МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ОРЛОВСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МВД РОССИЙСКОЙ ФЕДЕРАЦИИ»

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

ОРЕЛ
ОрЮИ МВД России
2009

УДК 004+34С33.2
ББК 32.97+67.99(2)116
О-75

О-75 «**Основы информационной безопасности в ОВД»: учебно-методическое пособие** / составители: Д.С. Мишин, Н.Г. Подчерняев. – Орел: Орловский юридический институт МВД России, 2009. – 69 с.

В учебно-методическом пособии рассмотрены порядок и организация работы курсантов и слушателей очной и заочной форм обучения при выполнении практических заданий по дисциплине «Основы информационной безопасности в ОВД».

УДК 004+34С33.2
ББК 32.97+67.99(2)116

ОГЛАВЛЕНИЕ

Тема 4.2. Практическое занятие: «Программные средства защиты компьютерной информации от неправомерного доступа»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных (АСОД);
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

1. Восстановление зараженных файлов
2. Профилактика проникновения «троянских программ»
3. Настройка безопасности почтового клиента Outlook Express
4. Настройка параметров аутентификации Windows 2000 (XP)
5. Шифрующая файловая система EFS и управление сертификатами в Windows 2000 (XP)

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:

Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 80 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 5 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет "Вычислительной техники".
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

УПРАЖНЕНИЕ № 1: Восстановление зараженных файлов.

Краткие теоретические сведения

Макровирусы заражают файлы — документы и электронные таблицы популярных офисных приложений.

Для анализа макровирусов необходимо получить текст их макросов. Для нешифрованных («не-стелс») вирусов это достигается при помощи меню Сервис/Макрос. Если же вирус шифрует свои макросы или использует «стелс»-приемы, то необходимо воспользоваться специальными утилитами просмотра макросов.

Задание: восстановить файл, зараженный макровирусом

Алгоритм выполнения работы

Для восстановления документов Word и Excel достаточно сохранить пораженные файлы в текстовый формат RTF, содержащий практически всю информацию из первоначальных документов и не содержащий макросы.

Для этого выполните следующие действия.

1. В программе **WinWord** выберите пункты меню **«Файл»** — **«Сохранить** как».
2. В открывшемся окне в поле **«Тип файла»** выберите **«Текст в формате RTF»** (рис. **1).**
3. Выберите команду **Сохранить,** при этом имя файла оставьте прежним.
4. В результате появится новый файл с именем существующего, но с другим расширением.
5. Далее закройте **WinWord** и удалите все зараженные Word-документы **и** файл-шаблон **NORMAL.DOT в** папке **WinWord.**
6. Запустите **WinWord** и восстановите документы из RTF-файлов в соответствующий формат файла (рисунок 2) с расширением (.doc).
7. В результате этой процедуры вирус будет удален из системы, а практически вся информация останется без изменений.

Примечание:

а) этот метод рекомендуется использовать, если нет соответствующих антивирусных программ;

б) при конвертировании файлов происходит потеря не вирусных макросов, используемых при работе. Поэтому перед запуском описанной процедуры следует сохранить их исходный текст, а после обезвреживания вируса — восстановить необходимые макросы в первоначальном виде.

8. Для последующей защиты файлов от макровирусов включите защиту от запуска макросов.
9. Для этого в **WinWord** выберите последовательно пункты меню: **Сервис — Макрос — Безопасность** (рис. **3).**
10. В открывшемся окне на закладке **Уровень безопасности** отметьте пункт Высокая (рис. 4).

Задания для самостоятельной работы

1. Создайте файл **virus.doc** (содержание – чистый лист) и выполните алгоритм восстановления файла (в предположении его заражения макровирусом).
2. Зафиксируйте этапы работы, используя команду **PrintScreen** клавиатуры (скопированные таким образом файлы вставьте в новый Word-документ для отчета преподавателю).

3. Сравните размеры файлов **virus.doc и virus.rtf,** используя пункт контекстного меню **Свойства (для** этого выделите **в Проводнике** файл, нажмите правую кнопку мыши и выберите пункт **Свойства).** [8]

УПРАЖНЕНИЕ № 2: Профилактика проникновения «троянских программ.

Краткие теоретические сведения

Реестр операционной системы Windows — это большая база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь копию реестра. Основным средством для просмотра и редактирования записей реестра служит специализированная утилита **«Редактор реестра».**

Файл редактора реестра находится в папке Windows. Называется он **regedit.exe.** После запуска появится окно редактора реестра. Вы увидите список из 5 разделов:

HKEY_CLASSES_ROOT;
HKEY_CURRENT_USER;
HKEY_LOCAL_MACHINE;
HKEYJJSERS;
HKEY CURRENT CONFIG.

Работа с разделами реестра аналогична работе с папками в Проводнике. Конечным элементом дерева реестра являются ключи или параметры, делящиеся на три типа:

■строковые (напр. «C:\Windows»);
■двоичные (напр. 10 82 AO 8F);

DWORD — этот тип ключа занимает 4 байта и отображается в шестнадцатеричном и в десятичном виде (например, 0x00000020 (32)).

В Windows системная информация разбита на так называемые ульи (hive). Это обусловлено принципиальным отличием концепции безопасности этих операционных систем. Имена файлов ульев и пути к каталогам, в которых они хранятся, расположены в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\hivelist**.

В таблице 1 даны краткие описания ульев реестра и файлов, в которых хранятся параметры безопасности. [8]

Таблица 1

Характеристика основных разделов системного реестра

HKEY LOCAL **MACHINE\SAM**	Содержит информацию SAM (Security Access Manager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке %System-root%\System32\Config

HKEY_LOCAL_MACHINE\SECURITY	Содержит информацию безопасности в файлах SECURITY, SECURITY.LOG, 3ECURITY.SAV в папке \%System root%\Sytem32\Config
HKEY_LOCAL_MACHINE\SYSTEM	Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлах SYSTEM, SYSTEM.LOG, SYSTEM.SAV в папке. \%Systemroot%\System32\Co nfig
HKEY_CURRENT_CONFIG	Содержит информацию о подразделе System этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке \%Syste m root%\System 32\Co nfig
HKEY_USERS\.DEFAULT	Содержит информацию, которая будет использоваться для создания профиля нового пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке \%System root%\Sy stem32\Co nfig
HKEY_CURRENT$_m$USER	Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT и NTUSER.DAT.LOG, расположенных в каталоге \%Systemroot%\Profiles\User name, где User name — имя пользователя, зарегистрированного в системе на данный момент

Задание: проверить потенциальные места записей «троянских программ» в системном реестре операционной системы Windows 2000 (XP).

Алгоритм выполнения работы

Потенциальными местами записей «троянских программ» в системном реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.

1. Запустите программу **regedit.exe.**
2. В открывшемся окне выберите ветвь **HKEY_LOCALJWACHINE** и далее **Software\ Microsoft\WindowsNT\CurrentVersion\Winlogon.**
3. **В** правой половине открытого окна программы **regedit.exe** появится список ключей.
4. Найдите ключ **TJserinit (REG_SZ)** и проверьте его содержимое.

5. По умолчанию (исходное состояние) 151 этот ключ содержит следующую запись **C:\WINDOWS\system32\userinit.exe**.

6. ЕСЛИ в указанном ключе содержатся дополнительные записи, то это могут быть «троянские программы».

7. В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время.

8. Если время создания файла совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен «троянским конем».

9. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду **Изменить** из меню **Правка** программы regedit.exe).

10. В открывшемся окне в поле **Значение** удалите ссылку на подозрительный файл.

11. Закройте программу regedit.exe.

12. Перейдите в папку с подозрительным файлом и удалите его.

13. Перезагрузите операционную систему и выполните пункты задания 1-4.

14. Если содержимое рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.

Еще одним потенциальным местом записей на запуск «троянских программ» является раздел автозапуска **Run.**

Для его проверки выполните следующее.

1, Запустите программу regedit.exe.

2. В открывшемся окне выберите ветвь **HKEYLOCALMACHINE** и далее **Software\Microsoft\Wmdows\CurrentVersion\Run\ (REG_SZ)** (рис. **6).**

3. В рассматриваемом примере автоматически запус кается резидентный антивирус и его планировщик заданий, а также утилита, относящаяся к программе Nero (запись на CD).

4. Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 6—14 предыдущего задания. [8]

Задания для самостоятельной работы

1. Проверьте содержимое ключа HKEY_LOCAL_MACHINE\Software\Microsoft\ WindowsNT\Cum^tVer^

2. Зафиксируйте этапы работы, используя команду PrintScreen клавиатуры.

3. Составьте отчет о результатах проверки.

УПРАЖНЕНИЕ № 3: Настройка параметров аутентификации Windows 2000 (XP)

Краткие теоретические сведения

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и/или идентификации.

Идентификация и аутентификация применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Идентификация — присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) — проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Настройка параметров аутентификации рассматриваемых операционных систем выполняется *в* рамках "локальной политики безопасности.

Оснастка «Локальная политика безопасности» используется для изменения политики учетных записей и локальной политики на локальном компьютере. При помощи оснастки «Локальная политика безопасности» можно определить;

- кто имеет доступ к компьютеру;
- какие ресурсы могут использовать пользователи на Вашем компьютере;
- включение и отключение записи действий пользователя или группы в журнале событий.

