

Захист інформації у комп'ютерних системах

Лабораторні роботи 2018-2019 навчальний рік

Модуль №1 «Основи інформаційної безпеки та захисту інформації»

Лабораторна робота №1.1. Дослідження систем безпеки операційних систем Windows та Linux

Мета роботи: ознайомитися з основними поняттями в галузі політик в середовищі сучасних операційних систем, основними засобами безпеки у сучасних операційних системах. Набути практичних навичок в роботі по налаштуванні політик безпеки ОС Windows.

Завдання роботи: ознайомитися з засобами безпеки, наявними у складі операційних систем Windows та Linux. Налаштувати політики безпеки ОС Windows відповідно до порядку виконання лабораторної роботи.

Аудиторний час – 4 акад. години.

Короткі теоретичні відомості

Безпека операційної системи (ОС) досягається шляхом застосування комплексу засобів та заходів, спрямованих на запобігання таких дій з боку користувача або програм, які можуть призвести до порушення нормального функціонування операційної системи. Вивчення безпеки ОС базується на теорії комп'ютерної безпеки, яка оперує трьома основними поняттями: загроза, уразливість і атака.

Короткі відомості про систему безпеки ОС Windows.

Менеджер безпеки перевіряє права доступу до об'єктів за запитами інших модулів Виконавчої системи (насамперед – Менеджера об'єктів) і генерує контрольні повідомлення. Для

отримання інформації про права та передачу контрольних повідомлень Менеджер безпеки взаємодіє з Розпорядником локальної безпеки.

Центр забезпечення безпеки Windows працює у фоновому режимі і активно контролює чотири категорії функціональності: брандмауер, автоматичні оновлення, захист від шкідливих програм (вірусів і шпигунського ПЗ), інші параметри безпеки (Інтернет і Управління обліковим записом користувача).

Брандмауером можна управління через: Панель управління \ Брандмауер Windows.

Захисник Windows (Windows Defender) – компонент, який захищає комп'ютер від шпигунського ПЗ (троянських програм). Windows Defender постійно стежить за ресурсами операційної системи, які зазвичай експлуатує шпигунське програмне забезпечення (зокрема, за реєстром і файловою системою). Windows Defender містить дев'ять агентів безпеки: автозавантаження, налаштування безпеки системи, надбудови Internet Explorer, налаштування Internet Explorer, завантаження Internet Explorer, служби і драйвери, виконання додатків.

Існує три типи перевірки в Захиснику Windows: швидке сканування, повне сканування, сканування, що налаштовується.

UAC (User Account Control) – компонент операційних систем Microsoft Windows, що захищає від несанкціонованого використання комп'ютера шляхом заборони всіх змін системного рівня без дозволу адміністратора.

В UAC виділяється 4 основних типи облікових записів: Адміністратор; Досвідчений користувач (Power User); Звичайний користувач (Standard User); Гість (як правило, цей обліковий запис блокований і не має пароля). У Windows 7 можна налаштовувати UAC на 4 різних рівнях повідомлень – від «Завжди повідомляти» до «Ніколи не повідомляти».

Центр оновлення Windows – це клієнтський компонент Windows, який стежить за тим, щоб в системі Windows завжди були встановлені останні версії програмних засобів і модулі корекції для системи безпеки.

DEP (Data Execution Prevention) – запобігання виконанню даних. Це набір програмних і апаратних технологій, що дозволяють виконувати додаткові перевірки вмісту оперативної пам'яті і

запобігати запуску шкідливого коду, який може бути прихований під виглядом даних.

Функція **батьківського контролю** дозволяє обмежити час, протягом якого дітям дозволено вхід в систему. Зокрема, можна визначити дні тижня і години доступу у відповідний день тижня.

Короткі відомості про систему безпеки ОС GNU/Linux


Успадкувавши від UNIX традиційну модель доступу, Linux зіткнулася з давно відомими проблемами безпеки. Використовуваний в ній метод контролю доступу надає занадто широкі можливості: будь-яка програма, запущена від імені користувача, володіє всіма його правами – може читати конфігураційні файли, встановлювати мережеві з'єднання і т. д.

Іншою великою проблемою є наявність облікового запису суперкористувача (або адміністратора) з дуже широкими повноваженнями. Як правило, під цією назвою розуміється рівень доступу самої системи – саме з ним працюють всі системні служби. У цьому сенсі системні програми рівні в правах, хоча насправді кожній з них потрібна лише «своя» частина прав суперкористувача – звернення до мережевого інтерфейсу, читання файлів з паролями, запис повідомлень в системний журнал та ін. Однак, зловмисникові достатньо отримати контроль над однією з таких служб, і він отримає необмежений доступ до системи.

Політика безпеки – це набір параметрів, які регулюють безпеку комп'ютера. У операційних системах MS Windows ці параметри управляються за допомогою локального об'єкта групової політики (GPO). Налаштовувати дані політики можна за допомогою оснащення «Редактор локальної групової політики» або «Локальна політика безпеки».

Перейти до перегляду та редагування локальних політик безпеки ви можете наступними способами:

1. Натиснути кнопку «Пуск» для відкриття головного меню, в полі пошуку ввести «Локальна політика безпеки» (Локальная политика безопасности). Відкрити у знайдених результатах;

2. Відкрити діалогове вікно «Виконати» (Run). Для цього можна скористатися відповідним пунктом головного меню, або комбінацією клавіш  + R . У діалоговому вікні «Виконати» ввести secpol.msc і натиснути кнопку «ОК»;

3. Відкрити «Консоль керування ММС». Для цього натиснути на кнопку «Пуск», у полі пошуку ввести mmc, а потім натиснути «ОК». Відкриється порожня консоль ММС. Тепер можна у меню «Консоль» вибрати команду «Додати або видалити оснащення», або скористатись комбінацією клавіш Ctrl+M. У діалозі «Додавання та видалення оснащень» вибрати оснащення «Редактор локальної групової політики» та натиснути кнопку «Додати». У діалозі «Вибір об'єкта групової політики» натиснути кнопку «Готово» (за умовчанням встановлений об'єкт «Локальний комп'ютер»), або ж натиснути кнопку «Огляд» для вибору іншого комп'ютера.

Секція *«Групи з обмеженим доступом»* містить налаштування, що надають можливість визначити членів даної групи, а також членства в групах для конкретної групи безпеки.

За централізоване управління службами ваших клієнтських машин відповідає секція *Системні служби*.

Секція *«Реєстр»* призначена для визначення права доступу та аудиту для різних розділів системного реєстру комп'ютерів, які вказані в області дії групової політики.

В області відомостей «Політик диспетчера списку мереж» можна налаштовувати:

- Мережі, які не вдається ідентифікувати через помилки мережі або відсутності ідентифікованих ознак («Невідомі мережі»);
- Тимчасовий стан мереж, що знаходяться в процесі ідентифікації («Ідентифікація мереж»);
- Всі мережі, до яких підключений користувач («Всі мережі»);
- А також поточне підключення до мережі (робоча група або домен).

Множинна локальна групова політика (MLGPO) є певним розширенням для оснащення «Об'єкти локальної групової політики», яке було присутнє у операційних системах Windows, що передували Windows Vista.

Політика локального комп'ютера. Ця політика також відома як «Локальна групова політика» і є основним об'єктом для множинної групової політики.

Політика групи «Адміністратори» і користувачів, що не входять до групи «Адміністратори». У будь-якій операційній системі Windows створюються кілька груп і користувачів за

умовчанням. Однією з цих груп є група «Адміністратори». Група «Адміністратори» створюється при встановленні або оновленні системи за замовчуванням і в цій групі за замовчуванням створюється один користувач – «Адміністратор».

Політика для окремих локальних користувачів. Крім вбудованих облікових записів, адміністратори систем Windows можуть самостійно створювати облікові записи з різними правами.

Порядок виконання роботи

1. Ознайомтесь із наведеними теоретичними відомостями.
2. Увімкніть Центр забезпечення безпеки Windows за допомогою редактора групової політики. Для цього виконайте наступні дії:
 - Запустіть оснастку «Редактор об'єктів групової політики» (у локальному варіанті):
 - Перейдіть до вузла *Конфігурація комп'ютера \ Адміністративні шаблони \ Компоненти Windows \ Центр забезпечення безпеки*.
 - Увімкніть політику «Увімкнути центр забезпечення безпеки» (тільки для комп'ютерів домена).
3. Випробуйте доступні способи запуску Брандмауеру Windows.
4. Запустіть Захисник Windows (Windows Defender). Виберіть у його вікні Програми | Параметри і розгляньте можливості налаштування параметрів попередження про погрози.
5. Прокрутіть вікно вниз до розділу «Параметри захисту в режимі реального часу» і виберіть, чи повинен Захисник Windows повідомляти вас про програми, які ще не були класифіковані за рівнем ризику, і про зміни, виконані на вашому комп'ютері програмами, яким дозволено виконуватися.
6. Знайдіть у своїй системі засіб налаштування UAC. Вивчіть наявні можливості налаштування контролю облікових записів.
7. Знайдіть у своїй системі опції налаштування Центру оновлення Windows.
8. Ознайомтеся з вікном, що дозволяє керувати функцією DEP (Властивості системи | Додаткові параметри | Параметри швидкодії, вкладка «Запобігання виконанню даних»).
9. Знайдіть у своїй системі засіб налаштування параметрів батьківського контролю. Вивчіть наявні можливості налаштування.

10. Для виконання другої частини роботи запустіть Linux, можна на віртуальній машині або з Live CD.

11. Запустіть систему GNU/Linux. Відкрийте у налаштуваннях ОС Linux панель «Керування користувачами та групами». Розгляньте можливості налаштування користувачів, налаштування груп, налаштування параметрів аутентифікації.

12. Перевірте, чи присутні у Вашій версії Linux можливості вимагати від користувача зміни пароля через певний термін, налаштування способу шифрування паролем, налаштування менеджера входу в систему (вхід в систему лише для певного користувача, безпарольний вхід і т.д.).

13. Перегляньте системні групи та фіктивних користувачів, що присутні у Вашій Linux-системі. Поясніть призначення кожної (кожного) з цих груп та користувачів. З'ясуйте, які права надані кожній групі та кожному з користувачів.

14. Ознайомтесь з оснащенням «Редактор локальної групової політики» та «Локальна політика безпеки», які дозволяють налаштувати дані політики.

15. Дізнайтесь про управління перевіркою автентичності користувача облікових записів, Розгляньте вузол «Політики облікових записів».

16. У вузлі «Політика паролів» змініть параметри безпеки, які застосовуються для управління паролями облікових записів.

17. Використовуючи вузол «Політика блокування облікового запису», обмежте кількість некоректних спроб входу користувача в систему трьома спробами; вкажіть також час, протягом якого після заданої кількості невдалих спроб входу обліковий запис буде заблокований до його автоматичного розблокування.

18. За допомогою вузла «Політика аудиту» внесіть налаштування, щоб створювався запис аудиту для кожної невдалої спроби входу в систему.

19. Використовуючи множинну локальну групову політику, забороніть користувачам змінювати своє географічне розташування.

20. За допомогою політики локального комп'ютера виконайте дію «Заборонити використання командного рядка».

21. Підготуйте звіт про виконану роботу. Наведіть скріншоти та пояснення щодо виконання кожного пункту завдання.

22. Здайте і захистіть звіт про виконання роботи. Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Поясніть вирази: «загроза безпеки комп'ютерної системи», «уразливість комп'ютерної системи», «атака на комп'ютерну систему».

2. Що таке дескриптор безпеки? Що до нього входить? Які об'єкти можуть мати дескриптор безпеки? Яке призначення дескриптора безпеки?

3. Поясніть поняття «авторизація». В чому різниця між ідентифікацією, аутентифікацією та авторизацією користувача?

4. Розгляньте алгоритм авторизації, що використовується у операційних системах Windows.

5. Поясніть призначення Центру забезпечення безпеки Windows.

6. Що таке брандмауер? Для чого він призначений?

7. Як керувати брандмауером Windows?

8. Поясніть призначення Захисника Windows (Windows Defender).

9. Що таке агенти безпеки Захисника Windows? Опишіть їх функції.

10. Поясніть призначення функції UAC в операційних системах Windows.

11. Що таке Центр оновлення Windows? Поясніть його роль у забезпеченні безпеки комп'ютерної системи.

12. Охарактеризуйте технологію запобігання виконання даних (DEP).

13. Охарактеризуйте можливості батьківського контролю в операційних системах Windows.

14. Охарактеризуйте принципи інформаційної безпеки, закладені у операційній системі Linux.

15. Що називається політикою в операційній системі?

16. Які компоненти входять до політик ОС Windows?

17. Які засоби застосовуються в ОС Windows для налаштування політик?

18. Як можна перевірити правильність налаштувань політик безпеки у ОС Windows?

19. Як налаштування політик можуть вплинути на стан захисту інформації в комп'ютерній системі?

20. За допомогою якої політики можна вказати користувачів або групи, призначені для виконання операцій резервного копіювання файлів, каталогів, розділів реєстру та інших об'єктів, які підлягають архівації? Для яких дозволів надає доступ дана політика?

21. Як заборонити для локальної групи гостей доступ до системного журналу?

22. Що називається аудитом в ОС Windows? Для чого застосовується «Політика аудиту»?

23. Які можливості надає адміністратору використання політики «Виконання завдань з обслуговування томів»?

24. Наведіть приклад застосування політик призначення прав користувачів.

25. Поясніть призначення журналу подій ОС Windows. Як переглянути журнал подій в ОС Windows?

26. Охарактеризуйте оснащення ОС Windows «Множинна локальна групова політика». Як відкрити це оснащення в ОС Windows?

Лабораторна робота №1.2. Надійне видалення інформації з жорсткого диску комп'ютера

Мета роботи: ознайомлення з питаннями захисту інформації при використанні жорстких дисків.

Завдання роботи: встановити програмне забезпечення для надійного видалення інформації з жорсткого диску комп'ютера, навчитися його використовувати.

Аудиторний час – 4 акад. години.

Короткі теоретичні відомості

Видалення файлів засобами операційної системи не приводить до фізичного знищення інформації, що зберігалася на диску. Знищується лише посилання на неї. Кластер помічається як «вільний», однак дані, що належали файлу, залишаються у ньому і легко можуть бути прочитані.

Ось короткий перелік місць на жорсткому диску, де після видалення файлів можуть бути присутні залишкові дані про них:

- вільні кластери/сектори диску;
- вільні частини частково зайнятих кластерів чи секторів, в яких можуть знаходитися залишки даних видалених файлів, що були записані в цих місцях раніше;
- таблиці файлової системи, де можна знайти відомості про імена та розміри файлів – як існуючих, так і видалених;
- файли підкачки Windows чи swap-розділ Linux;
- реєстр Windows, де залишаються записи про файли, які були відкриті різними програмами, відвідані директорії, тощо;
- конфігураційні та тимчасові файли деяких програм, в який залишається інформація про використані файли. Наприклад, тимчасові файли, які створює Microsoft Word. Ці файли містять резервні копії документа, який редагує користувач;
- кеш браузер, історія браузера, файли cookies; і т.д.

Для забезпечення максимально надійного захисту від небажаного відновлення видалених файлів, необхідно перезаписати як зайнятий цими файлами простір, так і вільний. Ідеальною є політика очищення вільного простору на регулярній основі

До кращих безкоштовних програм для безповоротного видалення даних можна віднести наступні:

Eraser – популярна вільна програма для безповоротного видалення файлів, директорій і чищення слідів у вільній області диска методом перезапису. Має кілька стандартних режимів роботи (14 стандартних шаблонів, включаючи стандарти DoD і Гутмана), і дозволяє створювати власні режими з довільною кількістю проходів при перезаписі. Призначення Eraser – видалення конфіденційних даних, історії, тимчасових файлів, файлів cookies браузера та ін. Програма застосовує новий алгоритм пошуку персональних даних, що дає можливість підвищити релевантність і точність видалення. Безпечно видаляє дані без можливості відновлення. Простий інтерфейс, є велика кількість підказок по будь-якій функції. Завдяки цьому з додатком легко працювати навіть недосвідченому користувачеві.

File Shredder – може як просто звільнити простір, видаляючи файли, так і безповоротно їх стерти. File Shredder має невеликий розмір, простий інтерфейс, і дуже простий у використанні. Він

використовує набагато менше оперативної пам'яті, ніж Eraser, але вимагає більше ресурсів процесора. Недоліки – відсутність планувальника завдань і вбудованої довідки, дуже обмежена інтерактивна допомога.

За замовчуванням File Shredder використовує для знищення файлів стандарт DoD (5220–22.M), але має для вибору ще чотири інші шаблони (в порівнянні з чотирнадцятьма в Eraser). Може бути дещо повільним при очищенні від непотрібних та застарілих файлів, тому (залежно від обставин) інколи краще налаштувати його на одну або дві фази.

Очищення в File Shredder працює трохи інакше, ніж в Eraser, і залишає після виконання операції певну кількість тимчасових файлів з беззмисловою інформацією. (Після роботи Eraser не залишається нічого).

CCleaner – ця програма відзначається тим, що досить добре обізнана з «таємними схованками», де накопичуються різноманітні дані. Ця програма допоможе вам віднайти дані, створені та покинуті системою, веб-браузером та іншими програмами. Все це сміття важко знайти і видалити самостійно.

Також CCleaner може провести перезапис вільного простору. Якщо ви захочете використати цю функцію, зайдіть у налаштування (Опції – Налаштування) та встановіть відмітку біля напису «Wipe MFT Free Space».

Нарешті, CCleaner також може очистити файли і папки, задані користувачем. Для цього їх спочатку потрібно внести у спеціальний список (Опції – Додати) та відмітити пункт «Вибіркові файли та папки» у розділі «Очистка»..

SDelete – це одна з розробок відомого дослідника Windows Марка Руссиновича. Ця утиліта не має графічного інтерфейсу і працює з командного рядка. Про команди для керування програмою можна дізнатися з документації. За допомогою SDelete можна надійно знищити файли і папки, або провести очистку вільного простору диска. Як і інші сучасні програми цього призначення, SDelete не просто позначає файл як видалений, а кілька раз записує поверх нього випадковий набір даних.

Деякі супутні програми:

- Revo Uninstaller – має інструменти для якісного знищення файлів та очищення вільного простору.

- Recuva – програма для відновлення видалених даних, також дозволяє безповоротно стерти окремі знайдені файли.

- EraserDrop (EraserDrop Portable) – ця гнучка портативна програма, дозволяє швидко видалити будь-який файл чи папку шляхом простого перетаскування на значок, відображений запусненою програмою на робочому столі комп'ютера. Цю програму також можна використовувати для очищення вільного простору.

- UltraShredder – невелика, проста у використанні портативна програма для безповоротного знищення файлів.

Порядок виконання роботи

1. Ознайомтесь з теоретичними відомостями.
2. Оберіть одну з програм для надійного видалення даних. Встановіть її та навчіться з нею працювати.
3. Підготуйте у звіті огляд доступних налаштувань програми.
4. Використовуючи одну з програм відновлення даних (Recuva, PC Inspector тощо), спробуйте відновити видалені вами дані. Відобразіть результати у звіті.
6. Здайте звіт викладачу та захистіть його. Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Що відбувається при видаленні файлів з жорсткого диску засобами операційної системи? Як це може вплинути на стан безпеки інформації?
2. Поясніть, яким чином можна добитися надійного видалення інформації з жорсткого диску..
3. Як Ви вважаєте, чому в деяких алгоритмах видалення інформації передбачено багаторазовий перезапис одних і тих же кластерів диску?
4. Охарактеризуйте відомі вам програми для безпечного знищення інформації.
5. Яку з цих програм вибрали Ви? Чим був продиктований Ваш вибір?

Лабораторна робота № 1.3. Резервне копіювання інформації

Мета роботи: ознайомитися з основними принципами застосування резервного копіювання інформації у складі заходів захисту інформації.

Завдання роботи: встановити програмне забезпечення резервного копіювання інформації та навчитися з ним працювати.

Аудиторний час – 2 акад. години.

Короткі теоретичні відомості

Кожен користувач зберігає на комп'ютері ту чи іншу інформацію, втрата якої може призвести і до значної матеріальної та моральної шкоди. Між тим, будь-які носії інформації (жорсткі диски, SSD-пристрої, флешки) не мають абсолютної надійності і іноді відмовляють. Крім того, і при справному носії інформація може бути знищена внаслідок помилки у програмному коді або через руйнівну діяльність вірусів. Нарешті, комп'ютерна техніка може бути вкрадена, або може постраждати внаслідок форс-мажорних подій, таких як пожежа або землетрус.

Для того, щоб убезпечити важливу інформацію від зникнення, необхідно виконувати резервне копіювання даних.

Резервне копіювання інформації – це процес створення копій важливої інформації, призначених для її відновлення у випадку, коли з тих чи інших причин неможливо буде скористатися оригіналом.

Розрізняють три основні методи створення резервних копій: повне, диференціальна та інкрементне резервне копіювання.

Повне резервне копіювання створює копію, що містить всі дані об'єкту резервного копіювання. Цей метод дозволяє забезпечити максимальну відповідність оригіналу даних та його копії. Однак він вимагає найбільше (порівняно з іншими методами) дискового простору для зберігання створених копій.

Диференціальне резервне копіювання полягає у копіюванні лише змін, що відбулись у об'єкті з моменту створення останньої повної копії. Створення такої копії потребує більше часу, ніж додаткове копіювання, але процес відновлення швидший. Диференціальна копія займає більший об'єм, ніж додаткова, але, звичайно ж,

менший об'єм, ніж повна. Загалом, цей метод займає проміжне положення між створенням повної або додаткової копії.

Додаткове (інкрементне) резервне копіювання полягає у копіюванні змін, що відбулись у об'єкті з моменту останнього повного, диференційного або додаткового копіювання. Загалом, на додаткове копіювання витрачається менше часу, ніж на створення повної чи диференціальної, оскільки копіюється менше файлів. Об'єм копії при додатковому копіюванні також виходить найменшим з усіх трьох методів

Традиційними засобами резервного копіювання для Unix-подібних систем є утиліти `cp`, `cpio`, `dd`, `scr`, а також утиліти-архіватори – `tar`, `tar+gzip`, `tar+bz2`.

Багато користувачів Windows для створення резервних копій користувацьких файлів також використовують архіватори, такі як Winzip, Winrar, 7zip.

До складу сучасних версій Windows включено ряд «штатних» засобів резервного копіювання: засіб «Архівація файлів», засіб «Архівація образу системи», засіб «Попередні версії», засіб «Відновлення системи».

Крім того, існує значна кількість програм сторонніх виробників, призначених спеціально для резервного копіювання та відновлення даних. Серед найбільш відомих програм цієї категорії – Acronis TrueImage; Norton Ghost; PartImage; BackupPC, Areca Backup, Amanda, DirSync Pro, LuckyBackup, Mondo Rescue, Handy Backup, Comodo BackUp та ін.

Важливим питанням резервного копіювання є вибір *схеми ротації носіїв* (наприклад, магнітних стрічок). Найчастіше використовують такі схеми: одноразове копіювання; проста ротація; «дід, батько, син»; «Ханойська башта»; «10 наборів».

Суттєвим моментом в організації резервного копіювання на виробництві є необхідність подолання психологічних перешкод (людського фактору). Резервне копіювання – це процес, що вимагає значних витрат часу та наявності певних матеріальних засобів. На думку багатьох мережевих і системних адміністраторів, забезпечення безперервного циклу резервного копіювання та архівування даних належить до найбільш неприємних і нецікавих службових обов'язків. Резервне копіювання – це, так би мовити, сірі будні роботи адміністратора. Однак, більшість керівників

підприємств та організацій, не будучи спеціалістами у галузі інформаційних технологій, не усвідомлюють важливості резервного копіювання та архівування даних, і через це не погоджуються асигнувати на ці цілі достатньо бюджетних та людських ресурсів. В результаті адміністратор змушений виконувати резервне копіювання з використанням випадкового, повільного і незручного обладнання, робити це на ініціативних засадах, в позаробочий час, тощо. Якщо ж втрата даних таки стається, то керівник негайно покладає провину за це на адміністратора.

Порядок виконання роботи

1. Ознайомтеся з наведеними теоретичними відомостями.
2. Ознайомтеся з Unix-утилітами резервного копіювання: `сріо`, `dd`, `срр`. Наведіть у звіті перелік основних можливостей та відповідних опцій цих програм.
3. Ознайомтеся з засобами резервного копіювання, що входять до складу сучасних версій Windows: «Архівація файлів», «Архівація образу системи», «Попередні версії», «Відновлення системи».
4. Ознайомтеся з однією з програм резервного копіювання (за варіантами): Acronis TrueImage, Norton Ghost, PartImage.
5. Ознайомтеся з однією з програм резервного копіювання (за варіантами): BackupPC, Aresca Backup, DirSync Pro, luckyBackup, Handy Backup, Backup Manager, Backup Studio, Second Copy.
6. Підготуйте звіт про виконану роботу. Наведіть скріншоти та пояснення щодо виконання кожного пункту завдання.
7. Здайте і захистіть звіт про виконання роботи. Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Поясніть поняття «резервне копіювання інформації».
2. Поясніть поняття: повна, інкрементна, диференціальна резервна копія.
3. Що таке схема ротації носіїв резервних копій? Наведіть приклади схем ротації носіїв резервних копій.
4. Розгляньте роль резервного копіювання інформації у складі комплексу заходів захисту інформації.

5. Від яких загроз безпеці інформації може захистити резервне копіювання?

6. Де (на яких носіях) може бути створена резервна копія інформації? Поясніть, які з цих розміщень доцільно, а які недоцільно використовувати у різних випадках.

7. Поясніть правила поводження з резервними копіями.

8. Які загрози безпеці інформації можуть виникнути в процесі створення та зберігання резервних копій? Як можна захиститися від цих загроз?

9. Порівняйте можливості відомих Вам програм резервного копіювання з графічним інтерфейсом. Які з цих програм, на Вашу думку, більш доцільно використовувати в тих чи інших випадках?

10. Розгляньте основні можливості утиліт `cpio`, `dd`, `scr`. Для розв'язання яких задач найкраще застосовувати кожен з них?

11. Розгляньте засоби резервного копіювання, що входять до складу сучасних версій Windows. Порівняйте їх можливості.

Лабораторна робота №1.4. Керування віддаленим комп'ютером

Мета роботи: ознайомлення з можливостями керування віддаленим комп'ютером.

Завдання роботи: ознайомитися з програмними засобами віддаленого адміністрування та відповідними протоколами; встановити програми віддаленого адміністрування та навчитися їх використовувати.

Аудиторний час – 2 акад. години.

Короткі теоретичні відомості

Віддалене управління комп'ютером – це можливість використовувати комп'ютер з будь-якого віддаленого місця світу так, ніби ви працюєте безпосередньо за ним. При цьому спілкування з керованим комп'ютером проходить через мережу (локальну або Інтернет).

Засоби віддаленого доступу можна умовно поділити на декілька груп за типом вирішуваних ними задач:

- Група 1: засоби організації термінальних сесій (термінальні сервери).

- Група 2: засоби «віддаленої допомоги».

- Група 3: засоби «віддаленого виконання завдань»,.

В операційній системі Windows є вбудовані функції, які дозволяють виконувати віддалене управління робочим столом. У Windows 7 цей інструмент називається «Віддалений помічник Windows 7», він може бути викликаний через головне меню системи. В Windows 8 і Windows 10 доступ до віддаленого помічника прибрати з головного меню, тому доведеться запускати його через командний рядок. В цілому, Віддалений помічник Windows – незручний інструмент, особливо якщо користуватися ним так, як це описано в керівництві. Для кожного сеансу зв'язку потрібно створити файл запрошення і відправити його людині, яка буде підключатися. Існує можливість налаштувати роботу без файлу запрошення, але тільки в межах локальної мережі. Для роботи через інтернет в кожному випадку доведеться створювати файл запрошення і відправляти його іншому учасникові.

Для реалізації віддаленого доступу для операційних систем Windows існує ряд програмних рішень сторонніх розробників.

Програма *Teamviewer* – розробка компанії Teamviewer GMBH. Teamviewer дозволяє організувати віддалений доступ до будь-якого комп'ютера буквально за декілька хвилин. Для роботи потрібний лише доступ в Інтернет. Ваш партнер має скачати клієнтський модуль Teamviewer і запустити його. Teamviewer включає декілька компонентів. На своєму комп'ютері (з якого ви збираєтесь керувати віддаленим) ви завжди запускаєте основний додаток – Teamviewer (full version). На віддаленому комп'ютері можуть бути запущені:

- Teamviewer;
- Teamviewer (full version);
- Teamviewer Host;

TightVNC – це вільно поширюваний програмний продукт для віддаленого управління комп'ютером. Програма поширюється під ліцензією GPL, доступний її повний початковий код. TightVNC – крос-платформенний продукт; програма доступна для Windows і Unix систем, сумісна з іншими VNC продуктами.

Програма TightVNC, як і всі додатки VNC, складається з двох частин: Сервер (також званий WinVNC), який надає доступ до

екрану на запущеній машині, і програма Viewer (TightVNC Viewer), яка відображає зображення екрану віддаленого комп'ютера, що отримується від сервера.

Програма *Remote Administrator* (скорочено *Radmin*) дозволяє адмініструвати всі робочі станції і сервери вашої локальної мережі прямо зі свого робочого місця. Ви бачитимете екран комп'ютера, що адмініструється, у вікні на своєму Робочому Столі.

Radmin здатна працювати із з'єднаннями по локальній мережі, а також через комутоване з'єднання (модем), оскільки висока швидкість з'єднання не є основною вимогою програми.

Порядок виконання роботи

1. Ознайомтесь із наведеними теоретичними відомостями.
2. Підготуйте дві системи, на яких будете виконувати досліди. Це може бути ваш комп'ютер і комп'ютер товариша, поєднані мережею, або група з двох віртуальних машин, з'єднаних сегментом віртуальної мережі.
3. Встановіть на дослідні системи компоненти програми Teamviewer.
4. Teamviewer дозволяє виконати підключення до віддаленого комп'ютера чотирма різними способами (доступ до віддаленого робочого столу; презентація; режим передачі файлів; VPN). Випробуйте їх. З'ясуйте можливості кожного режиму:
5. Ознайомтесь з додатком Teamviewer Manager.
6. Встановіть компоненти програмного продукту TightVNC.
- Після завершення встановлення програми, буде створена нова група "TightVNC" в меню Пуск – Програми.
7. Запустіть сервер TightVNC як додаток (тільки для поточного користувача): Start>Programs>TightVNC>Launch TightVNC Server;
8. Для перегляду і управління віддаленим робочим столом, де запущений сервер TightVNC, використайте програму TightVNC Viewer.
9. Запустіть програму Viewer в режимі listening (прослуховування, очікування), використовуючи відповідну кнопку вікна «New Connection». У цьому режимі вікно буде згорнуто в іконку і чекатиме з'єднання, ініціалізованого сервером TightVNC.
10. У вікні «New Connection» натисніть кнопку контекстної допомоги (F1). Вивчіть отриману інформацію.

11. Спробуйте провести віддалене оновлення сервера програми TightVNC.

12. Запустіть сервер TightVNC як службу (сервіс) Windows (для всієї операційної системи).

Для встановлення сервісу, виберіть меню Start > Programs > TightVNC > Administration > Install VNC Service.

13. Виконайте з меню програми TightVNC доступні команди і зафіксуйте результати.

14. Використайте веб-браузер як Viewer (для перегляду віддаленого робочого столу за допомогою TightVNC).

15. Встановіть компоненти програми Radmin (Viewer і Server).

16. Налаштуйте сервер програми Radmin. У вікні налаштувань, що відкриється, потрібно вибрати «Права доступу...». Відкриється вікно «Режим безпеки Radmin Server». Далі потрібно поставити перемикач (радіокнопку) у положення «Radmin» і натиснути кнопку «Права доступу». Права доступу користувачів можна редагувати встановленням прапорців («галочок») навпроти того чи іншого права у нижній частині вікна.

17. Переходимо до налаштування Radmin Viewer. Для того, щоб з'єднатись з щойно налаштованим сервером, потрібно вибрати пункт головного меню програми «З'єднання > З'єднатися з...»

18. Натисніть кнопку «ОК». Після цього почнеться процес встановлення з'єднання з віддаленим комп'ютером. Через деякий час програма запитас ім'я комп'ютера та пароль. Після натиснення кнопки ОК віддалений контроль буде встановлено.

19. Підготуйте звіт про виконану роботу. Проілюструйте виконання кожного завдання скріншотами та описами.

20. Здайте та захистіть свій звіт. Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Що називають віддаленим керуванням комп'ютером?

2. Для розв'язання яких задач може використовуватись віддалене керування комп'ютером?

3. Які можливості надають програми віддаленого керування? Як при цьому перевірити результати своєї роботи?

4. Розгляньте можливості програми TeamViewer.

5. Розгляньте можливості програми TightVNC.

6. Розгляньте можливості програми Radmin.
7. Порівняйте можливості програм TeamViewer, TightVNC, Radmin. Для яких задач краще використовувати кожен з них?
8. Як можливості віддаленого керування комп'ютером можуть вплинути на стан безпеки інформації?
9. Як Ви вважаєте, які можливості можуть закладати у свої розробки автори троянських програм, призначених для несанкціонованого доступу до чужих комп'ютерних систем?

Лабораторна робота №1.5. Аналіз інформації, що передається в мережі

Мета роботи: ознайомлення з можливостями реєстрації третьою стороною інформації, що передається у комп'ютерній мережі.

Завдання роботи: встановити програму перехоплення мережевої інформації Wireshark, ознайомитись з її можливостями.

Аудиторний час – 2 акад. години.

Короткі теоретичні відомості

Аналізатор трафіку, або сніффер (від англійського слова *to sniff* – винюхувати) – це програма, призначена для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку. Сніффер може перехоплювати трафік, призначений для інших вузлів мережі, відмінних від того вузла, на якому працює сніффер.

Перехоплення трафіку може здійснюватися:

- звичайним «прослуховуванням» мережевого інтерфейсу з підключенням сніффера в розрив каналу;
- відгалуженням трафіку (яке можна виконати програмним або апаратним способом) і спрямуванням його копії на сніффер;
- через аналіз побічних електромагнітних випромінювань і відновлення трафіку, що таким чином прослуховується;
- через атаку з підбійкою адрес на каналному (2) рівні (MAC-spoofing) або мережевому (3) рівні (IP-spoofing), що приводить до перенаправлення трафіку жертви або всього трафіку сегменту на сніффер, з подальшим поверненням трафіку в належну адресу.

Сніфтери застосовуються як в благих, так і в деструктивних цілях. Аналіз трафіку, що пройшов через сніффер, дозволяє виявити паразитний, вірусний і закільцьований трафік; виявити в мережі ознаки функціонування шкідливого і несанкціонованого ПЗ, наприклад, мережесканирувальників, флудерів, троянських програм; перехопити будь-який незашифрований (а інколи і зашифрований) трафік, з метою отримання паролів і іншої інформації; локалізувати несправність мережі або помилку конфігурації мережесканирувальників .

Wireshark – програма-аналізатор трафіку для комп'ютерних мереж Ethernet і деяких інших.

Wireshark є аналізатором мережесканирувальників пакетів. Ось кілька прикладів сценаріїв, у яких може бути доцільним використання Wireshark:

- для діагностики мережі;
- при дослідженні питань мережесканирувальників безпеки;
- для налагодження реалізації мережесканирувальників протоколу при розробці програмного забезпечення;
- для дослідження внутрішніх мережесканирувальників протоколів.

Порядок виконання роботи

1. Ознайомтеся з наведеними теоретичними відомостями.
2. Встановіть Wireshark.
3. Запустіть програму. Натисніть на кнопку *List the available capture interfaces...* (Список наявних відстежуваних інтерфейсів ...). Відкриється нове вікно зі списком мережесканирувальників інтерфейсів, що є у вашій системі.
4. Оберіть інтерфейс, за яким Ви будете перехоплювати трафік. У списку інтерфейсів оберіть відповідний рядок і натисніть на кнопку *Start* у цьому рядку
5. У головному вікні спостерігайте за пакетами для різних протоколів.
6. Щоб закінчити збирання даних, натисніть кнопку *Stop*. Після цього ви можете переглянути результати, застосувати фільтри, зайнятися пошуком проблем і т.п.
7. Для того, щоб виконати більш тонке налаштування, клацніть по кнопці *Show the capture options* (Показати параметри збору даних).

8. Застосуйте фільтр, щоб обмежити виведені дані лише пакетами одного з протоколів.

9. Підготуйте звіт про виконану роботу. Наведіть скріншоти та пояснення щодо виконання кожного пункту завдання.

10. Здайте і захистіть звіт про виконання роботи. Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Що таке сніффер? Яке його призначення?
2. Яким чином здійснюється перехоплення трафіку?
3. Наведіть приклади застосування сніффера.
4. Як застосування сніфферів може вплинути на стан безпеки інформації в інформаційних системах?
5. Пакети яких протоколів Вам вдалося перехопити? Яку інформацію можна з них отримати?

Лабораторна робота №1.6. Налаштування міжмережевих екранів

Мета роботи: ознайомитися з основними принципами функціонування міжмережевих екранів та їх налаштування.

Завдання роботи: встановити та настроїти програмне забезпечення міжмережевого екрану; сконфігурувати програмне забезпечення iptables для раціональної обробки мережевих пакетів.

Аудиторний час – 4 акад. години.

Короткі теоретичні відомості

Величезна кількість користувачів використовує комп'ютер не тільки для роботи з різними програмами, а й для виходу в Інтернет. Недосвідчені користувачі нерідко просто не уявляють, які небезпеки може таїти в собі їх вихід в мережу. В результаті небажаних впливів, які можуть подіяти на комп'ютер з мережі, інформація, що міститься на комп'ютері, піддається величезному ризику. Для захисту комп'ютера розроблено цілий ряд програм, серед яких величезне значення мають брандмауери, або фаєрволи.

Брандмауер – це програмний або апаратний комплекс, який перевіряє пакети даних, що входять з мережі у комп'ютер (або, навпаки, виходять з комп'ютера у мережу), і, залежно від налаштувань брандмауера, блокує їх або дозволяє їм пройти в комп'ютер чи з нього.

Коли пакет прибуває, брандмауер аналізує заголовок пакету і приймає рішення про виконання однієї з дій: відкинути пакет (DROP), прийняти пакет, тобто дозволити йому пройти далі (ACCEPT), або виконати деякі перетворення його вмісту. Те ж саме відбувається і з вихідними пакетами, які проходять брандмауер на шляху з комп'ютера до мережі.

Брандмауер захищає комп'ютер від проникнення хакерів або зловмисних програм (наприклад, від хробаків), що розповсюджуються по локальній мережі або через Інтернет. Брандмауер також допомагає запобігти відправці шкідливих програм або вкрадених даних на інші комп'ютери.

У Linux брандмауер є модулем ядра, його невід'ємною частиною. Утиліта `iptables` використовується у більшості розповсюджених дистрибутивів GNU/Linux як інтерфейс для модифікації правил, за якими брандмауер обробляє пакети. Також з подібною метою використовується новіша розробка – `nftables`, яка, однак, ще не набула значного поширення.

`Iptables` – утиліта командного рядка, вона є стандартним інтерфейсом управління роботою міжмережевого екрану (брандмауера) `netfilter` для ядер Linux, починаючи з версії 2.4.

У `Iptables` використовується три види таблиць: `mangle`, `nat`, `filter`. Розглянемо кожну з них.

1. *Таблиця `mangle`* (англ. «`mangle`» – спотворювати, змінювати) призначена головним чином для внесення змін в заголовки пакетів. Зокрема, у цій таблиці можна встановлювати біти TOS (Type Of Service). В ній не варто робити будь-якого роду фільтрацію, маскування або перетворення адрес (DNAT, SNAT, MASQUERADE). У цій таблиці допускається виконувати тільки перелічені нижче дії:

- TOS – дія, що виконує установку бітів поля Type of Service в пакеті.

- TTL – дія, що використовується для установки значення поля TTL (Time To Live) пакета.

- MARK – дія, що встановлює спеціальну мітку на пакет, що потім може бути перевірена іншими правилами в iptables або іншими програмами, наприклад iproute2.

Характерними для цієї таблиці ланцюжками є: PREROUTING, OUTPUT, POSTROUTING.

2. Таблиця Nat використовується для виконання перетворень мережевих адрес NAT (Network Address Translation). Для цієї таблиці характерні дії:

- DNAT (Destination Network Address Translation) – дія, що виконує перетворення адрес призначення в заголовках пакетів.

- SNAT (Source Network Address Translation) – дія, що використовується для зміни адрес відправників пакетів.

- Маскування (MASQUERADE) застосовується в тих же цілях, що і SNAT, але на відміну від SNAT, MASQUERADE дає більш сильне навантаження на систему.

Ця таблиця має п'ять ланцюжків: PREROUTING, POSTROUTING, INPUT, OUTPUT і FORWARD.

PREROUTING використовується для внесення змін на вході в брандмауер, перед прийняттям рішення про маршрутизацію.

3. Таблиця filter – в ній повинні міститися набори правил для виконання фільтрації пакетів. Звичайно ж, можна фільтрувати пакети і в інших таблицях, але ця таблиця існує саме для потреб фільтрації.

В цій таблиці є три вбудованих ланцюжки:

Ланцюжок FORWARD використовується для фільтрації пакетів, що йдуть транзитом через брандмауер.

Ланцюжок INPUT проходять пакети, які призначені локальним програмам (брандмауеру).

Ланцюжок OUTPUT використовується для фільтрації вихідних пакетів, згенерованих програмами на самому брандмауері.

Кожен рядок, який ви вставляєте в той чи інший ланцюжок, повинен містити окреме правило.

У загальному вигляді правила мають наступну форму:

```
iptables [-t table] command [match] [target / jump]
```

Квадратні дужки містять необов'язкові параметри.

Користувачі GNU/Linux часто використовують для налаштування фаєрвола програми з відкритим кодом та графічним інтерфейсом: Guarddog, Firestarter, або його наступника gufw.

Головні можливості Firestarter:

- майстер налаштувань;
- монітор подій реального часу;
- налаштування загального доступу до інтернету;
- налаштування ДНСП-сервера;
- налаштування зовнішніх і внутрішніх політик.

Порядок виконання роботи

1. Ознайомтеся з наведеними теоретичними відомостями. Розберіть призначення основних таблиць iptables.

2. Встановіть та налаштуйте Firestarter або gufw на свій дистрибутив Ubuntu.

3. Після завершення встановлення програми, запустіть її і виконайте початкове конфігурування. Для запуску програми виберіть у меню Система -> Адміністрування -> Firestarter.

4. Розгляньте всі елементи управління, які є на вкладках вікна програми.

5. Розгляньте інформацію, що виводиться під час роботи програми. Розгляньте вкладку Events (події). Опишіть її особливості.

6. Ознайомтеся з вікном вхідних політик.

7. Навчіться створювати мережеві правила для програми Firestarter. Виконайте дії (відкрити/змінити/видалити), для відповідного хосту чи портів.

8. Перевірте роботу створених правил, спробувавши в терміналі обмін пакетами.

9. Ознайомтеся з вікном вихідних політик.

10. Створіть чорний список і внесіть до нього декілька імен хостів чи IP-адрес.

11. Ознайомтеся з вікном білого списку ("Restrictive by default, whitelist traffic").

12. Перегляньте всі створені правила в терміналі. (Щоб швидко переглянути всі створені правила, введіть в терміналі команду: `sudo iptables -L`.)

13. Проведіть налаштування міжмережевого екрану в ОС Windows.

14. Для виконання наступного завдання утворіть групу з двох (можна віртуальних) комп'ютерів, під управлінням систем Windows

та Ubuntu Linux з налаштуваннями за замовчуванням (брандмауер Windows включений).

15. Використовуючи команду `ping`, виконайте перевірку міжмережевої взаємодії при працюючому і при відключеному брандмауері.

16. За допомогою команд в терміналі виконайте наступні налаштування `iptables`:

а) Перегляньте список стану правил брандмауера. Для цього в терміналі введіть команду: `iptables -L`.

б) Змініть прийняті за замовчуванням операції над вхідними, вихідними і транзитними пакетами. Зробіть так, щоб жоден пакет не входив і не виходив через мережеві інтерфейси. Для цього скористайтесь можливостями команд:

`iptables -P INPUT DROP`

`iptables -P OUTPUT DROP`

`iptables -P FORWARD DROP`

в) Запустіть знову команду `iptables -L`, щоби впевнитись, що прийнята за замовчуванням політика змінилась з АСЕРТ на DROP.

г) Збережіть введені раніше правила за допомогою команди `iptables-save > /path/file`. Наприклад: `iptables-save > /root/iptables.txt`.

17. Розгляньте додаткові ключі `iptables`, які можуть використовуватись спільно з командами. Опишіть їхнє призначення.

18. Розгляньте порядок проходження наступних пакетів пакетів (за варіантами):

- порядок руху транзитних пакетів;
- порядок руху пакетів, що призначені локальному процесу чи додатку;
- порядок руху пакетів від локальних процесів

19. Підготуйте звіт про виконану роботу. Наведіть скріншоти та пояснення щодо виконання кожного пункту завдання.

20. Здайте і захистіть звіт про виконання роботи. Дайте відповіді на контрольні запитання.

Контрольні запитання (1):

1. Що називають брандмауером?

2. Які можливості брандмауера? Для чого його використовують?
3. Для чого призначено пакети Firestarter, gufw? Розгляньте їх основні можливості.
5. Як у Firestarter, gufw перевірити підключені правила?
6. Яким чином можна перевірити роботу брандмауера Firestarter, gufw?
7. Як можна упевнитися в тому, що брандмауер Windows працює?
8. Що означає вираз «дозволити програмі встановлювати зв'язок через брандмауер»?
9. Що означає вираз «відкрити порт»?
10. Які параметри брандмауера Windows Ви б рекомендували встановити?
11. Яким загрозам не може запобігти брандмауер?
12. Як реалізований брандмауер, що входить до ядра Linux? З яких компонентів він складається? Розгляньте ролі цих компонентів.
13. Які існують способи налаштування iptables?
14. Яку роль виконують таблиці iptables?
15. Для чого створюють правила в iptables? Який загальний вигляд запису цих правил?
16. Що називають ланцюжками таблиць iptables? Про які ланцюжки Ви дізналися? Яке призначення цих ланцюжків?
17. Які ланцюжки містять таблиці mangle, nat, filter? Для чого використовується кожен з цих ланцюжків?
18. Яким чином можна переглянути список доступних команд для роботи з iptables?
19. Як можна зберегти правила iptables? Як завантажити вручну правила iptables, які були попередньо збережені?

Модуль №2 «Криптографічний та стеганографічний захист інформації»

Лабораторна робота №2.1. Ознайомлення з криптографічними алгоритмами

Мета роботи: ознайомитися з основними поняттями криптографії. Ознайомитися з поняттям дайджеста повідомлення та деякими засобами його отримання та перевірки.

Завдання роботи: створити програмні реалізації простих криптографічних алгоритмів. Ознайомитися з утилітами для отримання та перевірки дайджестів повідомлень. Ознайомитися з алгоритмами отримання дайджестів та на їх основі створити аналогічну утиліту самостійно.

Аудиторний час – 4 акад. години.

Короткі теоретичні відомості (1)

Криптографія (від грецьких слів *kryptos* – прихований і *graphein* – писати) – це дисципліна, що вивчає математичні методи забезпечення конфіденційності, цілісності і аутентичності авторства інформації.

Шифром називають пару алгоритмів шифрування і розшифрування. Дія шифру керується цими алгоритмами та ключем.

Ключ шифрування – це секретний параметр (в ідеалі, відомий лише двом сторонам), який використовується в алгоритмі шифрування для створення унікального контексту під час шифрування повідомлення. Ключі мають велике значення, оскільки без змінних ключів алгоритми шифрування легко «зламуються» і в більшості випадків були б непридатні для використання.

Наведемо кілька прикладів шифрів (алгоритмів шифрування).

Шифрування методом Цезаря

Римський імператор Гай Юлій Цезар (1 ст. до н.е.) використовував цей шифр для секретного листування зі своїми генералами. Шифр Цезаря полягає у зміщенні кожної літери повідомлення за алфавітом на певну кількість позицій *m*. Тобто, якщо буква кодованої фрази має позицію *j* в алфавіті, то при шифруванні вона замінюється буквою, що знаходиться в алфавіті

на позиції $(j + m) \bmod n$, де n – кількість букв в алфавіті. (У оригінальному шифрі Цезаря число n дорівнювало 3.)

Шифр Віженера

У шифрі Цезаря літера зміщується за алфавітом на декілька позицій, і ця операція виконується однаково з усіма літерами вхідного повідомлення. Шифр Віженера полягає у послідовному (циклічному) застосуванні до кожної наступної літери вхідного тексту одного з кількох шифрів Цезаря з різними значеннями зміщення. Для зашифровування може використовуватися таблиця алфавітів, звана *tabula recta*, або квадрат (таблиця) Віженера.

Шифр Вернама

Для застосування шифра Вернама вхідний текст необхідно перевести у двійкову форму. (Сам Вернам реалізував свій винахід для шифрування телеграфних повідомлень і, відповідно, використовував телеграфний код Бодє) Для отримання шифротекста відкритий текст об'єднується операцією «виключне АБО» (XOR) з секретним ключем. Так, наприклад, маючи відкритий текст (1 1 0 0 0), при застосуванні ключа (1 1 1 0 1) отримуємо зашифроване повідомлення (0 0 1 0 1). Отримавши зашифроване повідомлення (0 0 1 0 1) і застосувавши до нього повторно операцію «виключне АБО» з тим же ключем (1 1 1 0 1), отримаємо вихідне повідомлення – відкритий текст (1 1 0 0 0).

Шифр Вернама вважається однією з найпростіших криптосистем, і при цьому володіє абсолютною криптографічною стійкістю. Для абсолютної криптографічної стійкості ключі, що застосовуються, повинні мати три властивості:

- Мати випадковий рівномірний розподіл;
- Ключ має бути за розміром не меншим, ніж заданий відкритий текст;
- Кожен ключ може бути застосованим лише один раз. У випадку повторного застосування ключів супротивник легко розшифрує перехоплену шифровку.

Шифр перестановки «скітала» (scítala)

Цей шифр використовували у Спарті ще у V столітті до нашої ери. На стрижень циліндричної форми, який мав назву «скітала», намотували спіраллю (виток до витка) смужку пергаменту чи шкіри і писали на ній уздовж стрижня декілька рядків тексту повідомлення. Потім смужку пергаменту з написаним текстом

розмотували і знімали із стрижня. Букви на розгорнутій смужці виглядали розташованими хаотично. Для відновлення повідомлення потрібно було намотати смужку на такий же стрижень, який таким чином відігравав роль ключа шифрування.

Шифруючі таблиці

Простим прикладом табличного шифру перестановки є проста перестановка – метод шифрування, схожий з шифром скітала. Для реалізації такого шифру запишемо текст повідомлення в таблицю по рядках, а після цього прочитаємо символи по стовпцях. Для розшифрування виконуємо зворотню операцію – записуємо по стовпцях, читаємо по рядках. Ключем такого шифрування є сукупність двох чисел – розміри таблиці.

Хеш-функцією (англ. – hash function) називається така функція, яка обробляє вхідне повідомлення (вхідні дані) будь-якої довжини, і видає блок вихідних даних певної довжини, яка визначається тільки видом функції, але не залежить від розміру і вмісту вхідних даних. При цьому значення вихідних даних цілком залежить від вхідних даних і лише від них (хеш-функції не використовують ключів). Вихідні дані, отримані в результаті застосування хеш-функції до певних вхідних даних (вхідного повідомлення), називають хешем повідомлення, хеш-сумою повідомлення, відбитком повідомлення, дайджестом повідомлення (англ. – message digest).

Хеш-функції володіють наступними властивостями:

1. Хеш-функція має нескінченну область визначення.
2. Хеш-функція має скінченну область значень.
3. Хеш-функція – це одностороння функція (рус. – односторонняя, необратимая функция; англ. – one-way function) Це означає, що неможливо, знаючи тільки результат хеш-функції, відновити початкові дані, за якими був обчислений цей результат.
4. Хеш-функція непередбачуваним чином змінює своє значення навіть при зміні одного-єдиного біта у вхідних даних. Для хорошої хеш-функції зміна одного біта у вхідному потоці інформації міняє близько половини всіх даних вихідного потоку, тобто результату хеш-функції.

В сучасних електронних системах обробки інформації результати обчислення хеш-функцій мають вигляд послідовності нулів і одиниць певної довжини. Для кожного виду хеш-функції ця

довжина постійна (наприклад 160 біт для SHA-1 або 256 біт для SHA-256) і не залежить від кількості даних, які хешуються. Навіть якщо порахувати хеш-функцію від вмісту порожнього файлу (довжина вхідного потоку дорівнює нулю), довжина результату вийде та сама.

Хеш-функції широко використовуються в криптографії для забезпечення цілісності інформації, тобто гарантування того, що інформація в процесі її зберігання чи передачі не зазнала несанкціонованої зміни. Для забезпечення цілісності необхідно мати критерій виявлення будь-яких маніпуляцій з даними, тобто вставки, видалення або заміни окремих елементів. Таке виявлення має на меті запобігти цілеспрямованому нав'язуванню зловмисником фальсифікованої інформації, або випадковому пошкодженню даних внаслідок таких факторів, як шуми в каналі зв'язку або ненадійні пристрої зберігання.

Порядок виконання роботи

1. Ознайомтеся з наведеними теоретичними відомостями.
2. Для виконання роботи оберіть будь-яке середовище програмування на Ваш вибір.
3. Реалізуйте чотири пари алгоритмів шифрування і відповідного розшифрування – по одній парі (*шифрування-розшифрування*) з наступних категорій:
 - а) шифрування заміною;
 - б) шифрування перестановкою;
 - в) шифрування гамуванням (для цього можна використати отримані раніше псевдовипадкові послідовності);
 - г) шифрування аналітичним перетворенням.

Обирайте або розробляйте алгоритми індивідуально, так, щоб вони не повторювали алгоритми інших студентів.

4. Ознайомтеся з засобами командного рядка для Windows: HashConsole, HashUtils, rhash.

5. Ознайомтеся з одним із засобів розрахунку та перевірки хеш-сум з графічним інтерфейсом (за індивідуальним варіантом, рекомендується програму знайти самостійно).

6. Ознайомтеся з засобами розрахунку та перевірки хеш-сум, які можна використати з командного рядка GNU/Linux. В усіх

сучасних дистрибутивах Linux за умовчанням наявні утиліти md5, md5sum, sha* та інші.

7. Ознайомтесь з прикладами програмної реалізації алгоритму MD5. Спробуйте перевірити коректність реалізації алгоритму.

8. Підготуйте звіт про виконання роботи. Наведіть опис опцій використаних утиліт, скріншоти та пояснення щодо виконання кожного пункту завдання. Щодо кожного з програмно реалізованих алгоритмів занесіть до звіту код програми, опис алгоритму (словесний опис, схему перетворення даних, тощо), приклад шифрування або хешування (вхідний текст, використаний ключ і отриманий шифротекст чи хеш-сума).

9. Здайте і захистіть звіт про виконання роботи. Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Охарактеризуйте криптографію як галузь знань.
2. Поясніть поняття: «алгоритм шифрування» та «ключ шифрування».
3. Поясніть поняття: «конфіденційність інформації», «цілісність інформації», «автентичність інформації».
4. Поясніть поняття: «шифрування заміною», «шифрування перестановкою», «шифрування гамуванням», «шифрування аналітичним перетворенням».
5. Оцініть можливості використання функції random одного з середовищ програмування для отримання псевдовипадкових послідовностей чисел з метою застосування у криптографічних перетвореннях.
6. Що називається дайджестом повідомлення?
7. Яким чином дайджести повідомлення використовуються для захисту інформації?
8. Які вимоги висуваються до алгоритмів хешування? Поясніть необхідність цих вимог.
9. Що називається колізією при підрахунку хеш-сум?
10. Чому використовується ряд різних алгоритмів хешування? В чому полягає різниця між ними?
11. Охарактеризуйте засоби командного рядка Windows та Linux, за допомогою яких можна порахувати хеш-суми.

12. Що називається цілісністю інформації? Як можна використати утиліти хешування в цілях гарантування цілісності інформації?

13. Як би Ви могли використати дайджести повідомлень у власній професійній діяльності?

Лабораторна робота №2.2. Застосування криптографічних програмних бібліотек

Мета роботи: ознайомлення з програмними бібліотеками криптографічних функцій..

Завдання роботи: використовуючи можливості криптографічних програмних бібліотек, створити програмний додаток, що виконує прості криптографічні операції.

Аудиторний час – 2 акад. години.

Короткі теоретичні відомості

Криптографічна бібліотека – це спеціалізоване програмне забезпечення, призначене для виконання криптографічних задач (шифрування даних, створення цифрових підписів, використання хеш-функцій, створення цифрових сертифікатів та обміну ключами). У програмуванні криптобібліотеки використовуються, як спеціальні бібліотеки, що містять реалізації криптографічних алгоритмів шифрування та перетворення даних. Для використання їх потрібно підключити до проекту програми, як і будь-які інші бібліотеки. Після цього можна використовувати функції, описані у бібліотеці.

Botan – мобільна криптографічна бібліотека класів. Ця бібліотека в даний час включає широкий вибір блоків і потоків шифрування, хеш функцій, різні сервісні функцій і класи. Використовується з мовою C++ на системах Linux.

Crypto++ (також *Cryptopp*, *libcryptopp*, *libcrypto++*) – безкоштовна C++ бібліотека з відкритим кодом, що містить опис класів криптографічних схем. Розробляється з 1995 року. Це комплекс C++ файлів, в яких описані функції шифрування даних,

хеш-функції, функції генерації цифрових ключів, а також функції створення цифрових сертифікатів.

Network Security Services (NSS) – набір бібліотек, розроблених для підтримки крос-платформних серверних додатків і для забезпечення їх безпеки.

BeeCrypt – криптографічна бібліотека з відкритим початковим кодом, написана на C++ та асемблері. Вона містить реалізацію ряду відомих криптографічних алгоритмів, включаючи Blowfish, SHA-1, Diffie-Hellman. Ця бібліотека є універсальним інструментарієм, який може використовуватися при створенні різноманітних додатків. BeeCrypt поширюється під ліцензією GNU.

PassGuard Framework – бібліотека для управління паролями в зашифрованому файлі. Містить набір додатків, що підтримують будь-які типи кодованих файлів. Підтримуються платформи POSIX, зокрема Linux, UNIX.

RC5Simple – це проста мультиплатформенна криптографічна бібліотека C++, яка призначена для шифрування / дешифрування масивів і файлів.

Інтерфейс Microsoft CryptoAPI

У світі Windows одним з найбільш поширених криптографічних інтерфейсів є Microsoft CryptoAPI. Розповсюдження CryptoAPI пов'язане не тільки з його зручністю, документованістю та іншими об'єктивними чинниками. Сама Microsoft найактивнішим чином інтегрувала його в свої операційні системи і прикладні програми. Сучасні операційні системи Microsoft містять багато криптографічних підсистем різного призначення як прикладного рівня, так і рівня ядра, і ключову роль в реалізації цих підсистем відіграє інтерфейс CryptoAPI. На основі використання можливостей базових криптографічних функцій можна не тільки більш глибоко розуміти роботу всього інтерфейсу CryptoAPI, але й створювати власні криптографічні підсистеми будь-якого рівня.

Криптопровайдером називають незалежний модуль, що забезпечує безпосередню роботу з криптографічними алгоритмами. Кожен криптопровайдер повинен забезпечувати:

- реалізацію стандартного інтерфейсу криптопровайдера;
- роботу з ключами шифрування, призначеними для забезпечення роботи алгоритмів, специфічних для даного криптопровайдера;

- неможливість втручання третіх осіб в схему роботи алгоритмів.

Криптографічні функції у Microsoft .NET

Велика частина криптографічних класів (не абстрактних) .NET базується на криптопровайдерах CryptoAPI. Втім, є і виключення (наприклад, Sha256managed). Ієрархія класів .NET дозволяє абстрагуватися від конкретної реалізації алгоритму, що може забезпечити простий перехід на не прив'язані до CryptoAPI класи в майбутньому. На жаль, документація .NET щодо криптографічних класів залишає бажати кращого.

Порядок виконання роботи

1. Ознайомтесь із наведеними теоретичними відомостями.
2. Оберіть середовище розробки, в якому буде виконуватись програмний проект.
3. Створіть новий проект необхідного типу. (Рекомендується ConsoleApplication.)
4. Підключіть до нього необхідну бібліотеку. Використовуючи функції бібліотеки, реалізуйте в додатку можливість виконувати криптографічні операції. Для простоти візьміть такі операції, як підрахування хеш-сум і шифрування-розшифрування даних за одним з алгоритмів.
5. Перевірте роботу розробленої програми:
 - 5.1. Підрахуйте хеш-суму якогось об'єкта і порівняйте результат з результатом підрахунку хеш-суми, отриманої будь-яким іншим способом (за допомогою сторонніх утиліт).
 - 5.2. Зашифруйте просте повідомлення (наприклад, «hello world») і далі розшифруйте отриманий шифротекст.
6. Підготуйте звіт про виконану роботу. Включіть до нього код розробленої програми з детальними коментарями, опис використаних заголовочних файлів та функцій, наведіть приклади роботи програми на тестових вхідних даних.
7. Здайте та захистіть звіт. Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Дайте визначення понять «криптографічна бібліотека», «криптографічний інтерфейс», «криптопровайдер».

2. Як Ви вважаєте, чому виникла необхідність у розробці криптографічних бібліотек?

3. Яким чином можна використати функції криптографічної бібліотеки у програмному проекті?

4. Охарактеризуйте інтерфейс Microsoft CryptoAPI.

5. Охарактеризуйте бібліотеку CryptoPP.

6. Дайте характеристику функціям використаної Вами криптографічної бібліотеки.

5. Опишіть алгоритм шифрування, використаний Вами у програмі.

Лабораторна робота №2.3. Криптографічний захист даних у файлових системах

Мета роботи: ознайомитися з основними проблемами захисту інформації у файлових системах та засобами їх розв'язання.

Завдання роботи: встановити програмне забезпечення для криптографічного захисту даних у файлових системах та навчитися використовувати його функції.

Аудиторний час – 4 акад. години.

Короткі теоретичні відомості

Питання захисту даних, що зберігаються у комп'ютерній системі, від доступу неавторизованих осіб, мають надзвичайну важливість. На сучасних комп'ютерних системах можуть зберігатися особисті файли, вміст яких призначений тільки для їх власника; можуть зберігатися і дані, що складають комерційну або державну таємницю. Порушення конфіденційності цих даних, їх знищення чи модифікація можуть призвести до різноманітних небажаних наслідків, моральних та матеріальних втрат. Потреба у захисті інформації, що зберігається у комп'ютерній системі, привела до створення ряду програмних продуктів, що розв'язують цю задачу, шифруючи дані. Навіть якщо зловмисник отримає доступ до комп'ютера і скопіює вміст його дисків, він не зможе його розшифрувати, якщо не знатиме ключа.

Популярною програмою криптографічного захисту даних у файлових системах є *VeraCrypt*. Це програмне забезпечення

дозволяє створити та використовувати в реальному часі віртуальний пристрій зберігання даних – зашифрований дисковий том. У файловій системі такий том може виглядати як великий файл, що містить зашифровані дані. Зашифрована вся інформація віртуальної файлової системи, включаючи імена файлів, назви каталогів, вміст кожного файлу, вміст місця, позначеного як вільне, метадані тощо. Дані, збережені у зашифрованому томі, неможливо прочитати (дешифрувати) без використання правильного пароля або ключа (ключового файлу).

Файли можуть бути скопійовані в том VeraCrypt і з нього таким же способом, як вони копіюються на і з будь-якого звичайного диска (наприклад, за допомогою drag-and-drop). Файли автоматично розшифровуються «на льоту» (у оперативній пам'яті), коли вони читаються або копіюються із зашифрованого тому VeraCrypt. Аналогічно, файли, які записуються або копіюються в том VeraCrypt, автоматично шифруються «на льоту» у оперативній пам'яті прямо перед тим, як вони записуються на диск. Для цього не потрібно зберігати в оперативній пам'яті весь файл, який потрібно зашифрувати чи розшифрувати, великі файли можуть оброблятися по частинах. Таким чином, немає додаткових вимог до оперативної пам'яті для VeraCrypt.

VeraCrypt ніколи не зберігає будь-які розшифровані дані на диску – вони лише тимчасово зберігаються у оперативній пам'яті. При монтуванні тому VeraCrypt, дані, що зберігаються на ньому, залишаються зашифрованими. Під час перезавантаження Windows або вимкнення живлення комп'ютера том буде відмонтовано, а файли, що зберігаються в ньому, залишаться зашифрованими.

Порядок виконання роботи

1. Ознайомтеся з наведеними теоретичними відомостями.
2. Завантажте і встановіть програму VeraCrypt.
3. Запустіть VeraCrypt, двічі клацнувши виконуваний файл програми або натиснувши пункт VeraCrypt в головному меню Windows. Має з'явитися головне вікно програми VeraCrypt.
4. Натисніть кнопку Create Volume – Створити том. Має з'явитись вікно Майстра створення томів.

6. У діалоговому вікні Volume Type можна вказати, чи буде наш контейнер видно в файловій системі як звичайний диск, або буде створено прихований том.

7. У наступному вікні Volume Location необхідно вказати розміщення, у якому ваш файл-контейнер VeraCrypt буде створений. Необхідно вказати також ім'я файлу. .

8. У наступному вікні Encryption Options буде запропоновано обрати деталі алгоритму шифрування.

9. У наступному вікні Volume Size вказується обсяг дискового простору, що виділяється під контейнер. Цей розмір обмежений згори тільки розміром носія (розділу, тому), а його найменше значення залежить від файлової системи.

10. У наступному вікні потрібно вибрати пароль на доступ до даних.

11. Для генерації параметрів шифрування програмі, окрім пароля, потрібна ще деяка кількість випадкових даних. Для їх отримання програма запропонує вам водити курсором в рамках вікна майстра створення тому, випадково, наскільки це можливо, щонайменше протягом 30 секунд.

12. Після того, як том створено і користувач натиснув Exit, програма пропонує змонтувати його. Виберіть зі списку літеру, під якою новий диск буде змонтовано в системі. Далі натисніть кнопку Select File і виберіть файл-контейнер VeraCrypt. Після цього натисніть кнопку Mount. При цьому програма запитає пароль до тому. Мається на увазі пароль, який Ви задали при його створенні.

13. Підготуйте звіт про виконану роботу. Наведіть скріншоти та пояснення щодо виконання кожного пункту завдання.

14. Здайте і захистіть звіт про виконання роботи. Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Як шифрування даних на диску дозволяє підвищити безпеку інформації на комп'ютері?

2. Охарактеризуйте програмне забезпечення VeraCrypt

3. Охарактеризуйте види шифрів, що застосовуються у VeraCrypt.

4. Що таке файл-контейнер VeraCrypt? Які дії можна здійснювати з файл-контейнером VeraCrypt?

5. Які загрози безпеці інформації слід передбачити при використанні програм, подібних до VeraCrypt? Як можна подолати ці загрози?

6. Чи можна використовувати файл-контейнери, створені програмою VeraCrypt, для конфіденційної передачі інформації іншому суб'єкту? Якщо не можна, то чому? Якщо можна, то яким чином це зробити?

Лабораторна робота №2.4. Криптографічні програмні засоби з відкритим ключем

Мета роботи: ознайомитися з основними поняттями асиметричних криптографічних систем.

Завдання роботи: встановити програмне забезпечення для ОС Windows та GNU/Linux, що виконує криптографічні операції з відкритим ключем, та навчитися його використовувати.

Аудиторний час – 2 акад. години.

Короткі теоретичні відомості

Історично розвиток шифрування починався з методів та алгоритмів, які в даний час класифікують як «симетричні». Симетричність полягає в тому, що обидві сторони використовують для зашифрування та розшифрування повідомлення один і той самий секретний ключ. Перевагою симетричних методів шифрування є їх достатня теоретична вивченість та висока криптостійкість. До основних недоліків цих методів слід віднести потребу у додаткових заходах таємності під час поширення ключів, а також той факт, що методи з секретним ключем працюють тільки в умовах повної довіри партнерів один до одного.

В останні три десятиліття з'явилися й набули розвитку нові методи, що одержали назву методів *несиметричної* (або *асиметричної*) *криптографії*. Робота асиметричних криптографічних систем основана на тому, що кожен суб'єкт, що бажає отримувати зашифровані повідомлення, генерує два ключі, пов'язані між собою за визначеним правилом. Один з цих ключів – *відкритий* (публічний), а інший – *закритий* (секретний, приватний).

Початковий текст шифрується за обумовленим алгоритмом шифрування, при цьому використовується відкритий ключ адресата. Отриманий шифротекст передається адресату. Зашифрований текст практично неможливо розшифрувати, знаючи той же відкритий ключ, який використовувався для зашифрування. Дешифрування повідомлення можливе тільки з використанням закритого ключа, який відомий тільки самому адресатові.

Несиметрична криптографія використовує спеціальні математичні методи, розроблені в результаті розвитку нових галузей математики. Найбільш розповсюджені криптосистеми з відкритим ключем на сьогоднішній день – система Ель-Гамала; криптосистеми на основі еліптичних рівнянь; алгоритм RSA.

Криптосистеми з відкритим ключем дозволяють двом сторонам утворити закритий від сторонніх осіб, шифрований канал спілкування, незважаючи на те, що вони до цього ніколи не зустрічалися і не обмінювалися секретними ключами.

Порядок виконання роботи

1. Ознайомтеся з наведеними теоретичними відомостями.
2. Підготуйте для виконання роботи Windows-систему та встановіть на неї програмний продукт PGP Desktop.
3. Підготуйте для виконання роботи Linux-систему. У більшості сучасних дистрибутивів GNU/Linux (серверних та настільних загального призначення) за замовчуванням присутній комплекс утиліт GNU Privacy Guard (GPG) – це вільний аналог PGP.
4. Виконайте з обома програмами (PGP і GPG) наступні дії:
 - 4.1. Створіть пару ключів – публічний і приватний.
 - 4.2. Експортуйте публічний ключ, тобто отримайте його текстову форму, придатну, наприклад, для пересилки електронною поштою.
 - 4.3. Подивіться список наявних ключів, до яких має доступ ваша КСВК.
 - 4.4. Знайдіть в інтернеті відкриті ключі інших осіб. Завантажте який-небудь відкритий ключ, перевірте його цілісність за наведеним відбитком, і додайте його до програми (імпортуйте).
 - 4.5. Використовуючи свій публічний ключ, зашифруйте просте повідомлення. Використовуючи відповідний приватний ключ, розшифруйте його.

4.6. Підпишіть будь-який файл своїм цифровим підписом та передайте його (разом із Вашим підписом) товаришу. Отримайте від товариша інший файл разом з його підписом. Перевірте справжність файлу.

4.7. Підпишіть чужий публічний ключ. Своїм підписом Ви підтверджуєте, що Ви знаєте власника ключа і що цей ключ належить саме йому.

4.8. Отримайте підписаний ключ від товариша. Подивіться список підписів, наявних на ключі. Перевірте підпис Вашого товариша, яким він підписав який-небудь ключ.

4.9. Виконайте додання та видалення компонентів ключа.

4.10. Створіть відкликаючий сертифікат (revocation certificate).

4.11. Виконайте відкликання компонентів ключа.

5. Підготуйте звіт про виконану роботу. Наведіть скріншоти та пояснення щодо виконання кожного пункту завдання.

6. Здайте і захистіть звіт про виконання роботи. Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Поясніть різницю між симетричними та несиметричними криптосистемами.

2. Поясніть поняття «публічний ключ», «приватний ключ».

3. Як слід поводитися з публічним ключем? Чому?

4. Як слід поводитися з приватним ключем? Чому?

5. Поясніть, що таке головний ключ і його компоненти (підключі).

6. Поясніть поняття «відкликаючий сертифікат».

7. Поясніть призначення електронного цифрового підпису.

8. Як підписати документ електронним цифровим підписом?

9. Як перевірити справжність документа, підписаного електронним цифровим підписом? Що для цього необхідно мати?

Лабораторна робота №2.5. Стеганографічне приховування інформації

Мета роботи: ознайомитися з основними поняттями комп'ютерної стеганографії.

Завдання роботи: Навчитися використовувати програмне забезпечення для стеганографічного приховування інформації, виготовити стеганографічний об'єкт, здійснити читання та видалення інформації з нього.

Аудиторний час – 4 акад. години.

Короткі теоретичні відомості

Стеганографія – це наука і мистецтво про приховування інформації. На відміну від криптографії, метою якої є перешкодити стороннім особам дізнатися про зміст закодованої інформації, метою стеганографії є перешкодити стороннім особам дізнатися навіть про те, що прихована інформація *взагалі існує* (зберігається чи передається) в даному місці.

Найпростіша модель стеганографічного кодування інформації включає *носії* (Carrier), *повідомлення* (Message) і *пароль* (Password). Стеганографічний об'єкт створюється заміною обраних надлишкових бітів носія на біти повідомлення. Процес складається з двох етапів.

- 1) Визначення надлишкових бітів в носії.
- 2) Впровадження секретного повідомлення, яким замінюється підмножина надлишкових бітів.

В сучасній стеганографії використовуються різноманітні методи приховування інформації, що мають різні ступені складності: використання молодшого біта (least significant bit – LSB), маніпуляції з шумами, різноманітні алгоритми перетворення зображень; «патчворк» (patchwork), блокове кодування шаблонів (pattern block encoding), методи розширення спектру, маскування.

Методи маскування і фільтрації, як правило, застосовуються до кольорових (24 біт) і сірих зображень. У цих методах зображення позначається «цифровими водяними знаками», які за властивостями нагадують водяні знаки, що використовуються на папері. Ці методи проводять аналіз зображення, і далі вставляють інформацію в значні площі таким чином, що приховане послання має більш

інтегральний зв'язок з зображенням-контейнером, ніж у випадку простого впровадження його на рівні перешкод.

Порядок виконання роботи

1. Ознайомтесь з теоретичними відомостями.
2. Встановіть програму Fox Secret 1.00.
3. Розгляньте пункт меню *Secret | New*. Цей пункт меню дає можливість обрати повідомлення, яке ми будемо приховувати. Якщо обрати значок *Safe* (безпечний метод), ви зможете приховати цілі групи файлів і каталогів із збереженням їх структури).
4. Виберіть значок *File/Image/Sound/Document* та натисніть кнопку *Forward* (Вперед). Відкриється діалогове вікно вибору файла-контейнера.
5. Введіть пароль і натисніть кнопку *Next* (Далі).
6. Тепер слід обрати таємне повідомлення. Оберіть інший файл – наприклад, документ Word або зображення, та натисніть «Відкрити». Вкладення інформації виконане.
7. Закрийте програму і перевірте, що розмір зображення-контейнера збільшився на розмір вбудованого повідомлення.
8. Знову запустіть програму Fox Secret.
9. Для отримання даних про приховане повідомлення використайте пункт меню *Secret | Open* та оберіть зображення, в яке був прихований інший файл. На запит програми, введіть пароль.
10. У вікні, яке з'явилося, ви побачите інформацію про прихований файл (формат файлу, ім'я файлу, його розмір, дату створення та дату зміни).
11. Щоб отримати прихований файл та зберегти його на диску, натисніть *File*, далі натисніть *Get* і вкажіть місце для збереження .
12. Відкрийте зображення з вбудованими даними (стего-об'єкт) в програмі IrfanView (безкоштовний переглядач зображень). Оберіть пункт меню *Image / Information*. У вікні "*Image properties*" натисніть кнопку *Comment*. У вікні, що відкрилося, ви можете побачити, як приховане повідомлення зберігається у контейнері у формі коментаря.
13. Спробуйте видалити коментар. Після цього файл-контейнер повернеться до своєї первісної форми.

14. За матеріалами інтернету підготуйте коротку інформацію про декілька інших програм, що реалізують стеганографічні методи.

15. Підготуйте звіт про виконану роботу. Наведіть скріншоти та пояснення щодо виконання кожного пункту завдання щодо Fox Secret. Опишіть роботу з індивідуально обраною програмою (п.15 завдання).

16. Здайте і захистіть звіт про виконання роботи. Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Дайте визначення стеганографії.
2. Що називається носієм, повідомленням, паролем у стеганографії?
3. Які методи приховування повідомлень використовуються у стеганографії?
4. З яких двох етапів складається процес приховування інформації у стеганографії?
5. Яким чином програма Fox Secret зберігає приховане повідомлення в контейнері?