Лабораторная работа №5

Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов

Содержание задания

1. При работе в компьютерном классе университета все пункты выполняются в окне виртуальной ОС Windows XP. Установить программную систему PGP 6.0.2, запустив программу Setup.exe из указанной преподавателем сетевой папки. Выбрать для установки только следующие компоненты:
   PGP 6.0.2 Program Files;
   PGP 6.0.2 User's Manual;
   Unconfigured PGP 6.0.2 Client Install;
   PGPdisk for Windows.

На вопрос программы установки о существовании ключей ответить «Нет», а на вопрос о необходимости перезагрузки системы – «Да».

2. Запустить программу PGPtools (с помощью меню «Пуск» или значка PGPtray на панели задач), ознакомиться и отразить в отчете о лабораторной работе
   2.1. состав программных средств, входящих в систему PGP (при необходимости воспользоваться справкой о системе PGP).
3. Создать криптографические ключи с помощью программы PGPkeys. Включить в электронную версию отчета о лабораторной работе
   3.1. копии используемых при этом экранных форм.
   3.2. Включить в отчет ответы на вопросы: как обеспечивается случайность выбираемых криптографических ключей в системе PGP;
   3.3. как и где хранится секретный ключ пользователя в системе PGP;
   3.4. как может быть обеспечена в системе PGP возможность восстановления секретного ключа пользователя при его случайной потере.
4. Изучить (на примере документов с отчетами о ранее выполненных Вами лабораторных работах, обычных текстовых файлов, файлов изображений **только** из своей папки) способы шифрования и расшифрования файлов с помощью функций Encrypt и Decrypt программы PGPtools. Обязательно проверить на примере использование дополнительных параметров шифрования и результаты проверки отразить в отчете. Включить в электронную версию отчета
   4.1. копии используемых при этом экранных форм.
   4.2. Включить в отчет ответы на вопросы: какие дополнительные параметры шифрования могут быть использованы и в чем их смысл и возможное применение;
   4.3. как генерируется, как и где хранится ключ симметрического шифрования файла в системе PGP;
   4.4. как может быть обеспечен доступ к зашифрованному файлу со стороны других пользователей;
   4.5. изменяется ли и как размер файла после его шифрования (привести конкретные примеры для разных типов файлов).
5. Изучить (на примере документов из своей папки) способы получения и проверки электронной цифровой подписи под файлами с помощью функций Sign и Verify программы PGPtools. Обязательно проверить на примере использование дополнительных параметров получения электронной цифровой подписи и реакцию программы на нарушение целостности подписанного документа (при отсоединенной подписи), а результаты проверки отразить в отчете. Включить в электронную версию отчета
   5.1. копии используемых при этом экранных форм.

5.2. Включить в отчет ответы на вопросы: какие дополнительные параметры получения электронной цифровой подписи могут быть использованы,
5.3. в чем их смысл и возможное применение;
5.4. какова реакция на программы на нарушение целостности подписанного документа (обязательно проверить на примере и результаты проверки отразить в отчете).