Задание: настроить параметры локальной политики безопасности операционной системы **Windows 2000 (XP).**

Алгоритм выполнения работы

Для просмотра и изменения параметров аутентификации пользователей выполните следующие действия:

Выберите кнопку **Пуск** панели задач.

Откройте меню **Настроить — Панель управления**

В открывшемся окне выберите ярлык **Администрирование — Локальная политика безопасности .**

1. Выберите пункт **Политика учетных** записей (этот пункт включает два подпункта: **Политика паролей и Политика блокировки учетной записи).**
2. Откройте подпункт **Политика паролей.** В правом окне появится список настраиваемых параметров.
3. В показанном примере политика паролей соответствует исходному состоянию системы безопасности после установки операционной системы, при этом ни один из параметров не настроен. Значения параметров приведены в таблице 1.
4. Ознакомьтесь со свойствами всех параметров.
5. Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды щелкните на изменяемом параметре).
6. В результате этого действия появится одно из окон. [8]

Таблица 1

Значения параметров Политики паролей

Параметр	Значение
Требовать неповторяемости паролей	Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24.
Максимальный срок действия пароля	Определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Можно задать значение **в** диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0.
Минимальный срок действия пароля	Определяет период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет заменить его. Можно задать значение в диапазоне от 1 до 999 дней или разрешить немедленное изменение, установив число дней равным 0.
Минимальная длина пароля	Определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов равным 0.
Пароль должен отвечать требованиям сложности	Определяет, должны ли пароли отвечать требованиям СЛОЖНОСТИ. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям. Пароль не может содержать имя учетной записи пользователя или какую-либо его часть. Пароль должен состоять не менее чем из шести символов. В пароле должны присутствовать символы трех категорий из числа следующих четырех: 1) прописные буквы английского алфавита от A до Z; 2) строчные буквы английского алфавита от **a до** z; 3) десятичные цифры (от 0 до 9); 4) символы, не принадлежащие алфавитно-цифровому набору (например, !,$,#, %). Проверка соблюдения этих требований выполняется при изменении или создании паролей.
Хранить пароли всех пользователей в домене, используя обратимое шифрование	Определяет, следует ли **в** системах Windows 2000 Server, Windows 2000 Professional и Windows XP хранить пароли, используя обратимое шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранить пароли, зашифрованные обратимыми методами, - это все равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля.

10. Измените значение параметра и нажмите Ок.

11. Например (обязательно выполнить и сохранить), выберите параметр **Требовать неповторяемости паролей** и измените его значение на 1.

12. Для настройки **Политики блокировки учетной записи** выберите этот подпункт и откройте его.

13. Значения параметров данного подпункта **Политики учетных записей** приведены **в** таблице 2.

14. Ознакомьтесь со свойствами всех параметров.

15. Для изменения параметров воспользуйтесь алгоритмом, описанным **в** пунктах **8—10.** [8]

Таблица 2

Значения параметров
Политики блокировки учетных записей

Параметр	Значение
Пороговое значение блокировки	Определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока она не будет сброшена администратором или пока не истечет ее интервал блокировки. Можно задать значение в диапазоне от I до 999 или запретить блокировку данной учетной записи, установив значение 0.
Блокировка учетной записи на	Определяет число минут, в течение которых учетная запись остается блокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от I до 99 999 минут. Если установить значение 0, учетная запись будет блокирована на все время до тех пор, пока администратор не разблокирует ее явным образом. Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса.
Сброс счетчика блокировки через	Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от I до 99 999 минут. Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше интервала **Блокировка учетной записи на.**

Задания для самостоятельной работы

1. Измените параметр **«Пароль должен отвечать требованиям сложности» Политики паролей** на **«Включен»** (рисунок 3) и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения

системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения Вашего задания.

2. После успешного выполнения первого задания, измените пароль Вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

3. Проведите эксперименты с другими параметрами **Политики учетных записей.** [8]

УПРАЖНЕНИЕ № 4 Шифрующая файловая система EFS и управление сертификатами в Windows 2000 (XP)

Краткие теоретические сведения

Шифрующая файловая система EFS позволяет пользователям хранить данные на диске в зашифрованном виде.

Шифрование — это процесс преобразования данных в формат, не доступный для чтения другим пользователям. После того как файл был зашифрован, он автоматически остается зашифрованным в любом месте хранения на диске.

Расшифровка — это процесс преобразования данных из зашифрованной формы в его исходный формат.

При работе с шифрующей файловой системой EFS следует учитывать следующие сведения и рекомендации.

1. Могут быть зашифрованы только файлы и папки, находящиеся на томах **NTFS.**
2. Сжатые файлы и папки не могут быть зашифрованы- Если шифрование выполняется для сжатого файла или папки, файл или папка преобразуются к состоянию без сжатия.
3. Зашифрованные файлы могут стать расшифрованными, если файл копируется или перемещается на том, не являющийся томом **NTFS.**
4. При перемещении незашифрованных файлов в зашифрованную папку они автоматически шифруются в новой папке. Однако обратная операция не приведет к автоматической расшифровке файлов. Файлы необходимо явно расшифровать.
5. Не могут быть зашифрованы файлы с атрибутом **«Системный»** и файлы в структуре папок системный корневой каталог.
6. Шифрование папки или файла не защищает их от удаления. Любой пользователь, имеющий права на удаление, может удалить зашифрованные папки или файлы.
7. Процесс шифрование является прозрачным для пользователя.

Примечание. Прозрачное шифрование означает, что перед использованием файл не нужно расшифровывать. Можно как обычно открыть файл и изменить его. В системах прозрачного шифрования {шифрования «на лету») криптографические преобразования осуществляются в режиме реального времени незаметно для пользователя. Например,

пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.

Использование **EFS** сходно с использованием разрешений для файлов и папок. Оба метода используются для ограничения доступа к данным. Но злоумышленник, получивший несанкционированный физический доступ к зашифрованным файлам и папкам, не сможет их прочитать. При его попытке открыть или скопировать зашифрованный файл или папку появится сообщение, что доступа нет.

Шифрование и расшифровывание файлов выполняется установкой свойств шифрования для папок и файлов, как устанавливаются и другие атрибуты, например, **«только чтение», «сжатый»** или **«скрытый».** Если шифруется папка, все файлы и подпапки, созданные в зашифрованной папке, автоматически шифруются. Рекомендуется использовать шифрование на уровне папки. Шифрующая файловая система автоматически создает пару ключей шифрования для пользователя, если она отсутствует. Шифрующая файловая система использует алгоритм шифрования Data Encryption Standard (DESX). [8]

Задание: включить и отключить шифрование файлов шифрующей файловой системой EFS. Экспортировать сертификат с ключами для расшифровки файлов на другом компьютере.

Алгоритм выполнения работы

А. Для включения режима шифрования выполните следующие действия.

1. Укажите файл или папку (например, создайте файл **шифр.doc** в папке Мои документы), которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду Свойства.

2. В появившемся окне свойств на вкладке **Общие** нажмите кнопку Другие. Появится окно диалога **Дополнительные атрибуты.**

3. В группе **Атрибуты сжатия и шифрования** установите флажок **Шифровать содержимое для защиты данных** и нажмите кнопку «ОК».

4. Нажмите кнопку ОК в окне свойств зашифровываемого файла или папки, **в** появившемся окне диалога укажите режим шифрования: **только к этой папке** или **к этой папке и всем вложенным папкам и файлам.**

Внимание! После выполнения этих действий файл с Вашей информацией будет автоматически зашифровываться. Просмотр его на другой ПЭВМ будет невозможен.

В. Для выключения режима шифрования выполните следующие действия.

Выделите файл **шифр-doc** в папке **Мои** документы.

Нажмите правую клавишу мыши и выберите пункт **Свойства.**

На вкладке **Общие** нажмите кнопку Другие,

В открывшемся окне диалога **в** группе **Атрибуты сжатия и шифрования** сбросьте флажок **Шифровать содержимое для защиты данных.** [8]

Внимание! После выполнения этих действий файл с Вашей информацией не будет зашифровываться.

С. Создание резервной копии Сертификата средствами Windows 2000 (XP).

Примечание. Резервная копия сертификата необходима для расшифровки данных после переустановки операционной системы или для просмотра зашифрованной информации на другой **ПЭВМ.**

Внимание! Перед переустановкой операционной системы обязательно создайте копии Сертификатов, так как после переустановки Вы не сможете расшифровать информацию.

Для создания резервной копии сертификата выполните следующие действия.

1. Выберите кнопку **Пуск** в панели задач.
2. Перейдите к пункту **Выполнить.**
3. В открывшемся окне **в** поле ввода введите команду **mmc.**
4. В результате откроется консоль управления **mmc.**

Примечание. Консоль MMC — это средство для создания, Сохранения и открытия наборов средств администрирования, называемых консолями. Консоли содержат такие элементы, как оснастки, расширения оснасток, элементы управления, задачи, мастера и документацию, необходимую для управления многими аппаратными, программными и сетевыми компонентами системы Windows. Можно добавлять элементы в существующую консоль MMC, а можно создавать новые консоли и настраивать их для управления конкретными компонентами системы.

