користувачі зможуть отримувати доступ до тіньових копій через вкладку "Попередні версії" вікна властивостей файлів тіньового томи. Остання версія цього клієнтського ПЗ доступна за адресою: http://www.microsoft.com/windowsserver2003/ downloads/shadowcopyclient.mspx.

Тіньове копіювання тому не буде працювати для точок підключення, коли другий жорсткий диск підключається до першого у вигляді папки.

Створювати тіньові копії можна лише на томах з файловою системою NTFS. Тіньове копіювання буде виконуватися для всіх загальних папок, що зберігаються на цьому томі. Можливості вибрати окремі загальні папки на томі, для яких би створювалися тіньові копії, - ні! Для зберігання тіньових копій потрібно не

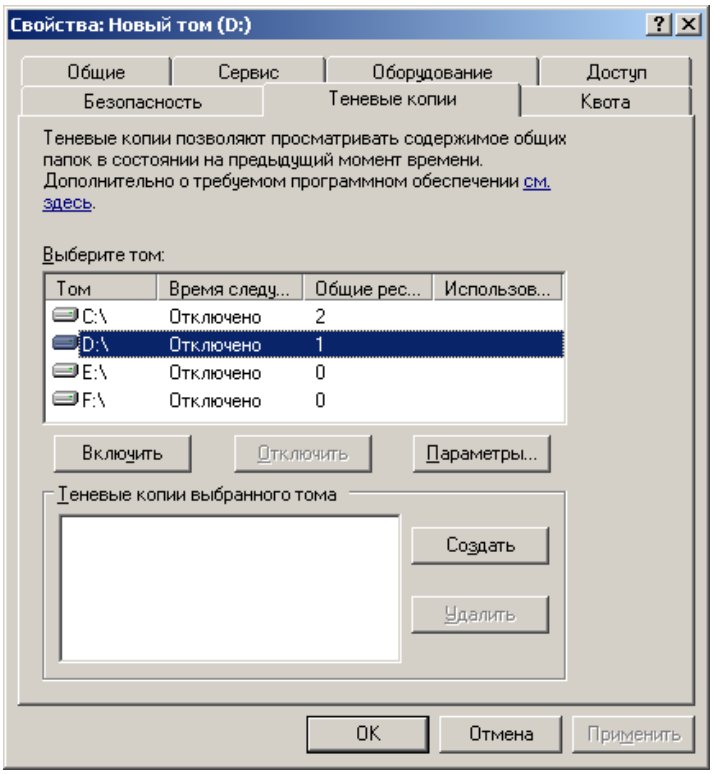
менше 100 Мб вільного місця на вибраному томі. Максимально допустиме значення - 64 тіньовікопії на один том, незалежно від того, скільки вільного місця залишається в області зберігання.

Установка і використання технології тіньового копіювання томів

На сервері під управлінням ОС Windows Server 2003 бажано розмістити загальні папки, для яких хочете використовувати тіньові копії, на окремому томі. Це вбереже від заповнення тіньовими копіями дискового простору і від зниження пропускної здатності засобів введення-виведення в результаті копіювання тих загальних папок, для яких функція тіньового копіювання не потрібна.

Для активізації створення тіньових копій на томі у вікні його властивостей перейдіть на вкладку "Тіньові копії".

На цій вкладці слід вибрати те, для загальних папок якого будуть створюватися тіньові копії. При великому завантаженні файлового сервера доцільно зберігати тіньові копії на окремому томі, який би розміщувався на іншому жорсткому диску. Це підвищить продуктивність сервера.

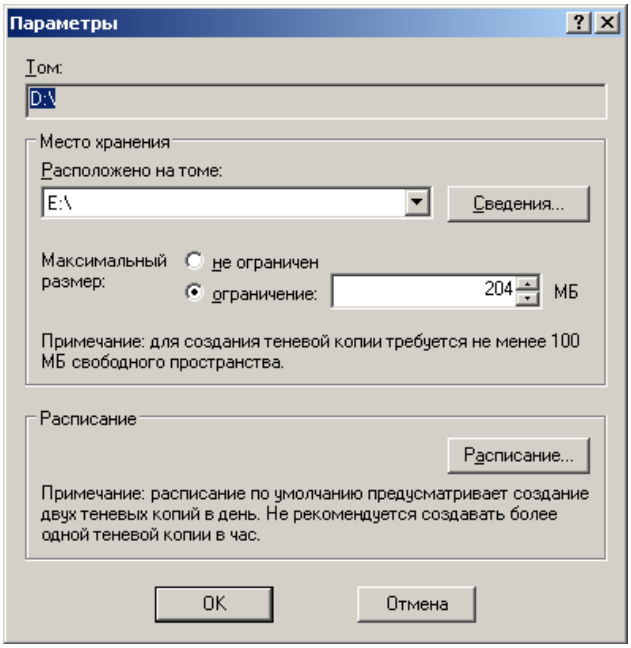


Вкладка "Тіньові копії" вікна властивостей диска

За замовчуванням тіньові копії зберігаються на тому ж диску, де зберігаються загальні папки. Прицьому встановлюються такі налаштування:

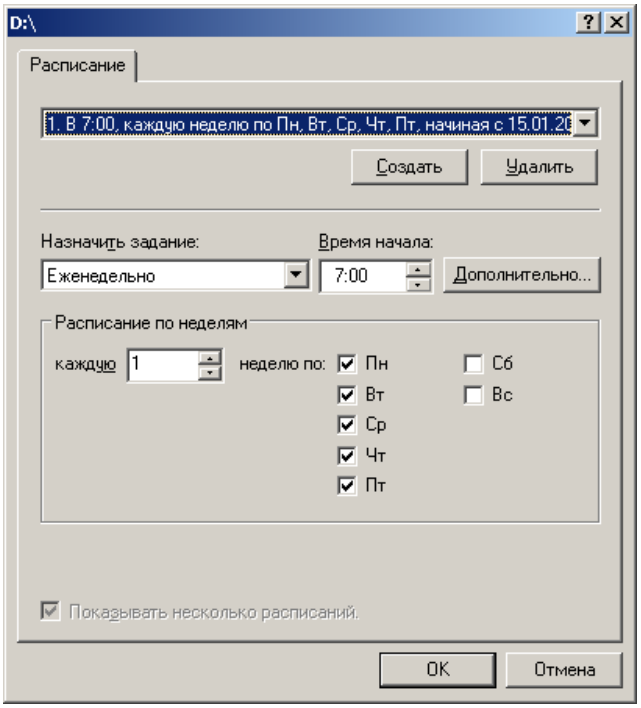
- максимальний розмір місця для зберігання тіньових копій дорівнює 10% від загального простору диска;
- автоматично проводити копіювання з понеділка по п'ятницю о 7 ранку і о 12 ночі;
- створюється перша тіньова копія.

Для змін и налаштувань тіньових копій томи, відмінних від заданих за замовчуванням, виберіть потрібний том зі списку і натисніть кнопку "Параметри".



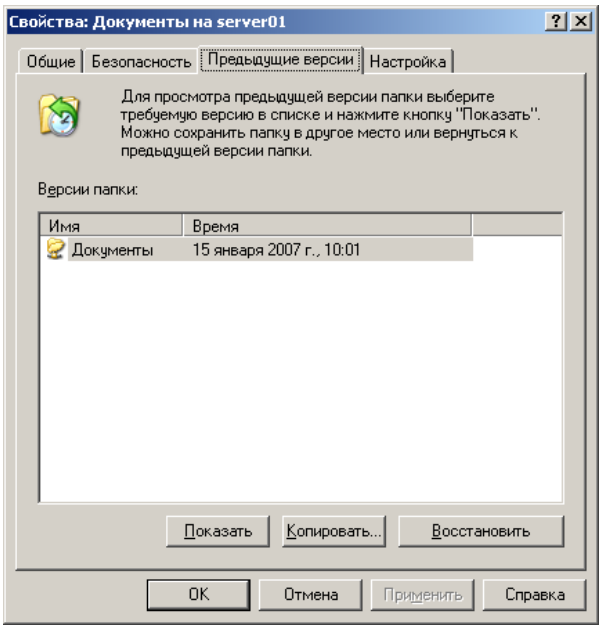
Вікно налаштування параметрів тіньового копіювання тому

Якщо ви вирішили змінити розклад створення тіньових копій, натисніть кнопку "Розклад": з'явиться вікно, представлене на рис. для його налаштування.



Вікно налаштування розкладу тіньового копіювання тому

Після виконаних налаштувань натисніть кнопку "Включити" - почнуть створюватися тіньові копії загальних папок на заданому томі. Тепер, якщо звернутися через контекстне меню до властивостей файлів, що зберігаються у спільних папках, з'явиться спеціальна вкладка "Попередні версії". Ця вкладка буде доступна у вікні властивостей файлу, тільки якщо ви звернулися до спільної папки як до мережного ресурсу (наприклад, UNC-шлях)!



Вкладка "Попередні версії" у вікні властивостей загальної папки

Внизу вкладки є три кнопки, що дозволяють здійснювати різні дії з копіями файлу:

- "Показати" - дозволяє переглянути обрану копію файлу;
- "Копіювати" - дозволяє копіювати обрану копію файлу в нове розташування;
- "Відновити" - дозволяє відновлювати обрану копію файлу поверх поточної версії файлу.

Далі розглянемо випадок, коли файл був видалений і потрібно його відновлення з тіньової копії. Так як об'єкт "файл", на якому можна клацнути правою кнопкою миші, у загальній папці в цьому випадку відсутня, необхідно звернутися до властивостей папки, де є така ж вкладка "Попередні версії". Натиснувши кнопку "Показати", можна переглянути, які файли і папки містилися в ній на вибраний момент часу. Звідси можна відновити видалений файл в будь-яке місце, в тому числі і в колишню папку.

Як бачимо, процедура відновлення файлу з тіньової копії - досить проста і швидка операція для користувачів. Але слід пам'ятати, що технологія тіньового копіювання не є стовідсотковим рішенням задачі забезпечення збереження даних. Вона вирішує проблему швидкого відновлення спільно використовуваних файлів із загальних папок.

Архівація даних

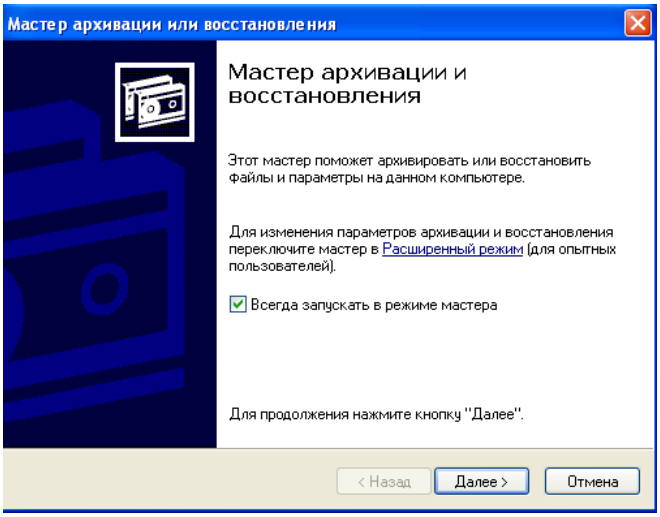
Під архівацією прийнято розуміти звичайне копіювання даних на резервний носій інформації, щоб у разі відмови або пошкодження основного пристрою зберігання можна було швидко відновити наявні на ньому дані. Архівація дає найвищу ступінь відмовостійкості у порівнянні з усіма іншими технологіями зберігання даних, які забезпечують відмовостійкість, такими як тіньове копіювання, надлишкові масиви

незалежних дисків, кластерні сервери і т.д.

Ефективність застосування архівації в мережевій інфраструктурі залежить від правильного вибору спеціального ПЗ і планування. До складу ОС Microsoft Windows 2003/XP входить службова програма Backup, що забезпечує основні функції архівації, включаючи можливості роботи за розкладом і взаємодія зі службою тіньового копіювання тому.

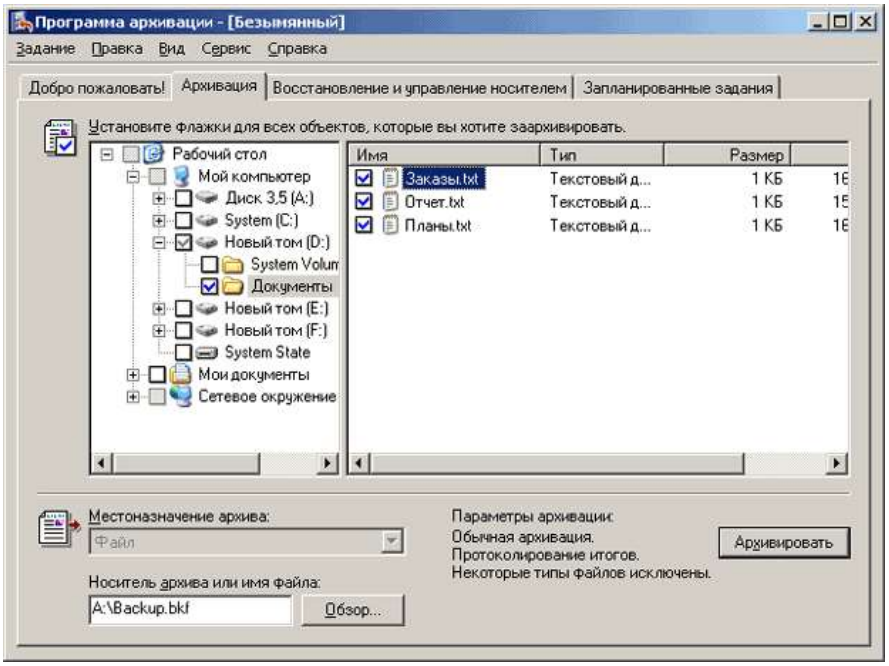
Робота з програмою архівації Backup

Виконувати архівацію всіх даних на комп'ютері майже ніколи не потрібно, так як при виході з ладу жорсткого диска можна досить швидко зробити інсталяцію ОС і основного прикладного ПЗ. Тому слід архівувати лише створювані користувачами файли (документи, бази даних і т. п.) і файли конфігурації додатків. Розумний вибір об'єктів для резервного копіювання заощадить загальний час і ресурси архівації.



Перша сторінка майстра програми архівації Backup

При першому запуску програма архівування Backup ("Пуск" / "Програми" / "Стандартні" / "Службові" / "Архівація даних") запускається в режимі майстра. На цьому занятті робота програми Backup Windows в режимі майстра вивчатися не буде. Натисніть посилання "Розширений режим", а потім перейдіть на вкладку "Архівація" - на екрані відобразиться деревоподібне меню для вибору даних, що архівуються.



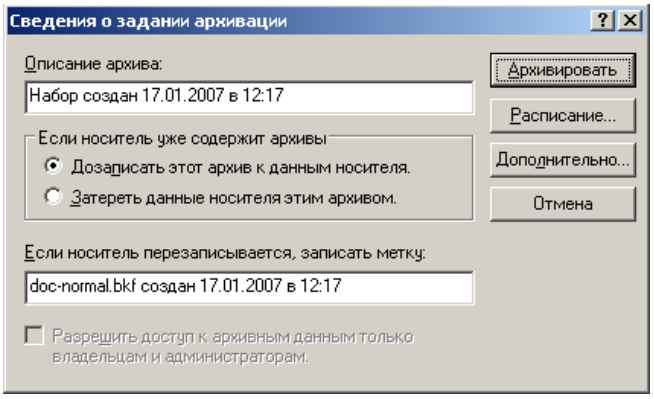
Вкладка "Архівація" у вікні програми Backup Windows

На цій вкладці необхідно вибирати файли і папки, які повинні бути заархівовані. Коли вибирається певна папка (диск), Backup автоматично позначає до архівації всі файли чи папки всередині неї. При цьому прапорець позначки буде синього кольору. Якщо потрібно виключити якісь файли чи папки з уже відзначених, клацніть на пов'язаний з ними прапорець і зніміть позначки про включення. При цьому у батьківської папки прапорець позначки змінить колір з синього на сірий, що означає не стовідсотковий вибір вмісту всередині папки. Використовуючи папку

"Мережеве оточення", можна включити в процес архівації дані з інших комп'ютерів мережі.

Зліва в нижній частині вікна потрібно задати ім'я файла-архіву та вибрати місце його збереження. Файли-архіви, створювані програмою Backup, можуть бути розміщені на будь-яких носіях інформації, таких як жорсткі диски, записувані компакт-диски у форматах CD і DVD, накопичувачі на змінних картриджах (Zip, Jaz) і на магнітній стрічці. При цьому розмір файлу-архіву буде обмежуватися місткістю використовуваного носія. Тому доцільно в мережевій інфраструктурі виділити спеціальний сервер з великим об'ємом дискового простору для зберігання архівів.

Після того як задані носій і ім'я архіву, обрані всі необхідні файли і папки для резервного копіювання, клацніть кнопку "Архівувати" для завдання параметрів архівації та запуску самого процесу.З'явиться вікно "Відомості про завдання архівації".



Вікно "Відомості про завдання архівації" програми Backup Windows

У цьому вікні можна задати опис архіву і мітку носія. Якщо буде обрано варіант "Дозапісать цей архів до даних носія" (за замовчуванням), то значення з текстового поля, де задається мітка носія, не використовується, і вона залишиться колишньою. Це вікно містить кнопки "Архівувати", "Додатково", "Розклад" і "Скасувати". Якщо натиснути кнопку "Архівувати", то запуститься процес архівації. Але до цього можна налаштувати додаткові параметри та розклад архівації, натиснувши відповідні кнопки.

Стратегії архівації

Програма Backup Windows підтримує п'ять стандартних типів архівації, які насправді представляють собою комбінації фільтрів. Для здійснення перших трьох типів архівації використовуються атрибути файлів. Факт зміни файлу визначається по установці атрибуту "архівний" (біт архіву). Під час архівації цей атрибут скидається.

Типи архівації

Нормальний - Всі вибрані файли, незалежно від того, архівувалися чи вони раніше.

Додатковий - Тільки файли, модифіковані з моменту останньої нормальної або додаткової архівації.Різницевий - Тільки файли, модифіковані з моменту останньої нормальної архівації.

Копіює всі вибрані файли.

Щоденний - Тільки файли, створені або модифіковані за поточну добу.

Представлені типи архівації можуть застосовуватися в різних комбінаціях один з одним, визначають стратегії архівації. При виборі стратегії архівації зазвичай враховують два критерії - час, необхідний для архівації та відновлення даних. У багатьох організаціях стратегії архівації розраховані на тижневий цикл.

В ОС Microsoft Windows 2003/XP відновлювати папки і файли з архіву можуть користувачі, що входять до групи адміністраторів або операторів архіву. Програма

Backup Windows дозволяє проводити процедуру відновлення даних двома способами: вручну і з використанням майстра. На даному занятті розглянемо тільки перший спосіб. Налаштувати параметри і запустити процес відновлення можна, перейшовши на вкладку "Відновлення і управління носієм" в головному вікні програми Backup.

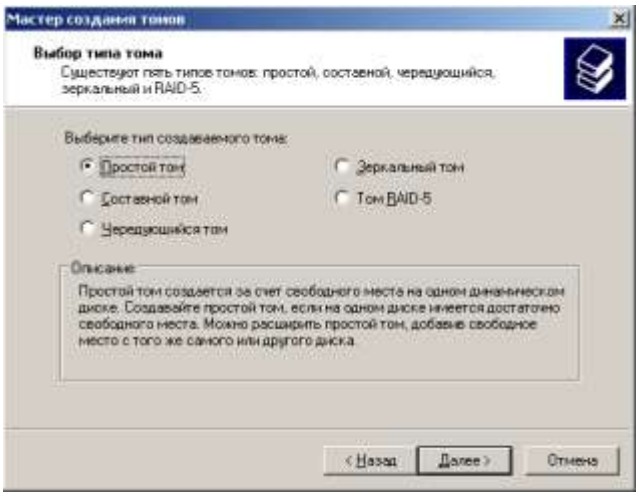
Створення відмовостійких томів для зберігання даних

В ОС Windows Server 2003 можливе створення відмовостійких томів RAID-1 (дзеркальний тому) і RAID-5, які підтримуються тільки на динамічних дисках. За замовчуванням ОС Microsoft Windows 2003/XP використовують традиційне базове зберігання. Для ефективності управління зберіганням даних базові диски перетворять в динамічні, на яких можна створювати різні типи томів.

Робота з дзеркальними томами

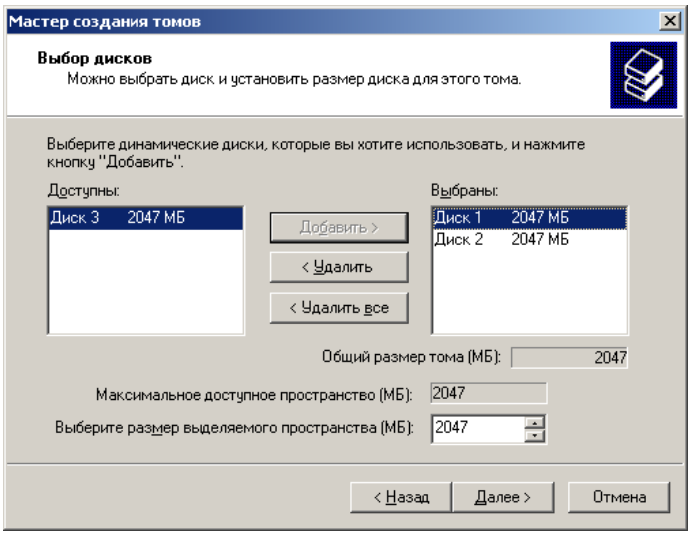
Дзеркальний том (RAID-1) складається з двох однакових копій томи, розташованих на різних фізичних дисках. Дані, записувані на такий тому, записуються одночасно на два диски, тому дзеркальний тому забезпечує відмовостійкість. Для більш високої відмовостійкості рекомендується використовувати диски, підключені до різних контролерам, що забезпечить найкращу продуктивність і дозволить впоратися з відмовами як контролера, так і диска.

В ОС Windows Server 2003 для роботи з дисками існує спеціальне оснащення "Керування дисками", яка входить в консоль "Керування комп'ютером". Для створення дзеркального тому необхідно спочатку з допомогою оснастки "Керування дисками" перетворити тип зберігання з базового в динамічне на двох підключених фізичних дисках. Після цього клацніть на нерозмічену область в графічному представленні диска і в контекстному меню виберіть команду "Дія" / "Усі завдання" / "Створити том". Запуститься майстер створення томів, який запропонує спочатку вибрати тип томи.



Доступні типи томів в ОС Windows Server 2003

Доступні типи томів залежать від числа встановлених на комп'ютері дисків, що містять нерозмічену області. Для створення дзеркального тому, як було сказано вище, необхідно два динамічних диска, мають нерозподілений місце. Коли потрібний тип томи обраний, майстер створення томів відкриє сторінку на якій слід вибрати диски для створення томи.

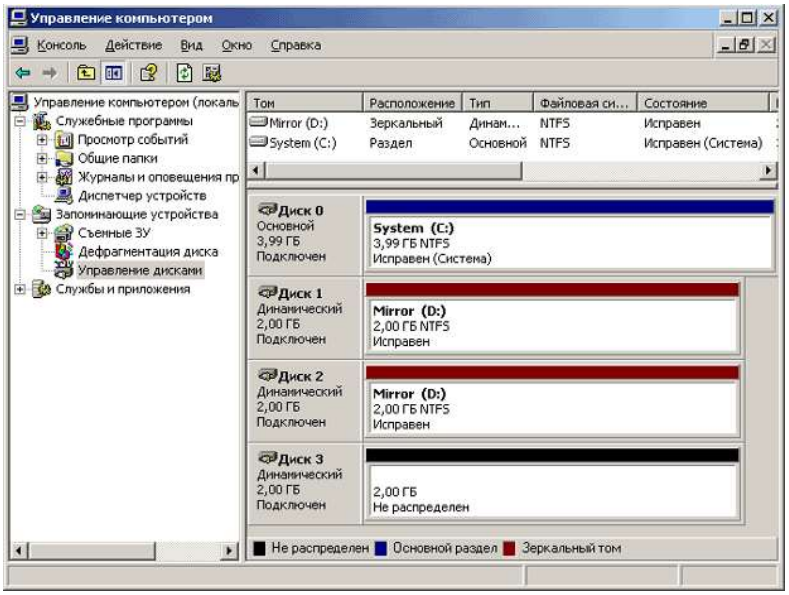


Сторінка вибору дисків для додавання в дзеркальний тому

Вибравши диски для створення томи, слід визначити ще його розмір. Для цього на кожному з дисків необхідно відвести області однакових розмірів. Після вибору дисків для томи вкажіть у полі "Виберіть розмір виділяється простору (Мб)" максимальний розмір області, доступної на кожному з обраних дисків (він обмежений розміром області на диску з мінімальним розміром вільного місця). При зміні розміру відведеного місця на одному з дисків майстер відповідним чином змінить розмір місця, відведеного для нового томи на

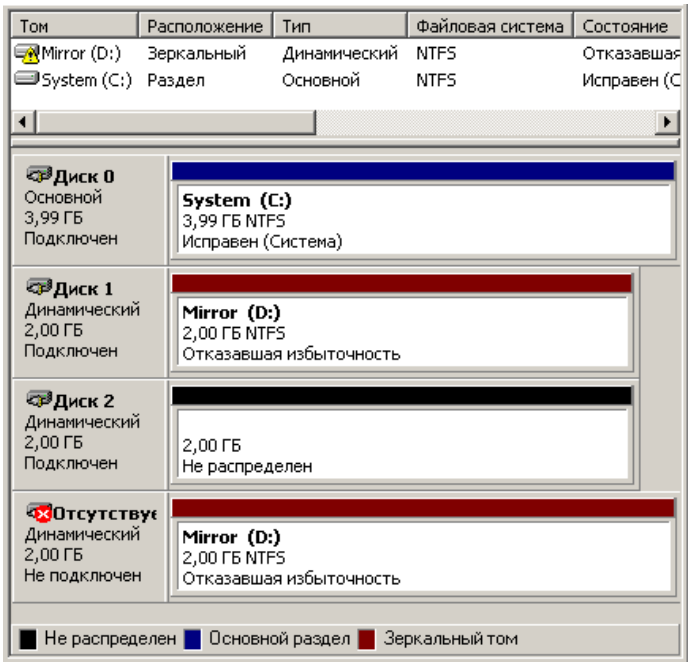
іншому диску. Загальний розмір дзеркального тому дорівнює виділеної області (у Мб), так як

диски даного типу томи містять однакові копії даних. Після завершення роботи майстра створення томів буде створений дзеркальний тому. Для початку експлуатації дзеркального тому потрібно дочекатися закінчення процесів його форматування і ресинхронізації.