6. Изучить способы одновременного шифрования (расшифрования) и получения (проверки) электронной цифровой подписи в системе PGP с помощью функций Encrypt Sign и Decrypt/Verify программы PGPtools. Включить в электронную версию отчета
   6.1. копии используемых при этом экранных форм.
   6.2. Включить в отчет сведения о порядке одновременного обеспечения конфиденциальности, аутентичности и целостности электронных документов
7. Изучить способы надежного удаления файлов с конфиденциальной информацией с помощью функции Wipe программы PGPtools. Включить в электронную версию отчета
   7.1. копии используемых при этом экранных форм.
   7.2. Включить в отчет сведения о порядке уничтожения конфиденциальных электронных документов в системе PGP.
8. Изучить способы надежного уничтожения остаточной информации, которая может содержать конфиденциальные сведения, с помощью функции Freespace Wipe программы PGPtools. Включить в электронную версию отчета
   8.1. копии используемых при выполнении этого пункта экранных форм.
   8.2. Включить в отчет сведения о порядке уничтожения конфиденциальных электронных документов в системе PGP.
   8.3. Включить в отчет ответы на вопросы: как достигается надежное уничтожение остаточной конфиденциальной информации в системе PGP;
   8.4. является ли подобный метод уничтожения абсолютно надежным и, если нет, как может быть обеспечено абсолютно надежное уничтожение остаточной информации
9. Изучить способы создания электронного хранилища конфиденциальных документов с помощью программы PGPdisk. Создать (с помощью функции New программы PGPdisk) новый PGP диск размером 10 Mb на указанном преподавателем локальном диске (в его корневом каталоге) и защитить его с помощью парольной фразы. Выполнить быстрое форматирование созданного диска (указав файловую систему FAT). Скопировать в созданный PGP диск папку с собственными документами. Если после создания виртуального диска Проводник Windows не отображает его содержимое, то нажать кнопку Назад на панели инструментов Проводника (под его меню). Размонтировать созданный диск с помощью функции Unmount программы PGPdisk и завершить работу с этой программой. Заново смонтировать (с помощью функции Mount программы PGPdisk) созданный PGP диск, удалить из него все файлы, размонтировать и уничтожить его (с помощью функции Wipe программы PGP). Включить в электронную версию отчета
   9.1. копии используемых экранных форм.
   9.2. Включить в отчет сведения о назначении и порядке использования программы PGPdisk.
   9.3. Включить в отчет ответы на вопросы: как защищаются файлы и папки, помещенные в виртуальный PGP диск;
   9.4. в чем отличие программы PGPdisk от шифрующей файловой системы операционной системы Windows и в чем общие черты этих систем;
   9.5. какая из этих систем, на Ваш взгляд, более удобна для защиты конфиденциальной информации и почему.
10. Изучить способы быстрого выполнения функций системы PGP с помощью программы PGPtray, ярлык которой размещен в правой части панели задач. Включить в электронную версию отчета

10.1. копии используемых экранных форм.

11. Изучить способы управления настройками системы PGP при ее использовании в организациях с помощью программы PGPadmin (пройти все шаги диалога с мастером вплоть до последнего, на котором вместо кнопки «Save» нажать кнопку «Отмена»). Включить в электронную версию отчета
    11.1. копии используемых при этом экранных форм.
    11.2. Включить в отчет сведения о возможностях и порядке администрирования системы PGP.
    11.3. Включить в отчет ответы на вопросы: какие функции по управлению шифрованием и обеспечением целостности информационных ресурсов предоставляет администратору программа PGPAdmin;
    11.4. какие функции по управлению криптографическими ключами пользователей PGP предоставляет администратору программа PGPadmin;
    11.5. какие возможности предоставляет программа PGPadmin по управлению доступными для пользователей функциями программы PGP и где сохраняется подобная информация.
12. Изучить состав программной документации, поставляемой с системой PGP. Включить в отчет
    12.1. сведения о составе программной документации и кратком содержании руководств:
    12.2. пользователя PGP;
    12.3. администратора PGP;
    12.4. по установке PGP.
13. Предъявить преподавателю электронную версию отчета о лабораторной работе с копиями использовавшихся экранных форм и соответствующими им номерами пунктов задания (3.1, 4.1, 5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1).
14. После проверки электронной версии отчета о выполнении лабораторной работы преподавателем удалить систему PGP, установленную при выполнении п. 1, с помощью функции «Установка и удаление программ» *Панели управления* Windows.
15. Включить в отчет о лабораторной работе
    15.1. ответы на контрольные вопросы, выбранные в соответствии с номером варианта и приложением.
16. 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 (2.1, 3.2-3.4, 4.2-4.5, 5.2-5.4, 6.2, 7.2, 8.2-8.4, 9.2-9.5, 11.2-11.5, 12.1-12.4);
    - ответы на контрольные вопросы.

Контрольные вопросы

Каковы основные параметры симметрических криптографических систем?

Какие виды современных симметрических криптосистем Вы знаете?

Какие асимметрические криптосистемы Вам известны, чем они отличаются друг от друга?

Каковы основные этапы алгоритмов получения и проверки электронной цифровой подписи?

Какие требования предъявляются к идеальному (абсолютно стойкому по К.Шеннону) алгоритму симметрического шифрования?

Как должен создаваться, храниться и распространяться ключ симметрического шифрования?

Какая информация содержится в сертификате открытого ключа асимметрического шифрования?

Какие требования предъявляются к функциям хеширования?

Какие функции хеширования Вам известны и чем они различаются?

Чем вызвана необходимость использования удостоверяющих центров (центров сертификации)?

Как выбрать длину криптографического ключа в системе PGP?
Где применяются криптографические методы защиты информации?
Может ли контроль целостности объекта с помощью функции хеширования или электронной цифровой подписи гарантировать его неизменность?
В чем недостатки криптографических методов защиты информации?
Что такое доверенная вычислительная среда (Trusted Computing Base, TCB)?
Какие компьютерные системы называются безопасными?
В чем заключаются основные требования к защищенности компьютерных систем?
Для выполнения каких требований к защищенности компьютерных систем могут применяться криптографические методы защиты?
Насколько, на Ваш взгляд, надежные методы криптографической защиты используются в программе PGP?
Какие требования к защищенности компьютерных систем объединены в группе «Политика»?
Зачем в составе программы PGP предусмотрены административные функции?
Какие требования к защищенности компьютерных систем объединены в группе «Подотчетность»?
Какими основными функциями защиты информации обладает программа PGP?
Какие требования к защищенности компьютерных систем объединены в группе «Гарантии»?
Какой принцип лежит в основе функции надежного уничтожения остаточной конфиденциальной информации программы PGP?
Применение какого средства защиты информации является, на Ваш взгляд, более предпочтительным: шифрующей файловой системой в защищенных версиях операционной системы Windows или программы PGP?
Как выбирается длина криптографического ключа в системе PGP?
Какие стандарты безопасности компьютерных систем Вам известны и в чем разница между ними?
Какие классы безопасности компьютерных систем предусмотрены в TCSEC?
Какие классы безопасности автоматизированных систем предусмотрены в руководящих документах Гостехкомиссии РФ?
В чем разница между средством вычислительной техники и автоматизированной системой в соответствии с руководящими документами Гостехкомиссии РФ?
К каким классам безопасности в соответствии со стандартом TCSEC и руководящими документами Гостехкомиссии РФ можно отнести операционные системы Windows NT/2000/XP Professional?

Варианты для выбора номеров контрольных вопросов

№	Номера вопросов	№	Номера вопросов	№	Номера вопросов
1	1, 2, 9, 18, 32	11	4, 10, 13, 23, 29	21	1, 8, 16, 28, 31
2	3, 10, 11, 19, 31	12	5, 9, 16, 24, 28	22	2, 17, 25, 27, 32
3	4, 12, 20, 21, 30	13	8, 15, 19, 23, 27	23	3, 11, 13, 18, 31
4	5, 13, 22, 27, 29	14	7, 14, 20, 22, 26	24	4, 14, 24, 27, 30
5	6, 14, 18, 23, 28	15	2, 12, 21, 31, 32	25	5, 15, 20, 25, 29
6	7, 11, 15, 24, 27	16	3, 15, 20, 25, 30	26	6, 12, 16, 26, 31
7	8, 12, 16, 20, 25	17	4, 9, 26, 27, 32	27	7, 11,17, 23, 27
8	1, 11, 17, 26, 31	18	5, 10, 19, 22, 25	28	8, 9, 18, 22, 28
9	2, 10, 21, 27, 32	19	6, 16, 20, 26, 30	29	1, 10, 19, 24, 31
10	3, 12, 22, 28, 31	20	7, 10, 11, 20, 32	30	2, 11, 17, 22, 30