5. В меню Консоль выберите команду Добавить или удалить оснастку (рис. 1) и нажмите кнопку Добавить.
6. В поле Оснастка дважды щелкните Сертификаты (рис. 2), установите переключатель в положение учетной записи компьютера и нажмите кнопку Далее.
7. Выполните одно из следующих действий:
   - Чтобы управлять сертификатами локального компьютера, установите переключатель в положение локальным компьютером и нажмите кнопку Готово.
   - Чтобы управлять сертификатами удаленного компьютера, установите переключатель в положение другим компьютером и введите имя компьютера или нажмите кнопку Обзор для выбора компьютера, затем нажмите кнопку Готово.
8. Нажмите кнопку Закрыть.
9. В списке выбранных оснасток для новой консоли появится элемент Сертификаты (имя_компьютера).
10. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку

ОК.

11.Чтобы сохранить эту консоль, в меню Консоль выберите команду Сохранить и укажите имя оснастки Сертификаты.

12.Закройте окно Консоли и выберите команду Пуск и далее Все программы.

13.Найдите пункт Администрирование и выберите подпункт Сертификаты (теперь оснастка с Сертификатами доступна в меню Пуск).

14.В левом подокне оснастки Сертификаты откройте папку Доверенные корневые сертификаты, а затем папку Сертификаты. В правом подокне появится список сертификатов.

15. Укажите переносимый сертификат (например, первый в списке, рис. 3) и щелкните правой кнопкой мыши. В появившемся контекстном меню выберите команду Все задачи и далее выберите команду Экспорт.

16. В результате запустится Мастер экспорта сертификатов .

17. Нажмите кнопку Далее.

18. В следующем окне мастера выберите опцию Да, экспортировать закрытый ключ.

19. Затем нажмите кнопку Далее.

20. В следующем окне мастера доступен только один формат (PFX), предназначенный для персонального обмена информацией. Нажмите кнопку Далее.

21. В следующих окнах сообщите пароль (например, 11), защищающий данные файла сертификат.pfx, а также путь сохранения файла (запишите путь к папке, в которой Вы сохранили копию Сертификата) сертификат.pfx.

22. Нажмите кнопку Далее.

23. Отобразится список экспортируемых сертификатов и ключей. Нажмите кнопку Готово.

24. Завершите работу Мастера экспорта сертификата нажатием кнопки ОК в окне диалога, сообщающем об успешном выполнении процедуры экспорта,

В результате сертификат и секретный ключ будут экспортированы в файл с расширением сертификат.pfx, который может быть скопирован на гибкий диск и перенесен на другой компьютер или использован после переустановки операционной системы. [8]

D. Для восстановления сертификата из резервной копии выполните следующие действия.

1. Перенесите созданный на предыдущем этапе файл с расширением сертификат.pfx на компьютер (Вам необходимо вспомнить путь к копии Сертификата).

2. Запустите оснастку Сертификаты, для этого выберите кнопку Пуск панели задач и далее Все программы/Администрирование/Сертификаты.

3. В окне структуры оснастки Сертификаты откройте папку Доверенные корневые сертификаты, затем папку Сертификаты. В правом подокне появится список Ваших сертификатов.

4. Щелкните правой кнопкой мыши на пустом месте правого подокна.
5. В появившемся контекстном меню выберите команду Все задачи.
6. В ее подменю выберите команду Импорт (Import).
7. Запустится Мастер импорта сертификатов.
8. Следуйте указаниям мастера — укажите местоположение файла сертификат.pfx и сообщите пароль защиты данного файла.
9. Для начала операции импорта нажмите кнопки Готово и ОК.
10. После завершения процедуры импорта нажмите кнопку ОК и закройте окно Мастера импорта.

В результате Ваших действий текущий пользователь или Вы сами получите возможность работать **с** зашифрованными данными на этом компьютере.

Задания для **самостоятельной работы**

1. Экспортируйте сертификат № 2 из папки **Промежуточные центры сертификации Root** Agency (сохраните иллюстрации для отчета).
2. Импортируйте экспортированный сертификат **в** папку **Личные** (сохраните иллюстрации для отчета). [8]

Контрольные вопросы:

1. Какие файлы заражают макровирусы?
2. Как просмотреть код макровируса?
3. Как восстановить файл, зараженный макровирусом?
4. Что такое реестр?
5. Поясните особенности «троянских программ».
6. Почему профилактика «троянских программ» связана с системным реестром?
7. Какие разделы и ключи являются потенциальными местами записей «троянских программ»?
8. Для чего используется механизм электронной цифровой подписи?
9. Что понимается под сертификатом?
10. Какой метод шифрования использует электронная цифровая подпись?
11. Что такое аутентификация и идентификация?
12. Для чего применяются эти механизмы?
13. 3. Что можно настроить с помощью оснастки Локальная политика безопасности.
14. Что входит в криптосистему?
15. Сравните методы шифрования с открытым и закрытым ключом (асимметричное и симметричное шифрование).
16. Что такое mmc?
17. Назначение шифрующей файловой системы EFS.

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

Список литературы:

1. Еременко В.Т., Чистяков М.В. Теоретические основы создания и применения профилей протоколов архитектур безопасности. Монография. / Под редакцией Еременко В.Т. – Екатиренбург: Уральский Государственный технический университет, 2000.

2. Макаров В.Ф. Теоретические основы передачи и защиты информации в системах теледоступа в вычислительных ресурсах./Под ред. А.П. Полежаева. - М.: Академия МВД РФ, 1992. - 228 с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006. – 211 с.

4. Расследование неправомерного доступа к компьютерной информации. Учебное пособие. Изд-е 2, дополненное и переработанное / Под.ред. д.ю.н., проф. Н.Г. Шурухнова. – М.: Московский Университет МВД России, 2007.

5. Родионов А.Н. Компьютерные преступления и организация борьбы с ними//Системы безопасности. Межотраслевой тематический каталог. М., 2006г.

6. Теоретические основы развития информационно-телекоммуникационной среды (организационно-правовые и социокультурные аспекты)/Мишин Д.С., Скрыль С.В., Третьяков О.В., Чуев А.В. – Орел: ОрЮИ МВД России, 2005.

7. Уфимцев Ю.С., Ерофеев Е.А. Информационная безопасность России. М.: «Экзамен», 2003 г.

8. Информационная безопасность /П.Н. Башлы. – Ростов н/Д: Феникс, 2006. – 253с.

Тема 4.3. Практическое занятие: «Каналы утечки, искажения и порчи компьютерной информации»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;

- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

1. Назначение прав пользователей произвольном управлении доступом в Windows 2000 (XP)
2. Настройка параметров регистрации и аудита в Windows 2000 [XP]
3. Управление шаблонами безопасности в Windows 2000 (XP)
4. Настройка и использование межсетевого экрана в Windows 2000 (XP)
5. Создание VPN-подключения средствами Windows 2000 (XP)

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:

Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 80 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 5 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет "Вычислительной техники".
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

УПРАЖНЕНИЕ № 1: Назначение прав пользователей произвольном управлении доступом в Windows 2000 (XP)

Краткие теоретические сведения

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются списком ресурсов, доступным пользователю и правами по доступу к каждому ресурсу из списка.

При разграничении доступа по спискам задаются соответствия: каждому пользователю — список ресурсов и прав доступа к ним или каждому ресурсу — список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных. [8]

Задание: Создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и блокировать учетную запись пользователя.

Алгоритм выполнения работы

А. Создание учетной записи.

1. Откройте оснастку **Управление компьютером** в разделе **Администрирование Панели управления.**

2. В оснастке **Локальные пользователи и группы** установите указатель мыши на папку **Пользователи и** нажмите правую кнопку.

3. В появившееся контекстном меню выберите команду **Новый пользователь**. Появится окно диалога Новый пользователь.

4. В поле **Пользователь** введите имя создаваемого пользователя, например, свою фамилию.

Примечание. Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо:»/ \ []:; =,+*?<> Имя пользователя не может состоять целиком из точек и пробелов.

5. В поле **Полное имя** введите полное имя создаваемого пользователя.

6. В поле **Описание** введите описание создаваемого пользователя или его учетной записи, например, *«курсант».*

7. В поле **Пароль** введите пароль пользователя и **в** поле **Подтверждение** подтвердите его правильность вторичным вводом.

Примечание. Длина пароля не может превышать 14 символов.

8.Установите или снимите флажки:

■ потребовать смену пароля при следующем входе в систему;

■ запретить смену пароля пользователем;

■ срок действия пароля не ограничен;

■ отключить учетную запись.

9. Чтобы создать еще одного пользователя, нажмите кнопку **Создать** и повторите шаги с **1** по 8. Для завершения работы нажмите кнопку Создать и затем **Закрыть.**

В. Создание локальной группы.

1. **В** окне оснастки **Локальные пользователи и группы** установите указатель мыши на папке **Группы** и нажмите правую кнопку.

2. В появившемся контекстном меню выберите команду **Новая группа.**

3. В поле **Имя группы** введите имя новой группы, например, **Курсанты.**

Примечание. Имя локальной группы должно быть уникальным в пределах компьютера. Оно может содержать до 256 символов в верхнем и нижнем регистрах.

4. В поле **Описание** введите описание новой группы.

5. В поле **Члены группы** можно сразу же добавить пользователей и

группы, которые войдут **в** данную группу: для этого нужно нажать кнопку **Добавить** и выбрать их в списке.

Для завершения нажмите кнопку **Создать** и затем Закрыть.

C. Изменение членства в локальной группе.

1. **В** окне оснастки **Локальные пользователи и группы** щелкните на папке **Группы.**

2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду Добавить **в** группу или Свойства.