Список дисків в оснащенні "Керування дисками"

Процес відновлення несправного диска дзеркального тому залежить від типу несправності. Якщо на диску виникли поодинокі помилки введення-виведення, обидва диска томи перейдуть в стан "відмовився надмірність", диск з помилками знаходиться в стані "Офлайн" або "Відсутній".



Дзеркальний тому в стані "відмовився надмірність"

Усунувши джерело помилок введення-виведення, наприклад, погане з'єднання кабелю, необхідно вибрати те збійному диска або сам диск і в контекстному меню вказати пункт "Реактивізувати том" чи " Реактивізувати диск" відповідно. Повторна

активізація переводить диск або том в оперативний режим. Повторна синхронізація дзеркального тому виконується автоматично.

Видалити дзеркальний тому можна трьома способами:

- Видалити тому повністю з усіма даними.
- Видалити один з дисків дзеркального тому. При цьому на одному з дисків залишається нерозмічена область, а вміст дзеркального тому зберігається на іншому диску.
- Розділити дзеркальний тому. При цьому залишаються два диски з ідентичними копіями даних.

У разі виходу з ладу одного фізичного диска дзеркального тому можна його замінити, а потім перестворювати дзеркальний тому. Для цього слід спочатку розділити дзеркальний тому, потім видалити несправний диск. Другий справний диск стане простим томом. Після заміни несправного диска на сервері клацніть правою кнопкою миші на що залишився простому томі від колишнього "дзеркала" та за допомогою команди "Додати дзеркальний том" створіть новий дзеркальний тому на основі доданого диска.

Робота з томами RAID-5

Том RAID-5 складається як мінімум з трьох дисків (максимум з 32). У порівнянні з дзеркальними томами, він забезпечує кращу продуктивність операції читання даних і ефективність використання дискового простору. У мінімальному томі RAID-5 із трьох дисків, тільки одна третина дискового простору використовується для забезпечення відмовостійкості (для зберігання даних парності), на відміну від дзеркального тому, де цей показник дорівнює одній другій. Відмовостійкість дзеркальних томів і RAID-5 захищає тільки від одиночних збоїв одного диска!

Створюється тому RAID-5 аналогічно дзеркальному через оснастку "Керування дисками", за винятком того, що спочатку потрібно мінімум три вільних диска. При відмові одного з дисків в томі RAID-5 дані все одно будуть доступні. Загальна продуктивність томи знизиться, так як при читанні відсутні дані будуть обчислюватися з решти даних та інформації про парність.

Після відновлення або заміни відмовив диска, можливо, доведеться скористатися командою "Повторити сканування" оснащення "Керування дисками" та реактивувати тому на відновленому диску. При цьому система відновить відсутні дані за значеннями парності і заново заповнить диск, в результаті те відновить функціональність і відмовостійкість.

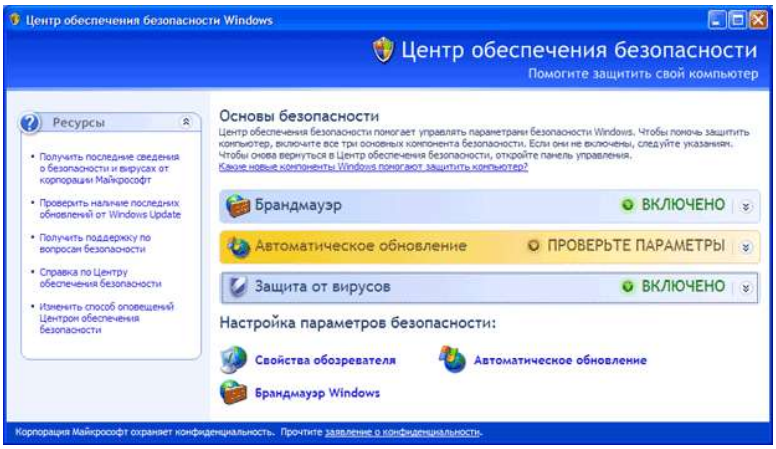
Лекція 4. Центр обеспечения безопасности

У цій лекції буде розглянуто "Центр забезпечення безпеки Windows" (Windows Security Center), що входить до складу Windows XP SP2. Він розроблений компанією Microsoft для автоматичної перевірки стану трьох основних компонентів ОС (брандмауер, антивірус, система автоматичного оновлення). За допомогою цього інструменту користувач має можливість не тільки контролювати стан перерахованих вище компонентів, але і отримувати рекомендації щодо усунення з цими компонентами проблем.

Введення

Якщо ваш комп'ютер підключений до комп'ютерної мережі (неважливо, Інтернет це або Інтранет), то він уразливий для вірусів, атак зловмисників та інших вторгнень. Для захисту комп'ютера від цих небезпек необхідно, щоб на ньому постійно працювали міжмережевий екран (брандмауер) і антивірусне ПЗ (з останніми оновленнями). Крім того, необхідно, щоб всі останні оновлення були також встановлені на вашому комп'ютері.

Не кожний користувач може постійно стежити за цим. Не кожен користувач знає, як це здійснити. І навіть якщо користувач компетентний в цих питаннях, у нього просто може не вистачати часу на такі перевірки. Компанія Microsoft подбала про всіх цих користувачів, включивши до складу SP2 для Windows XP такий інструмент. Він називається "Центр забезпечення безпеки Windows" (Windows Security Center).



Центр забезпечення безпеки Windows

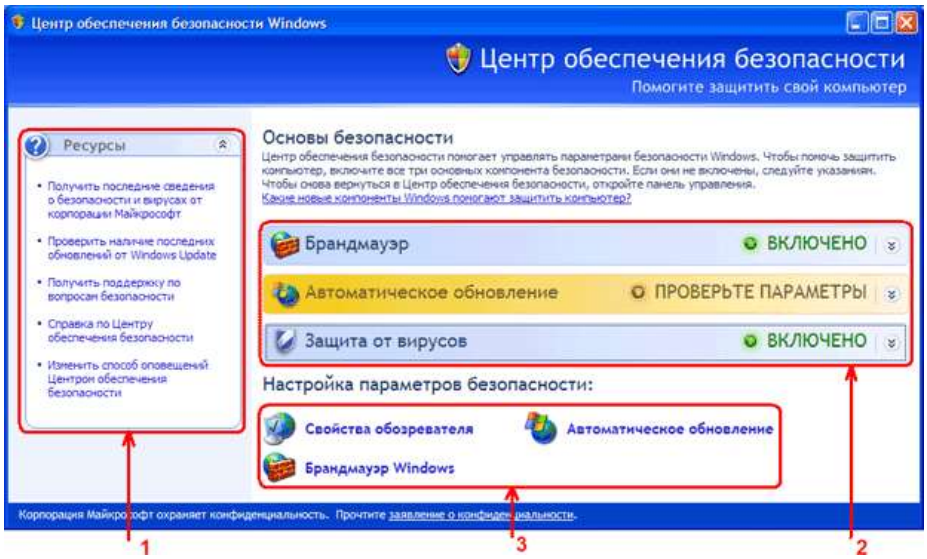
Основне призначення цього інструменту - інформувати і направляти користувача в потрібному напрямку. По-перше, він постійно контролює стану трьох основних компонентів ОС (брандмауер, антивірус, система автоматичного оновлення). Якщо параметри будь-якого з цих компонентів не будуть задовольняти вимогам безпеки комп'ютера, то користувач отримає відповідне повідомлення.

По-друге, при відкритті "Центру безпеки Windows" користувач може не тільки отримати конкретні рекомендації про те, як виправити ситуацію, що склалася, але також дізнатися, де знаходяться інші параметри, пов'язані з безпекою комп'ютера, і де на сайті Microsoft можна прочитати додаткову інформацію по забезпеченню безпеки.

Необхідно відразу зазначити, що при підключенні комп'ютера до домену в "Центрі забезпечення безпеки Windows" не відображаються відомості про стан безпеки комп'ютера і не виконується відправлення повідомлень безпеки. Вважається, що в цьому випадку параметрами безпеки повинен управляти адміністратор домену. Щоб включити "Центр для забезпечення безпеки Windows" для комп'ютера, що входить до складу домену, необхідно в груповій політиці домену включити параметр "Конфігурація комп'ютера, Адміністративні шаблони, Компоненти Windows, Центр забезпечення безпеки, Включити" Центр забезпечення безпеки "(тільки для комп'ютерів в домені) ".

Параметри безпеки Windows

Щоб відкрити "Центр забезпечення безпеки Windows", натисніть кнопку "Пуск", виберіть команду "Панель управління", потім двічі клацніть на значок "Центр забезпечення безпеки".



Вікно Центру безпеки Windows можна умовно розділити на три частини:

Центр забезпечення безпеки

1. Ресурси. Тут розташовуються посилання для переходу до Інтернет-ресурсів, до вбудованої в Windows довідковій службі і до вікна налаштування параметрів оповіщень.

2. Компоненти безпеки. Тут розташовуються інформаційні елементи трьох основних компонентів безпеки: брандмауер, автоматичне оновлення, антивірусний захист.

3. Параметри безпеки. Тут розташовуються кнопки переходу до налаштувань безпеки наступних компонентів: браузер Internet Explorer, автоматичне оновлення, брандмауер Windows.

Розглянемо ці частини більш докладно. Ресурси

У розділі 1 перші три посилання призначені для переходу на відповідні сторінки на сайті Microsoft. Передостання посилання призначена для відкриття довідкової служби Windows на сторінці "Загальні відомості про центр забезпечення безпеки Windows". Остання посилання призначена для відкриття вікна "Параметри оповіщень".

Якщо на комп'ютері встановлений брандмауер і антивірусне ПЗ, не визначуване Центром забезпечення безпеки, ви можете відключити відповідні оповіщення.

Компоненти безпеки

У розділі 2 кожне інформаційне табло повідомляє про стан відповідного

A	ВКЛЮЧЕНО
B	ПРОВЕРЬТЕ ПАРАМЕТРЫ
C	ВЫКЛЮЧЕНО
D	НЕ НАЙДЕНО
E	СРОК ИСТЕК
F	НЕ НАБЛЮДАЕТСЯ

компонента.

Стани A C зрозумілі без коментарів. Стан D - "Не знайдено" - відповідає неможливості визначити присутність відповідного ПЗ (наприклад, антивірус або брандмауер). Стан E - "Термін закінчився" - можливо для антивірусного захисту, коли оновлення антивірусних баз застаріли. Стан F - "Не спостерігається" - відповідає відключеному контролю над відповідним компонентом.

Центром забезпечення безпеки застосовується дворівневий підхід до визначення стану компонентів:

1. Перевірка вмісту реєстру і файлів з відомостями про стан ПО (Microsoft отримує перелік файлів і параметрів реєстру від виробників ПО).

2. Відомості про стан ПО передаються від встановлених програм засобами інструментарію WMI (Windows Management Instrumentation - Інструментарій управління Windows).

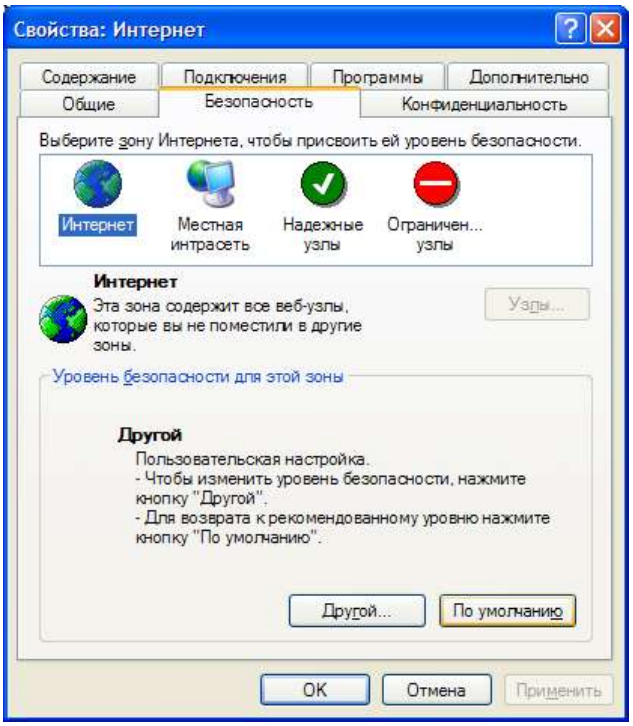
Параметри безпеки

Як вже було зазначено раніше, в розділі 3 розташовані кнопки переходу до налаштувань безпеки наступних компонентів: браузер Internet Explorer, автоматичне оновлення, брандмауер Windows.

У Windows XP SP2 для позначення налаштувань, що стосуються безпеки, а також при оповіщенні про стан безпеки комп'ютера використовуються такі індикатори:

1. - Означає важливі відомості та параметри безпеки.
2. - Попереджає про потенційний ризик порушення безпеки.
3. - Ситуація більш безпечна. На комп'ютері використовуються рекомендовані настройки безпеки.
4. - Попередження: ситуація потенційно небезпечна. Змініть налаштування параметрів безпеки, щоб підвищити безпеку комп'ютера.
5. - Використовувати поточні настройки параметрів безпеки не рекомендується. Властивості оглядача

Як вже зазначалося раніше, натиснувши кнопку в "Центрі забезпечення безпеки Windows", ви потрапите у вікно налаштувань браузера Internet Explorer на закладку "Безпека".

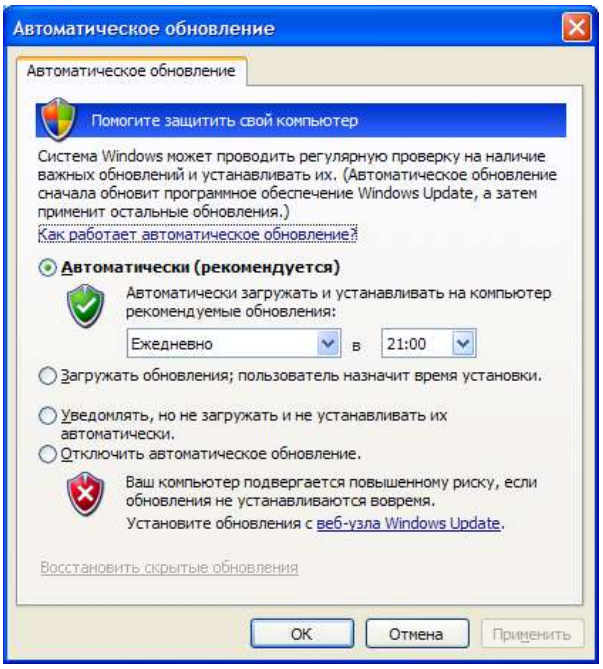


Налаштування безпеки Internet Explorer

Розглянемо параметри, доступні на цій закладці. У верхній частині розташовані чотири зони: Інтернет, Місцева інтрамережа, Надійні вузли, Обмежені вузли.

Автоматичне оновлення

Як вже зазначалося раніше, натиснувши кнопку в "Центрі забезпечення безпеки Windows", вивідкриєте вікно налаштувань "Автоматичного оновлення".



Параметри автоматичного оновлення

Вбудована в Windows XP довідкова система дуже докладно описує систему автоматичного оновлення. Для того щоб скористатися цією довідкою, клацніть по напису "Як працює автоматичне оновлення?". Зупинимося лише на деяких моментах.

По-перше, необхідно розрізняти поняття "завантаження" і "установка" оновлень. Завантаження означає процес передачі файлів оновлень з сервера Microsoft (або з внутрішнього сервера оновлень в організації) на комп'ютер користувача. Установка позначає власне процес інсталяції оновлень на комп'ютері користувача. Можлива ситуація, коли оновлення завантажені на комп'ютер користувача, але ще не встановлені.

По-друге, якщо ви вибрали варіант "Автоматично", то оновлення будуть завантажуватися і встановлюватися у вказаний вами час. Якщо комп'ютер у вказаний час завжди вимкнений, то установка оновлень ніколи не виконається. При реєстрації на комп'ютері користувач з правами локального адміністратора може запустити установку вручну, не чекаючи запланованого часу. При настанні запланованого часу користувачеві буде видане відповідне попередження про початок встановлення оновлень. Якщо в цей момент у системі працює адміністратор, у нього буде можливість відкласти установку до наступного запланованого часу. У інших користувачів (без прав адміністратора) можливості скасувати заплановану установку оновлень не буде.

У всіх інших випадках (крім варіанту "відключити автоматичне оновлення") повідомлення про існуючі оновленнях для вашого комп'ютера (готових до завантаження чи до установки) будуть з'являтися тільки при реєстрації на вашому комп'ютері користувача з правами локального адміністратора. Таким чином, якщо на комп'ютері ви постійно працюєте з обліковим записом, що не входить у групу локальних адміністраторів, то установка оновлень ніколи не виконається.

Описані вище настройки автоматичного оновлення також доступні для налаштування через групову політику (Конфігурація комп'ютера, Адміністративні шаблони, Компоненти Windows, Windows Update). Крім того, тільки через групову політику можна задати додаткові параметри. Наприклад, можна вказати адресу внутрішнього сервера оновлень, який централізовано отримує оновлення з серверів Microsoft і віддає їх внутрішнім комп'ютерам організації. Як приклад такого сервера можна привести Microsoft ® Windows Server
™ Update Services (WSUS).

Брандмауер Windows

Як вже зазначалося раніше, натиснувши кнопку в "Центрі забезпечення безпеки Windows", ви відкриєте вікно налаштувань "Брандмауер Windows".

Рис. 4.23. Налаштування брандмауера Windows

Якщо ви клацніть по напису "Детальніше про брандмауер Windows", то зможете прочитати коротку інформацію про можливості брандмауера (міжмережевого екрану), що входить до складу Windows XP SP2. Немає необхідності повторювати цю інформацію тут.

Відзначимо лише, що, на відміну від продуктів інших виробників, вбудований брандмауер Windows призначений тільки для контролю вхідного трафіку, тобто він захищає комп'ютер тільки від зовнішніх вторгнень. Він не контролює вихідний трафік вашого комп'ютера. Таким чином, якщо на ваш комп'ютер вже потрапив троянський кінь або вірус, які самі встановлюють з'єднання з іншими комп'ютерами, брандмауер Windows не буде блокувати їх мережеву активність.

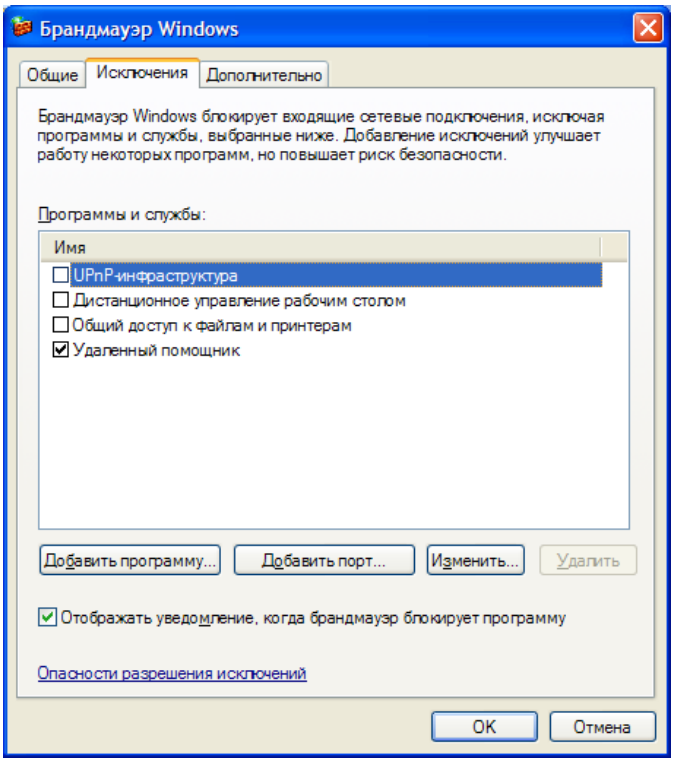
Крім того, за замовчуванням брандмауер захищає всі мережеві з'єднання, і запит входить луни по протоколу ICMP заборонений. Це означає, що якщо на комп'ютері включений брандмауер Windows, то перевіряти наявність такого комп'ютера в мережі за допомогою команди PING - безглузде заняття.

Дуже часто в організаціях, де використовується програмне забезпечення, що вимагає дозволу вхідних з'єднань на комп'ютери користувачів, виникає необхідність відкрити деякі порти на комп'ютерах з встановленою Windows XP SP2. Для вирішення цього завдання необхідно задати виключення в настройках брандмауера Windows. Існує два способи вирішити цю задачу:

1. Можна задати виключення, вказавши програму, що вимагає вхідні з'єднання. У цьому випадку брандмауер сам визначить, які порти необхідно відкрити, і відкриє їх тільки на час виконання зазначеної програми (точніше, на час, коли програма буде прослуховувати цей порт).

2. Можна задати виключення, вказавши конкретний порт, по якому програма очікує вхідні з'єднання. У цьому випадку порт буде відкритий завжди, навіть коли ця програма не буде запущена. З точки зору безпеки цей варіант менш кращий.

Існує декілька способів задати виключення в настройках брандмауера Windows. Можна скористатися графічним інтерфейсом. Цей варіант досить докладно висвітлений в Центрі довідки й підтримки Windows XP SP2. Можна використовувати доменну групову політику. Цей варіант кращий при великій кількості комп'ютерів в організації. Розглянемо його детальніше.



Закладка Винятки

Параметри брандмауера Windows у груповій політиці розміщуються у вузлі "Конфігурація комп'ютера, Адміністративні шаблони, Мережа, Мережеві підключення, Брандмауер Windows".

При налаштуванні через групову політику вам необхідно налаштувати два профілі:

1. Профіль домену. Налаштування цього профілю використовуються, коли комп'ютер підключений до мережі, що містить контролер домену організації.

2. Стандартний профіль. Налаштування цього профілю застосовуються, коли комп'ютер не підключений до мережі, що містить контролер домену організації. Наприклад, якщо ноутбук організації використовується у відрядженні і приєднаний до Інтернету через Інтернет-провайдера. У цьому випадку настройки брандмауера повинні бути більш суворими у порівнянні з настройками доменного профілю, так як комп'ютер підключається до публічної мережі, минаючи міжмережеві екрани своєї організації.

Розглянемо, як задати виключення для програми і для заданого порту. В якості конкретного прикладу візьмемо звернення Сервера адміністрування Kaspersky Administration Kit до комп'ютера, на якому встановлений Агент адміністрування, для отримання інформації про стан антивірусного захисту.

Створення виключення для програми

Налаштуємо параметри групової політики так, щоб брандмауер завжди працював, але пропускав вхідні з'єднання для програми "C: \ Program Files \ Kaspersky Lab \ NetworkAgent \ klnagent.exe". Вкажемо також, що ця програма буде приймати вхідні з'єднання тільки з адреси 192.168.0.1.

Для цього необхідно змінити параметри, розташовані у вузлі "Конфігурація комп'ютера, Адміністративні шаблони, Мережа, Мережеві підключення, Брандмауер Windows, Профіль домену". Параметри, не зазначені в цій таблиці, можуть мати стан "Не задана".

Параметри групової політики

Брандмауер Windows: Захистити всі мережеві підключення Включена Брандмауер Windows: Не дозволяти винятки Відключена

Брандмауер Windows: Поставити виключення для програм Включена. % Programfiles% \ Kaspersky Lab \ NetworkAgent \ klnagent.exe: 192.168.0.1: enabled: KasperskyAgent

Формат завдання винятку для програм наступний:

ProgramPath: Scope: Enabled | Disabled:

ApplicationName де ProgramPath - шлях до програми та ім'я файлу,

Scope - один або декілька адрес, розділених комами (наприклад, "*" - всі мережі (лапки не вказуються); 192.168.0.1 - одна адреса; 192.168.10.0/24 - підмережа; "localsubnet" - локальна підмережа),

Enabled | Disabled - стан винятку

(увімкнене), ApplicationName - опис виключення (текстовий рядок).

Створення винятків для портів

Налаштуємо параметри групової політики так, щоб брандмауер завжди працював, але пропускав вхідні з'єднання з адреси 192.168.0.1 на порт UDP 15000.

Для цього необхідно змінити параметри, розташовані у вузлі "Конфігурація комп'ютера, Адміністративні шаблони, Мережа, Мережеві підключення, Брандмауер Windows, Профіль домену". Параметри, не зазначені в цій таблиці, можуть мати стан "Не задана".

Параметри групової політики

Брандмауер Windows: Захистити всі мережеві підключення Включена Брандмауер Windows: Не дозволяти винятки Відключена

Брандмауер Windows: Поставити виключення для портів Включена. 15000: UDP: 192.168.0.1: enabled:Kaspersky Agent Port

Формат завдання винятку для програм наступний [[28]]:Port #: TCP | UDP: Scope: Enabled | Disabled: PortName де Port #-номер відкривається порту,

TCP | UDP - тип порту,

Scope - один або декілька адрес, розділених комами (наприклад, "*" - всі мережі (лапки не вказуються); 192.168.0.1 - одна адреса; 192.168.10.0/24 - підмережа; "localsubnet" - локальна підмережа),

Enabled | Disabled - стан винятку (увімкнене), PortName - опис виключення (текстовий рядок).

Резюме

"Центр забезпечення безпеки Windows" є прекрасним прикладом дружнього інтерфейсу для контролю функціонування таких важливих для безпеки комп'ютера компонентів, як "брандмауер", "система автоматичного оновлення" і антивірусне ПЗ. Він інформує користувача про стан цих компонентів і рекомендує користувачам, як виконати їх правильну настройку.

При підключенні комп'ютера до домену "Центр забезпечення безпеки Windows" перестає повідомляти користувача про проблеми з безпекою Windows. Вважається, що в цьому випадку параметрами безпеки повинен управляти адміністратор домену - наприклад, через групову політику.

Лекція 5. Системи аналізу захищеності мережі

Від ефективності захисту операційних систем безпосередньо залежить рівень безпеки мережевої інфраструктури організації в цілому. Системи аналізу захищеності здатні виявляти уразливості в мережевій інфраструктурі, аналізувати і видавати рекомендації щодо їх усунення, а також створювати різного роду звіти. У даній лекції ми познайомимося з такими програмними засобами для аналізу захищеності ОС, як Microsoft Baseline Security Analyzer і сканер безпеки XSpider 7.0

Одними з головних елементів інформаційної безпеки мережевої інфраструктури є операційні системи комп'ютерів, так як в них акумулюється переважна частина використовуваних механізмів захисту: засоби розмежування доступу до ресурсів, аутентифікація користувачів, аудит подій та ін Від ефективності захисту операційних систем безпосередньо залежить рівень безпеки мережевої інфраструктури організації в цілому.

На цьому занятті будуть розглянуті програмні засоби для аналізу захищеності операційних системMicrosoft, такі як:

- Microsoft Baseline Security Analyzer (MBSA);
- Сканер безпеки XSpider 7.0 (виробник ТОВ "Позитив Технолоджиз", Росія).

Принципи роботи систем аналізу захищеності

Для розуміння принципів роботи систем аналізу захищеності необхідно позначити деякі терміни та визначення. Ключове поняття даного заняття - це "вразливість". Під вразливістю захисту ОС розуміється така її властивість (недолік), яке може бути використане зловмисником для здійснення несанкціонованого доступу (НСД) до інформації. Системи аналізу захищеності здатні виявляти уразливості в мережевій інфраструктурі, аналізувати і видавати рекомендації щодо їх усунення, а також створювати різного роду звіти. До типових вразливостям можна віднести:

- відсутність оновлень системи безпеки ОС;
- неправильні налаштування систем безпеки ОС;
- невідповідні паролі;
- сприйнятливість до проникнення із зовнішніх систем;
- програмні закладки;
- неправильні настройки системного і прикладного ПЗ, встановленого на ОС.

Більшість систем аналізу захищеності (XSpider, Internet Scanner, LanGuard, Nessus) виявляють уразливості не тільки в операційних системах, але і в найбільш поширеному прикладному ПЗ. Існують два основні підходи, за допомогою яких системи аналізу захищеності виявляють уразливості: сканування і зондування. Через першого підходу системи аналізу захищеності ще називають "сканерами безпеки" або просто "сканерами".

При скануванні система аналізу захищеності намагається визначити наявність уразливості за непрямими ознаками, тобто без фактичного підтвердження її наявності - це пасивний аналіз. Даний підхід є найбільш швидким і простим у реалізації. При зондуванні система аналізу захищеності імітує ту атаку, яка використовує перевіряється уразливість, тобто відбувається активний аналіз. Даний підхід повільніше сканування, але дозволяє переконатися, присутній чи ні на аналізованому комп'ютері уразливість.

На практиці ці два підходи реалізуються в сканерах безпеки через такі методи перевірки [[48]]:

1. Перевірка заголовків (Banner check);
2. Активні зондувальні перевірки (Active probing check);
3. Імітація атак (Exploit check).

Перший метод заснований на підході "сканування" і дозволяє робити висновок про вразливості,спираючись на інформацію в заголовку відповіді на запит сканера безпеки. Прикладом такої перевірки може

бути аналіз заголовків поштової програми Sendmail, в результаті якого можна дізнатися її версію і зробити висновок про наявність в ній уразливості.

Активні зондувальні перевірки також засновані на підході "сканування". Даний метод порівнює фрагменти сканованого програмного забезпечення з сигнатурою відомої вразливості, що зберігається в базі даних системи аналізу захищеності. Різновидами цього методу є, наприклад, перевірки контрольних сум або дати сканованого програмного забезпечення.

Метод імітації атак заснований на використанні різних дефектів у програмному забезпеченні та реалізує підхід зондування. Існують уразливості, які не можуть бути виявлені без блокування чи порушення функціонування сервісів операційної системи в процесі сканування. При скануванні критичних серверів корпоративної мережі небажано застосування даного методу, оскільки він може вивести їх з ладу - і в такому випадку сканер безпеки успішно реалізує атаку "Denial of service" (відмова в обслуговуванні). Тому в більшості систем аналізу захищеності за замовчуванням такі перевірки, засновані на імітації атак, вимкнені. При їх включенні в процес сканування зазвичай видається попереджувальне повідомлення.

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) - вільно поширюване засіб аналізу захищеності операційних систем Windows і ряду програмних продуктів компанії Microsoft (Internet Information Services, SQL Server, Internet Explorer та ін.) Термін "Baseline" в назві MBSA слід розуміти як деякий еталонний рівень, при якому безпека ОС можна вважати задовільною. MBSA дозволяє сканувати комп'ютери під управлінням операційних систем Windows на предмет виявлення основних вразливостей і наявності рекомендованих до установки оновлень системи безпеки. Критично важливо знати, які оновлення встановлені, а які ще слід встановити на вашій ОС. MBSA забезпечує подібну перевірку, звертаючись до постійно поповнюється Microsoft базі даних у форматі XML, яка містить інформацію про оновлення, випущених для кожного з програмних продуктів Microsoft. Працювати з програмою MBSA можна через графічний інтерфейс і командний рядок. На даному занятті буде розглянуто тільки перший варіант роботи.

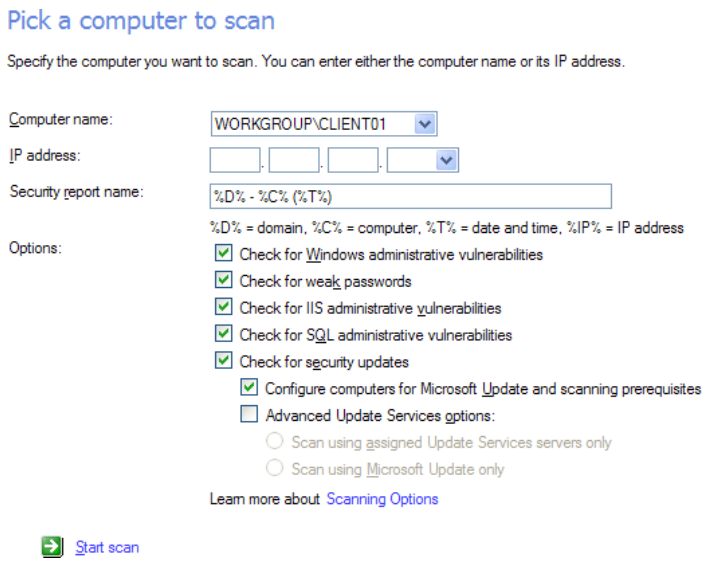
Інтерфейс MBSA виконаний на основі браузера Internet Explorer. Головне вікно програми розбито на дві області. Так як сеанс роботи з MBSA налаштовується за допомогою майстра, то в лівій області представлені кроки майстра, а в правій - основне вікно з описом дій кожного кроку.

Головне вікно програми Microsoft Baseline Security Analyzer 2.0На першому кроці "Welcome" необхідно вибрати одну з дій:

- Сканувати даний комп'ютер (Scan a computer);
- Сканувати декілька комп'ютерів (Scan more than one computer);
- Переглянути існуючі звіти, зроблені MBSA раніше (View existing security reports).

При першому запуску MBSA необхідно вибрати перший або другий варіант. На наступному кроці майстра в основному вікні потрібно задати параметри сканування комп'ютера(ів) підуправлінням ОС Windows (рис. 6.3). Можна ввести ім'я або IP-адресу сканованого комп'ютера (за умовчаннямвибирається комп'ютер, на якому був запущений MBSA).

Користувач, що запустив MBSA, повинен мати права адміністратора даного комп'ютера або входити до групи адміністраторів системи. У разі сканування декількох комп'ютерів користувач повинен мати права адміністратора на кожному з комп'ютерів, а краще - правами адміністратора домену.



Вибір комп'ютера і параметрів сканування в програмі MBSA 2.0

Вибравши комп'ютер (и) для сканування, необхідно задати параметри сканування:

- перевірка ОС Windows;
- перевірка паролів;
- перевірка служб IIS;
- перевірка сервера SQL;
- перевірка встановлених оновлень безпеки.

Більш детальну інформацію про перевірки MBSA можна отримати на офіційному сайті Microsoft. Наприклад, коли задана опція "перевірка паролів", MBSA перевіряє на комп'ютері облікові записи локальних користувачів, які використовують порожні або прості паролі (ця перевірка не виконується на серверах, які виступають в ролі контролерів домену) з наступних комбінацій:

- пароль порожній;
- пароль збігається з ім'ям облікового запису користувача;
- пароль збігається з ім'ям комп'ютера;
- паролем служить слово "password";
- паролем слугують слова "admin" або "administrator".

Дана перевірка також виводить повідомлення про заблокованих облікових

записах.

Після того як всі опції будуть задані, необхідно натиснути на посилання внизу "Start scan". При першому скануванні MBSA необхідне підключення до Інтернету, щоб завантажити з сайту Microsoft Download Center (http://www.microsoft.com/downloads) XML-файл, що містить поточну довідкову базу вразливостей. MBSA спочатку викачує цей файл у архівувати cab-файлі, потім, перевіривши його підпис, розархівуйте його на комп'ютер, з якого буде запускатися.

Можлива також робота MBSA без підключення до Інтернету в автономному режимі. Для цього потрібно завантажити вище описаний файл і розмістити у відповідному каталозі.

Після того як cab-файл буде розархівувати, MBSA почне сканувати заданий комп'ютер (и) на предмет визначення операційної системи, наборів оновлень і використовуваних програм. Потім MBSA аналізує XML- файл і визначає оновлення системи безпеки, які доступні для встановленого ПЗ. Для того щоб MBSA

визначив, яке оновлення встановлено на сканованого комп'ютері, йому необхідно знати три пункти: ключ реєстру, версію файлу і контрольну суму для кожного файлу, встановленого з оновленням.

У разі якщо будь-які дані на сканованого комп'ютері не співпадуть з відповідними пунктами в XML- файлі, MBSA визначить відповідне оновлення як відсутнє, що буде відображено в підсумковому звіті.

Після сканування єдиного комп'ютера MBSA автоматично запустить вікно "View security report" і відобразить результати сканування. Якщо було виконано сканування декількох комп'ютерів, то слід вибрати режим "Pick a security report to view", щоб побачити результати сканування. Створюваний MBSA звіт розбивається на п'ять секцій:

- Security Update Scan Results,
- Windows Scan Results,
- Internet Information Services (IIS) Scan Results,
- SQL Server Scan Results,
- Desktop Application Scan Results.

Деякі секції розбиваються ще на розділи, присвячені певним проблемам безпеки комп'ютера, і надають системну інформацію по кожній з перевірок, зазначених в таблиці 6.1. Опис кожної перевірки операційної системи відображається у звіті разом з інструкцією по усуненню виявлених вразливостей.

Опис перевірок, виконуваних MBSA

Server	Administrators Виводить список облікових записів локальних адміністраторів комп'ютера Auditing Виводить налаштування аудиту на локальному комп'ютері
	Autologon Перевіряє, чи увімкнено функцію Autologon
	Domain Controller Test Перевіряє, не запущена служба IIS на контролері домену (DC)
	Exchange Server Security Updates Перевіряє пропущені виправлення для системи безпеки Exchange
	File System Перевіряє тип файлової системи (наприклад, NTFS) Guest Account Перевіряє, не активована обліковий запис Guest IE Zones Виводить зони безпеки IE для кожного користувача
	IIS Admin Virtual Directory Переглядає віртуальний каталог
	IISADMPWD IIS Lockdown Tool Перевіряє, чи проведено процедура захисту IIS Lockdown
	IIS Logging Enabled Видає рекомендації по Журналювання

с в HTTP і FTP IIS Security Updates Перевіряє пропущені
а виправлення для системи безпеки IIS
й Local Account Password Test Перевіряє наявність порожніх або слабких
т паролів для локальних
і
облікових записів

Macro Security Виводить установки для макросів Office по користувачам

Msadc and Scripts Virtual Directories Переглядає віртуальний каталог MSADC і ScriptsOutlook Zones Виводить зони безпеки Outlook для кожного користувача

Parent Paths Виводить інформацію про наявність посилань на каталоги верхнього рівня від Web-вузлів або віртуальних каталогів

Password Expiration Виводить облікові записи з необмеженим терміном дії паролів, не перераховані вNoExpireOk.txt

Restrict Anonymous Виводить налаштування реєстру, що забороняють анонімним користувачамперегляд списку облікових записів

Sample Applications Виводить встановлені приклади додатків для IIS (наприклад, Default Web Site, IISHelp)

Services Виводить список несуттєвих служб (наприклад, FTP, SMTP, Telnet, WWW), які можуть послабити безпеку

Shares Перевіряє і виводить список загальних ресурсів, а також їх списки ACL

SQL Server Security Updates Перевіряє пропущені виправлення для системи безпеки SQL ServerSQL: CmdExec role Перевіряє обмеження на запуск CmdExec тільки для SysAdmin

SQL: Domain Controller Test Перевіряє, не запущений Чи SQL Server на DC

SQL: Exposed SQL Password Перевіряє, не присутсвует чи пароль адміністратора (SA) у текствомфайлі (наприклад, setup.iss або sqlstp.log)

SQL: Folder Permissions Перевіряє дозволу файлів в каталозі установки SQL ServerSQL: Guest Account Виводить бази даних з активною обліковим записом гостя SQL: Registry Permissions Перевіряє дозволу реєстру на розділи SQL Server

SQL: Service Accounts Перевіряє членство в групах облікових записів SQL Server і SQL Server agent SQL: SQL Account Password Test Перевіряє на порожні або слабкі паролі локальних облікових записів SQL

SQL: SQL Server Security Mode Перевіряє, запущений SQL Server в режимі Windows Only або MixedSQL: SysAdmin Role Members Виводить членів ролі SysAdmin

SQL: SysAdmins Виводить кількість SysAdmins

Windows Media Player Security Updates Перевіряє пропущені виправлення для системи безпеки WMPWindows Security Updates Перевіряє пропущені виправлення для системи безпеки Windows

Windows Version Виводить версію Windows

Сканер безпеки XSpider

Останнім часом в Росії все більшої популярності серед фахівців із захисту інформації набирає сканер безпеки XSpider версії 7.0, що випускається вітчизняною компанією Positive Technologies.

Є ряд особливостей, які дають переваги сканеру XSpider як системі аналізу захищеності над іншими продуктами даного класу. Як підкреслюють самі розробники, головна особливість XSpider 7 - це його скануючий ядро, яке здатне імітувати сценарій поведінки потенційного зловмисника. Також слід відзначити потужну "інтелектуальну начинку" XSpider 7, яка реалізується у вбудованих евристичних алгоритмах, що дозволяють надійно ідентифікувати ще не опубліковані нові уразливості.

Надійні та вичерпні перевірки XSpider 7 базуються, зокрема, на наступних інтелектуальних підходах:

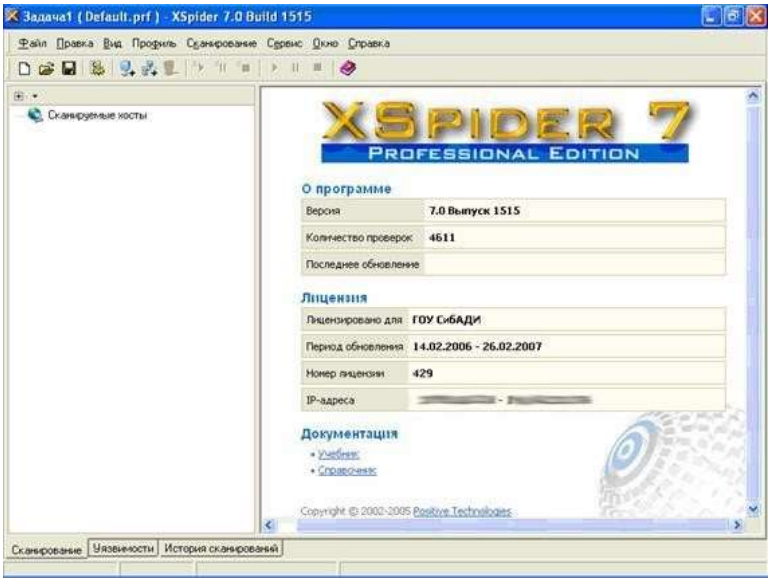
- повна ідентифікація сервісів на випадкових портах;
- евристичний метод визначення типів та імен серверів (HTTP, FTP, SMTP, POP3, DNS, SSH)незалежно від їх відповіді на стандартні запити;
- обробка RPC-сервісів з їх повною ідентифікацією;
- проведення перевірок на нестандартні DoS-атаки.

З моменту виходу першої версії сканера XSpider пройшло вже більше 6 років. Версія 7.0, з якою ми познайомимося на цьому занятті, є комерційною на відміну від попередніх вільно розповсюджуваних версій (6.5 і раніше). У компанії Positive

Technologies існує гнучка система ліцензування сканера XSider 7. Вартість ліцензії залежить від кількості IP-адрес, кількості робочих місць, з яких проводиться сканування, і терміну дії підписки на оновлення. Більш детальну інформацію щодо придбання продукту можна отримати на сторінці компанії: http://www.ptsecurity.ru/xs7rates.asp.

Для вивчення можливостей сканера XSider 7 достатньо придбати версію XSpider 7 Professional Edition з числом сканируемих IP-адрес від 4 до 16. Встановлюється XSpider 7 на яку операційну систему Microsoft Windows в режимі майстра.

При запуску XSpider 7 на екран буде виведено головне вікно програми (рис. 6.4), в якому відобразиться інформація про поточну версію сканера і ліцензії.



Головне вікно сканера XSpider 7.0, що з'являється при його запуску

У нижній частині головного вікна, в розділі "Документація" є посилання на вбудовані підручник і довідник по продукту XSpider. Дані розділи документації теж можна віднести до важливих переваг XSpider. По-перше, підручник і довідник написані російською мовою, що є далеко не у всіх подібних системах. По- друге, автор підручника - директор з розвитку Positive Technologies Євген Кірєєв - виклав досить цікаво і зрозуміло весь матеріал, з розрахунком на звичайних користувачів-непрофесіоналів в області інформаційної безпеки.

Далі, щоб не дублювати вміст вбудованого підручника, будуть викладені основні концепції, на яких базується організація роботи сканера безпеки XSpider 7.

XSpider 7 має багатовіконний інтерфейс. Важливо відзначити, що кожне вікно служить інтерфейсом певної задачі XSpider. Поняття "задача" є центральною концепцією сканера безпеки XSpider 7, вона дозволяє організувати і систематизувати процес сканування мережі. Будь сканування хостів завжди відбувається в рамках певної задачі, навіть якщо для цього нічого спеціально не робилося: при первісному запуску XSpider завжди створюється порожня завдання.

Будь-яка задача в XSpider визначається наступними атрибутами:

- список перевіряються хостів (в задачу об'єднують хости, які планується перевіряти схожим чином);
- журнал історій сканувань даної задачі;
- профіль сканування.

Завдання може бути збережена у вигляді файлу (за замовчуванням каталог Program Files \ Positive Technologies \ XSpider 7.0 \ Tasks), і перші два атрибути - список хостів і журнал історії сканувань - будуть записані в її структуру даних.

Профіль сканування - це ще одна концепція сканера XSpider, що представляє набір налаштувань, які визначають параметри сканування хостів. Профіль можна призначити завданню, як тільки вона сформована. Якщо цього не зробити, то буде використовуватися профіль за замовчуванням (Default - Стандартний). Після

установки сканера безпеки XSpider 7 користувачеві доступні 14 базових профілів.

Резюме

Від ефективності захисту операційних систем безпосередньо залежить рівень безпеки мережевої інфраструктури організації в цілому. В процесі експлуатації операційних систем виявляються уразливості їх захисту, які потенційно можуть бути використані зловмисниками для здійснення несанкціонованого доступу (НСД) до інформації. Системи аналізу захищеності здатні

виявляти уразливості в мережевій інфраструктурі, аналізувати і видавати рекомендації щодо їх усунення, а також створювати різного роду звіти.

Microsoft Baseline Security Analyzer (MBSA) - вільно поширюване засіб аналізу захищеності операційних систем Windows і ряду програмних продуктів компанії Microsoft. MBSA дозволяє виявити основні вразливості та перевіряє наявність рекомендованих до установки оновлень системи безпеки. Працювати з програмою MBSA можна через графічний інтерфейс і командний рядок.

Сканер безпеки XSpider 7.0 - потужний засіб аналізу захищеності, яке випускається вітчизняною компанією Positive Technologies. XSpider 7.0 базується на застосуванні концепцій завдань і профілів, має гнучкий планувальник завдань для автоматизації роботи, менеджер оновлень, вбудований підручник російською мовою. XSpider 7.0 дозволяє генерувати звіти з різними рівнями деталізації. Сканер безпеки XSpider працює під управлінням операційних систем Microsoft Windows, але він може перевіряти уразливості на вузлах, що мають іншу програмну або апаратну платформи.

Лекція 6. Windows Defender

Версія Захисника Windows, що входить до складу Windows Vista, надає додаткові поліпшення в продуктивності і безпеки (перевірка тільки змінених файлів, перевірка файлів при їхньому запуску і т. д.). При використанні Internet Explorer 7 Захисник Windows також дозволяє сканувати файли, які завантажуються.

Введення

Microsoft пропонує наступне визначення для "шпигунського" ПО.

"Шпигунські" називаються програми, що виконують певні дії (наприклад, показ реклами,збір особистої інформації або зміна налаштувань комп'ютера) без відома і контролю користувача.

Як вказується в, ймовірними ознаками наявності на вашому комп'ютері "шпигунського" абоіншого небажаного програмного забезпечення є:

- поява спливаючої реклами, навіть коли ви не перебуваєте в Інтернеті;
- домашня сторінка або налаштування пошуку в оглядачі змінилися без вашого відома;
- поява в оглядачі нових непотрібних панелей інструментів, від яких важко позбутися;
- несподіване значне зниження продуктивності;
- кількість збоїв в роботі комп'ютера несподівано збільшилося.Деякі з програм-шпигунів можуть також виконувати наступне:
- реєструвати натискання клавіш, що дозволяє програмам-шпигунам перехоплювати паролі і дані для входу в систему;
- збирати особисті дані, такі як ідентифікаційні номери, номери соціального страхування (у США) або інформація про банківські рахунки, і пересилати їх третім особам;
- дозволяти дистанційно керувати комп'ютером для отримання доступу до файлів, установки і зміни програмного забезпечення, а також використання комп'ютера для розповсюдження вірусів і інших дій.

Всі форми програм-шпигунів володіють однією загальною ознакою: вони встановлюються без відома користувача і не надають йому відомостей про свої дії.

Для захисту від програм-шпигунів і вірусів компанія Microsoft пропонує наступні технології:

- Захисник Windows (Windows Defender) - інструмент захисту від "шпигунського" ПО. Здійснює не тільки пошук і видалення "шпигунського" ПЗ, але й постійний моніторинг дій користувача і додатків з метою виявлення спроб установки на комп'ютер небажаного ПЗ. Заснований на технологіях компанії GIANT Company

Software Inc., Придбаної Microsoft у грудні 2004 року.

• Windows Live Safety Center - веб-служба, що забезпечує нормальну роботу комп'ютера завдяки коштам сканування і видалення небажаних програм. Також дозволяє виконувати резервне копіювання файлів і дефрагментацію жорстких дисків.

• Засіб видалення шкідливих програм (Malicious Software Removal Tool) - засіб безпеки, який перевіряє комп'ютер і видаляє виявлені віруси та інші шкідливі програми. Засноване на технологіях придбаної Microsoft в червні 2003 року румунської антивірусної компанії GeCAD.

• Windows Live OneCare - набір засобів безпеки, які майже не вимагають вашого втручання в своїй роботі. Крім антивірусного захисту, здійснює на комп'ютері користувача дії, необхідні для підвищення продуктивності і для забезпечення збереження даних (управління брандмауером, резервне копіювання, дефрагментація жорстких дисків).

• Microsoft Client Protection - засіб захисту робітників, переносних комп'ютерів і

файлових серверів від таких загроз, як програми-шпигуни і rootkit, а також від вірусів і інших традиційних способів атаки. На відміну від OneCare, даний продукт не містить брандмауера, засобів моніторингу продуктивності та інструментів резервного копіювання.

Для установки програми вам необхідно мати права адміністратора на локальному комп'ютері. Процес інсталяції дуже простий і після закінчення не вимагає перезавантаження комп'ютера.

Після установки для запуску програми достатньо привілеїв звичайного користувача, але деякі дії можуть вимагати привілеїв адміністратора.

Вимоги до системи

Мінімальними вимогами для установки є:

• Процесор: Intel Pentium з частотою не менше 233 МГц. Рекомендується Pentium III.

• Операційна система: Windows XP з пакетом оновлень 2 (SP2) або більш пізнім, WindowsServer 2003 з пакетом оновлень 1 (SP1) або більш пізнім.

• ОЗУ: не менше 64 МБ; рекомендується 128 МБ.

• 20 МБ вільного місця на жорсткому диску.

• Microsoft Internet Explorer 6.0 або вище.

• Підключення до Інтернету зі швидкістю не менше 28,8 Кбіт / с.

• Windows Installer версії 3.1 або вище.

Завантаження Захисника Windows

Для встановлення програми необхідно завантажити інсталятор з веб-вузла центру завантаження Microsoft. Для цього на "Домашньої сторінці Захисника Windows" клацніть по напису "Завантажити тут".

На сторінці, що з'явилася, виберіть російську мову та натисніть кнопку "Change".

Захисник Windows є безкоштовною програмою для власників справжньої версії Windows. Тому на сторінці, що з'явилася перед завантаженням установника вам пропонується перевірити справжність вашої версії Windows. Про це свідчить напис "Необхідна перевірка" ("Validation Required") на сторінці завантаження.

Натисніть кнопку "Продовжити" для перевірки операційної системи вашого комп'ютера. Після цього ви перейдете на сторінку установки компонента перевірки автентичності Windows (the Genuine Windows Validation Component). Цей компонент є елементом управління ActiveX під назвою "Windows Genuine Advantage". У відповідності з налаштуваннями за замовчуванням, в Internet Explorer (версія, що

входить до складу Windows XP SP2) заборонена автоматична установка елементів ActiveX. Про це свідчить з'явилася панель інформації зі значком. Для продовження установки необхідно виконати клацання лівою кнопкою миші по цій панелі. У меню, виберіть команду "Установити елемент керування ActiveX ...".

Після появи попередження системи безпеки про встановлення ActiveX компонентунатисніть кнопку "Встановити".

Після успішної перевірки вашої операційної системи ви повернетеся на сторінку завантаження Windows Defender. Але зовнішній вигляд цієї сторінки тепер буде інший. Замість кнопки "Continue" буде кнопка "Download". Натисніть її.

Після появи попередження системи безпеки натисніть кнопку "Зберегти" і виберіть місце для збереження файлу WindowsDefender.msi. У разі виникнення помилок під час установки Захисника Windows, ви завжди зможете запустити установку повторно, якщо збережіть установник на диск.

Поверніться до кроку 2 і спробуйте повторно почати установку Windows Defender.

Оновлення служби Windows Update

Для установки Захисника Windows необхідно оновити на вашому комп'ютері службу Windows Update. Для цього запустіть Internet Explorer і виконайте команду меню "Сервіс | Windows Update" або перейдіть за адресою http://windowsupdate.microsoft.com/. Через декілька секунд ви побачите попередження системи безпеки з пропозицією встановити додаток Windows Update. Натисніть кнопку "Встановити". Якщо після установки потрібно перезавантаження - виконайте її. Поверніться до кроку 2 і спробуйте повторно почати установку Windows Defender.

Майстер установки Захисника Windows

Після появи на екрані вікна вітання майстра установки натисніть кнопку "Далі" ("Next"). Перед початком установки Захисника Windows необхідно перевірити справжність використовуваної копії Microsoft Windows. Натисніть кнопку "Перевірити".

Якщо перевірка пройшла успішно, на екрані з'явиться вікно "Ліцензійна угода для" Windows Defender "". Прочитайте його. Якщо ви його приймаєте, то виберіть "Приймаю умови ліцензійної угоди" ("I accept the terms in the license agreement") і натисніть кнопку "Далі" ("Next").

На наступній сторінці вам буде запропоновано вступити в Інтернет-спільнота Microsoft SpyNet. Microsoft рекомендує обрати перший варіант ("Використовувати рекомендовані настройки", "Use recommended settings"). У цьому випадку ви будете автоматично отримувати оновлення інформації про "шпигунських" програмах і вступите в Інтернет-спільнота Microsoft SpyNet.

Інтернет-спільнота Microsoft SpyNet (або мережа голосування) дозволяє входять у неї користувачам отримувати інформацію про програми, які були заборонені, вилучені або дозволені іншими користувачами при роботі з Захисником Windows. Крім того, ваші рішення з цього питання також будуть доступні іншим користувачам. Дані про рішення користувачів відображаються в Захиснику Windows у вигляді графіка, який містить інформацію про процентне співвідношення людей, які дозволили, заборонили або видалити конкретну програму.

Якщо ви не хочете вступати спільнота Microsoft SpyNet, але бажаєте

отримувати оновлення інформації про "шпигунських" програмах, то виберіть варіант "Установити тільки оновлення визначень" ("Install definition updates only").

При виборі варіанту «Відкласти» ("Ask me later") ви не будете отримувати оновлення та вступати в спільноту Microsoft SpyNet.

Виберіть перший варіант і натисніть кнопку "Далі" ("Next"). На наступній сторінці вам буде запропоновано вибрати тип установки: "Повна" ("Complete") або "Вибіркова" ("Custom"). Виберіть варіант "Повна" ("Complete") і натисніть кнопку "Далі" ("Next").

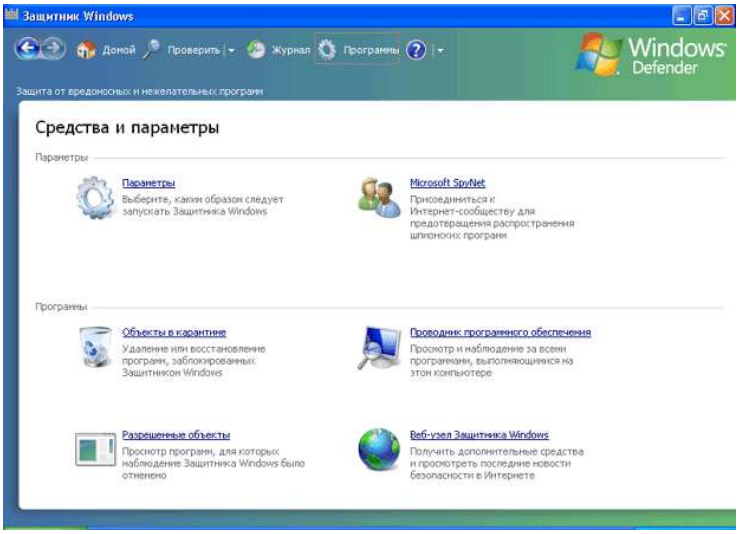
На наступному екрані вам буде повідомлено про готовність до установки Захисника Windows. Натисніть кнопку "Встановити" ("Install").

Після завершення установки з'явиться відповідна сторінка з пропозицією перевірити наявність оновлень інформації про "шпигунських" програмах і запустити швидкесканування вашого комп'ютера. Натисніть кнопку "Готово" ("Finish").

Для запуску Захисника Windows в меню "Пуск" виберіть пункт "Всі програми", а потім -пункт "Windows Defender" (Захисник Windows).

Налаштування Windows Defender

Для перегляду та зміни параметрів роботи Захисника Windows на панелі інструментіввиберіть "Програми" ("Tools") і в сторінці, що з'явилася виберіть пункт "Параметри" ("Options").



Сторінка "Tools" (Сервіс)

Налаштування Захисника Windows складаються з п'яти розділів:

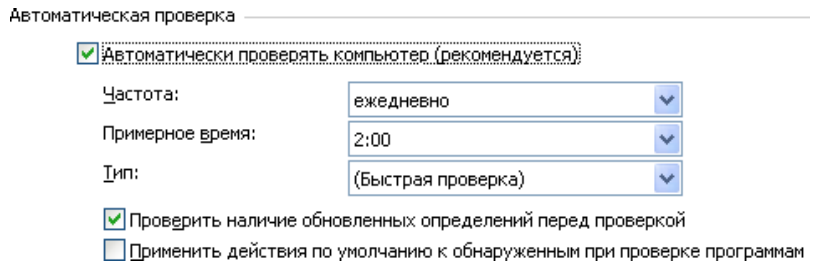
- Автоматична перевірка (Automatic scanning).
- Дії за замовчуванням (Default actions).
- Параметри захисту в режимі реального часу (Real-time protection options).
- Додаткові параметри (Advanced options).
- Адміністративні параметри (Administrator options).

Якщо ви зміните будь-який з параметрів, то для збереження цих змін необхідно натиснутикнопку "Зберегти" ("Save") внизу екрану.

Розглянемо кожен з цих розділів більш докладно.

Автоматична перевірка (Automatic scanning)

У цьому розділі зосереджені налаштування планування перевірки комп'ютера на наявність програм-шпигунів і інших потенційно небажаних програм. Параметр "Автоматично перевіряти комп'ютер (рекомендується)" ("Automatically scan my computer [recommended]") дозволяє запланувати проведення періодичних перевірок комп'ютера.


Автоматическая проверка
Автоматически проверять компьютер (рекомендуется)
Частота:
ежедневно
Примерное время:
2:00
Тип:
(Быстрая проверка)
Проверить наличие обновленных определений перед проверкой
Применить действия по умолчанию к обнаруженным при проверке программам

Налаштування автоматичного сканування

Параметр "Частота" ("Scan frequency") дозволяє задати періодичність автоматичного сканування. Доступні варіанти: "щодня" ("Daily"), "Понеділок", "Вівторок", ..., "Неділя".

Параметр "Зразковий час" ("Time of day") визначає час початку сканування.

Параметр "Тип" ("Type of scan") дозволяє вибрати, яка перевірка буде виконуватися: "Швидка перевірка" ("Quick scan") або "Повна перевірка системи" ("Full system scan"). При швидкій перевірці перевіряються ті області комп'ютера, які найбільш схильні до впливу небажаного програмного забезпечення. При повній перевірці системи перевіряються всі файли на жорсткому диску і всі виконувані в даний момент програми. При цьому можливе уповільнення роботи комп'ютера до завершення сканування. Microsoft рекомендує запланувати щоденну швидку перевірку, а в разі підозри на зараження комп'ютера програмами-шпигунами - виконувати повну перевірку системи.

Параметр "Перевірити наявність оновлених визначень перед перевіркою" ("Check for updateddefinitions before scanning") дозволяє перед скануванням комп'ютера перевірити наявність оновлень інформації про небажаних програмах на сервері оновлень Windows.

Параметр "Застосувати дії за замовчуванням до виявлених при перевірці програмами" ("Apply default actions to items detected during a scan") дозволяє при виявленні небажаного програмного забезпечення виконувати дії за умовчанням, задані в наступному розділі. Якщо цей параметр вимкнено, то при виявленні програм-шпигунів і інших потенційно небажаних програм Захисник Windows буде запитувати в користувача, що необхідно зробити з виявленим підозрілим об'єктом.

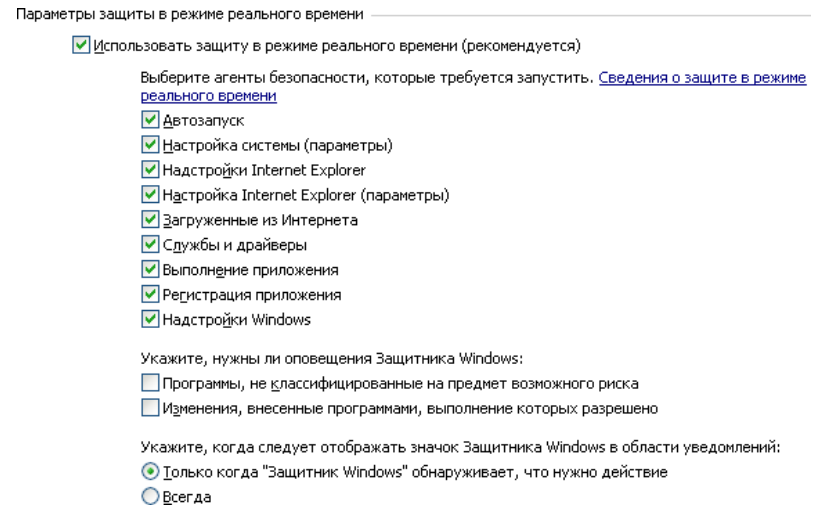
Дії за замовчуванням (Default actions)

У цьому розділі ви можете визначити, які дії необхідно виконувати при виявленні підозрілих об'єктів . Для різних типів попереджень (високий - high, середній - medium, низький - low) ви можете задати свій варіант реагування. Доступні наступні варіанти:

- Дія за замовчуванням (Definition recommended action).
- Ігнорувати (Ignore) (ігнорувати підозрілий об'єкт і дозволити йому виконуватися).
- Видалити (Remove) (видалити об'єкт і не допустити його виконання).
- Карантин (помістити об'єкт в інше місце на комп'ютері і блокувати його запуск до тих пір,поки ви не відновите або не видалите його).

Параметри захисту в режимі реального часу (Real-time protection options)

У цьому розділі знаходяться налаштування, пов'язані із захистом в реальному



часі.

Установки захисту в реальному часі

Захист в режимі реального часу (постійний захист) контролює стан найважливіших компонентів операційної системи (ОС). Коли сторонні програми проводять зміни в налаштуваннях ОС або намагаються встановитися на комп'ютер, постійний захист фіксує ці дії і повідомляє про це користувача.

Параметр "Використовувати захист в режимі реального часу (рекомендується)" ("Use real- time protection [recommended]") дозволяє включити або виключити постійний захист.

Нижче перераховані агенти безпеки, контролюючі різні компоненти ОС. Ви можете включити або виключити потрібні вам компоненти, але Microsoft рекомендує не вимикати захист у реальному часі і використовувати всі існуючі агенти безпеки.

Агенти безпеки захисту в реальному часі

Автозапуск (Auto Start) Контроль списку програм, автоматично запускаються при старті комп'ютера

Налаштування системи (параметри) [System Configuration (settings)] Контроль налаштувань, пов'язаних з безпекою Windows

Компоненти браузера Internet Explorer (Internet Explorer Add-ons) Контроль програм, якіавтоматично запускаються при старті Internet Explorer

Налаштування Internet Explorer (параметри) [Internet Explorer Configurations (settings)] Контроль налаштувань безпеки Internet Explorer

Наступний параметр ("Вкажіть, коли слід відображати значок Захисника Windows в області повідомлень" ["Choose when the Windows Defender icon appears in the notification area"]) визначає, коли буде з'являтися значок Захисника Windows в області повідомлення (права нижня частина екрану). Варіант "Завжди" ("Always") відповідає постійній наявності значка. Варіант "Тільки коли" Захисник Windows "виявляє, що потрібно дія" ("Only if Windows Defender detects an action to take") відповідає відображенню значка тільки у разі виникнення якої-небудь події - наприклад, коли Захисник Windows давно не з'єднувався з сервером оновлень Windows і не скачував нові описи небажаних програм.

Додаткові параметри (Advanced options)

У цьому розділі знаходяться наступні параметри, назва яких говорить саме за себе.

• "Перевіряти вміст архівних файлів і папок" ("Scan the contents of archived files and folders for potential threats"). На жаль, в довідці Захисника Windows відсутня інформація про типи підтримуваних архівів.

• "Використовувати евристичні методи для виявлення небезпечних або небажаних програм серед ще не класифікованих програм" ("Use heuristics to detect potentially harmful or unwanted behaviorby software that hasn't been analyzed for risks").

• "Створити точку відновлення перед виконанням дій для виявлених об'єктів".

• "Не перевіряти такі файли і папки" ("Do not scan these files or location") (не сканувати зазначені файли чи папки). Для завдання списку файлів або папок, що не підлягають перевірці, натисніть кнопку "Додати ..." ("Add ..."). Кнопка "Видалити" ("Remove") дозволяє видалити з цього списку раніше зазначені файли чи папки.

Адміністративні параметри (Administrator options)

У цьому розділі знаходяться наступні настройки:

• "Використовувати" Захисника Windows "" ("Use Windows Defender"). Якщо цей

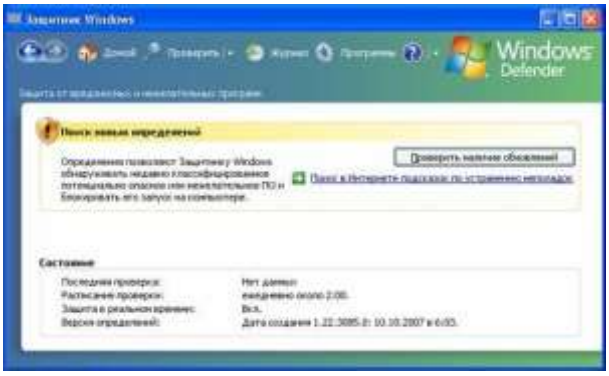
параметр включений - всі користувачі будуть отримувати попередження у разі виявлення шпигунського ПЗ або виконання небажаних дій. Захисник Windows буде періодично перевіряти наявність оновлень на сервері оновлень Windows, регулярно перевіряти ваш комп'ютер і автоматично видаляти небажане ПО, виявлене при скануванні.

• "Дозволити всім використовувати Захисник Windows" ("Allow users to use Windows Defender"). Якщо цей параметр увімкнено, користувачі, що не володіють адміністративними привілеями, зможуть взаємодіяти з Захисником Windows.

Оновлення Windows Defender

Захисник Windows працює тим ефективніше, чим більшою інформацією про існуючі у світі шпигунських та інших небажаних програмах він володіє. Цю інформацію Windows Defender отримує з сервера оновлень Windows (Windows Update). Відповідно, якщо ваш комп'ютер налаштований на автоматичне оновлення ("Пуск", "Панель управління", "Центр забезпечення безпеки") і періодично отримує оновлення з сервера Windows Update, то Захисник Windows буде також отримувати свої оновлення.

Інформація про те, яка версія інформаційних баз зараз використовується Захисником Windows, відображається на головній сторінці. Якщо Захисник Windows вважає, що бази застаріли, то на головній сторінці з'являється попередження.



Головна сторінка Захисника Windows

Для того щоб скачати свіжі оновлення з сервера Microsoft, натисніть кнопку "Перевірити наявність оновлень" ("Check Now"). В області повідомлення (права частина панелі завдань) з'явиться значок з повідомленням "Захисник Windows виконує пошук оновлень" ("Windows Defender is connecting to the Internet to acquire new definitions and engine upgrades").

Примітка. Насправді, якщо у вашій організації розгорнуть внутрішній сервер оновлень (наприклад, Microsoft Windows Server Update Services, WSUS) і ваш комп'ютер для отримання оновлень налаштований на з'єднання з цим сервером, то Захисник Windows буде з'єднуватися не з Інтернетом, а з внутрішнім сервером

оновлень . Налаштування внутрішнього сервера оновлень не входить в тему даного заняття. Проте відзначимо, що сервер WSUS за замовчуванням не викачує з Інтернету поновлення визначень для Захисника Windows, і його необхідно відповідним чином налаштовувати.

Після успішного отримання останніх оновлень з'явиться відповідне повідомлення в області повідомлення.

Головна сторінка Захисника Windows

Якщо ви хочете виконати оновлення Захисника Windows, ви завжди можете натиснути поруч зі значком на панелі задач Захисника Windows і вибрати команду "Перевірити наявність оновлень" ("Check for Updates").

Перевірка комп'ютера

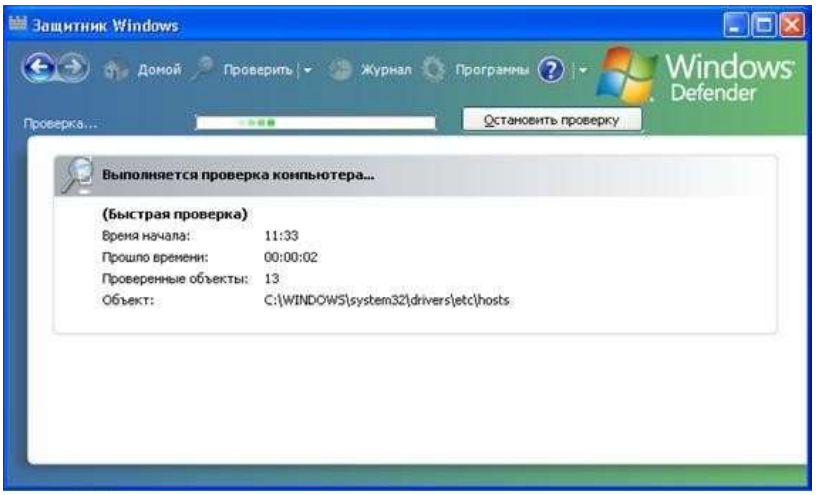
Як було сказано вище, щоб перевірити ваш комп'ютер на наявність шпигунського та іншого небажаного ПЗ, необхідно виконати сканування за допомогою Windows Defender. Існує три типи сканування:

- Швидка перевірка (Quick Scan).
- Повна перевірка (Full Scan).
- Вибіркова перевірка (Custom Scan ...).

При швидкій перевірці перевіряються ті області на жорсткому диску, зараження яких програмами-шпигунами найбільш ймовірно. У цьому режимі перевіряються не тільки системні папки Windows, але і важливі для безпеки вітки реєстру. У режимі повної перевірки перевіряються не тільки всі файли на жорсткому диску, але і всі виконувані в даний момент програми. При виконанні повної перевірки комп'ютера можливе уповільнення роботи системи. Тому рекомендується налаштувати Захисник Windows на щоденну швидку перевірку, а при підозрі на зараження комп'ютера програмами-шпигунами - виконувати повну перевірку системи.

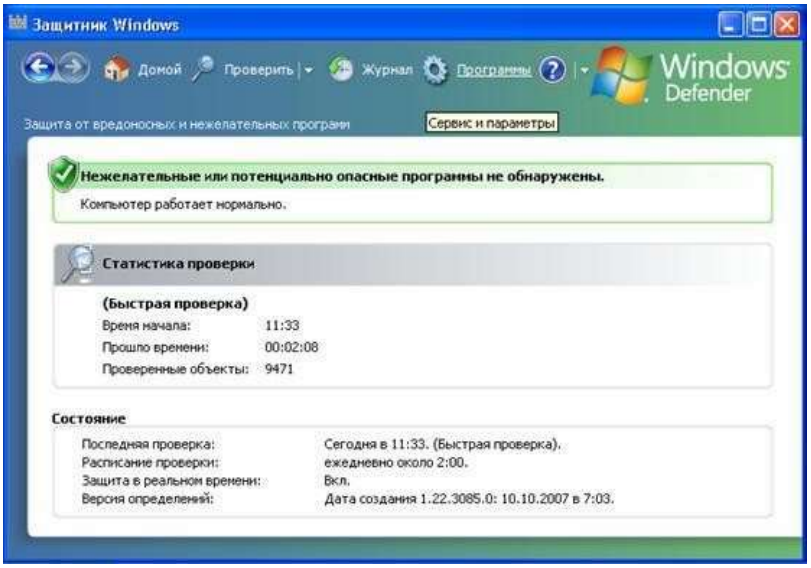
Вибіркове сканування дозволяє провести сканування тільки вибраних дисків і папок.

Для вибору потрібного вам режиму сканування комп'ютера натисніть трикутник поруч із кнопкою "Перевірити" ("Scan") на панелі завдань Windows Defender. Якщо відразу натиснути кнопку "Перевірити" ("Scan"), то буде виконана швидка перевірка комп'ютера.



Швидка перевірка комп'ютера

Після її виконання на екран буде виведена статистка перевірки.



Результат швидкої перевірки

Виявлення підозрілих дій

Щоб отримувати повідомлення про всі підозрілі дії, що вчиняються на вашому комп'ютері, необхідно в розділі "Вкажіть, чи потрібні оповіщення Захисника Windows" ("Choose if Windows Defender should notify you about") включити параметр "Програми, не класифіковані на предмет можливого ризику" ("Software that has not yet been classified for risks"). У цьому випадку Захисник Windows буде попереджати вас про всі підозрілі дії. Інакше (за умовчанням цей параметр вимкнений) він буде попереджати вас тільки про ті дії (і тих програмах), інформація про яких входить у визначення (definitions), створені розробниками Windows Defender.

Для того щоб дізнатися, що виявив Захисник Windows, необхідно клацнути по цьому повідомленню або двічі клацнути лівою кнопкою миші по значку Windows Defender. На екрані з'явиться вікно із зазначенням виявлених подій.

Виявлені події перераховані у вигляді таблиці в середній частині екрана. У

нижній частині екрана для виділеного в даний момент події відображається більш докладна інформація. У розділі "Підсумок" ("Summary") відображається загальна інформація по події. Далі йде більш докладний опис. У розділі "Шлях" ("Path") вказується розташування файлу, який викликав дану подію. У розділі

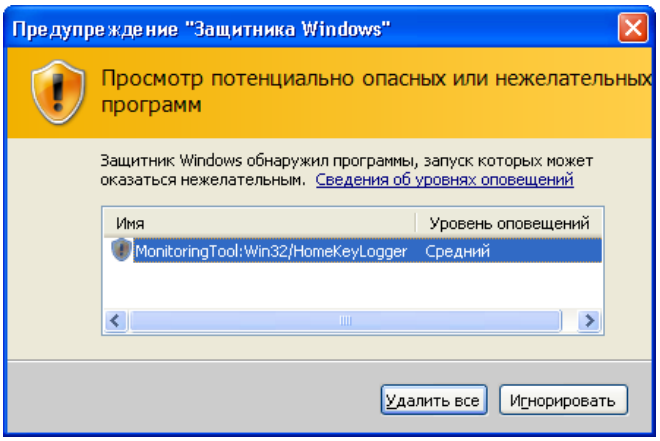
"Виявлені зміни" ("Detected changes") - зафіксовані в системі зміни. У розділі "Рада"("Advice") дається рекомендація, що в даному випадку слід вжити.

Детальний опис підозрілого події

Якщо ви довіряєте розробнику тієї програми, яка викликала ця подія, то в стовпці "Дія" ("Action") виберіть варіант "Дозволити" ("Allow"). Інакше - виберіть варіант "Заборонити" ("Block"). В останньому випадку дії, які були виконані зазначеною програмою, будуть скасовані. Після вибору потрібних дій для всіх подій натисніть кнопку "Застосувати дії" ("Apply Actions"). Якщо зазначена вами дія вдалося виконати, у стовпці "Стан" ("Status") буде виведено "Успішно" ("Succeeded").

Виявлення програм-шпигунів

У попередньому пункті був описаний приклад виявлення так званого "не классифицируемого події". У такої події в розділі "Категорія" ("Category") відображається "Немає класифікації" ("Not Yet Classified"). За замовчуванням користувачеві про такі події не повідомляється, але вони фіксуються у вікні "Журнал" ("History"). Якщо інформація про програму або подію існує в інформаційних базах (визначеннях) Захисника Windows, то попередження про такуподію виглядає інакше.


Предупреждение "Защитника Windows"
Просмотр потенциально опасных или нежелательных программ
Защитник Windows обнаружил программы, запуск которых может оказаться нежелательным. Сведения об уровнях оповещений
Имя
Уровень оповещений
MonitoringTool:Win32/HomeKeyLogger
Средний
Удалить все
Игнорировать

Повідомлення з рівнем "Medium"

В даному випадку Захисник Windows зафіксував подію з середнім (Medium) рівнем оповіщення (Alert level). Як вказується в довідці, рівні оповіщення (alert levels) допомагають користувачеві прийняти правильне рішення про те, як реагувати на виявлене шпигунське або небажане ПЗ. Незважаючи на те, що Захисник Windows буде рекомендувати вам видалити (кнопка "Видалити все" ["Remove All"]) програму, не всі виявлені програми є небезпечними або небажаними.

Рівні попередження

Severe (Критичний) Широко поширені або винятково небезпечні програми (наприклад, віруси або черв'яки), які наносять шкоду вашої особистої інформації і захисту вашого комп'ютера. Ці програми можуть пошкодити ваш комп'ютер. Негайно видаліть цю програму.

High (Високий) Програми, які можуть збирати вашу особисту інформацію і пошкодити ваш комп'ютер. Наприклад, без вашого відома або згоди збирають інформацію або змінюють налаштування вашого комп'ютера. Негайно видаліть цю програму.

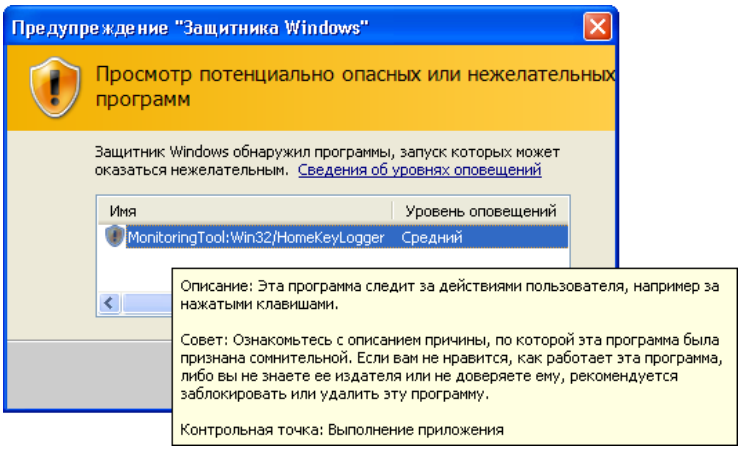
Medium (Середній) Програми, які можуть впливати на вашу особисту інформацію або виконувати зміни на вашому комп'ютері. Перегляньте подробиці цього попередження, щоб з'ясувати, чому це програма була виявлена. Якщо вам не подобаються ті дії, які виконує ця програма або ви не довіряєте розробнику цієї програми, вирішите, заблокувати або видалити цю програму.

Low (Низький) Потенційно небажані програми, які можуть збирати інформацію про вас, вашому комп'ютері або змінювати налаштування вашого комп'ютера, але про ці дії повідомляється в ліцензійній угоді при їх установці. Такі програми зазвичай не небезпечні при виконанні на вашому комп'ютері, якщо тільки вони не були встановлені без вашого відома. Якщо ви не впевнені, чи дозволяти роботу такої програми, перегляньте подробиці цього попередження і визначте, чи довіряєте ви розробнику цієї програми.

Not yet classified (не класифікований) Зазвичай безпечні програми, якщо тільки вони не були встановлені без вашого відома. Якщо ви знаєте цю програму і довіряєте її розробнику, дозвольте її виконання. Інакше - перегляньте подробиці цього попередження, для того щоб прийняти обгрунтоване рішення. Якщо ви вступили до спільноти Microsoft SpyNet, перевірте рейтинг мережі голосування, щоб дізнатися, чи довіряють цій програмі інші користувачі.

Для того щоб переглянути подробиці цієї події, підведіть курсор до рядка з назвою виявленої програми. З'явиться спливаюче повідомлення з описом виявленої програми і радою від розробників Захисника Windows. Якщо ви натиснете кнопку "Видалити все" ("Remove All"), то Захисник Windows спробує видалити виявлену програму. Про успішність цієї дії можна буде судити, переглянувши вікно "Журнал"

("History"). Якщо ви натиснете кнопку "Ігнорувати" ("Ignore"), Windows Defender нічого не буде робити з виявленою програмою, про що також з'явиться повідомлення у вікні "Журнал" ("History").



Опис виявленої програми

Описаний вище приклад показує реакцію Захисника Windows на операцію запису на диск програми установника. У разі виявлення реально працюючої в даний момент (тобто вже встановленої на вашому комп'ютері) програми вікно з попередженням матиме додаткову кнопку "Перевірити" ("Review"). При натисканні на цю кнопку з'явиться головне вікно Захисника Windows з можливістю не тільки видалити виявлену програму (кнопка "Remove All"), але і переглянути подробиці виявленого події. Для цього необхідно клацнути по напису "Перегляд об'єктів, виявлених захистом в режимі реального часу" ("Review items detected by real-time protection"). В результаті на екрані з'явиться вікно з докладним описом події і з можливістю вибору потрібної дії.

Можливі наступні дії:

- Ігнорувати (Ignore) - ігнорувати підозрілий об'єкт і дозволити йому виконуватися.
- Карантин (Quarantine) - перемістити підозрілий об'єкт на карантин.
- Видалити (Remove) - видалити підозрілий об'єкт і не допустити його виконання.
- Завжди дозволяти (Always allow)-дозволити підозрілому об'єкту виконуватися і занести його до списку дозволених об'єктів (allowed list).

Крім того, в кінці списку з описом цього об'єкту, є посилання "Показати додаткові відомості про цей елемент з Інтернету", яка дозволяє переглянути додаткову інформацію про цей об'єкт на сайті Microsoft.

Робота з карантином

При переміщенні підозрілої програми на карантин Захисник Windows переміщує її в інше місце на комп'ютері і перешкоджає її роботі до тих пір, поки ви не вирішите видалити або відновити її.

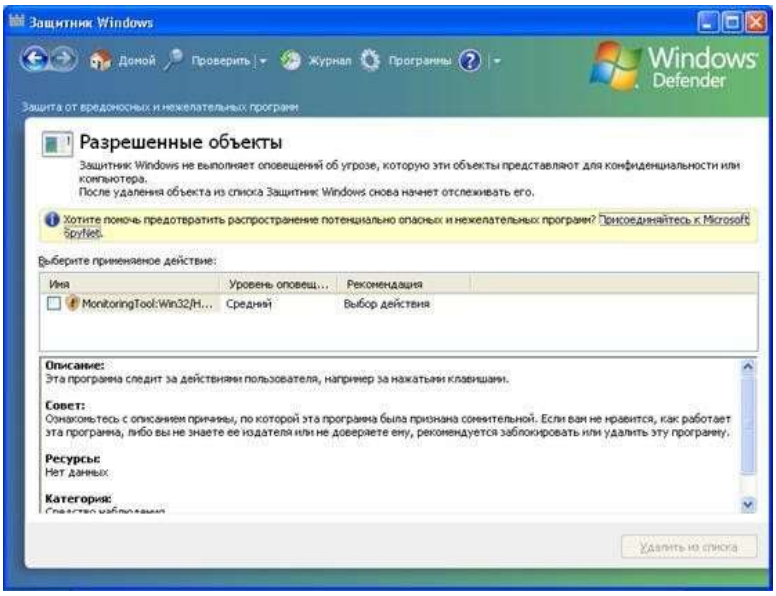
Для перегляду об'єктів, що знаходяться на карантині, необхідно на панелі інструментів вибрати "Програми" ("Tools") і в сторінці, що з'явилася вибрати пункт "Об'єкти в карантині" ("Quarantined items ").

Для того щоб видалити всі об'єкти, що знаходяться на карантині, необхідно просто натиснути внизу кнопку "Видалити все" ("Remove All"). Для того щоб видалити або відновити тільки деякі об'єкти, що знаходяться на карантині, необхідно виділити їх (тобто відзначити їх галочками) і натиснути одну з кнопок:

- Видалити (Remove)-видалення з комп'ютера виділених об'єктів;
- Відновити (Restore) - відновлення в початкове місцеположення виділених об'єктів.Робота зі списком дозволених об'єктів

При виборі дії "Завжди дозволяти" ("Always allow") виявлений об'єкт заноситься в

список дозволених програм (allowed list). Для перегляду цього списку необхідно на панелі інструментів вибрати "Програми" ("Tools") і в сторінці, що з'явилася вибрати пункт "Дозволені об'єкти" ("Allowed items").



Список дозволених об'єктів

Якщо ви видалите програму з цього списку, то Захисник Windows знову почне контролювати дії, виконувані нею. Для видалення програми зі списку необхідно виділити її (поставити галочку) і натиснути внизу кнопку "Видалити зі списку" ("Clear").

Використання Провідника програмного забезпечення (Software Explorer)

На сторінці "Програми" ("Tools") крім вже розглянутих засобів присутня утиліта "Провідник програмного забезпечення" ("Software Explorer"), яка дозволяє переглядати докладну інформацію про запущені на комп'ютері програми. Ця утиліта допомагає контролювати наступні елементи:

• Автоматично завантажувані програми (Startup Programs). Програми, що запускаються одночасно з початком роботи системи Windows. Для програм в цій категорії доступні наступні дії: "Видалити" ("Remove"), "Відключити" ("Disable") і "Включити" ("Enable").

• Поточні виконувані програми (Currently Running Programs). Програми, що виконуються в даний момент (відображаються на екрані або працюють у фоновому режимі). Для деяких програм в цій категорії доступна операція "Завершити процес" ("End Process"). Крім того, існує можливість запустити диспетчер завдань за допомогою кнопки "Диспетчер завдань" ("Task Manager").

• Програми з підключенням до мережі (Network Connected Programs). Програми або процеси, які можуть встановлювати з'єднання з Інтернетом або іншою мережею. Для програм в цій категорії доступні наступні дії: "Завершити процес" ("End Process"), "Блокувати вхідні підключення" ("Block Connection").

• Постачальники служби Winsock (Winsock Service Provider). Це програми, які забезпечують низькорівневі мережеві служби і служби зв'язку для систем Windows і програм, що працюють з Windows.

Залежно від обраної категорії, за кожною програмою у "Провіднику програмного забезпечення" ("Software Explorer") можна переглянути такі відомості.

Автозапуск (Auto Start) Показує, чи зареєстрована програма для автоматичного запуску при запуску операційної системи

Тип запуску (Startup Type) Адреса реєстрації програми для автоматичного запуску(реєстр або папка автозавантаження)

Поставка з операційною системою (Ship with OS) Показує, чи була дана програмавстановлена в ході установки операційної системи Windows

Класифікація (Classification) Показує, чи представляє програма загрозу конфіденційнихвідомостей або безпеки комп'ютера

Резюме

Шпигунські "програми - одна з найбільш неприємних проблем, з якими зараз стикаються користувачі комп'ютерів. У всьому світі програми-шпигуни вважаються серйозною проблемою, яка загрожує підірвати довіру суспільства до комп'ютерних технологій.

Одним з рішень, пропонованих компанією Microsoft для захисту комп'ютера від програм- шпигунів та інших небажаних програм, є Захисник Windows (Windows Defender). Цей продукт інтегрований в Windows Vista, а для користувачів Windows XP доступний у вигляді окремого безкоштовного доповнення.

Захисник Windows допомагає користувачам виявити, а потім відключити або видалити з комп'ютера відомі програми-шпигуни і інші потенційно небажані програми.

У той же час Windows Defender не є антивірусною програмою і забезпечує захист тільки від одного з підмножин існуючих шкідливих програм. Він не захищає комп'ютер від вірусів, троянських програм, черв'яків і т. д. Для захисту від цих загроз користувач може вибрати рішення як від самої Microsoft (наприклад, Microsoft OneCare), так і від стороннього виробника.

Лекція 6. DES (Data Encryption Standard)

DES (Data Encryption Standard) - Симетричний алгоритм шифрування, в якому один ключ використовується як для шифрування, так і для розшифрування даних. DES розроблений фірмоюIBM і затверджений урядом США в 1977 році як офіційний стандарт (FIPS 46-3). DES має блоки по 64 біт і 16 циклову структуру мережі Фейстеля, для шифрування використовує ключ з довжиною 56 біт. Алгоритм використовує комбінацію нелінійних (S-блоки) і лінійних (перестановки E, IP, IP-1) перетворень. Для DES рекомендовано декілька режимів:

- режим електронної кодової книги (ECB - Electronic Code Book),
- режим зчеплення блоків (CBC - Cipher Block Chaining),
- режим зворотного зв'язку по шіфротекста (CFB - Cipher Feed Back),
- режим зворотного зв'язку по виходу (OFB - Output Feed Back).

Історія

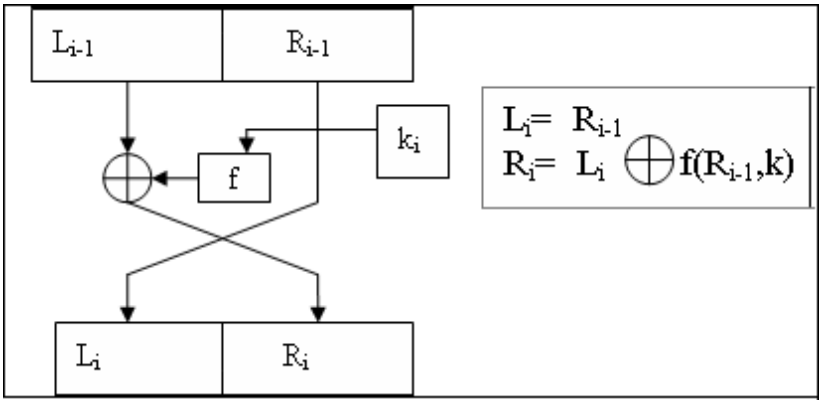
У 1972 році, після проведення дослідження потреб уряду США в комп'ютерній безпеці, американське НБС (Національне Бюро Стандартів) - тепер перейменовано ність (Національний Інститут Стандартів і Технологій) - визначило необхідність в загальноурядовий стандарті шифрування некритичною інформації. 15 травня 1973, після консультації з АНБ (Агентством національної безпеки), НБС оголосило конкурс на шифр, який задовольнить суворим критеріям проекту, але жоден конкурсант не забезпечував виконання всіх вимог. Другий конкурс був початий 27 серпня 1974. Цього разу, шифр Lucifer, представлений IBM і розвинений протягом періоду 1973-1974 визнали прийнятним, він був заснований на більш ранньому алгоритмі Хорста Фейстеля.

17 березня 1975 запропонований алгоритм DES був виданий у Федеральному Реєстрі. У наступному році було проведено 2 відкритих симпозіуму по обговоренню цього стандарту, де піддалися жорсткій критиці зміни, внесені АНБ в алгоритм: зменшення початкової довжини ключа і S-блоки (блоки підстановки), критерії проектування яких не розкривалися. АНБ підозрювалося в свідомому ослабленні алгоритму з метою, щоб АНБ могло легко переглядати зашифровані повідомлення. Після чого сенатом США була проведена перевірка дій АНБ, результатом якої стало заяву, опубліковану в 1978, в якому йшлося про те, що в процесі розробки DES АНБ переконало IBM, що зменшеною довжини ключа більш ніж достатньо для всіх комерційних додатків, що використовують DES, побічно допомагало в розробці S-перестановок, а також, що остаточний алгоритм DES був кращим, на їх думку, алгоритмом шифрування і був позбавлений статистичної або математичної слабкості. Також було виявлено, що АНБ ніколи не втручалося в розробку цього алгоритму.

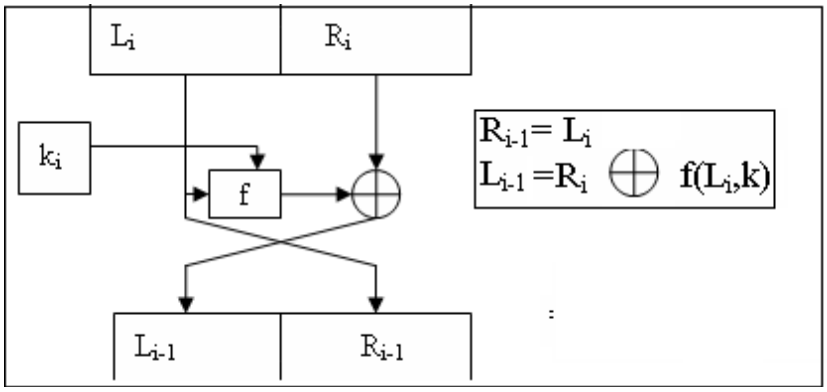
Частина підозр у прихованій слабкості S-перестановок була знята в 1990, коли були опубліковані результати незалежних досліджень Елі Біхама (Eli Biham) і Аді Шаміра (Adi Shamir) по диференціальному криптоаналізу - основного методу злому блочних алгоритмів шифрування з симетричним ключем. S-блоки алгоритму DES виявилися набагато більш стійкими до атак, ніж, якби їх вибрали випадково. Це означає, що така техніка аналізу була відома АНБ ще в 70-х роках XX століття.

DES є блоковим шифром. Щоб зрозуміти як працює DES насамперед ми трохи розглянемо блоковий шифр, мережа Фейстеля.

Блоковий шифр



Пряме перетворення мережею Фейстеля



Зворотне перетворення мережею Фейстеля

Вхідними даними для блочного шифру служать блок розміром n біт і k-бітний ключ. На виході, після застосування шифрувального перетворення, виходить n-бітний зашифрований блок, причому незначні відмінності вхідних даних як правило призводять до істотної зміни результату. Блокові шифри реалізуються шляхом багаторазового застосування до блоків вихідного тексту деяких базових перетворень.

Базові перетворення:

• Складне перетворення на одній локальній частині блоку.

• Просте перетворення між частинами блоку.

Так як перетворення виробляється поблочно, як окремий крок потрібно поділ вихідних даних на блоки необхідного розміру. При цьому незалежно від формату вихідних даних, будь то текстові документи, зображення або інші файли, вони повинні бути інтерпретовані в бінарний вигляд і тільки після цього розбиті на блоки. Все вищеперелічене може здійснюватися як програмними, так і апаратними засобами.

Перетворення Мережею Фейстеля

Це перетворення над векторами (блоками) представляють собою ліву і праву половини регістра зсуву. В алгоритмі DES використовуються пряме перетворення мережею Фейстеля в шифруванні (див. Рис.1) і зворотне перетворення мережею Фейстеля в розшифрування.

Схема шифрування алгоритму DES

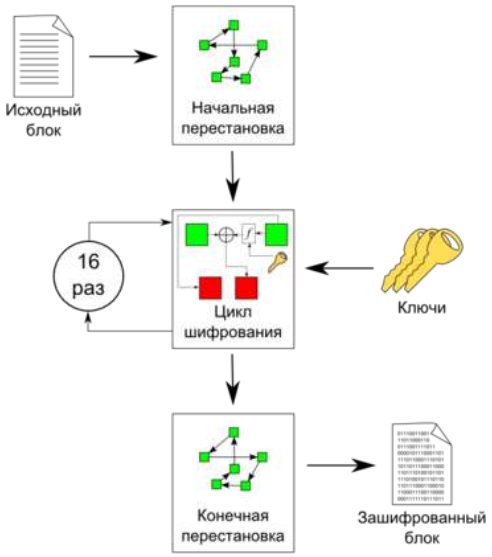
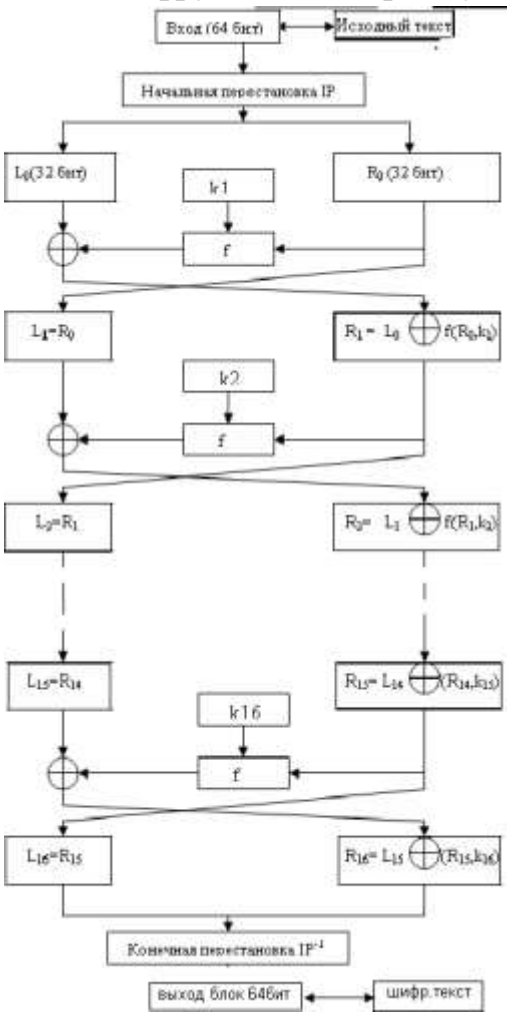


Схема шифрування алгоритму DES



Детальна схема шифрування

алгоритму DESОригінальний текст -

блок 64 біт.

Процес шифрування полягає в початковій перестановці, 16 циклах шифрування і кінцевоїперестановці.

Шифрований текст - блок 64 біт.

Початкова перестановка

- Оригінальний текст T (блок 64 біт) перетвориться с допомогою початкової перестановки IPяка визначається таблицею 1:

Таблиця 1. Початкова перестановка IP

58 50 42 34 26 18 10 2 60 52 44 36 28 20 12 4

62 54 46 38 30 22 14 6 64 56 48 40 32 24 16 8

57 49 41 33 25 17 9 1 59 51 43 35 27 19 11 3

61 53 45 37 29 21 13 5 63 55 47 39 31 23 15 7

По таблиці перші 3 біта результуючого блоку IP (T) після початкової перестановки IP єбітами 58, 50, 42 вхідного блоку T, а його 3 останні біта є бітами 23, 15, 7 вхідного блоку.

Цикли шифрування

Отриманий після початкової перестановки 64-бітовий блок IP (T) бере участь у 16-циклахперетворення Фейстеля.

16 циклів перетворення Фейстеля:

Розбити IP (T) на дві частини L0, R0, де L0, R0 - відповідно 32 старших бітів і 32 молодшихбітів блоку T0 IP (T) = L0R0.

Нехай Ti - 1 = Li - 1Ri - 1 результат (i-1) ітерації, тоді результат i-ой ітерації Ti = LiRiвизначається: Li = Ri - 1

Ліва половина Li дорівнює правій половині попереднього вектора Li - 1Ri - 1. А праваполовина Ri - це бітове складання Li - 1 і f (Ri - 1, ki) по модулю 2.

У 16-циклах перетворення Фейстеля функція f грає роль шифрування. Розглянемо докладнофункцію f.

Основна функція шифрування (функція Фейстеля)

Аргументи функції f є 32 бітовий вектор Ri - 1, 48 бітовий ключ ki, які є результатомперетворення 56 бітового початкового ключа шифру k.

Для обчислення функції f використовуються функція розширення E, перетворення S, щоскладається з 8 перетворень S-блоків, і перестановка P.

Функція E розширює 32 бітової вектор Ri - 1 до 48 бітового вектора E (Ri - 1) шляхомдублювання деяких бітів з Ri - 1 при цьому порядок бітів вектора E (Ri - 1) подано в таблиці 2.

Таблиця 2. Функція

розширення E32 1 2 3 4 5

4 5 6 7 8 9

8 9 10 11 12 13

12 13 14 15 16 17

16 17 18 19 20 21

20 21 22 23 24 25

24 25 26 27 28 29

28 29 30 31 32 1

Перші три біта вектора E (Ri - 1) є бітами 32, 1, 2 вектора Ri - 1. По таблиці 2 видно що біти1, 4, 5, 8, 9, 12, 13, 16, 17, 20, 21, 24, 25, 28, 29, 32 дублюються. Останні 3 біти вектора E (Ri - 1) - це біти 31, 32, 1 вектора Ri - 1. Отриманий після перестановки блок E (Ri - 1) складається по модулю 2 з ключами ki і потім представляються у вигляді восьми послідовних блоків B1, B2, ... B8.

E (Ri - 1) = B1B2 ... B8

Кожен Bj є 6-бітовим блоком. Далі кожен з блоків Bj трансформується в 4 бітової блок B'j задопомогою перетворень Sj. Перетворення Sj визначається таблицею 3.

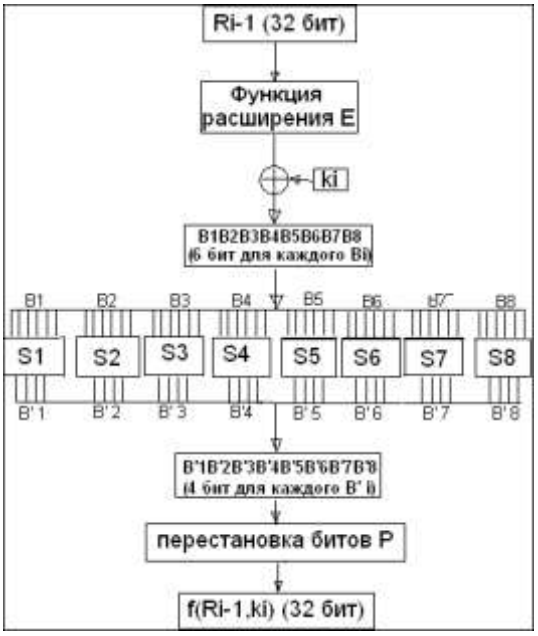


Схема роботи функції f

Таблиця 3. Перетворення Si, i = 1 ... 16

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

0 14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7
1 0 15 7 4 14 2 13 1 10 6 12 11 9 5 3 8 S1
2 4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0
3 15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13

0 15 1 8 14 6 11 3 4 9 7 2 13 12 0 5 10
1 3 13 4 7 15 2 8 14 12 0 1 10 6 9 11 5 S2
2 0 14 7 11 10 4 13 1 5 8 12 6 9 3 2 15
3 13 8 10 1 3 15 4 2 11 6 7 12 0 5 14 9

0 10 0 9 14 6 3 15 5 1 13 12 7 11 4 2 8
1 13 7 0 9 3 4 6 10 2 8 5 14 12 11 15 1 S3
2 13 6 4 9 8 15 3 0 11 1 2 12 5 10 14 7
3 1 10 13 0 6 9 8 7 4 15 14 3 11 5 2 12

0 7 13 14 3 0 6 9 10 1 2 8 5 11 12 4 15
1 13 8 11 5 6 15 0 3 4 7 2 12 1 10 14 9 S4
2 10 6 9 0 12 11 7 13 15 1 3 14 5 2 8 4
3 3 15 0 6 10 1 13 8 9 4 5 11 12 7 2 14

0 2 12 4 1 7 10 11 6 8 5 3 15 13 0 14 9

1 14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6 S5
2 4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14

3 11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3

0 12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11
1 10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8 S6
2 9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6
3 4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13

0 4 11 2 14 15 0 8 13 3 12 9 7 5 10 6 1
1 13 0 11 7 4 9 1 10 14 3 5 12 2 15 8 6 S7
2 1 4 11 13 12 3 7 14 10 15 6 8 0 5 9 2
3 6 11 13 8 1 4 10 7 9 5 0 15 14 2 3 12

0 13 2 8 4 6 15 11 1 10 9 3 14 5 0 12 7
1 1 15 13 8 10 3 7 4 12 5 6 11 0 14 9 2 S8
2 7 11 4 1 9 12 14 2 0 6 10 13 15 3 5 8
3 2 1 14 7 4 10 8 13 15 12 9 0 3 5 6 11

Припустимо що B3 = 101111 і ми хочемо знайти B'3. Перший і останній розряди B3 є двійковій записом числа a, 0 <= a <= 3, середні 4 розряди представляють число b, 0 <= b <= 15. Рядки таблиці S3 нумеруються від 0 до 3, стовпці таблиці S3 нумеруються від 0 до 15. Пара чисел (a, b) визначає число, що знаходить в перетині рядка a й стовпця b. Двійкове подання цього числа дає B'3. У нашому випадку a = 112 = 3, b = 01112 = 7, число визначається парою (3,7) дорівнює 7, слід B'3 = 0111.

Значення функції f (Ri - 1, ki) (32 біт) виходить перестановкою P, застосовуваної до 32бітовому блоку B'1B'2 ... B'8. Перестановка P задана таблицею 4.

Таблиця 4.

Перестановка P16 7 20
21 29 12 28 17
1 15 23 26 5 18 31 10
2 8 24 14 32 27 3 9
19 13 30 6 22 11 4 25

f (Ri - 1, ki) = P (B'1B'2 ... B'8)

Згідно таблиці 4, перші чотири біта результуючого вектора після дії функції f - це бита 16, 7,20, 21 вектора B'1B'2 ... B'8

Генерування ключів ki

Ключі ki виходять з початкового ключа k (64 біт = 8 байтів або 8 символів у ASCII) таким чином. Вісім бітів, що знаходять в позиціях 8, 16, 24, 32, 40, 48, 56, 64 додаються в ключ k такий спосіб щоб кожен байт містив непарне число одиниць. Це використовується для виявлення помилок при обміні і зберіганні ключів. Потім роблять перестановку для розширеного ключа (крім додаються бітів 8, 16, 24, 32, 40, 48, 56, 64). Така перестановка визначена як в таблиці 5.

Рис.6 Схема розшифрування
алгоритму DESТаблиця 5.
57 49 41 33 25 17 9 1 58 50 42 34 26 18 C0
10 2 59 51 43 35 27 19 11 3 60 52 44 36
63 55 47 39 31 23 15 7 62 54 46 38 30 22 D0

14 6 61 53 45 37 29 21 13 5 28 20 12 4

Ця перестановка визначається двома блоками C0 і D0 по 28 біт кожен. Перші 3 біти C0 є біти 57, 49, 41 розширеного ключа. А перші три біти D0 є біти 63, 55, 47 розширеного ключа. Ci, Di i = 1,2,3 ... виходять з Ci - 1, Di - 1 одним або двома лівими циклічними зрушеннями відповідно до таблиці 6.

Таблиця 6.

i 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Число зсуву 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1

Ключ ki, i = 1, ... 16 складається з 48 біт, вибраних з бітів вектора CiDi (56 біт) згідно зтаблицею 7. Перший і другий біти ki є біти 14, 17 вектора CiDi

Таблиця 7.

14 17 11 24 1 5 3 28 15 6 21 10 23 19 12 квітня

26 8 16 7 27 20 13 2 41 52 31 37 47 55 30 40

51 45 33 48 44 49 39 56 34 53 46 42 50 36 29 32

Кінцева перестановка

Кінцева перестановка IP - 1 діє на T16 і використовується для відновлення позиції. Вона єзворотною до перестановки IP. Кінцева перестановка визначається таблицею 8.

Таблиця 8. Зворотній перестановка

IP - 1 40 8 48 16 56 24 64 32 39 7 47

15 55 23 63 31

38 6 46 14 54 22 62 30 37 5 45 13 53 21 61 29

36 4 44 12 52 20 60 28 35 3 43 11 51 19 59 27

34 2 42 10 50 18 58 26 33 1 41 9 49 17 57 25

При розшифрування даних всі дії виконуються в зворотному порядку. У 16 циклах розшифрування, на відміну від шифрування с допомогою прямого перетворення мережею Фейстеля, тут використовується зворотне перетворення мережею Фейстеля.

Ri - 1 = Li

Ключ ki, i = 1, ..., 15, функція f, перестановка IP і IP - 1 такі ж як і в процесі шифрування.

Режими використання DES

DES може використовуватися в чотирьох режимах.

1. Режим електронної кодової книги (OCB - Electronic Code Book): звичайне використання DES як блокового шифру. Шіфруемий текст розбивається на блоки, при цьому, кожен блок шифрується окремо, не взаємодіючи з іншими блоками.

2. Режим зчеплення блоків (CBC - Cipher Block Chaining). Кожен черговий блок Ci i> = 1, перед зашіфровиваніем складається по модулю 2 з наступним блоком відкритого тексту Mi + 1. Вектор C0 - початковий вектор, він змінюється щодня і

зберігається в секреті.

3. Режим зворотного зв'язку по шіфротекста (CFB - Cipher Feed Back) (див. Рис.9). У режимі CFB виробляється блокова «гамма» Z0, Z1, ... Zi = DESk (Ci - 1). Початковий вектор C0 зберігаєтьсяв секреті.

4. Режим зворотного зв'язку по виходу (OFB - Output Feed Back) (див. Мал.10). У режимі OFB виробляється блокова «гамма» Z0, Z1, ... , I> = 1

Переваги і недоліки режимів:

• Режим ECB простий в реалізації, але можливе проведення криптоаналізу за словником. [Джерело не вказано 273 дні].

• У режимах ECB та OFB спотворення при передачі одного 64-бітового блоку шіфротекста Сі призводить до спотворення після розшифрування тільки відповідного відкритогоблоку Мі, тому такі режими використовується для передачі по каналах зв'язку з великим числомспотворень.

• У режимах CBC і CFB спотворення при передачі одного блоку шифрованого тексту Сі призводить до спотворення на приймачі не більше двох блоків відкритого тексту Мі, Мі + 1 [джерело не вказано 273 дні]. Зміна Мі призводить до зміни всіх інших блоковМі + 1, Мі + 2 ... Ця властивість використовується для вироблення коду аутентифікації повідомлення.

Криптостійкість алгоритму DES

Нелінійність перетворень в DES засобами тільки S-блоків, у разі, якщо вони мають слабину, дозволяє здійснювати контроль за шифрованого листуванням. Вибір S-блоків вимагає дотримання декількох умов:

• Кожен рядок кожного блоку повинна бути перестановкою множини {0,1,2,, 15}

• S-блоки не повинні бути лінійною або афінною функцією своїх аргументів.

• Зміна одного біта на вході S-блоку повинно приводити до зміни принаймні двох бітів на

виході.

• Для кожного S-блоку і будь-якого аргументу x значення S (x) і повинні розрізнятися

принаймні двома бітами.

Через невеликого числа можливих ключів (всього 256), з'являється можливість їх повного перебору на швидкодіючої обчислювальної техніки за реальний час. У 1998 році The Electronic Foundation використовуючи спеціальний комп'ютер DES-Cracker, вдалося зламати DES за 3 дні.

В алгоритмі DES існують слабкі і частково-слабкі ключі. Слабкими ключами називається ключі k такі що DESk (DESk (x)) = x, x - блок 64 біт. Частково-слабкі ключі - пари ключів (k1, k2) такі що DESk1 (DESk2 (x)) = x

Відомі 4 слабких ключа, вони наведені в таблиці 9. Для кожного слабкого ключа існує 232

«постійні точки», тобто таких 64-бітових блоків x, в яких

DESk (x) = xТаблиця 9. DES-Слабкі ключі

Слабкі ключі (hexadecimal)

C0 D0 0101-0101-0101-0101

[0] 28 [0] 28

FEFE-FEFE-FEFE-FEFE [1] 28 [1] 28

1F1F-1F1F-0E0E-0E0E [0] 28 [1] 28

E0E0-E0E0-F1F1-F1F1 [1] 28 [0] 28

[0] 28 позначає вектор, що складається з 28 нульових бітів.

Існують 6 частково-слабких пар ключів, вони приведені в таблиці 10. Для кожного з 12частково-слабких ключів існують 232 «анти-постійні точки», тобто такі блоки x, що

Таблиця 10. Частково-слабкі ключі

C0 D0 Пари частково-слабких ключів C0 D0

[01] 14 [01] 14 01FE-01FE-01FE-01FE, FE01-FE01-FE01-FE01 [10] 14 [10] 14

[01] 14 [01] 14 1FE0-1FE0-1FE0-1FE0, ---- E0F1-E0F1-E0F1-E0F1 [10] 14 [10] 14

[01] 14 [0] 28 01E0-01E0-01F1-01F1, ---- E001-E001-F101-F101 [10] 14 [0] 28

[01] 14 [1] 28 1FFE-1FFE-0EFE-0EFE, ---- FE1F-FE1F-FE0E-FE0E [0] 28 [1] 28

[0] 28 [01] 14 O11F-011F-010E-010E, ---- 1F01-1F01-0E01-0E01 [0] 28 [10] 14

[1] 28 [01] 14 E0FE-E0FE-F1FE-F1FE, FEE0-FEE0-FEF1-FEF1 [1] 28 [10] 14

Відомі атаки на DES.
Повний пошук 1 - Незначний 255
Лінійний Криптоаналіз 243 (85%) - Для тексту 243
Лінійний Криптоаналіз 238 (10%) - Для
тексту 250Диффер. Криптоаналіз - 247 Для
тексту 247 Диффер. Криптоаналіз 255 -
Для тексту 255

• Метод повного пошуку вимагає одну відому пару шифрованого і розшифрованого тексту, незначний обсяг пам'яті, і для його виконання потрібні 255 кроків.

• Диференціальний криптоаналіз - першу таку атаку на DES заявили Biham й Shamir. Ця атака вимагає шифрування 247 відкритих текстів обраних нападаючим, і для її виконання потрібні 247 кроків. Теоретично будучи крапкою розриву, ця атака непрактична через надмірні вимоги до підбору даних і складності організації атаки по обраному відкритому тексту. Самі автори цієї атаки Biham й Shamir заявили, що вважають DES захищеним для такої атаки.

• Лінійний криптоаналіз розроблений Matsui. Цей метод дозволяє відновити ключ DES за допомогою аналізу 243 відомих відкритих текстів, при цьому потрібно 243 кроків для виконання. Перший експериментальний криптоаналіз DES, заснований на відкритті Matsui, був успішно виконаний протягом 50 днів на автоматизованих робочих місцях 12 HP 9735.

Для лінійної та диференціальної атак потрібно досить великий обсяг пам'яті для збереження вибраних (відомих) відкритих текстів до початку атак.

Збільшення криптостійкості DES

Щоб збільшувати криптостойкость DES з'являються кілька варіантів: double DES (2DES), triple DES (3DES), DESX, G-DES.

• Методи 2DES і 3DES засновані на DES, але збільшують довжину ключів (2DES - 112 біт, 3DES - 168 біт) і тому збільшується криптостійкість.

• Схема 3DES має вигляд DES (k3, DES (k2, DES (k1, M))), де k1, k2, k3 ключі для кожного шифру DES. Це варіант відомий як в EEE оскільки три DES операції являюся шифруванням. Існує 3 типи алгоритму 3DES:

• DES-EEE3: Шифрується три рази з 3 різними ключами.

• DES-EDE3: 3DES операції шифровка-розшифровка-шифровка з 3 різними ключами.

• DES-EEE2 і DES-EDE2: Як і попередні, за винятком того, що перша і третя операціївикористовують однаковий ключ.

Найпопулярніший тип при використанні 3DES - це DES-EDE3, для нього алгоритм виглядає так:

Зашифрування:.

Розшифрування:

При виконанні алгоритму 3DES ключі можуть вибрати так:

- k1, k2, k3 незалежні.
- k1, k2 незалежні, а k1 = k3
- k1 = k2 = k3.
- Метод DESX створений Рональдом Рівестом і формально продемонстрована Killian і Rogaway.

Лекція 7. RSA - алгоритм з відкритим ключем

RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису. Алгоритм використовується в великому числі криптографічних додатків.

Історія

Опублікована в листопаді 1976 року стаття Уітфілд Діффі і Мартіна Хеллмана «Нові напрямки в криптографії» перевернула уявлення про криптографічних системах, заклавши основи криптографії з відкритим ключем. Розроблений згодом алгоритм Діффі-Хеллмана-Меркле дозволяв двом сторонам одержати загальний секретний ключ, використовуючи незахищений канал зв'язку. Однак цей алгоритм не вирішував проблему аутентифікації. Без додаткових коштів, один з користувачів не міг бути впевнений, що він обмінявся ключами саме з тим користувачем, який йому був потрібний.

Вивчивши цю статтю, троє вчених Рональд Райвест (Ronald Linn Rivest), Аді Шамір (Adi Shamir) і Леонард Адлеман (Leonard Adleman) з Массачусетського Технологічного Інституту (MIT) приступили до пошуків математичної функції, яка б дозволяла реалізувати сформульовану Уітфілд Діффі і Мартіном Хеллманом модель криптографічної системи з відкритим ключем. Після роботи над більш ніж 40 можливими варіантами, їм вдалося знайти алгоритм, заснований на відмінності в тому, наскільки легко знаходити великі прості числа і наскільки складно розкладати на множники добуток двох великих простих чисел, який отримав згодом назву RSA. Система була названа за першими літерами прізвищ її творців.

Опис RSA було опубліковано в серпні 1977 року в журналі Scientific American. Автори RSA підтримували ідею її активного поширення. У свою чергу, Агентство національної безпеки (США), побоюючись використання цього алгоритму в недержавних структурах, протягом декількох років безуспішно вимагало припинення розповсюдження системи. Ситуація часом доходила до абсурду - наприклад, коли програміст Адам Бек (Adam Back) описав алгоритм RSA на мові Perl, який складається з п'яти рядків, уряд США заборонило розповсюдження цієї програми за межами країни. Люди, незадоволені подібним обмеженням, на знак протесту надрукували текст цієї програми на своїх футболках.

У 1983 році MIT був виданий патент 4405829 США, термін дії якого закінчився 21 вересня 2000 року.

У 1977 році творцями RSA була зашифрована фраза «The Magic Words are Squeamish Ossifrage» («Чарівні слова - це гидливий ягнятник»). За розшифровку була обіцяна нагорода в 100 доларів США. Лише в кінці 1995 року вдалося практично

реалізувати розкриття шифру RSA для 500-значного ключа. Протягом півроку більше 600 добровольців жертвували процесорний час 1600 машин (дві з яких були факс-машинами). Координування проходило через Інтернет, і це був один з перших подібних проектів розподілених обчислень. Отриману нагороду переможці пожертвували у фонд вільного програмного забезпечення.

У грудні 1997 року була оприлюднена інформація, згідно з якою британський математик Кліффорд Кокс (Clifford Cocks), що працював в центрі урядового зв'язку (GCHQ) Великобританії, описав аналогічну систему в 1973 році [2], кількома місяцями пізніше в 1974 році Малькольм Вільямсон винайшов математичний алгоритм , заснований на комутативності зведення в ступінь, аналогічний алгоритму Діффі-Хеллмана-Меркле.

Опис алгоритму

Введення

Криптографічні системи з відкритим ключем використовують так звані односпрямовані функції, які мають наступну властивість:

• Якщо відомо x, то обчислити f(x) відносно просто

• Якщо відомо f(x), то для x немає простого шляху обчислення

Під односпрямованість розуміється не теоретична односпрямованим, а практична неможливість обчислити зворотне значення, використовуючи сучасні обчислювальні засоби, за осяжний інтервал часу.

В основу криптографічної системи з відкритим ключем RSA покладена задача множення і розкладання складових чисел на прості співмножники, яка є обчислювально односпрямованої завданням. (Дод.Інформація див. тест простоти, факторизація)

В криптографічного системі з відкритим ключем кожен учасник має в своєму розпорядженні як відкритим ключем (англ. public key), так і секретним ключем (англ. secret key). Кожен ключ - це частина інформації. В криптографічного системі RSA кожен ключ складається з пари цілих чисел. Кожен учасник створює свій відкритий і секретний ключ самостійно. Секретний ключ кожен з них тримає в секреті, а відкриті ключі можна повідомляти кому завгодно або навіть публікувати їх. Відкритий і секретний ключі кожного учасника обміну повідомленнями утворюють «узгоджену пару» в тому сенсі, що вони є взаємно зворотними.

Алгоритм створення відкритого і секретного ключів

RSA-ключі генеруються таким чином:

1. Вибираються два випадкових простих числа p і q заданого розміру (наприклад, 1024 біта кожне).
2. Обчислюється їх добуток n = pq, яке називається модулем.
3. Обчислюється значення функції Ейлера від числа n:
4. Вибирається ціле число e, взаємно просте з значенням функції Ейлера. Звичайно як e беруть прості числа, що містять невелику кількість одиничних бітів в двійковій запису, наприклад,прості числа Ферма 17, 257, або 65 537.
   - Число e називається відкритою експонентою (англ. public exponent)
   - Час, необхідний для шифрування з використанням швидкого зведення в ступінь,пропорційно числу одиничних біт в e.
   - Занадто малі значення e, наприклад 3, потенційно можуть послабити безпеку схеми RSA.
5. Обчислюється число d, мультиплікативно зворотне до числа e по модулю.

- Число d називається секретної експонентою.
- Зазвичай, воно обчислюється за допомогою розширеного алгоритму Евкліда.

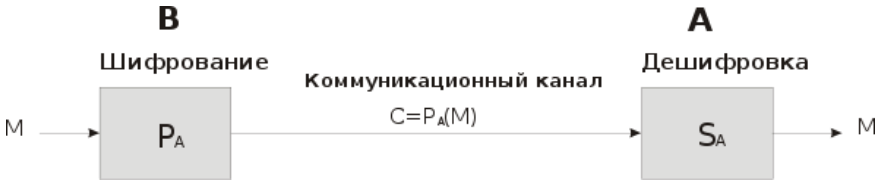
6. Пара P = (e, n) публікується в якості відкритого ключа RSA (англ. RSA public key).
7. Пара S = (d, n) відіграє роль секретного ключа RSA (англ. RSA private key) і тримається в

секреті.

Шифрування і розшифрування

Схема RSA

Припустимо, сторона хоче послати стороні повідомлення.



Цифровий підпис

Система RSA може використовуватися не тільки для шифрування, але і для цифрового підпису. Припустимо, що стороні потрібно відправити стороні відповідь, підтверджений цифровим підписом.

Алгоритм:

• Взяти відкритий текст

• Створити цифровий підпис за допомогою свого таємного ключа

• Надіслати пару, що складається з повідомлення і

підпису.Алгоритм:

• Прийняти пару

• Взяти відкритий ключ боку

• Перевірити справжність підпису:

Оскільки цифровий підпис забезпечує як аутентифікацію автора повідомлення, так і підтвердження цілісності вмісту підписаного повідомлення, вона служить аналогом підпису, зробленого від руки в кінці рукописного документа.

Важлива властивість цифрового підпису полягає в тому, що її може перевірити кожен, хто має доступ до відкритого ключа її автора. Один з учасників обміну повідомленнями після перевірки справжності цифрового підпису може передати підписане повідомлення ще комусь, хто теж в змозі перевірити цю підпис. Наприклад, сторона може переслати стороні електронний чек. Після того як сторона перевірить підпис боку на чеку, вона може передати його у свій банк, службовці якого також мають можливість перевірити підпис і здійснити відповідну грошову операцію.

Зауважимо, що підписане повідомлення не зашифровано. Воно пересилається в початковому вигляді і його вміст не захищене. Шляхом спільного застосування представлених вище схем шифрування і цифрового підпису в системі RSA можна створювати повідомлення, які будуть і зашифровані, і містити цифровий підпис. Для цього автор спочатку повинен додати до повідомлення свою цифровий підпис, а потім - зашифрувати вийшла в результаті пару (що складається з самого повідомлення і підписи до нього) за допомогою відкритого ключа належить одержувачу. Одержувач розшифровує отримане повідомлення за допомогою свого таємного ключа. Якщо проводити аналогію з пересилкою звичайних паперових документів, то цей процес схожий на те, як якщо б автор документа поставив під ним свій друк, а потім поклав його в паперовий конверт і запечатав, з тим щоб конверт був роздрукований лише тією

людиною, кому адресоване повідомлення.

Швидкість роботи алгоритму RSA

Оскільки генерація ключів відбувається значно рідше операцій, що реалізують шифрування, розшифрування, а також створення та перевірку цифрового підпису, задача обчислення представляє основну обчислювальну складність. Ця задача може бути вирішена за допомогою алгоритму швидкого зведення в ступінь. Таким чином для обчислення потрібно операцій множення по модулю.

Щоб проаналізувати час виконання операцій з відкритими і секретними ключами, припустимо, що відкритий ключ і секретний ключ задовольняють співвідношенням. Тоді в процесахїх застосування виконаються відповідно і множень по модулю.

Таким чином час виконання операцій зростає зі збільшенням кількості ненульових бітів у двійковому поданні відкритої експоненти e. Щоб збільшити швидкість шифрування, значення e часто вибирають рівним 17, 257 або 65 537 - простим числам, двійкове подання яких містить лише дві одиниці: 17 = 0x11, 257 = 0x101, 65537 = 0x10001 (прості числа Ферма).

За евристичним оцінками довжина секретної експоненти d, нетривіальним чином залежноювід відкритої експоненти e і модуля n, з великою ймовірністю близькою до довжини n. Томурозшифрування даних йде повільніше ніж шифрування, а перевірка підпису швидше ніж підписання. Алгоритм RSA набагато повільніше ніж DES і інші алгоритми блокового шифрування. Програмна реалізація DES працює швидше, принаймні, в 100 разів і від 1000 до 10 000 - в апаратнійреалізації (в залежності від конкретного пристрою). [Джерело не вказано 300 днів]

Криптоаналіз RSA

На 2009 рік система шифрування на основі RSA вважається надійною, починаючи з розмірув 1024 біта.

Групі вчених з Швейцарії, Японії, Франції, Нідерландів, Німеччини та США вдалося успішно вирахувати дані, зашифровані за допомогою криптографічного ключа стандарту RSA довжиною 768 біт. [6] За словами дослідників, після їх роботи в якості надійної системи шифрування можна розглядати тільки RSA- ключі довжиною 1024 біта і більше. Причому від шифрування ключем довжиною в 1024 біт варто відмовитися в найближчі три-чотири роки.

Як випливає з опису роботи, обчислення значень ключа здійснювалося загальним методом решета числового поля.

На перший крок (вибір пари поліномів ступеня 6 і 1) було витрачено близько півроку обчислень на 80 процесорах, що склало близько 3% часу, витраченого на головний етап алгоритму (просіювання), який виконувався на сотнях комп'ютерів протягом майже двох років. Якщо інтерполювати цей час на роботу одного процесора AMD Opteron 2.2ГГц з 2Гб пам'яті, то вийшло б близько 1500 років. Обробка даних після просіювання для наступного ресурсоемкого кроку (лінійної алгебри) знадобилося кілька тижнів на малій кількості процесорів. Заключний крок після знаходження нетривіальних рішень ослу зайняв не більше 12 годин.

Рішення ослу проводилося за допомогою методу Відемана на декількох роздільних кластерах і тривало трохи менше 4 місяців. При цьому розмір розрідженої

матриці склав 192 796 550х192 795 550 за наявності 27795115920 ненульових елементів (тобто в середньому 144 ненульових елементів на рядок). Для зберігання матриці на жорсткому диску знадобилося близько 105 гігабайт. У той же час знадобилося близько 5 терабайт стиснених даних для побудови даної матриці.

У підсумку групі вдалося обчислити 232-цифровий ключ, що відкриває доступ до зашифрованих даних.

Дослідники впевнені, що використовуючи їх метод факторизації, зламати 1024-бітний RSA- ключ буде можливо протягом наступної декади.

Елементарні атаки

Розглянемо кілька атак пов'язаних з неправильним використанням алгоритму RSA.

Генерація простих чисел

На випадкові прості числа і накладаються наступні додаткові обмеження:

• і не повинні бути занадто близькі один до одного, інакше можна буде їх знайти, використовуючи метод факторизації Ферма. Однак, якщо обидва простих числа і були згенеровані незалежно, то це обмеження з величезною ймовірністю автоматично виконується.

• Необхідно вибирати «сильні» прості числа, щоб не можна було скористатися p-1 методом Полларда.

Схема із загальним модулем n

Початкові дані: Щоб уникнути генерування різних модулів для кожного користувача, захищений сервер використовує єдиний n для шифрування всіх повідомлень. Сторона використовує цей сервер для отримання повідомлення

Завдання: противник хоче розшифрувати повідомлення сторони.

Здавалося б, шифротекст відправлений стороні, не може бути розшифрований стороною, якщо вона не володіє секретним ключем. Однак сторона може використовувати свої експоненти, щоб розкласти модуль, і після цього, знаючи, обчислити секретну експоненту.

Захист: для кожного користувача повинен використовуватися свій модуль.

Атака на підпис RSA в схемі з нотаріусом

Початкові дані: - відкритий ключ нотаріуса. Противник отримує відмову при спробіпідписання нотаріусом повідомлення

Завдання: противник хоче отримати підпис нотаріуса на повідомленні.

Противник вибирає довільне обчислює і відправляє це повідомлення на підпис нотаріуса.

Якщо нотаріус підписує це повідомлення, то противник, обчисливши, отримує підписповідомлення.

Захист: при підпису додавати в повідомлення деяке випадкове число (наприклад, час).

Малі значення секретної експоненти

Початкові дані: Щоб збільшити швидкість розшифрування (або створення цифрового підпису) було зменшено кількість ненульових бітів двійкового представлення секретної експоненти (див. швидкість алгоритму RSA).

Завдання: обчислити секретну експоненту.

У 1990 році Міхаель Вінер (Michael J. Wiener) показав, що в разі малого

значення d можливий злом системи RSA.

Захист: Таким чином якщо n має розмір 1024 біта, необхідно щоб d був не менше 256 біт довжиною.

Малі значення відкритої експоненти

Щоб збільшити швидкість шифрування та перевірки цифрового підпису, використовують малі значення відкритої експоненти. Найменша з них. Однак, щоб підвищити криптостійкість алгоритму RSA, рекомендовано використовувати.

Лекція 8. PGP

Як діє PGP

PGP поєднує в собі кращі сторони симетричної криптографії і криптографії з відкритим ключем. PGP - це гібридна криптосистема.

Коли користувач зашифровує дані за допомогою PGP, програма для початку їх стискає. Стиснення скорочує час модемного передачі і заощаджує дисковий простір, а також, що більш важливо, підвищує криптографічну стійкість. Більшість криптоаналітичних технік засноване на статистичному аналізі шифртексту в пошуках ознак відкритого тексту. Стиснення зменшує число таких ознак (знижує надмірність даних), чим суттєво посилює опірність криптоаналізу. (Занадто короткі файли і файли, які не стискаються досить добре, не стискуються зовсім.)

Потім, PGP створює сеансовий ключ, тобто одноразовий симетричний ключ, застосовуваний тільки для однієї операції. Цей сеансовий ключ являє собою псевдовипадкове число, згенероване від випадкових рухів мишки і натискань клавіш. Сеансовий ключ працює на основі дуже надійного, швидкого симетричного алгоритму, яким PGP зашифровує стиснуте повідомлення; в результаті виходить шифртексту. Як тільки дані зашифровані, сеансовий ключ також шифрується, але уже

відкритим ключем одержувача. Цей зашифрований відкритим ключем сеансовий ключ прикріплюється до шифртексту і передається разом з ним одержувачеві.

Розшифрування відбувається в зворотному порядку. PGP одержувача використовує його закритий ключ для витягу сеансового ключа з повідомлення, яким шифртексту вихідного послання відновлюється у відкритий текст.

Таким чином, комбінація цих двох криптографічних методів поєднує зручність шифрування відкритим ключем зі швидкістю роботи симетричного алгоритму. Симетричне шифрування в тисячі разів швидше асиметричного. Шифрування відкритим ключем, в свою чергу, надає просте рішення проблеми управління ключами і передачі даних. Використовувані разом, швидкість виконання і керування ключами взаємно доповнюються і поліпшуються без якого-небудь збитку безпеки.

Ключі

Ключ - це деяка величина, яка, працюючи в поєднанні з криптоалгоритмом, виробляє певний шифртексту. Ключі, як правило, - це дуже-дуже-дуже великі числа. Розмір ключа виміряється в бітах; число, яке представляє 2048-бітовий ключ, з біса велика. У асиметричної криптографії, чим більше ключ, тим захищеності отриманий шифртексту.

Однак, розмір асиметричного ключа і розмір симетричного таємного ключа, абсолютно непорівнянні. Симетричний 80-бітовий ключ еквівалентний у стійкості 1024-бітовому відкритому ключу. Симетричний 128-бітовий ключ приблизно дорівнює 3000-бітовому відкритого. Знову ж таки, більше ключ - вище надійність, але механізми, що лежать в основі кожного з типів криптографії абсолютно різні, і порівнювати їх ключі в абсолютних величинах неприпустимо.

Незважаючи на те, що ключова пара математично зв'язана, практично неможливо з відкритого вирахувати закритий; в той же час, обчислення закритого ключа завжди залишається можливим, якщо розпорядженні достатній час і обчислювальними потужностями. Ось чому критично важливо створювати ключ вірною довжини: досить великий, щоб був надійним, але досить малий, щоб залишався швидким в роботі. Для цього подумайте і оцініть, хто може спробувати
«прочитати ваші файли», наскільки вони можуть бути наполегливі, скільком часом розташовують, які їхні ресурси.

Більш великі ключі будуть криптографічно захищені більший проміжок часу. Якщо те, що ви хочете зашифрувати, повинно зберігатися в таємниці багато-багато років, вам, можливо, варто скористатися дуже великим ключем. Хто знає, скільки буде потрібно часу, щоб розкрити ваш ключ, використовуючи завтрашні більш швидкі, більш ефективні комп'ютери? Був час, коли 56-бітовий симетричний ключ DES вважався вкрай надійним.

За сучасними уявленнями 128-бітові симетричні ключі абсолютно надійні і не схильні злому, принаймні до тих пір, поки хтось не побудує функціонуючий квантовий суперкомп'ютер. 256-бітові ключі за оцінками криптологів не можуть бути зламані навіть теоретично і навіть на гіпотетичному квантовому комп'ютері. Саме з цієї причини алгоритм AES підтримує ключі довжиною 128 і 256 біт. Однак історія вчить нас тому, що всі ці запевнення через пару десятиліть можуть виявитися порожнім базіканням.

PGP зберігає ключі в зашифрованому вигляді. Вони містяться в двох файлах на жорсткому диску; один файл для відкритих ключів, інший - для закритих. Ці файли називаються зв'язками (keyrings). Використовуючи PGP, ви, час від часу, будете додавати відкриті ключі своїх кореспондентів на в'язку відкритих. Ваші закриті ключі знаходяться на зв'язці закритих. Якщо ви втратите (видаліть) в'язку закритих ключів,

то вже ніяким чином не зможете розшифрувати інформацію, зашифровану для ключів з цієї зв'язки. Отже, збереження пари резервних копій цього файлу є корисною практикою.

Цифрові підписи

Додаткова перевага від використання криптосистем з відкритим ключем полягає в тому, що вони надають можливість створення електронних цифрових підписів (ЕЦП). Цифровий підпис дозволяє одержувачеві повідомлення переконатися в автентичності джерела інформації (іншими словами, в тому, хто є автором інформації), а також перевірити, чи була інформація змінена (перекручена), поки знаходилася в шляху. Таким чином, цифровий підпис є засобом авторизації і контролю цілісності даних. Крім того, ЕЦП несе принцип неотреченія, який означає, що відправник

не може відмовитися від від факту свого авторства підписаної ним інформації. Ці можливості настільки ж важливі для криптографії, як і таємність.

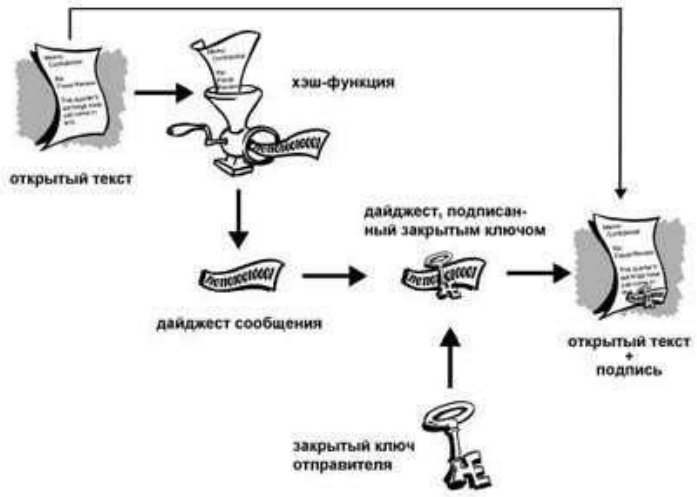
ЕЦП служить тієї ж мети, що печатка або власноручний автограф на паперовому аркуші. Однак внаслідок своєї цифрової природи ЕЦП перевершує ручну підпис і печатку в ряді дуже важливих аспектів. Цифровий підпис не тільки підтверджує особистість підписала, але також допомагає визначити, чи було зміст підписаної інформації змінений. Власноручний підпис і печатка не володіють подібним якістю, крім того, їх набагато легше підробити. У той же час, ЕЦП аналогічна фізичної печатки в тому плані, що, як печатка може бути проставлена будь-якою людиною, що отримав в розпорядження печатку, так і цифровий підпис може бути сгенерирована ким завгодно з копією потрібного закритого ключа 4.

Деякі люди використовують цифровий підпис набагато частіше шифрування. Наприклад, ви можете не хвилюватися, якщо хтось дізнається, що ви тільки що помістили $ 1000 на свій банківський рахунок, але ви повинні бути абсолютно впевнені, що виробляли транзакцію через банківського касира.

Простий спосіб генерації цифрових підписів показаний на малюнку 6. Замість зашифрування інформації чужим відкритим ключем, ви шифруєте її своїм власним закритим. Якщо інформація може бути розшифрована вашим відкритим ключем, значить її джерелом є ви.

Хеш-функція

Однак описана вище схема має ряд істотних недоліків. Вона вкрай повільна і робить занадто великий обсяг даних - щонайменше вдвічі більше обсягу вихідної інформації. Поліпшенням такої схеми стає введення в процес перетворення нового компонента - однобічної хеш-функції. Одностороння хеш-функція бере введення довільної довжини, називаний прообразом, - у даному випадку, повідомлення будь-якого розміру, хоч тисячі або мільйони біт - і генерує строго залежний від прообразу висновок фіксованої довжини, допустимо, 160 біт.



Хеш-функція гарантує, що якщо інформація буде будь-яким чином змінена - навіть на один біт, - у результаті вийде зовсім інше хеш-значення.

У процесі цифрового підписання PGP обробляє повідомлення криптографічно стійким однобічним хеш-алгоритмом. Ця операція приводить до генерації рядка обмеженої довжини, називаної дайджестом повідомлення (message digest) 5. (Знову ж, будь-яка зміна прообразу призведе до абсолютно іншому дайджесту.)

Потім PGP зашифровує отриманий дайджест закритим ключем відправника, створюючи

«електронний підпис», і прикріплює її до прообразу. PGP передає ЕЦП разом з вихідним повідомленням. По отриманні повідомлення, адресат за допомогою PGP заново обчислює дайджест підписаних даних, розшифровує ЕЦП відкритим ключем відправника, тим самим звіряючи, відповідно, цілісність даних і їх джерело; якщо обчислений адресатом і отриманий з повідомленням дайджести збігаються, значить інформація після підписання не була змінена. PGP може як зашифрувати саме підписується повідомлення, так і не робити цього; підписання відкритого тексту без зашифрування корисно в тому випадку, якщо хто-небудь з одержувачів не зацікавлений або не має можливості звірити підпис (допустимо, не має PGP).

Якщо в механізмі формування ЕЦП застосовується стійка однобічна хеш-функція, немає ніякого способу взяти чиюсь підпис з одного документа і прикріпити її до іншого, або ж будь-яким чином змінити підписане повідомлення. Найменша зміна в підписаному документі буде виявлено в процесі звірки ЕЦП.

ЕЦП відіграють найважливішу роль в посвідченні і завіренні ключів інших користувачів

PGP

.

Цифрові сертифікати

Одна з головних проблем асиметричних криптосистем полягає в тому, що користувачі повинні постійно стежити, зашифровують чи вони повідомлення істинними ключами своїх кореспондентів. У середовищі вільного обміну відкритими

ключами через громадські сервери- депозитарії атаки за принципом «людина в середині» представляють серйозну потенційну загрозу. У цьому виді атак зловмисник підсовує користувачеві підроблений ключ з ім'ям передбачуваного адресата; дані зашифровуються підставним ключем, перехоплюються його власником-зловмисником, потрапляючи в підсумку в чужі руки.

У середовищі криптосистем з відкритим ключем критично важливо, щоб ви були абсолютно впевнені, що відкритий ключ, яким збираєтеся щось зашифрувати - не майстерна імітація, а

справжня власність вашого кореспондента. Можна просто шифрувати тільки тими
ключами, які були передані вам їх власниками з рук в руки на дискетах. Але припустимо, що потрібно зв'язатися з людиною, що живуть на іншому краю світу, з яким ви навіть незнайомі; як ви можете бути впевнені, що отримали його справжній ключ?

Цифрові сертифікати ключів спрощують завдання визначення приналежності відкритих ключів передбачуваним власникам.

Сертифікат є форма посвідчення. Інші види посвідчень включають ваші водійські права, державний паспорт, свідоцтво про народження, і т.п. Кожне з них несе на собі деяку ідентифікує вас інформацію і певний запис, що хтось інший (держструктура, приватна особа) встановив вашу особу. Деякі сертифікати, такі як паспорт, - самодостатнє підтвердження вашої особистості; буде досить кепсько, якщо хтось украде його, щоб видати себе за вас.

Цифровий сертифікат у своєму призначенні аналогічний фізичному. Цифровий сертифікат ключа - це інформація, прикріплена до відкритого ключа користувача, що допомагає іншим встановити, чи є ключ справжнім і вірним. Цифрові сертифікати потрібні для того, щоб зробити неможливою спробу видати ключ однієї людини за ключ іншого.

Цифровий сертифікат складається з трьох компонентів:

• відкритого ключа, до якого він прикладений;

• даних, або записів, сертифіката (відомості про особу користувача, як то, ім'я, електроннапошта і т.п., а також, за необхідності, додаткові відомості: права допуску, робочі ліміти та інше);

• однієї або декількох цифрових підписів, «зв'язують» ключ із сертифікатом.

Мета ЕЦП на сертифікаті - вказати, що відомості сертифіката були завірені довіреною третьою особою чи організацією. У той же час цифровий підпис не підтверджує достовірність сертифіката як цілого; вона є поручительством тільки того, що підписана запис сертифіката (ідентифікує інформація) пов'язані з даним відкритим ключем.

Таким чином, сертифікат, звичайно, - це відкритий ключ з прикріпленими до нього однією або декількома формами ID плюс відмітка підтвердження від довіреної особи, «зв'язує» ID і відкритий ключ.

Поширення сертифікатів

Сертифікати застосовуються, коли потрібно обмінятися з ким-небудь ключами. Невеликим групам людей, що потребують захищеного зв'язку, не складе труднощів просто передати один одному дискети або відправити електронні листи, що містять копії їх ключів.

Це - ручне поширення відкритих ключів, і воно ефективне тільки до певного

етапу. Подальше - за межами можливостей даного методу, і тоді виникає необхідність розгортання системи, яка б забезпечувала достатню надійність і безпеку, надавала можливості зберігання і обміну ключами, так що колеги, бізнес-партнери або незнайомці змогли б відправляти один одному зашифровані повідомлення, якщо в тому виникне необхідність.

Така система може реалізуватися у формі простого сховища-депозитарію, званого сервером сертифікатів, або сервером-депозитарієм відкритих ключів, або мати складнішу і комплексну структуру, яка передбачає додаткові можливості адміністрування ключів, і звану інфраструктурою відкритих ключів (Public Key Infrastructure, PKI).

Сервери-депозитарії

Сервер-депозитарій, також званий сервером сертифікатів, або сервером ключів, - цемережева база даних, що дозволяє користувачам залишати і витягати з неї цифрові сертифікати.

Сервер ключів також може мати деякі функції адміністрування, допомагають організації підтримувати свою політику безпеки. Наприклад, на зберігання можуть залишати тільки ключі, щозадовольняють певним критеріям.

Інфраструктури відкритих ключів (PKI)

PKI, як і простий сервер-депозитарій, має базу даних для зберігання сертифікатів, але, в той же час, надає сервіси і протоколи з управління відкритими ключами. У них входять можливості випуску (видання), відкликання (анулювання) і системи довіри сертифікатів. Головною ж особливістю PKI є наявність компонентів, відомих як Центр сертифікації (Certification Authority, CA) і Центр реєстрації (Registration Authority, RA).

Центр сертифікації (ЦС) видає цифрові сертифікати і підписує їх своїм закритим ключем. Через важливості своєї ролі, ЦС є головним компонентом інфраструктури PKI. Використовуючи відкритий ключ ЦС, будь-який користувач, що бажає перевірити справжність конкретного сертифіката, звіряє підпис Центру сертифікації і, отже, засвідчується в цілісності міститься в сертифікаті інформації і, що більш важливо, під взаімосвязності відомостей сертифіката і відкритого ключа.

Як правило, Центром реєстрації (ЦР) називається система людей, механізмів і процесів, службовець цілям зарахування нових користувачів в структуру PKI і подальшого адміністрування постійних користувачів системи. Також ЦР може виробляти «Веттінген» - процедуру перевірки того,чи належить конкретний відкритий ключ передбачуваному власникові.

ЦР - це людське співтовариство: особа, група, департамент, компанія або інша асоціація. З іншого боку, ЦС - зазвичай, програма, що видає сертифікати своїм зареєстрованим користувачам. Існують і захищені від злому апаратні реалізації ЦС, споруджені з куленепробивних матеріалів і забезпечені «червоною кнопкою», анулюється в критичній ситуації всі видані ключі.

Роль ЦР-ЦС аналогічна тій, що виконує державний паспортний відділ: одні його співробітники перевіряють, чи потрібне видача паспорта (робота ЦР), а інші виготовляють самдокумент і передають його власнику (робота ЦС). Наявність ЦР для ЦС не обов'язково, але воно забезпечує поділ функцій, яке іноді необхідно.

Формат сертифікатів

Цифровий сертифікат - це набір ідентифікуючих відомостей, пов'язаних з відкритим ключем і підписаних довіреною третьою особою, щоб довести їх достовірність і взаімосвязность. Сертифікат може бути представлений безліччю різних форматів.

PGP підтримує два формати сертифікатів:

• Сертифікати OpenPGP (частіше звані просто ключами PGP)

• Сертифікати X.509

Формат сертифіката

PGP

Сертифікат PGP містить, зокрема, такі відомості:

• Відкритий ключ власника сертифіката - відкрита частина ключової пари і її алгоритм: RSAv4, RSA Legacy v3, DH або DSA.

• Відомості про власника сертифіката - інформація, що ідентифікує особу користувача: йогоім'я, адресу електронної пошти, номер ICQ, фотографія і т.д.

• ЕЦП власника сертифіката - підпис ключової пари, пов'язаної з сертифікатом (т.зв.автоподпісь).

• Період дії сертифіката - дата початку дії сертифіката та дата закінчення його дії;

вказує на те, коли сертифікат стане недійсним (аналогічно терміну дії водійських прав). Якщо ключова пара містить додаткові підключи шифрування, то тут буде зазначено період дії кожного з них.

• Бажаний алгоритм шифрування - вказує на те, зашифровану яким алгоритмом інформацію воліє одержувати власник сертифіката. Підтримуються наступні: CAST, AES, IDEA, Triple-DES і Twofish.

Ви можете уявити сертифікат PGP у вигляді відкритого ключа з однією або декількома прив'язаними до нього «бирками» (рис. 9). На цих «бирках» вказана інформація, що ідентифікує власника ключа, а також підпис цього ключа, що підтверджує, що ключ і ідентифікаційні відомості взаємопов'язані. (Цей вид підпису називається автопідпису (self-signature); її містить кожен PGP- сертифікат.)

Унікальний аспект формату сертифікатів PGP в тому, що кожен сертифікат може містити безліч підписів. Будь-яка людина може підписати ідентифікаційний-ключову пару, щоб запевнити, покладаючись на своє особисте переконання, що відкритий ключ належить саме зазначеному в ID користувачеві. Якщо пошукайте на громадських серверах-депозитаріях, то можете виявити деякі ключі, як, наприклад, належить автору PGP Філу Ціммерманн, що містять величезну кількість підписів.

Деякі PGP-сертифікати складаються з відкритого ключа з декількома «бирками», кожна з яких містить власні відомості, що ідентифікують власника ключа (наприклад, ім'я власника і його робочий e-mail, прізвисько власника і його домашній e-mail, фотографія власника - все на одному сертифікаті). Список підписів на кожній з «бирок» може бути різним; підписи вказують на достовірність певної «бирки» і її приналежність відкритого ключа, а не на те, що всі «бирки» достовірні. (Зауважте, що «достовірність» залежить від встановив її: підписи - це думки, і різні люди приділяють різний ступінь уваги перевірці справжності перед підписанням ключа.)

Формат сертифіката X.509

X.509 - це інший дуже поширений формат. Всі сертифікати X.509 відповідають міжнародному стандарту ITU-T X.509; таким чином (теоретично), сертифікат X.509, створений для однієї програми, може бути використаний в будь-якому іншому, що підтримує цей стандарт. На практиці, однак, склалася ситуація, що різні компанії створюють власні розширення для X.509, не всіз яких між собою сумісні.

Всякий сертифікат вимагає, щоб хтось запевнив взаімосвязность відкритого ключа й ідентифікує власника ключа інформації. Маючи справу з PGP-сертифікатом, кожен може виступати в якості завірителя містяться в ньому відомостей (за винятком випадків, коли ця можливість навмисно обмежена політикою безпеки). Але в разі сертифікатів X.509 завірителя може бути тільки Центр сертифікації або хтось, спеціально уповноважений їм на цю роль. (Майте на увазі, що PGP- сертифікати також

в повній мірі підтримують ієрархічне структурування системи довіри, що використовує ЦС для посвідчення сертифікатів.)

Сертифікат X.509 - це набір стандартних полів, що містять відомості про користувача або пристрою, та їх відповідний відкритий ключ. Стардарт X.509 визначає, які відомості входять усертифікат і як вони кодуються (формат даних).

Сертифікат X.509 містить такі відомості:

• Версія X.509 - вказує, на основі якої версії стандарту X.509 побудований даний сертифікат, що визначає, яка інформація може в ньому міститися.

• Відкритий ключ власника сертифіката - відкритий ключ поряд з ідентифікатором використовуваного алгоритму (криптосистему, до якої належить даний ключ) та інша інформаціяпро параметри ключа.

• Серійний номер сертифікату - організація-видавець сертифіката зобов'язана присвоїти йому унікальний серійним (порядковий) номер для його впізнання серед інших сертифікатів, виданих даною організацією. Ця інформація застосовується в ряді випадків; наприклад, при анулюванні сертифіката, його серійний номер поміщається в реєстр анульованих сертифікатів (Certificate Revocation List, CRL).

• Унікальний опізнавач власника ключа (або DN, distinguished name - унікальне ім'я) - це ім'я має бути унікальним і єдиним у всьому Інтернеті. DN складається з декількох підпунктів і може виглядати приблизно так:

CN = Bob Davis, EMAIL = bdavis@pgp.com, OU = PGP Engineering,

O = PGP Corporation, C = US

(Що позначає Ясна ім'я суб'єкта, Електронну пошту, Підрозділ організації, органіції і Країну відповідно.)

• Період дії сертифіката - дата початку дії сертифіката та дата закінчення його дії; вказує на те, коли сертифікат стане недійсний.

• Унікальне ім'я видавця - унікальне ім'я організації, що підписала сертифікат. Зазвичай, це найменування Центру сертифікації. Використання сертифіката увазі довіру організації, його підписала. (У випадках з кореневими сертифікатами видала організація - цей же ЦС - підписує його сама.)

• ЕЦП видавця - електронний підпис, створена закритим ключем організації, що видаласертифікат.

• Ідентифікатор алгоритму підпису - вказує алгоритм, використаний ЦС для підписаннясертифіката.

Існує ряд фундаментальних відмінностей між форматами сертифікатів X.509 і PGP:

• ви можете особисто створити власний сертифікат PGP; ви повинні запросити й одержатисертифікат X.509 від Центру сертифікації;

• сертифікати X.509 містять тільки одне ім'я власника сертифіката;

• сертифікати X.509 містять тільки одну ЕЦП, що підтверджує дійсність сертифіката.

Щоб отримати сертифікат X.509, ви повинні попросити ЦС видати його вам. Ви надаєте системі свій відкритий ключ, ніж доводите, що володієте відповідним закритим, а також деякі ідентифікуючі вас відомості. Потім ви електронно підписуєте ці відомості і відправляєте весь пакет - запит сертифіката - в Центр сертифікації. ЦС виконує певний процес перевірки автентичності наданої інформації та, якщо все сходиться, створює сертифікат, підписує і повертає вам.

Ви можете уявити сертифікат X.509, як звичайний паперовий сертифікат або атестат з приклеєним до нього відкритим ключем. На ньому зазначено ваше ім'я, а

також деякі відомості про вас, плюс підпис видавця сертифіката.

Ймовірно, найбільша користь від сертифікатів X.509, це їхнє застосування в Веб-браузерах.

Справжність і довіра

Будь-який користувач в середовищі криптосистем з відкритим ключем ризикує рано чи пізно прийняти підроблений ключ (сертифікат) за справжній. Достовірність (справжність) є переконаність у тому, що конкретний відкритий ключ належить передбачуваному власникові, чия ідентифікаційна

інформація вказана в сертифікаті ключа. Справжність є одним з найважливіших критеріїв
в середовищі системи відкритих ключів, де ви повинні визначати автентичність кожного конкретного сертифіката.

Переконавшись, що чужий відкритий ключ достовірний (тобто дійсно належить саме передбачуваному власникові), ви можете підписати копію цього ключа на своїй зв'язці, ніж засвідчите факт, що ви його перевірили і знайшли достовірним. Якщо захочете, щоб інші знали вашу ступінь довіри до сертифіката, ви можете експортувати свою підтверджуючу підпис на сервер- депозитарій з тим, щоб інші могли її бачити і могли на неї покластися при визначенні достовірності цього ключа.

Як було описано в параграфі «Інфраструктури відкритих ключів (PKIs)», деякі компанії уповноважують один або кілька Центрів сертифікації (ЦС) на перевірку достовірності сертифікатів. В організації, що використовує PKI з сертифікатами X.509, завдання Центрів реєстрації полягає в прийомі запитів на сертифікати, а завдання Центрів сертифікації - у видачі сертифікатів кінцевим користувачам: процес відповіді на запит користувача на отримання сертифікату. В організації, що використовує сертифікати PGP без PKI, завдання ЦС - в перевірці достовірності всіх PGP-сертифікатів і підписанні справжніх.

Перевірка справжності

Один із способів визначення справжності сертифіката - деяка механічна процедура. Існує кілька методик її проведення. Наприклад, ви можете попросити свого кореспондента передати копію його відкритого ключа «фізично», тобто вручити на жорсткому носії - магнітному або оптичному диску і т.п. Але найчастіше це буває незручно і неефективно.

Інший варіант - звірити відбиток (fingerprints) сертифіката. Наскільки унікальні відбитки пальців людей, настільки ж унікальні і відбитки кожного сертифіката PGP. Відбиток - це хеш- значення сертифікату користувача, яке показано як одна з його властивостей. У PGP відбиток може бути представлений або як шістнадцяткове число, або як набір т.зв. біометричних слів, фонетично чітких і застосовуваних для спрощення вербальної ідентифікації відбитка.

Ви можете визначити справжність сертифікату зателефонувавши власнику ключа (таким чином, що ви почнете комунікацію) і попросивши його прочитати відбиток з його ключа; вам же потрібно звірити цей відбиток проти того, який перебуває на отриманій вами копії. Такий спосіб допустимий, якщо вам знайомий голос кореспондента, але як ви встановите особистість того, з ким навіть незнайомі? Деякі з цією метою поміщають відбитки ключів на свої візитні картки.

Ще один метод визначення автентичності чужого сертифікату - покластися на думку третьої сторони, вже встановила його справжність.

ЦС, наприклад, відповідально за детальну перевірку належності відкритого

ключа передбачуваному власникові перед видачею йому сертифіката. Будь-який користувач, що довіряє ЦС, буде автоматично розцінювати справжніми всі сертифікати, підписані ЦС.

Паралельний аспект перевірки автентичності і достовірності полягає в тому, щоб переконатися, що сертифікат не був анульований (відкликаний). За додатковою інформацією з цього питання звертайтеся до параграфу «Анулювання сертифіката».

Встановлення довіри

Ви самі засвідчуєте сертифікати. Але ви також довіряєте людям. Тому ви можете довірити людям і право засвідчувати сертифікати. Як правило, якщо тільки власник сам не вручив вам копію ключа, ви повинні покластися на чиєсь чуже думка про його справжності.

Мета-поручителі і довірені поручителі

У більшості випадків користувачі повністю покладаються на ЦС в перевірці достовірності сертифікатів. Іншими словами, користувачі переконані, що ЦС провів всю механічну процедуру перевірки за них, і впевнені в його поручительства за достовірність засвідчених ним сертифікатів. Така схема працює тільки до певної межі в кількості користувачів PKI, перейшовши який ЦС не зможе дотримуватися колишнього рівня ретельності процедури перевірки. У цьому випадку стає необхідним додавання в систему додаткових «поручителів».

ЦС також може бути мета-поручителем (мета-представником). Мета-поручитель не тільки сам запевняє ключі, але надає й іншим особам (організаціям) повноваження запевнення. За аналогією з тим, як король передає свою особисту печатку або факсиміле наближеним радникам, щоб ті могли діяти від його імені, так і мета-поручитель уповноважує інших діяти в якості довірених поручителів (довірених представників). Ці довірені поручителі можуть засвідчувати ключі з тим же результатом, що і мета-поручитель. Однак, вони не можуть створювати нових довірених поручителів.

«Мета-поручитель» та «довірений поручитель» - це терміни PGP. У середовищі X.509 мета- поручитель називається кореневим Центром сертифікації (root CA), а довірені поручителі - підлеглими, або проміжними, Центрами сертифікації (subordinate CAs, intermediate CAs).

Кореневий ЦС для підписання ключів використовує закритий ключ, пов'язаний з особливим типом сертифіката, званим кореневим сертифікатом ЦС. Будь сертифікат, підписаний кореневим ключем ЦС, стає достовірним будь-якому іншому сертифікату, підписаного кореневим. Такий процес посвідчення діє навіть для сертифікатів, підписаних іншим ЦС в [пов'язаної] системі - якщо ключ проміжного ЦС підписаний ключем кореневого ЦС, будь-який сертифікат підписаний першим розцінюється вірним в межах ієрархії. Цей процес відстеження вздовж гілок ієрархії того, хто підписав які сертифікати, називається відстеженням шляху, або ланцюга, сертифікатів.

Моделі відносин довіри

У відносно закритих системах, таких як невеликі організації і фірми, можна без праці відстежити шлях сертифіката назад до кореневого ЦС. Однак, користувачам часто доводиться зв'язуватися з людьми за межами їх корпоративної середовища, включаючи і таких, з якими вони раніше ніколи не зустрічалися, наприклад, з постачальниками, споживачами, клієнтами та ін Встановлення лінії довіри з тими, хто не був явно посвідчений ЦС, стає непростим завданням.

Організації слідують одній з декількох моделей відносин довіри, які диктують користувачам їх дії за визначенням достовірності сертифікатів. Існують три різні моделі:

• Пряме довіру

• Ієрархічне довіру

• Мережа довіри (Web of

Trust)Пряма довіра

Пряме довіра - це найпростіша з моделей відносин довіри. У цій схемі користувач переконаний, що ключ справжній, оскільки точно знає, від кого отримав цей ключ. Всі криптосистеми в тій чи іншій мірі використовують цю форму довіри. Наприклад, у веб-браузерах кореневі ключі Центрів сертифікації довіряються безпосередньо, тому що знаходилися в дистрибутиві даного програмного продукту. Якщо і існує який-небудь вид ієрархії, то він поширюється з цих безпосередньо довіряємо сертифікатів.

У PGP користувач, який посвідчує ключі самостійно, не вдаючись до допомоги довірених поручителів, використовує схему прямого довіри.

Ієрархічна довіра

В ієрархічній системі існує ряд кореневих сертифікатів, від яких распросраняется довіру. Ці сертифікати можуть або самі завіряти сертифікати кінцевих користувачів, або вони можуть уповноважувати інші сертифікати, які будуть завіряти сертифікати користувачів за деякою ланцюга. Уявіть, що це велике «дерево» довіри. Справжність сертифікатів-«листя» (сертифікатів кінцевих користувачів) визначається відстеженням ланцюжка до їх удостоверітелям, а від них уже до удостоверітелям цих удостоверітелей, і так до тих пір, поки не буде знайдений безпосередньо довіряють кореневий сертифікат.

Мережа довіри

Мережа довіри об'єднує обидві попередні моделі, також привносячи принцип, що довіра єпоняття суб'єктивне (що співвідноситься з життєвим поданням), та ідею про те, що чим більшеінформації, тим краще. Таким чином, це накопичувальна модель довіри. Сертифікат може бутидовіряємо безпосередньо або довіряємо за деякою ланцюжку, минаючої до напряму довіряютькореневого сертифікату (мета-поручителю), або може бути завірений групою довірених поручителів.

Можливо, вам знайоме поняття «шість ступенів поділу», що означає, що будь-який індивід може встановити деяку ланцюжок до будь-якого іншого індивіду на планеті, використовуючи шість або менше людина в якості посередників. Це - мережа представників.

Таке ж і уявлення PGP про довіру. PGP використовує цифрові підписи як власний вид поруки. Коли один користувач підписує ключ іншого, він ставати поручителем цього ключа (поручительство за достовірність ключа і його приналежність передбачуваному власникові). Цей процес, розширюючись, і утворює мережа довіри.

У середовищі PGP будь-який користувач може виступати в якості центру сертифікації. Кожен користувач може запевнити відкритий ключ іншого користувача. Однак, такий сертифікат буде розцінений справжнім іншим користувачем тільки тоді, коли останній визнає завірителя своєю довіреною поручителем. (Іншими словами, ви довіряєте мою думку про справжність інших ключів, тільки якщо вважаєте мене своїм довіреної поручителем. В іншому випадку, моя суб'єктивна оцінка достовірності чужих ключів для вас щонайменше неоднозначна.)

На зв'язці відкритих ключів кожного користувача містяться такі показники:

• чи вважає користувач певний ключ справжнім;

• рівень довіри, наданий користувачем певному ключу, з яким його власник буде виступати поручителем у справжності інших ключів.

Ви вказуєте на своїй копії мого ключа, наскільки вагомим вважаєте моя думка про справжність підписаних мною ключів. Це виключно система репутації: деякі користувачі відомі тим, що ретельно перевіряють ключі і дають гарні підписи, яким

люди довіряють як беззастережному показником автентичності.

Ступені довіри в PGP

Найвищий рівень довіри - безумовне довіру (Implicit Trust) - це довіра вашої власної ключової парі. PGP вважає, що якщо ви володієте закритим ключем, то повинні довіряти і діям соотвествующего відкритого. Всі ключі, підписані вашим безумовно довіряє, для вас вірні і справжні.

Існує три ступені довіри, які ви можете присвоїти чужому відкритому ключу:

- Повна довіра
- Часткове довіру

• Немає довіри

Щоб ще більше все заплутати, існує також три рівні достовірності:

• Дійсний

• Можливо справжній

• Невизначений

Щоб дати іншій ключу повноваження поручительства, ви:

1. Берете справжній ключ,

якийабо підписаний вами,

або іншим довіреним поручителем, і потім

2. Встановлюєте рівень довіри, якого, як вам здається, заслуговує власник.

Для прикладу уявімо, що на вашій зв'язці є ключ Аліси. Ви визначили справжність її ключа і, підписуючи його, вказуєте на це. Вам відомо, що Аліса - активний прихильник ретельної перевірки чужих ключів. Тому ви наділяє її Повним довірою, що, фактично, перетворює її в Центр сертифікації: якщо Аліса підпише чужий ключ, він буде вірним на вашій зв'язці апріорі.

PGP вимагає одну повністю довіряє або дві Частково довіряємо підписи, щоб встановити ключ як справжній. Метод PGP прирівнювання двох частково до однієї Повної аналогічний тому, як іноді від вас вимагають два види документів, що засвідчують особу. Ви можете порахувати Алісу частково надійної, також порахувати Боба частково заслуговуючим довіри. Є ризик, що кожен з них окремо може випадково підписати липовий ключ, так що ви, ймовірно, не станете надавати Повного довіри жодному. Однак, ймовірність того, що обидва вони підпишуть один і той же липовий ключ, досить мала.

Анулювання сертифіката

Застосування сертифіката допустимо тільки поки він достовірний. Небезпечно покладатися на те, що сертифікат буде захищений і надійний вічно. У більшості організацій і у всіх PKI сертифікат має обмежений термін «життя». Це звужує період, в який система може опинитися під загрозою, якщо сертифікат буде зламаний.

Таким чином, сертифікат створюється з певним заданим періодом достовірності, що починається з дати створення (аналогічно терміну придатності харчових продуктів або дії водійських прав). Сертифікат може бути використаний протягом усього періоду дії, після закінчення якого перестає бути вірним, оскільки достовірність його ідентифікаційний-ключової пари більше не може бути гарантована. (Тим не менш, сертифікат і раніше може застосовуватися для підтвердження інформації, зашифрованої або підписаної ним раніше протягом періоду життя; проте він стає непридатний для майбутніх криптографічних потреб.)

Але іноді з'являється потреба зробити сертифікат недійсним до закінчення терміну його життя, наприклад, у випадку звільнення власника сертифіката з цього

місця роботи або коли у власника виникає підозра, що закритий ключ даного сертифікату був скомпрометований. Такий процес називається відкликанням або анулюванням. Анульований сертифікат набагато більш підозрілий, ніж минулий. Минулий сертифікат більш непридатний до використання, однак, не несе такої загрози скомпрометованості, як анульований.

Будь-який користувач, який запевнив сертифікат (поручився за взаємозв’язок ключа і відомостей сертифіката), в будь-який момент може відкликати з нього свій підпис, використовуючи той же закритий ключ, яким її створював. Відкликана підпис вказує на те, що завірителя визнав, що відкритий ключ і ідентифікаційна інформація більше не зв'язані один з одним, або що відкритий

ключ сертифіката (або закритий) був скомпрометований. Відкликана підпис має практично таке ж значення, як і анульований сертифікат.

У разі сертифікатів X.509 відкликана підпис фактично являє те ж саме, що і анульований сертифікат, оскільки взагалі лише один підпис була порукою справжності сертифіката - підпис Центру сертифікації. PGP надає додаткову можливість анулювання всього сертифіката (а не тільки підписів на ньому), якщо ви раптом порахуєте, що він був якимось чином скомпрометований.

Тільки власник сертифіката (володар закритого ключа) або хтось, спеціально уповноважений власником (т.зв. «довірений отменітель», designated revoker), може анулювати PGP-сертифікат. (Довіреність третій особі функції анулювання вельми корисно, тому що втрата пароля до закритого ключа, яка часто і є приводом до анулювання, робить виконання цієї процедури самим власником сертифікату неможливою.) Сертифікат X.509 може бути відкликаний тільки його видавцем - ЦС - за запитом власника.

Повідомлення про анулювання сертифіката

Після анулювання сертифіката вкрай важливо оповістити всіх потенційних кореспондентів, що він більше недійсний. Найбільш простий спосіб оповіщення в середовищі PGP - це розміщення анульованого сертифіката на сервері-депозитарії; таким чином, всі, хто можуть вирішити зв'язатися з вами, будуть попереджені не використовувати цей відкритий ключ.

У середовищі PKI повідомлення про анулювання сертифікатів здійснюється за допомогою спеціального механізму, званого реєстром анульованих сертифікатів (Certificate Revocation List, CRL), що публікується Центром сертифікації. CRL містить датований, завірений список всіх анульованих непрострочених сертифікатів системи. Анульовані сертифікати залишаються в списку тільки до моменту свого фактичного закінчення, після чого видаляються звідти - це запобігає нескінченне розростання списку.

ЦС оновлює CRL через регулярні проміжки часу. Теоретично, це повинно звести до мінімуму ризик ненавмисного використання анульованого сертифіката. Хоча, все ж залишається ймовірність випадкового застосування скомпрометованого сертифіката в часовому проміжку між публікаціями CRL.

Що таке ключова фраза

Більшості користувачів знаком метод обмеження доступу до комп'ютера або комп'ютерних ресурсів за допомогою пароля, який являє собою унікальну послідовність символів, що вводиться як ідентифікаційний код.

Ключова фраза - це більш довгий, складний і, теоретично, більш надійний варіант пароля. Зазвичай складається з декількох слів, ключова фраза набагато

надійніше проти стандартних атак
«по словнику», в ході яких зломщик перебирає всі слова зі словника в спробі вгадати ваш пароль. Найкращі ключові фрази досить довгі і комплексні, містять як заголовні, так і рядкові букви, а також цифри, розділові знаки та інші символи.

PGP використовує ключову фразу щоб зашифрувати ваш закритий ключ. Закритий ключ зберігається на диску, зашифрований хешем-значенням ключової фрази як симетричним таємним ключем. Ви ж використовуєте ключову фразу, щоб розшифрувати і застосовувати закритий ключ. Ключова фраза повинна бути такою, щоб вам її було важко забути, а іншим - здогадатися. Вона повинна бути чимось, вже давно і надійно зберігаються в довгостроковій пам'яті вашого мозку, а не вигаданим з нуля. Чому? Тому що якщо ви забудете ключову фразу - ви у великій біді. Закритий

ключ абсолютно і зовсім марний без його ключової фрази, і з цим нічого не можна вдіяти. Пам'ятайте цитату на початку цієї глави? PGP - це криптографія, яка не дозволить урядам могутніхдержав читати ваші файли. І вже тим більше вона не дозволить читати їх вам. Врахуйте це, якщораптом вирішите змінити ключову фразу на уривок з анекдоту, який ніколи не могли толкомзапам'ятати.

Поділ ключа

Кажуть, що секрет - це вже не секрет, коли його знають дві людини. Поділ закритого ключа спростовує таку думку. Хоча це і не рекомендована практика, поділ закритого ключа в певних ситуаціях буває необхідно. Наприклад, корпоративні ключі підписання (Corporate Signing Keys, CSK)
- це особливо важливі закриті ключі, використовувані організацією, наприклад, для запевнення правових документів, особистої інформації співробітників або прес-релізів для засвідчення авторства. У даному випадку буде корисно, щоб кілька членів компанії мало доступ до закритого ключа. Але це однаково буде означати, що кожен з членів команди зможе вільно і повною мірою виступати від імені компанії.

Література

1. Jerry Honeycutt Microsoft Virtual PC 2004 Technical Overview
2. Microsoft Windows XP Professional. Учебный курс MCSA/MCSE. М.: Русская редакция, 2003. -1008 с.
13. Windows Defender: System requirements.
14. Frequently asked questions about Windows Defender.
15. Microsoft Baseline Security Analyzer.
16. Microsoft Baseline Security Analyzer (MBSA) версии 1.2.1
17. Феллинг Д. Microsoft Baseline Security Analyzer

Навчальне видання

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни

«Безпека інформаційних систем»

для здобувачів першого (бакалаврського) рівня освіти

за спеціальністю

126 «Інформаційні системи та технології

(Електронне видання)

Укладач:

Іванов Віталій Геннадійович

Оригінал-макет В. Г. Іванов

Підписано до друку__.__.202__.
Формат 60x84 1/16. Папір типогр. Гарнітура Times.
Друк офсетний. Умов. друк. арк. ___. Обл.-вид. арк.___.
Тираж ___ екз. Вид. № ___. Замов. № ____. Ціна договірна.
Видавництво Східноукраїнського національного університету
імені Володимира Даля

Свідоцтво про реєстрацію: серія ДК № 1620 від 18.12.03 р.
Адреса університету: вул. Іоанна Павла II., 17
м. Київ, 01042, Україна
e-mail: vidavnictvosnu.ua@gmail.com