Лабораторная работа №4

Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ

Содержание задания

1. При работе в компьютерном классе университета пункты 1-8 выполняются в окне виртуальной ОС Windows XP. Скопировать в произвольную папку на локальном жестком диске файл mosafe21.exe из указанного преподавателем сетевого диска.
2. Запустить программу mosafe21.exe и разархивировать все файлы из этого самораспаковывающегося архива.
3. Запустить программу шифрования файлов MyOldSafe. На примере работы с произвольными (несистемными) файлами различного типа изучить функции программы и включить в электронную версию отчета о лабораторной работе копии экранных форм, полученных при использовании этой программы, после чего завершить работу с ней. Включить в отчет ответы на вопросы:
   3.1. как выполняется шифрование и расшифрование файлов;
   3.2. к какой криптосистеме относится эта программа и почему;
   3.3. как формируется ключ шифрования;
   3.4. изменяется ли размер зашифрованного файла и, если изменяется, то почему;
   3.5. есть ли возможность выбора алгоритма шифрования;
   3.6. возможен ли совместный доступ к зашифрованным файлам.
4. Скопировать в произвольную папку на локальном жестком диске файл citadel.zip из указанного преподавателем сетевого диска.
5. Извлечь файлы из архива, скопированного в пункте 4.
6. Запустить программу setup.exe для установки программы шифрования файлов Citadel Safstor.
7. На примере работы с произвольными (несистемными) файлами различной природы изучить функции программы шифрования файлов Citadel Safstor, учитывая, что:

   • доступ к шифрованию (расшифрованию) возможен через контекстное меню *Проводника* Windows. Если соответствующая команда не появилась в контекстом меню Проводника, то шифрование файла возможно с помощью команды главного меню Пуск | Выполнить | “C:\Program Files\Citadel Data Security\Citadel Safstor\csenc” полный путь к шифруемому файлу. Для расшифрования файла следует в этом случае использовать команду Пуск | Выполнить | “C:\Program Files\Citadel Data Security\Citadel Safstor\csdec” полный путь к зашифрованному файлу с расширением .css;

   • другие пользователи программы Citadel Safstor могут быть созданы с помощью функции Citadel Safstor Панели управления (вкладка User Profiles, кнопка New User);

   • «переключение» на другого пользователя программы Citadel Safstor производится также с помощью Панели управления (функция Citadel Safstor, вкладка Current User).

   Включить в электронную версию отчета о лабораторной работе копии экранных форм, полученных при использовании этой программы, после чего завершить работу с ней.
   7.1. Включить в отчет ответы на те же вопросы, что и в пунктах 3.1-3.6, а также ответы на вопросы:
   7.2. какие действия выполняет пользователь при установке программы;
   7.3. для чего предназначена парольная фраза.
   7.4. Дополнительно включить в отчет краткое сравнение двух изученных программ шифрования файлов.
8. Данный пункт выполняется в операционных системах Windows 2000 / Windows XP Professional на дисках, использующих файловую систему NTFS. На примере папок и файлов из папки Мои документы освоить средства обеспечения конфиденциальности информационных ресурсов с помощью шифрующей файловой системы (команда

Свойств контекстного меню объекта, вкладка Общие, кнопка Другие, выключатель Шифровать содержимое для защиты данных). Включить в отчет ответы на вопросы:

8.1. скрывается ли наличие в системе зашифрованных файлов и папок;
8.2. где хранится ключ шифрования файла;
8.3. как обеспечивается в системе возможность восстановления зашифрованных файлов при невозможности входа пользователя в систему или при его отсутствии;
8.4. на дисках с какой файловой системой возможно использование функции шифрования файлов.
8.5. При выполнении работы в операционной системе Windows XP Professional дополнительно освоить средства обеспечения совместного доступа к зашифрованным файлам 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.
8.6. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.

9. Начать работу с Microsoft Word из пакета Microsoft Office (версии XP или старше) или текстовым процессором из пакета Open Office. Освоить средства управления параметрами шифрования конфиденциальных документов (команда Сервис | Параметры, вкладка Безопасность, кнопка Дополнительно). Включить в отчет ответы на вопросы:
   9.1. какие дополнительные параметры шифрования могут быть установлены;
   9.2. от чего зависит список доступных типов шифрования и можно ли им управлять.
   9.3. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.
10. Повторить п. 9 для программы Microsoft Excel или табличного процессора из пакета Open Office. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.
11. С помощью программы selfcert.exe из пакета Microsoft Office (в версиях Office 2003 и старше вызов этой программы возможен через меню Пуск | Программы | Средства Microsoft Office | Цифровой сертификат) создать собственную пару ключей асимметричного шифрования и «самоподписанный» сертификат своего открытого ключа. Если эта программа не установлена, то создать самоподписанный сертификат с помощью утилиты makecert (makecert /r /n "cn=Фамилия И.О." /ss my), для вызова которой использовать командную строку Пуск | Программы | Microsoft Visual Studio | Visual Studio Tools | Visual Studio Command Prompt).
    11.1. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.
12. Освоить средства добавления электронной цифровой подписи к документам Microsoft Office (версии XP или старше) или Open Office на примере программы Microsoft Word (команда Сервис | Параметры, вкладка Безопасность, кнопки Цифровые подписи и Добавить) или текстового процессора Open Office. С помощью кнопки Просмотр сертификата ознакомиться с содержанием сертификата открытого ключа. Включить в отчет ответы на вопросы:
    12.1. какая информация содержится в сертификате открытого ключа;
    12.2. что такое путь сертификации.
    12.3. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.
13. При работе в компьютерном классе университета пункты 13-15 выполняются в окне виртуальной ОС Windows XP. Скопировать в произвольную папку на локальном жестком диске файлы contrabd.zip и test.bmp из указанного преподавателем сетевого диска и извлечь файлы из архива contrabd.zip.

14. Запустить программу setup.exe для установки стеганографической программы Contraband.
15. Запустить стеганографическую программу contrab.exe. На примере работы с произвольными файлами изучить функции программы и включить в электронную версию отчета копии экранных форм, полученных при использовании этой программы, после чего завершить работу с ней. В качестве файла-контейнера можно использовать файл test.bmp или произвольный графический файл в формате BMP. Включить в отчет ответы на вопросы:
    15.1. как происходит скрытие и извлечение сообщений из контейнеров;
    15.2. в чем разница между методами криптографии и стеганографии;
    15.3. каким должно быть соотношение между размерами файла-контейнера и файла-сообщения при использовании программы contrab.exe и почему.
16. Запустить установленную в системе программу антивирусного сканирования и освоить работу с ней. Включить в электронную версию отчета о выполнении лабораторной работы копии экранных форм, полученных при использовании этой программы. Включить в отчет о лабораторной работе
    16.1. сведения о назначении и основных функциях программы, а также ответы на вопросы:
    16.2. как задаются области сканирования;
    16.3. как задаются объекты проверки на наличие вирусов;
    16.4. как определяется реакция сканера в случае обнаружения зараженного файла.

    Завершить работу с программой.
17. Проверить, обеспечена ли в системе возможность автоматического запуска (после загрузки Windows) антивирусной программы-монитора. Включить в отчет ответы на вопросы:
    17.1. в чем разница в назначении антивирусных программ-сканеров и программ-мониторов;
    17.2. как может быть обеспечена возможность автоматического запуска программ антивирусного мониторинга.
18. Начать работу с Microsoft Word или текстовым процессором пакета Open Office. Включить средства защиты от вирусов в макросах в документах Word или Open Office. Освоить использование других рассмотренных на лекциях средств защиты от вирусов в макросах (для проверки их эффективности создать новый документ с собственными автоматически выполняемыми и (или) стандартными макросами, используя в них строку с вызовом макрокоманды вывода сообщения MsgBox “Текст сообщения”). Завершить работу с Word.
    18.1. Включить в отчет сведения о способах защиты от вирусов в документах Word.
    18.2. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.
19. Повторить п. 18 для программы Microsoft Excel или табличного процессора из пакета Open Office. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.
20. Освоить средства добавления электронной цифровой подписи к макросам, включаемым в состав документов Microsoft Office версии XP или старше (на примере программы Microsoft Word) или пакета Open Office: добавить в документ автоматически выполняющийся макрос (команда Сервис | Макрос | Макросы) и воспользоваться командой Редактора Visual Basic Tools | Digital Signature.
    20.1. Включить в отчет ответ на вопрос, что произойдет после внесения изменений в документ, снабженный электронной цифровой подписью.
    20.2. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.

21. Включить в отчет титульный лист и сохранить файл с электронной версией отчета в произвольной папке на локальном жестком диске.
22. Предъявить преподавателю электронную версию отчета о лабораторной работе с копиями использовавшихся экранных форм и соответствующими им номерами пунктов задания (3, 7, 8.6, 9.3, 10, 11.1, 12.3, 15, 16, 18.2, 19, 20.2).
23. После проверки электронной версии отчета о выполнении лабораторной работы преподавателем удалить файл с отчетом о лабораторной работе и файлы программы MyOldSafe. Удалить программы Citadel Safstor и Contraband с помощью Панели управления Windows. Удалить файлы архивов mosafe21.exe, citadel.zip и contrabd.zip, а также файл test.bmp.
24. Включить в отчет ответы на контрольные вопросы, номера которых выбираются в соответствии с номером варианта.
25. Предъявить преподавателю для защиты лабораторной работы отчет на твердом носителе, содержащий
    - титульный лист,
    - сведения, полученные при выполнении работы, и ответы на общие вопросы с указанием соответствующих пунктов задания (3.1-3.6, 7.1-7.4, 8.1-8.5, 9.1, 9.2, 12.1, 12.2, 15.1-15.3, 16.1-16.4, 17.1, 17.2, 18.1, 20.1);
    - ответы на контрольные вопросы.

    Примечание: если данная лабораторная работа выполняется на заключительном занятии, то для защиты может быть представлен отчет в электронном виде.

Контрольные вопросы

1. В чем разница между симметричной и асимметричной криптографией?
2. Какой шифр является абсолютно стойким (по К.Шеннону)?
3. Что такое криптографический ключ?
4. В чем заключается основная проблема при использовании симметричной криптографии?
5. Для решения каких задач защиты информации применяются криптографические методы и средства?
6. Как происходит шифрование и расшифрование файлов при использовании программы MyOldSafe?
7. Как осуществляется совместный доступ к зашифрованным файлам при использовании программы MyOldSafe?
8. Увеличивает ли степень защищенности конфиденциальных данных совмещение их шифрования со сжатием (архивацией) и почему?
9. Как происходит шифрование и расшифрование файлов при использовании программы Citadel Safstor?
10. Как осуществляется совместный доступ к зашифрованным файлам при использовании программы Citadel Safstor?
11. Как происходит генерация ключа шифрования при установке программы Citadel Safstor?
12. Какие средства операционной системы Windows использует шифрующая файловая система (EFS)?
13. Для чего предназначен агент восстановления данных при использовании шифрующей файловой системы ОС Windows?
14. Что происходит при шифровании и расшифровании данных при использовании шифрующей файловой системы ОС Windows?
15. Как обеспечивается возможность восстановления зашифрованных файлов при использовании шифрующей файловой системы ОС Windows?
16. Какие достоинства и недостатки имеет шифрующая файловая система ОС Windows?
17. Какие симметричные криптосистемы наиболее распространены в настоящее время?

18. В чем разница между блочными и потоковыми шифрами?
19. Как обеспечивается защита конфиденциальных документов в пакете Microsoft Office?
20. Что такое провайдер криптографического обслуживания в ОС Windows?
21. Как обеспечивается защита целостности провайдера криптографического обслуживания в ОС Windows?
22. От каких угроз безопасности информации защищает электронная цифровая подпись?
23. Как вычисляется и проверяется электронная цифровая подпись?
24. Как обеспечивается подлинность и целостность документов в пакете Microsoft Office?
25. В чем заключатся роль удостоверяющего центра (центра сертификации)?
26. Что такое сертификат открытого ключа и для чего он применяется?
27. Для решения каких задач защиты информации в первую очередь применяются асимметричные криптосистемы?
28. Какие асимметричные криптосистемы применяются в настоящее время?
29. Что такое функция хеширования и какие требования к ней применяются?
30. Для решения каких задач защиты информации применяются функции хеширования?
31. В чем сущность методов компьютерной стеганографии?
32. Какие методы скрытия сообщений применяются в компьютерной стеганографии?
33. Для чего могут применяться методы компьютерной стеганографии?
34. Как осуществляется скрытие конфиденциальных файлов при использовании программы Contraband?
35. Для чего применяется ключ в программе Contraband?
36. Что может использоваться в качестве контейнера в программах компьютерной стеганографии?
37. Что такое компьютерный вирус?
38. В чем разница между загрузочными и файловыми вирусами?
39. Какие разновидности компьютерных вирусов наиболее опасны и почему?
40. Какие типы файлов могут поражаться компьютерными вирусами?
41. Какие существуют методы обнаружения компьютерных вирусов?
42. В чем опасность вирусов в макросах электронных документов?
43. В чем заключается встроенная в программы пакета Microsoft Office защита от вирусов в макросах?
44. Какие существуют методы защиты от вирусов в макросах документов Microsoft Office?
45. Как добавить электронную цифровую подпись к макросу в документе Microsoft Office?
46. В чем достоинства и недостатки антивирусных сканеров и мониторов?
47. Какие существуют основные каналы заражения компьютерными вирусами?
48. В чем заключается профилактика заражения компьютерными вирусами?

Варианты для выбора номеров контрольных вопросов

№	Номера вопросов	№	Номера вопросов	№	Номера вопросов
1	1, 2, 9, 18, 32, 35	11	4, 13, 23, 29, 41, 48	21	1, 8, 16, 28, 38, 48
2	3, 10, 11, 19, 34, 36	12	16, 24, 28, 33, 38, 43	22	2, 17, 25, 27, 32, 35
3	4, 12, 20, 21, 37, 43	13	8, 15, 23, 27, 36, 37	23	3, 11, 13, 18, 36, 38
4	5, 13, 22, 27, 38, 44	14	7, 14, 20, 22, 34, 35	24	4, 14, 24, 30, 34, 44
5	6, 14, 23, 28, 39, 45	15	2, 12, 21, 31, 32, 44	25	5, 15, 20, 25, 35, 40
6	7, 15, 24, 29, 40, 46	16	3, 15, 20, 25, 39, 45	26	6, 16, 26, 31, 36, 42
7	8, 16, 25, 30, 41, 47	17	4, 9, 26, 27, 32, 47	27	7, 11,17, 27, 37, 47
8	17, 26, 31, 33, 42, 48	18	5, 10, 19, 22, 37, 46	28	8, 9, 18, 22, 38, 43
9	2, 10, 21, 27, 39, 46	19	6, 16, 26, 30, 40, 48	29	1, 10, 19, 33, 41, 45
10	3, 12, 22, 28, 40, 47	20	10, 11, 20, 32, 33, 43	30	2, 11, 17, 30, 37, 46