4. Для того, чтобы добавить новые учетные записи в группу, нажмите кнопку Добавить.

5. Далее следуйте указаниям окна диалога Выбор: Пользователи или Группы.

6. Для того, чтобы удалить из группы некоторых пользователей, в поле Члены группы окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку Удалить.

Примечание. В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и глобальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в нее пользователей.

D. Временная блокировка учетной записи.

1. Откройте оснастку Управление компьютером.

2. Для этого либо выберите на Рабочем столе ярлык Мой компьютер и нажмите правую клавишу мыши, после чего выберите пункт контекстного меню Управление, либо воспользуйтесь разделом Администрирование в Панели управления.

3. В открывшейся оснастке выберите пункты Служебные программы/Локальные пользователи и группы.

4. Откройте папку Пользователи и выберите учетную запись Гость.

5. Нажмите правую клавишу мыши и выберите пункт Свойства.

6. В открывшемся оке снимите отметку пункта Отключить учетную запись.

7. Нажмите кнопку ОК и сделайте вывод о состоянии учетной записи.

8. Выполните пункт 5 и отметьте пункт Отключить учетную запись. [8]

Задания для самостоятельной работы

1. Создайте учетную запись с именем ПЗ-6, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера (для этого после нажатия клавиши Print Screen вставьте скопированное изображение в новый документ Word) для представления в качестве отчета.

2. Создайте группу Информационная безопасность и, как в первом

задании, сохраните окно со списком групп Вашего компьютера для отчета.

3. Заблокируйте учетную запись ПЗ-6 и после этого удалите.

УПРАЖНЕНИЕ № 2 Настройка параметров регистрации и аудита в Windows 2000 [XP]

Краткие теоретические сведения

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности. Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т. д.

Аудит — это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемому администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал ~ это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Задание: активизировать механизмы регистрации и аудита операционной системы Windows 2000 (XP) и настроить параметры просмотра аудита папок и файлов.

Алгоритм выполнения работы

А. Активизация механизма регистрации и аудита с помощью оснастки Локальные политики безопасности.

1. Выберите кнопку Пуск панели задач.
2. Откройте меню Настроить/Панель управления.
3. В открывшемся окне выберите ярлык Администрирование/Локальная политика безопасности.
4. Выберите пункт Политика аудита.
5. Для включения или отключения параметров аудита выберите требуемый параметр и дважды щелкните левой клавишей мыши.

6. Для каждого параметра можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа.

7. Значения параметров политики аудита приведены в таблице 1.

8. По умолчанию все параметры политики аудита выключены.

9. Включите аудит успеха и отказа для всех параметров.

10. Для этого выполните пункт 5.

11. Нажмите кнопку ОК. [8]

Таблица 1

Значение параметров аудита системы

Параметр	**Значение**
Аудит событий входа в систему	Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из нее на другом компьютере при условии, что данный компьютер используется для проверки подлинности учетной записи. Если этот параметр политики определен, можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.
Аудит управления учетными записями	Определяет, подлежат ли аудиту все события, связанные с управлением учетными записями на компьютере. К таким событиям относятся следующие события: ■ создание, изменение или удаление учетной записи пользователя или группы; ■ переименование, отключение или включение учетной записи пользователя; ■ задание или изменение пароля.
Аудит доступа к службе каталогов	Определяет, подлежит ли аудиту событие доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом.
Аудит входа в систему	Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из нее на данном компьютере, или подключиться к нему через сеть.
Аудит доступа к объектам	Определяет, подлежит ли аудиту событие доступа пользователя к объекту – например, к файлу, папке, разделу реестра, принтеру и т. п. – для которого задана собственная системная таблица управления доступом.

Аудит изменения политики	Определяет, подлежит ли аудиту каждый факт изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.
Аудит использования привилегий	Определяет, подлежит ли аудиту каждая попытка пользователя воспользоваться предоставленным ему правом.
Аудит отслеживания процессов	Определяет, подлежат ли аудиту такие события, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.
Аудит системных событий	Определяет, подлежат ли аудиту события перезагрузки или отключения компьютера, а также события, влияющие на системную безопасность или на журнал безопасности.

В. Настройка и просмотр аудита папок и файлов (Доступно только на томах NTFS).

1. Установите указатель мыши на файл или папку, для которой следует выполнить аудит, и нажмите правую кнопку.
2. В появившемся контекстном меню выберите команду Свойства.
3. В окне свойств папки или файла перейдите на вкладку Безопасность.
4. На вкладке Безопасность нажмите кнопку Дополнительно и затем перейдите на вкладку Аудит.
5. Если Вы хотите настроить аудит для нового пользователя или группы на вкладке Аудит нажмите кнопку Добавить.
6. Появится диалоговое окно Выбор: Пользователь, Компьютер или Группа.
7. Выберите имя нужного пользователя или группы и нажмите кнопку ОК. Откроется окно диалога Элемент аудита для. Здесь Вы сможете ввести все необходимые параметры аудита.
8. В списке Применять укажите, где следует выполнять аудит (это поле ввода доступно только для папок).
9. В группе Доступ следует указать, какие события следует отслеживать: окончившиеся успешно (Успех), неудачно (Отказ) или оба типа событий.
10. Применять этот аудит к объектам и контейнерам только внутри этого контейнера — определяет, распространяются ли введенные Вами настройки аудита на файлы и папки, находящиеся ниже по дереву каталогов файловой системы (флажок не установлен). В обратном случае, установите флажок (или выберите в списке) Применять опцию Только для этой папки. Это позволит не выполнять аудит для тех объектов файловой системы, которые не представляют интереса.
11. После завершения настройки аудита для папки или файла нажмите несколько раз кнопку ОК, чтобы закрыть все окна диалога.
12. Если Вы хотите просмотреть или изменить настройки аудита для уже существующего пользователя или группы, нажмите кнопку Показать/Изменить.

Появится окно диалога Элемент аудита для. Здесь Вы сможете выполнить все необходимые изменения параметров аудита для выбранного Вами пользователя или группы. По окончании внесения изменений нажмите кнопку ОК.

Примечание. После включения аудита операционная система Windows 2000 (XP) начинает отслеживать события, связанные с безопасностью. Полученную в результате информацию можно просмотреть с помощью оснастки Просмотр событий. При просмотре журнала событий можно выяснить, кто предпринял попытку выполнения неразрешенного ему действия. Для того чтобы иметь возможность настраивать аудит для файлов и папок, необходимо иметь права администратора.

С. Просмотр событий в журнале событий.

1. Выберите кнопку Пуск панели задач.
2. Откройте меню Настроить/Панель управления.
3. В открывшемся окне выберите ярлык Администрирование и далее Просмотр событий.
4. В открывшемся окне выберите пункт Безопасность.
5. В правой половине открытого окна появится список всех зарегистрированных событий.
6. Для просмотра требуемого события вызовите его свойства из контекстного меню или дважды щелкните по его названию левой клавишей мыши.
7. В результате появится окно.
8. В показанном примере зафиксирован успех отключения учетной записи Гость пользователем Админ 8.05.04 в 18.28.31.
9. В примере зафиксирован отказ входа в систему пользователю NT AUTHORITY\SYSTEM (системная учетная запись) 08.05.04 в 17:39:58 по причине «неизвестное имя пользователя или неверный пароль».
10. Таким образом, просмотр журнала событий позволяет в полной мере проанализировать действия пользователей и процессов. [8]

Задания для самостоятельной работы

1. Включите аудит успеха и отказа всех параметров (используйте задание А).
2. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись и скопируйте экран в буфер **(Print Screen)** для отчета.
3. Удалите созданную ранее учетную запись ПЗ-6 и зафиксируйте все события системного журнала, связанные с этим: действием для отчета.

УПРАЖНЕНИЕ № 3: Управление шаблонами безопасности в Windows 2000 (XP)

Краткие теоретические сведения

Управление шаблонами безопасности в Windows 2000 (XP) осуществляется с помощью Редактора шаблонов безопасности, реализованного в виде оснастки MMC.

Он предназначен для создания и редактирования текстовых файлов конфигурации безопасности операционной системы Windows 2000 (XP). Такие файлы значительно легче переносятся с одной системы на другую, чем соответствующие им базы данных безопасности.

Созданные при помощи оснастки Шаблоны безопасности текстовые файлы хранятся на жестком диске и при необходимости могут быть импортированы в базу данных безопасности. В этом случае все хранимые настройки безопасности начнут действовать.

Значения параметров обеспечения безопасности заносятся в текстовые файлы с расширением inf, называемые Шаблонами безопасности.

Примечание. Новые **Шаблоны безопасности** не изменяют все старые настройки параметров системы безопасности, они лишь дополняют их, увеличивая (инкрементируя) степень защищенности компьютера.

Задание: загрузить редактор **Шаблона безопасности,** редактировать шаблон безопасности **и** сохранить его с новым именем.

Алгоритм выполнения работы

А. Загрузка оснастки Шаблоны безопасности.

1. Выберите кнопку Пуск в панели задач.
2. Перейдите к пункту **Выполнить.**
3. В открывшемся окне в поле ввода введите команду mine.
4. В результате откроется консоль управления mmc.
5. В меню **Консоль** выберите команду **Добавить или удалить оснастку** и нажмите кнопку **Добавить.**
6. В поле **Оснастка** дважды щелкните **Шаблоны безопасности.**
7. Нажмите кнопку **Закрыть.**
8. В списке выбранных оснасток для новой консоли появится элемент **Шаблоны безопасности.**
9. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку ОК.
10. Чтобы сохранить эту консоль, в меню Консоль выберите команду **Сохранить** и укажите имя оснастки **Шаблоны** безопасности.
11. Закройте окно Консоли и выберите команду Пуск **и** далее Все **программы.**
12. Найдите пункт **Администрирование** и выберите подпункт **Шаблоны безопасности** (Теперь оснастка с **Шаблоны безопасности** доступна **в** меню **Пуск).**
13. Для просмотра значений имеющихся шаблонов в окне оснастки откройте, например, узел **Шаблоны безопасности,** щелчком выберите шаблон безопасности compatws и просмотрите его папки **Политика учетных записей, Локальная политика и др.**

14. Помимо раскрытого шаблона безопасности compatws.inf существуют **и** другие стандартные шаблоны, конфигурации которых позволяют получить различные по надежности системы безопасности. [8]

Б. Редактирование и сохранение шаблона безопасности.

1. Щелкните на одном из стандартных шаблонов безопасности (например, compatws), которые Вы видите **в** окне оснастки **Шаблоны безопасности.**
2. Если Вы хотите модифицировать какую-либо настройку безопасности, дважды щелкните на ней и отредактируйте значения параметров.
3. Для сохранения откорректированного стандартного шаблона безопасности под другим именем выполните следующие действия.
4. Укажите откорректированный стандартный шаблон (например, compatws), и нажмите правую кнопку мыши.
5. В появившемся контекстном меню выберите команду **Сохранить как.**
6. Введите с клавиатуры новое имя файла (например, custom). По умолчанию шаблоны безопасности располагаются в каталоге *%SystemRoot%\Secunfy* \Templates.
7. Пользовательский шаблон будет добавлен в определенную заранее конфигурацию безопасности и сохранен под введенным Вами именем.

Настроив Шаблон безопасности для одной ПЭВМ, Вы можете перенести его и на другие ПЭВМ Вашей рабочей группы. Шаблоны безопасности являются гибким и удобным инструментом по настройке системы безопасности операционной системы. [8]

Задания для самостоятельной работы

Создайте на базе существующего Шаблона безопасности новый шаблон и дайте ему имя ПЗ-8. После этого зафиксируйте список шаблонов, скопировав изображение экрана в буфер и далее в файл для отчета.

УПРАЖНЕНИЕ № 4: Настройка и использование межсетевого экрана в Windows 2000 (XP)

Краткие теоретические сведения

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет **межсетевой экран** или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация

информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Брандмауэр в **Windows XP** — это система защиты подключения к Интернету (Internet Connection Firewall, ICF), представляет собой программу настройки ограничений, регулирующих обмен данными между Интернетом и небольшой сетью или локальным компьютером. Брандмауэр ICF необходимо установить для любого компьютера, имеющего прямое подключение к Интернету.

При включении брандмауэра для локального компьютера, подключенного к Интернету с помощью модема удаленного доступа, брандмауэр ICF обеспечивает защиту этого подключения. [8]

Задание: Активизировать встроенный брандмауэр операционной системы Windows XP и настроить его параметры.

Алгоритм выполнения работы

А. Активизация встроенного межсетевого экрана.

1. Откройте компонент Сетевые подключения.
2. Для этого выберите последовательно Пуск — Панель управления — Сетевые подключения.
3. Выделите подключение удаленного доступа, подключение по локальной сети или высокоскоростное подключение к Интернету, которое требуется защитить брандмауэром, и затем выберите в контекстном меню (при выделенном подключении нажать правую клавишу мыши) команду **Свойства.**
4. На вкладке **Дополнительно** в группе **Брандмауэр подключения к Интернету** отметьте пункт **Защитить мое подключение к Интернету.**

Примечание. Для отключения брандмауэра достаточно снять флажок Защитить мое подключение к Интернету.

В. Настройка параметров брандмауэра.

1. Выполните пункты 1—3 предыдущего задания.
2. Выберите кнопку Параметры в нижней части открытого окна.
3. В результате откроется окно **Дополнительные параметры** с тремя закладками (Службы, Ведение журнала безопасности и ICMP) .
4. Выберите закладку Службы.

Примечание. На закладке Службы вы можете в явном виде указать службы Интернета, прохождение трафика которых вы допускаете. Например, чтобы обеспечить прохождение веб-страниц из Интернета на компьютер, необходимо включить службу «Веб-сервер HTTP».

5. Отметьте все службы.
6. Выберите закладку Ведение журнала безопасности.

Примечание. Для брандмауэра подключения к Интернету предусмотрен журнал безопасности для записи событий, связанных с его работой. Журнал безопасности ICF поддерживает следующие возможности.

Запись пропущенных пакетов. Этот параметр задает запись в журнал сведений обо всех потерянных пакетах, исходящих из сети (компьютера) или из Интернета. Если установить флажок Записывать потерянные пакеты, будут собираться сведения о каждом пакете, который пытался пройти через ICF, но был обнаружен и отвергнут брандмауэром.

Запись успешных подключений. Этот параметр задает запись в журнал сведений обо всех успешных подключениях, инициированных из сети (компьютера) или из Интернета.

7. Отметь пункты Записывать пропущенные пакеты и Записывать успешные подключения. Обратите внимание на расположение журнала безопасности.

Примечание. Журнал безопасности брандмауэра состоит из двух разделов. В заголовке содержатся сведения о версии журнала и полях, в которые можно записывать данные. Содержимое заголовка имеет вид статического списка. Содержимое журнала безопасности представляет собой откомпилированные данные, которые вводятся при обнаружении трафика, пытающегося пройти через брандмауэр. Поля журнала заполняются слева направо, как они расположены на странице. Для того чтобы в журнал вводились данные, необходимо выбрать хотя бы один параметр ведения журнала или оба параметра.

8. Теперь Ваш брандмауэр настроен и готов к защите Вашего компьютера от внешних угроз. [8]

Задания для самостоятельной работы

1. Настройте брандмауэр на работу с Веб-сервером (HTTP), FTP-сервером и зафиксируйте соответствующее окно для отчета.
2. Включите журнал безопасности.
3. После выполнения задания 1 и 2 подключитесь к Интернету и посетите любой веб-сервер.
4. Завершите работу в Интернете и просмотрите журнал безопасности.
5. Зафиксируйте записи журнала безопасности для отчета.

УПРАЖНЕНИЕ № 5: Создание VPN-подключения средствами Windows 2000 (XP)

Краткие теоретические сведения

Технология виртуальных частных сетей (VPN — Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности: шифрования, экранирования и туннелиро-вания.

Задание: Создать VPN-подключение и выполнить его настройку.

Алгоритм выполнения работы

А. Создание VPN-подключения.

1. Откройте компонент Сетевые подключения.
2. Для этого выберите последовательно Пуск — Панель управления — Сетевые подключения.
3. Выберите пункт Создание нового подключения и нажмите кнопку Далее.
4. В зависимости от операционной системы выполните следующие действия:

■ для Windows XP — в открывшемся окне выберите пункт Подключить к сети на рабочем месте и нажмите Далее. После этого выберите Подключение к виртуальной частной сети и нажмите Далее.

■ для Windows 2000 — в открывшемся окне выберите пункт Подключение к виртуальной частной сети через Интернет и нажмите Далее.

5. Введите имя подключения и перейдите к следующему шагу командой Далее.
6. Если перед установкой «туннельного доступа» требуется подключение к провайдеру услуг Интернета, то выберите Набрать номер для следующего предварительного подключения и, выбрав нужное подключение, нажмите Далее. В противном случае, выберите Не набирать номер для предварительного подключения и нажмите Далее.
7. Введите имя узла (сети) или его IP-адрес, к которому идет подключение.
8. Завершите работу Мастера сетевых подключений.
9. В результате в папке Подключения появится новое подключение.
10. Для настройки параметров подключения выделите подключение VPN и вызовите его свойства из контекстного меню (нажатие правой клавиши мыши).
11. Рассмотрите все имеющиеся параметры VPN-подключения и при необходимости воспользуйтесь соответствующими разделами справки. [8]

Задания для самостоятельной работы

Создайте VPN-подключение к узлу с адресом 122Л22.122.122 и зафиксируйте окно его свойств (Print Screen) на закладке **Общие** (как показано на рис. 5) в качестве отчета.

Контрольные вопросы

1. Какие методы управления доступом Вам известны?
2. Чем отличается мандатное управление доступом от дискретного?
3. Допустимо ли имя пользователя П38/44? Почему?
4. 1. Чем отличаются регистрация и аудит?
5. Что является средствами регистрации и аудита?
6. Какие события фиксируются в системном журнале?
7. Что фиксирует система при регистрации событий?
8. Для чего используются Шаблоны безопасности?

9.В каком месте на диске хранятся (по умолчанию) шаблоны безопасности?

10.Какие разделы включает стандартный Шаблон безопасности?

11.Что такое брандмауэр?

12.Какие бывают брандмауэры?

13.Что фиксирует журнал безопасности брандмауэра?

14.Какие механизмы безопасности используются при реализации VPN-подключения?

15.Что такое «туннель» и в чем состоит принцип «туннелирования>>?

16.В чем заключаются защитные функции виртуальных частных сетей?

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

Список литературы:

1. Еременко В.Т., Чистяков М.В. Теоретические основы создания и применения профилей протоколов архитектур безопасности. Монография. / Под редакцией Еременко В.Т. – Екатиренбург: Уральский Государственный технический университет, 2000.

2. Макаров В.Ф. Теоретические основы передачи и защиты информации в системах теледоступа в вычислительных ресурсах./Под ред. А.П. Полежаева. - М.: Академия МВД РФ, 1992. - 228 с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006. – 211 с.

4. Расследование неправомерного доступа к компьютерной информации. Учебное пособие. Изд-е 2, дополненное и переработанное / Под.ред. д.ю.н., проф. Н.Г. Шурухнова. – М.: Московский Университет МВД России, 2007.

5. Родионов А.Н. Компьютерные преступления и организация борьбы с ними//Системы безопасности. Межотраслевой тематический каталог. М., 2006г.

6. Теоретические основы развития информационно-телекоммуникационной среды (организационно-правовые и социокультурные аспекты)/Мишин Д.С., Скрыль С.В., Третьяков О.В., Чуев А.В. – Орел: ОрЮИ МВД России, 2005.

7. Уфимцев Ю.С., Ерофеев Е.А. Информационная безопасность России. М.: «Экзамен», 2003 г.

8. Информационная безопасность /П.Н. Башлы. – Ростов н/Д: Феникс, 2006. – 253с.

Тема 4.4. Практическое занятие: «Поиск и обнаружение устройств негласного съема информации»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

3.1 Работа с программами: Acronis Privacy Expert Suite, Steganos Crypt; Kerio WinRoute Firewall.

3.2 Работа с программами защиты информации от несанкционированного доступа Tiny Firewall Pro; McAfee Personal; CrypKey SDK.

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:

Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 80 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 5 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет "Вычислительной техники".
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

ВВЕДЕНИЕ

Что такое Acronis Privacy Expert Suite

Acronis Privacy Expert Suite — это интегрированный программный пакет, обеспечивающий конфиденциальность и безопасность работы на персональном компьютере (ПК), отдельно стоящем или подключенном к локальной или глобальной сети (World Wide Web, WWW). С помощью Acronis Privacy Expert Suite вы сможете:

- удалить вредоносные программы, которые внедряются в систему пользователя и осуществляют свою деятельность без его ведома;
- обеспечить своему компьютеру активную упреждающую защиту от программ, занимающихся несанкционированной деятельностью без ведома пользователя;
- очистить жесткий диск компьютера и любые разделы операционной системы Windows от каких бы то ни было свидетельств работы пользователя за компьютером или в интернете;
- блокировать появление «всплывающих окон» с навязчивой рекламной информацией во время посещения различных интернет-сайтов;
- произвести гарантированное уничтожение конфиденциальной информации на выбранных дисках и/или разделах жестких дисков.

В отличие от других программ Acronis Privacy Expert Suite удаляет свидетельства работы пользователя без возможности восстановления благодаря использованию методов гарантированного уничтожения информации.

Программа Acronis Privacy Expert Suite предоставляет возможность удалить свидетельства работы пользователя во всех разделах операционной системы Windows. Acronis Privacy Expert Suite позволяет:

- удалять вредоносное программное обеспечение с помощью Мастера удаления вредоносных программ;
- осуществлять активную упреждающую защиту своего компьютера от программ-шпионов;
- регулярно и своевременно обновлять информацию о вредоносного ПО с помощью Мастера обновлений.
- очищать кэш интернет-браузеров;
- удалять файлы cookies;
- удалять загружаемые компоненты;
- очищать журнал истории посещений сайтов, а также список недавно посещенных сайтов, сохраненный в адресной строке браузера;
- удалять формы автозаполнения и пароли, используемые на веб-страницах, требующих авторизации пользователя.
- удалять сообщения электронной почты (в почтовых программах MS Outlook и MS Outlook Express), а также очищать список контактов и адресную книгу;
- удалять резервные копии реестра Windows, сохраняющие свидетельства работы пользователя за ПК и в интернете;
- удалять временные файлы в стандартных папках Windows;
- удалять файлы любых типов в пользовательских папках на любых подключенных к компьютеру дисках;
- очищать Корзину в Windows;
- очищать свободное пространство жесткого диска;
- очищать папку Prefetch в Windows;
- удалять системные пароли;

- очищать список недавно открывавшихся и сохранявшихся документов;
- удалять свидетельства использования функций поиска файлов, компьютеров в локальной сети;
- блокировать открытие нежелательных «всплывающих окон» при посещении различных интернет-ресурсов;
- гарантированно уничтожать в случае необходимости все данные на выбранных разделах или/и дисках компьютера;
- восстанавливать или удалять объекты (файлов, ключей реестра и т.д.) в папке Карантин, удаленные в процессе очистки компьютера от вредоносного ПО;
- очищать файл подкачки Windows.

Программа Acronis Privacy Expert Suite удаляет свидетельства пользовательской активности за ПК без возможности восстановления какими бы то ни было средствами. Для этого Acronis Privacy Expert Suite использует методы гарантированного уничтожения конфиденциальной информации, удовлетворяющие наиболее известным национальным стандартам (подробно см. Приложение А к данному Руководству).

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Главное окно Acronis Privacy Expert Suite

Работа с Acronis Privacy Expert Suite осуществляется из Главного окна программы, которое доступно пользователю после запуска программы через меню Пуск – Все программы – Acronis PrivacyExpert – Acronis Privacy Expert Suite либо с помощью ярлыка программы, который автоматически помещается после ее установки на Рабочем столе пользователя.

В Главном окне Acronis Privacy Expert Suite вы можете увидеть две основных группы категорий очистки компьютера пользователя.

Группа Вредоносные программы включает в себя «Удаление вредоносных программ» - инструмент для удаления с компьютера пользователя вредоносных программ, которые представляют собой угрозу для конфиденциальности информации, поскольку осуществляют свою деятельность без ведома пользователя.

Группа Конфиденциальность включает следующие категории:

- Интернет-компоненты – полное удаление следов работы пользователя с интернетом и электронной почтой
- Очистка системы – гарантированная очистка компонентов операционной системы Windows, которые хранят следы работы пользователя за компьютером;
- Удаление следов работы приложений – удаление следов работы с теми или иными программами;

- Дополнительные инструменты – дополнительные инструменты обеспечения конфиденциальности работы пользователя на компьютере, включая средство гарантированного уничтожения файлов File Shredder и утилиту для полной очистки содержимого жесткого диска пользователя без возможности последующего восстановления - Acronis Drive Cleanser.

Для перехода из одной категории в другую и для возврата в главное окно программы, пользуйтесь кнопками Вернуться, Дальше и Другие категории, расположенными на Панели инструментов. Кроме того, вернуться в главное окно можно с помощью кнопки Другие категории, расположенной на боковой панели.

Основные принципы работы

Основные операции в программе Acronis Privacy Expert Suite осуществляются с помощью удобных и простых в использовании Мастеров:

- Мастер удаления вредоносных программ – удаляет с компьютера программы-шпионы и программы-паразиты, деятельность которых не санкционирована пользователем.
- Мастер удаления вредоносных программ системы – производит полную очистку разделов операционной системы Windows от следов работы пользователя на данном ПК, включая временные файлы, список недавно использовавшихся файлов, строку поиска файлов, корзину Windows и др.
- Мастер удаления вредоносных программ интернет-компонентов – позволяет быстро уничтожить все следы работы пользователя с интернетом и электронной почтой на данном ПК;
- Мастер удаления следов работы с программами – удаляет следы работы пользователя с различными программами на данном ПК

Каждый вариант очистки компьютера с помощью Acronis Privacy Expert Suite может запускаться вручную, либо автоматически.

Удаление вредоносных программ с помощью Мастера удаления вредоносных программ

Чтобы запустить Мастер удаления вредоносных программ, выберите пункт Удалить вредоносные программы в списке задач (категория Удаление вредоносных программ).

После запуска Мастера ваш компьютер будет проверен на наличие вредоносного ПО. Результаты поиска будут показаны в правой части окна. Вы можете увидеть, какие вредоносные программы обнаружены на вашем компьютере, а также получите информацию, где они разместили свои системные файлы и в какие ключи (записи) системного реестра они внесли изменения:

Информацию о каждой из найденных вредоносных программ вы можете найти в левой части окна Мастера при выделении курсором мыши соответствующего элемента в списке обнаруженного вредоносного ПО. Все обнаруженные вредоносные программы автоматически помечены для удаления.

Если вы по каким-то причинам не хотите удалять те или иные разновидности вредоносного ПО или отдельные их компоненты, снимите соответствующий флажок в списке результатов поиска. После того, как вы полностью сформировали список вредоносных программ, подлежащих удалению, нажмите кнопку Далее. В следующем окне вы увидите окончательный сценарий планируемых операций по удалению вредоносного ПО.

Чтобы выполнить все указанные в сценарии операции, нажмите кнопку Завершить.

По окончании процедуры удаления вредоносных программ вы получите итоговый отчет, в котором будет указано, какое количество компонентов было удалено.

Учебное упражнение № 1

Проведите очистку компьютера от вредоносных программ с помощью программного пакета Acronis Privacy Expert Suite вручную.

Запуск Планировщика

Чтобы настроить запуск очистки вашего компьютера по расписанию, щелкните на значке Назначить задание на боковой панели главного окна программы Acronis Privacy Expert Suite. После того, как будет запущен Мастер планирования операций, вы должны в открывшемся списке выбрать тот вариант очистки, запуск которого вы хотите осуществлять по расписанию автоматически. Вы можете:

- Запускать по расписанию любой из вариантов Быстрая очистка, который позволяет производить очистку всего компьютера целиком или отдельной категории компонентов.
- Осуществлять автоматическую очистку по расписанию любых компонентов, относящихся к той или иной категории.

Мастер настройки запуска по расписанию предоставляет пользователю гибкие возможности автоматического запуска любого выбранного варианта очистки компьютера. Вы можете выполнять автоматическую очистку компьютера:

1. Ежедневно, в заранее назначенное время с возможностью запуска, например, только по рабочим дням или периодически — раз в несколько дней;
2. Еженедельно, в заранее назначенное время с возможностью запуска в определенные дни недели;
3. Ежемесячно, в заранее заданное время и день месяца; поддерживается возможность запуска очистки;
4. Однократно, в заранее заданное время (часы: минуты) на определенную дату (день-месяц-год);
5. При включении компьютера;
6. При входе в систему под своим именем;
7. Непосредственно Перед выключением компьютера;
8. Перед выходом из системы.

Учебное упражнение № 2

Назначьте задание на произведение еженедельной очистки компьютера с помощью программного пакета Acronis Privacy Expert Suite.

Просмотр журнала событий

Журнал событий сохраняет информацию обо всех действиях, которые совершаются с помощью Acronis Privacy Expert Suite. С его помощью можно найти сведения обо всех ошибках, которые возникли в процессе работы с программой.

Настройки журнала позволяют вам отслеживать события с разной степенью подробности. Вы можете выбрать один из следующих вариантов:

- Все события
- Наиболее важные события (рекомендуется) – ошибки и сообщения о программах-шпионах
- Ничего не записывать

Учебное упражнение № 3

Произведите просмотр журнала ведущегося программным пакетом Acronis Privacy Expert Suite за последнюю неделю и проведите необходимый анализ.

Каковы признаки наличия вредоносных программ на компьютере?

Хотя во многих случаях вредоносные приложения осуществляют свою деятельность незаметно для пользователя, однако существует ряд признаков, которые могут послужить поводом для того, чтобы проверить свой компьютер на наличие в нем вредоносных программ.

- Светодиодный индикатор состояния жесткого диска показывает, что на диске производятся операции чтения/записи информации даже в тех случаях, когда у вас не запущены никакие программы и не открыты никакие документы;
- Ваш компьютер принимает или передает информацию через интернет, хотя ваш веб-браузер и программа электронной почты закрыты;
- Без вашего согласия изменилась стартовая страница (home page) вашего веб-браузера;
- При работе с некоторыми программами или в интернете время от времени появляются рекламные баннеры, всплывающие окна и т.п.

В случае, если вы заметили какие-либо из приведенных здесь признаков, вам необходимо запустить программу Acronis Privacy Expert Suite, которая обнаружит и удалит программы, осуществляющие несанкционированную деятельность на вашем ПК. Если вы хотите:

- Обнаружить и удалить любые разновидности вредоносных программ на вашем компьютере, запустите Удаление вредоносных программ.

- Предотвратить проникновение вредоносного ПО на ваш компьютер, включите и настройте Службу защиты Acronis.

Настройка параметров Мастера удаления вредоносных программ

Чтобы настроить параметры работы Мастера удаления вредоносных программ, выберите пункт Настройка параметров удаления вредоносных программ.

Выбор режима сканирования

Поиск вредоносных программ может осуществляться в двух режимах:

- Интеллектуальный поиск – данный режим используется в Acronis Privacy Expert Suite по умолчанию. В этом случае поиск вредоносного ПО осуществляется только в наиболее вероятных местах их нахождения на компьютере пользователя: в системных папках, папках профиля пользователя, папках, содержащих временные файлы, а также производится поиск соответствующих записей в системном реестре. Выберите данный режим, если хотите провести быструю проверку своего компьютера.
- Полный поиск – развернутый алгоритм поиска вредоносного ПО. В данном случае поиск осуществляется во всех папках и на всех дисках компьютера пользователя. Данный вариант поиска может занять существенно большее время (в зависимости от объема жесткого диска вашего компьютера).

Учебное упражнение № 4

Произведите интеллектуальный поиск вредоносных программ в памяти компьютера с помощью программного пакета Acronis Privacy Expert Suite.

Обновление базы данных вредоносных программ через Интернет

Новые вредоносные программы появляются каждый день, и, чтобы обеспечить надежную и своевременную защиту от них, Acronis Privacy Expert Suite предлагает вам специальную службу обновления базы данных вредоносного ПО через интернет.

Запуск Мастера обновлений

Запустить Мастер обновлений можно следующими способами:

- С помощью пункта Интернет-обновления на боковой панели главного окна программы Acronis Privacy Expert Suite
- С помощью пункта Установки → Интернет-обновления в строке меню
- С помощью кнопки Интернет-обновления на панели инструментов.

Выбор режима обновления

После того, как Мастер обновлений запущен, вы можете выбрать режим, в котором будет осуществляться обновление. Вы можете производить его самостоятельно вручную или же настроить автоматическое обновление по расписанию:

- Если вы хотите немедленно обновить информацию о программах-шпионах, выберите пункт Обновить базу данных сейчас
- Если вы хотите получать все обновления в автоматическом режиме согласно удобному для вас расписанию, выберите пункт Обновлять по расписанию.

Учебное упражнение № 5

Произведите обновление базы данных вредоносных программ программного пакета Acronis Privacy Expert Suite через Интернет.

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

Список литературы:

1. Еременко В.Т., Чистяков М.В. Теоретические основы создания и применения профилей протоколов архитектур безопасности. Монография. / Под редакцией Еременко В.Т. – Екатиренбург: Уральский Государственный технический университет, 2000.
2. Макаров В.Ф. Теоретические основы передачи и защиты информации в системах теледоступа в вычислительных ресурсах./Под ред. А.П. Полежаева. - М.: Академия МВД РФ, 1992. - 228 с.
3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006. – 211 с.
4. Расследование неправомерного доступа к компьютерной информации. Учебное пособие. Изд-е 2, дополненное и переработанное / Под.ред. д.ю.н., проф. Н.Г. Шурухнова. – М.: Московский Университет МВД России, 2007.
5. Родионов А.Н. Компьютерные преступления и организация борьбы с ними//Системы безопасности. Межотраслевой тематический каталог. М., 2006г.
6. Теоретические основы развития информационно-телекоммуникационной среды (организационно-правовые и социокультурные аспекты)/Мишин Д.С., Скрыль С.В., Третьяков О.В., Чуев А.В. – Орел: ОрЮИ МВД России, 2005.
7. Уфимцев Ю.С., Ерофеев Е.А. Информационная безопасность России. М.: «Экзамен», 2003 г.

Тема 4.5. Практическое занятие: «Программные методы и средства очистки компьютера»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

3.1 Работа с программами: Acronis Privacy Expert Suite, Knoppix-STD; Process Explore.

3.2 Работа с программами восстановления информации Forensic and Incident Response Environment; Process Explorer.

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:

Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 80 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 5 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет "Вычислительной техники".
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Очистка диска с помощью Acronis Drive Cleanser

Во многих случаях пользователям бывает недостаточно тех средств уничтожения данных, которые присутствуют в операционных системах стандартно. Удаленные с диска файлы могут быть легко восстановлены с помощью несложных программ, и даже полное форматирование жесткого

диска не дает гарантий безусловного уничтожения конфиденциальной информации.

Решить данную проблему помогает Acronis Drive Cleanser – инструмент гарантированного уничтожения всех данных на выбранных разделах или/и дисках компьютера. Он предоставляет возможность использовать — в зависимости от степени важности информации — один из существующих стандартов уничтожения данных и создавать собственные методы.

Работа с Acronis Drive Cleanser

Acronis Drive Cleanser позволяет производить следующие операции:

- Очистку выбранных разделов жесткого диска (или дисков) от содержащейся на них информации с помощью набора предустановленных методов
- Создание и использование пользовательских методов очистки жесткого диска

Работа инструмента Acronis Drive Cleanser построена по принципу Мастера – все действия над жесткими дисками осуществляются на основе создаваемых в процессе диалога с пользователем сценариев. До того, как вы запустите созданный сценарий на выполнение, никаких реальных действий по уничтожению информации не происходит. На любом этапе работы с программой вы можете вернуться к предыдущим этапам создания сценария и выбрать для уничтожения другие разделы и/или диски или другие методы очистки жесткого диска.

В начале вам необходимо выбрать разделы жестких дисков, на которых вы хотите уничтожить информацию.

Щелкните мышью на прямоугольнике, представляющем раздел жесткого диска. В правом верхнем углу прямоугольника появится красный крест. Это означает, что раздел выбран для уничтожения содержащейся на нем информации.

Вы можете выбрать для уничтожения информации диск целиком (или несколько дисков). Для этого щелкните мышью на прямоугольнике, представляющем жесткий диск (со значком устройства, номером диска и его емкостью).

Вы можете одновременно выбрать несколько различных разделов, расположенных на разных дисках, или несколько дисков.

Для продолжения работы щелкните мышью на кнопке Далее.

В окне Заключительные действия вы можете выбрать, что делать с разделом, информация на котором уничтожается. Acronis Drive Cleanser предоставляет вам три возможности:

Оставить разделы как есть — то есть только уничтожить информацию в соответствии с методом, который вам будет предложено выбрать ниже;

Удалить раздел — уничтожить информацию и удалить раздел;

Форматировать раздел — уничтожить информацию и отформатировать раздел (установлено по умолчанию).

В приведенном ниже примере предполагается, что переключатель установлен в положение Оставить разделы как есть. Это позволит увидеть, к каким результатам приводит уничтожение информации раздела само по себе (без форматирования или удаления раздела).

Использование предустановленных методов уничтожения данных

Acronis Drive Cleanser использует ряд наиболее распространенных стандартов уничтожения данных.

После того, как вы выберете необходимый метод, Acronis Drive Cleanser произведет все необходимые операции по удалению информации с выбранного вами раздела или диска. По окончании вы получите сообщение об успешном завершении процедуры очистки диска или раздела.

Инструмент Acronis Drive Cleanser предоставляет вам еще одну возможность — оценить результаты выполнения процедуры (метода) очистки раздела или/и жесткого диска. Acronis Drive Cleanser имеет встроенную программу просмотра жесткого диска.

Рассмотренные выше методы предлагают различные варианты уничтожения конфиденциальной информации. Таким образом, картина, которую вы увидите на разделе или/и диске зависит от выбранного до этого метода уничтожения информации, но фактически вы можете увидеть сектора, заполненные либо нулями, либо случайными символами.

Учебное упражнение № 1.

Проведите гарантированную очистку диска с помощью предустановленных методов уничтожения программного пакета Acronis Privacy Expert Suite.

Создание пользовательских методов удаления данных

Acronis Drive Cleanser предоставляет пользователю возможность использовать для очистки жестких дисков не только предустановленные методы, но и создать свои собственные. Несмотря на то, что в программу включены методы всех классов — быстрые, но не слишком надежные, очень надежные, но медленные, компромиссные между теми и другими, — квалифицированный пользователь может почувствовать необходимость в своих собственных методах.

Для создания собственного метода очистки жесткого диска в окне Выбор метода в списке предустановленных методов найдите строку «Создать метод…» и щелкните по ней мышью. Обратите внимание, что в списке также присутствует строка «Загрузить из файла…».

После выбора одного из предустановленных методов на экране сразу появлялось окно сценария очистки раздела жесткого диска (раздел и/или жесткий диск выбирался на одном из предыдущих шагов). На этот раз будет запущен мастер создания пользовательского метода, в результате чего вы попадете в окно Количество проходов.

Давайте создадим в качестве иллюстрации простой пользовательский метод, аналогичный, например, американскому стандарту. Как вы, вероятно,

помните, американский стандарт предполагает три прохода по жесткому диску, во время которых на диск пишутся разного рода символы, плюс еще один проход, во время которого осуществляется процедура верификации, — итого 4 прохода.

Напомним, что предустановленные методы для очистки жесткого диска выполняют от 1 (быстрый метод, российский стандарт) до 35 проходов (метод Питера Гутмана).

Определение метода: шаблон

В окне Определение метода вам представляется нечто вроде шаблона будущего метода: список в этом окне содержит столько записей, сколько проходов вы определили для своего метода на предыдущем этапе.

Обозначения в окне имеют следующее значение. В первой колонке списка находится номер прохода по диску; во второй — тип операции над диском (таких операции всего две: запись на диск символа, «запись», и верификация, «проверка», записанного); в третьей колонке содержится записываемый на диск образец.

Записываемый на диск образец — это всегда шестнадцатеричное число, то есть число, например, вида: 0x00, 0xAA или 0xCD и т.п. В данном случае приведены числа длиной 1 байт, но они могут иметь длину до 512 байт. Кроме таких чисел вы можете ввести для записи случайное шестнадцатеричное число любой длины (до 512 байт). Наконец, вы можете включить в метод для записи еще одно число, обозначаемое как «дополнительный код числа», то есть число, дополнительное к записанному на диск на предыдущем проходе.

В окне Определение метода вам предложен только шаблон метода. Что именно программа должна писать на диск, чтобы уничтожить конфиденциальную информацию, вы должны определить сами.

Для этого щелкните мышью, например, на строке 1-го прохода:

Для продолжения работы нажмите кнопку Далее.

На экране появится окно, в котором вы сможете определить записываемый на диск образец (шестнадцатеричное число).

На этом рисунке, по умолчанию, переключатель установлен в положение Записать число, в поле введено шестнадцатеричное число 0x00.

Поясним значение элементов управления окна. В поле, расположенное ниже положения переключателя Записать число, вы можете ввести произвольное шестнадцатеричное число для записи его на произвольном проходе жесткого диска (в данном случае — на 1-м проходе).

Установив переключатель в положение Записать случайное число, вы, во-первых, тем самым выберете для записи на диск случайное число, во-вторых, сможете в поле ниже (спинере) указать длину случайного числа в байтах.

Американский национальный стандарт как раз предусматривает во время первого прохода диска запись случайных чисел в каждый байт каждого сектора, поэтому вы должны установить переключатель в положение Записать случайное число и ввести в поле значение, равное 1.

Для продолжения работы нажмите кнопку Далее.

Вы снова попадете в окно шаблона метода и сможете увидеть, что прежняя запись («1 – запись – 00») сменилась на «1 – запись – случайное число размером 1 байт».

Для определения следующего прохода выделите вторую строку в списке и нажмите кнопку Далее.

Вы попадете в окно, уже знакомое вам, но на этот раз в нем вам будет доступно большее число положений переключателя: доступны для выбора два дополнительных положения переключателя:

Записать число, дополнительное к записанному на предыдущем проходе

Проверка записи.

Эти положения логически имеют смысл, только после первого прохода по диску: до того, как осуществлен первый проход, бессмысленно выражение «предыдущий» и нечего, собственно говоря, проверять.

Как вы помните, американский стандарт предусматривает во время второго прохода запись в каждый сектор диска шестнадцатеричных чисел, дополнительных к записанным на предыдущем проходе. Поэтому на этот раз в этом окне вам предлагается выбрать положение переключателя Записать дополнительный код числа, записанного на предыдущем проходе и нажать кнопку Далее.

Вы вновь попадете в окно шаблона метода. В этом окне 2-я запись, прежде имевшая вид: «1 – запись – 00», сменилась на: «1 – запись – дополнительный код числа из предыдущего прохода».

Аналогичным образом, следуя спецификации американского стандарта, создаем 3-й и 4-й проходы перезаписи жесткого диска. Стоит отметить, что таким образом может быть создан любой метод, соответствующий вашим требованиям к безопасности.

Учебное упражнение № 2.

Проведите создание пользовательского метода удаления данных программного пакета Acronis Privacy Expert Suite и проведите с его помощью удаление

Сохранение созданного метода в файле

В следующем окне Сохранение созданного метода вы можете сохранить метод на диске в файле, который по умолчанию имеет расширение *.alg. Это может быть полезно, если вы собираетесь использовать созданный метод в дальнейшем.

Для сохранения метода в следующем окне введите имя файла, в котором будет храниться метод, вместе с путем к нему в соответствующее поле или найдите существующий файл на диске.

Таким образом, все проходы метода определены, сам метод сохранен в файле, так что, нажав на кнопку Далее, вы попадете в окно сформированного сценария уничтожения информации, основанного на вашем методе.

Нажав на кнопку Приступить, вы тем самым запустите сформированный сценарий на выполнение.

Учебное упражнение № 3.

Проведите сохранение созданного метода гарантированного удаления программным пакетом Acronis Privacy Expert Suite в файле.

Загрузка метода из файла

Если во время работы с Acronis Drive Cleanser вы создали и сохранили на диске (в файлах) собственные методы уничтожения конфиденциальной информации, то воспользоваться ими вы можете следующим образом.

В окне Выбор метода выберите в ниспадающем списке строку Загрузить из файла… и далее укажите файл, в котором были сохранены параметры пользовательского метода уничтожения информации. По умолчанию такой файл имеет расширение *.alg.

Создание загрузочных дисков с помощью программы Acronis Drive Cleanser

Если вы не создали загрузочную дискету или CD, на которой установлен Acronis Drive Cleanser, во время установки программы Acronis Privacy Expert Suite, то вы можете это сделать в любое удобное время с помощью утилиты Создание загрузочных дисков.

Благодаря наличию такого диска вы можете легко производить гарантированное уничтожение данных на вашем компьютере, даже если на нем не установлена программа Acronis Privacy Expert Suite.

Чтобы создать загрузочную дискету, выберите щелчком мыши на боковой панели главного окна Acronis Privacy Expert Suite пункт Создание загрузочных дисков и выполняйте все указания соответствующего Мастера.

Учебное упражнение № 4.

Проведите загрузку метода гарантированного метода удаления из файла созданного при помощи программного пакета Acronis Privacy Expert Suite в файле.

Список литературы:

1. Еременко В.Т., Чистяков М.В. Теоретические основы создания и применения профилей протоколов архитектур безопасности. Монография. / Под редакцией Еременко В.Т. – Екатиренбург: Уральский Государственный технический университет, 2000.
2. