Лабораторная работа

*Изучение программных средств защиты от несанкционированного доступа*

Содержание задания

1. Пункты 1-3 выполняются в виртуальной машине Windows или с правами администратора. Скопировать в личную папку на локальном жестком диске файл whisper.msi.
2. Если программа Whisper 32 не установлена (соответствующий пункт отсутствует в главном меню), то установить ее с помощью файла whisper.msi.
3. Запустить программу whisper.exe, предназначенную для создания и ведения базы данных паролей пользователя.
   1. Изучить назначение и основные функции программы и включить в отчет соответствующие сведения.
   2. Создать 2-3 записи о паролях к различным ресурсам (записи обязательно должны содержать фамилию и инициалы студента в поле имени учетной записи пользователя или в поле комментариев Memo).
   3. Включить в отчет копии экранных форм, использованных при выполнении данного пункта.
   4. Завершить работу с программой whisper.exe.
4. Пункт выполняется на дисках, использующих файловую систему NTFS. На примере папок и файлов из папки с личными документами освоить средства обеспечения конфиденциальности информационных ресурсов с помощью шифрующей файловой системы Windows (команда Свойства контекстного меню объекта, вкладка Общие, кнопка Другие, выключатель Шифровать содержимое для защиты данных). Включить в отчет ответы на вопросы:
   1. Скрывается ли наличие в системе зашифрованных файлов и папок.
   2. Как создается и где хранится ключ шифрования файла.
   3. Как обеспечивается в системе возможность восстановления зашифрованных файлов при невозможности входа пользователя в систему или при его отсутствии.
   4. Освоить средства обеспечения совместного доступа нескольких пользователей к зашифрованным файлам (с помощью кнопки Подробно окна его дополнительных атрибутов) и включить в отчет сведения о порядке использования этих средств и ответ на вопрос, среди каких пользователей возможен выбор тех, кому будет разрешен доступ к зашифрованному файлу.
   5. Включить в отчет копии экранных форм, полученных при выполнении данного пункта.
5. Начать работу с Microsoft Word из пакета Microsoft Office (версии XP или старше).
   1. Освоить средства управления параметрами шифрования конфиденциальных документов (команды Файл | Сведения | Защита документа | Зашифровать с использованием пароля в Office 2013, Файл | Сведения | Защитить документ | Зашифровать паролем в Office 2010, Кнопка Microsoft Office | Подготовка | Зашифровать документ в Office 2007, Сервис | Параметры | Безопасность и кнопка Дополнительно в Office 2003).
   2. Включить в отчет копии экранных форм, полученных при выполнении данного пункта.
6. С помощью программы selfcert.exe из пакета Microsoft Office (вызов этой программы возможен через меню Пуск | Программы | Средства Microsoft Office | Средство создания цифровых сертификатов для проектов VBA) создать собственную пару ключей асимметричного шифрования и «самоподписанный» сертификат своего открытого ключа на имя, содержащее фамилию и инициалы студента. Если эта программа не установлена или создание сертификатов невозможно в соответствии с выбранной в системе политики безопасности, то создать самоподписанный сертификат с помощью утилиты makecert (makecert /r /n "cn=*Фамилия И.О.* *студента*" /ss my), для вызова которой использовать командную строку Пуск | Программы | Microsoft Visual Studio | Visual Studio Tools | Visual Studio Command Prompt. Включить в отчет копии экранных форм, полученных при выполнении данного пункта.
7. Освоить средства добавления электронной подписи к документам Microsoft Office на примере программы Microsoft Word (команды Файл | Сведения | Защита документа | Добавить цифровую подпись в Office 2013, Файл | Сведения | Защитить документ | Добавить цифровую подпись в Office 2010, Кнопка Microsoft Office | Подготовка | Добавить цифровую подпись в Office 2007, Сервис | Параметры | Безопасность, кнопки Цифровые подписи и Добавить). С помощью кнопки Просмотреть свойства сертификата ознакомиться с содержанием сертификата открытого ключа. Включить в отчет ответы на вопросы:
   1. Какая информация содержится в сертификате открытого ключа.
   2. Что такое путь сертификации.
   3. Что происходит с электронной подписью в случае попытки сохранения документа после внесения в него изменений.
   4. Включить в отчет копии экранных форм, полученных при выполнении данного пункта.
8. Пункты 8-10 выполняются в виртуальной машине Windows или с правами администратора. Скопировать в произвольную папку на локальном жестком диске файл QS12Setup.zip и извлечь файлы из этого архива.
9. Если программа QuickStego не установлена (отсутствует соответствующий пункт в главном меню), то запустить программу QS12Setup.exe для установки стеганографической программы QuickStego..
10. Запустить стеганографическую программу QuickStego. С произвольными файлами контейнеров (изображений) и сообщений (текстовых файлов, которые можно выбирать или создавать непосредственно в окне программы) изучить функции программы и включить в электронную версию отчета копии экранных форм, полученных при использовании этой программы, после чего завершить работу с ней. Включить в отчет ответы на вопросы:
    1. Как происходит скрытие и извлечение сообщений из контейнеров.
    2. В чем разница между методами криптографии и стеганографии.
    3. Каким должно быть соотношение между размерами файла-контейнера и файла-сообщения при использовании программы QuickStego и почему.
11. Освоить средства добавления электронной подписи к макросам, включаемым в состав документов Microsoft Office (на примере программы Microsoft Word): добавить в документ автоматически выполняющийся макрос (команды Вид | Макросы | Макросы в Office 2013, 2010 и 2007, Сервис | Макрос | Макросы в Office 2003) и воспользоваться командой Редактора Visual Basic for Application Tools | Digital Signature. Включить в отчет копии экранных форм, полученных при выполнении данного пункта.
12. Пункты 12-25 выполняются в операционной системе Linux. Открыть Консоль (Главное меню | Приложения | Система | Терминал | Терминал). Получить справку о программе gpg (для получения справки воспользоваться командой gpg -?). Включить в отчет о выполнении лабораторной работы сведения о вариантах использования этой программы (командах и параметрах).
13. Создать для себя пару ключей асимметричного шифрования:
    1. Выполнить команду gpg с параметром -v команды --gen-key.
    2. Выбрать тип ключа с использованием дополнительной информации об используемых алгоритмах
    3. Выбрать длину ключа.
    4. Выбрать срок действия ключей 60 дней.
    5. Подтвердить выбранные параметры ключа.
    6. Ввести информацию для идентификации владельца ключа (User ID), указав свои фамилию и инициалы (латиницей без пробелов, например, IvanovPS), а также адрес электронной почты и произвольный комментарий.
    7. Принять созданный User ID.
    8. Ввести и подтвердить пароль для защиты секретного (закрытого) ключа.
    9. Сгенерировать случайное значение создаваемого ключа
    10. Включить в отчет о лабораторной работе протокол работы программы gpg в режиме создания пары ключей.
    11. Экспортировать созданный открытый ключ в текстовый файл в своем домашнем каталоге с помощью команды gpg с параметрами --export -ao *имя файла*.asc (в качестве имени файла указать имя из идентификатора владельца ключа User ID). Включить в отчет о лабораторной работе стоку с вызовом этой команды.
14. Зашифровать текстовый файл случайным сеансовым ключом для конкретного получателя:
    1. Создать текстовый файл example.txt в своем домашнем каталоге (в файле обязательно должны быть строки, содержащие фамилию и инициалы студента, номер учебной группы и номер лабораторной работы).
    2. Выполнить программу gpg с командой -e example.txt.
    3. Ввести свой идентификатор владельца ключа User ID в качестве получателя зашифрованного файла.
    4. Зашифрованный файл получит те же имя и расширение, а также еще одно расширение имени .gpg.
    5. Включить в отчет о лабораторной работе протокол работы программы gpg в режиме шифрования случайным ключом.
15. Расшифровать файл, зашифрованный случайным сеансовым ключом, с выводом в файл:
    1. Выполнить программу gpg с командой -d example.txt.gpg >example.txt.
    2. Ввести пароль для получения доступа к своему закрытому ключу (закрытому ключу получателя).
    3. Включить в отчет о лабораторной работе протокол работы программы gpg в режиме расшифрования с выводом в файл.
16. Зашифровать текстовый файл сеансовым ключом, генерируемым из парольной фразы:
    1. Выполнить программу gpg с командой -c example.txt.
    2. Ввести парольную фразу с подтверждением для генерации сеансового ключа.
    3. Зашифрованный файл получит те же имя и расширение, а также еще одно расширение имени .gpg.
    4. Включить в отчет о лабораторной работе протокол работы программы gpg в режиме шифрования ключом из парольной фразы.
17. Расшифровать файл, зашифрованный сеансовым ключом из парольной фразы, с выводом в файл:
    1. Выполнить программу gpg с командой -d -o example.txt example.txt.gpg.
    2. Ввести парольную фразу для генерации ключа расшифрования.
    3. Включить в отчет о лабораторной работе протокол работы программы gpg в режиме расшифрования с выводом в файл.
18. Подписать текстовый файл:
    1. Выполнить программу gpg с командой -s example.txt.
    2. Ввести пароль для получения доступа к своему закрытому ключу.
    3. Подписанный файл получит те же имя и расширение, а также еще одно расширение имени .gpg.
    4. Включить в отчет о лабораторной работе протокол работы программы gpg в режиме получения электронной подписи (ЭП).
19. Проверить ЭП:
    1. Выполнить программу gpg с командой --verify example.txt.gpg.
    2. Включить в отчет о лабораторной работе протокол работы программы gpg в режиме проверки ЭП.
20. Получить отсоединенную подпись под текстовым файлом:
    1. Выполнить программу gpg с командой -b example.txt.
    2. Ввести пароль для получения доступа к своему закрытому ключу.
    3. Файл с отсоединенной подписью получит те же имя и расширение, а также еще одно расширение имени .sig.
    4. Включить в отчет о лабораторной работе протокол работы программы gpg в режиме получения отсоединенной подписи.
21. Проверить отсоединенную подпись:
    1. Выполнить программу gpg с командой --verify example.txt.sig.
    2. Включить в отчет о лабораторной работе протокол работы программы gpg в режиме проверки ЭЦП.
22. Проверить отсоединенную подпись после изменения подписанного файла:
    1. Изменить файл example.txt. Сохранить изменения без закрытия текстового редактора.
    2. Выполнить программу gpg с командой --verify example.txt.sig.
    3. Отменить сделанные изменения и сохранить файл. Закрыть текстовый редактор.
    4. Выполнить программу gpg с командой --verify example.txt.sig.
    5. Включить в отчет о лабораторной работе протокол работы программы gpg в режиме проверки ЭЦП.
23. Зашифровать файл для указанного получателя с выводом в текстовый файл:
    1. Выполнить программу gpg с командой -ea –r *Имя идентификатора владельца ключа User ID* example.txt.
    2. Зашифрованный файл получит те же имя и расширение, а также еще одно расширение имени .asc.
    3. Включить в отчет о лабораторной работе протокол работы программы gpg в этом режиме.
24. Расшифровать зашифрованный в текстовом формате файл:
    1. Выполнить программу gpg с командой -do example.txt example.txt.asc.
    2. Ввести пароль для получения доступа к своему закрытому ключу (закрытому ключу получателя).
    3. Включить в отчет о лабораторной работе протокол работы программы gpg в этом режиме.
25. Завершить сеанс работы с консолью с помощью команды exit.
26. Добавить в отчет о лабораторной работе титульный лист и сохранить его.
27. Предъявить преподавателю отчет о выполнении лабораторной работы.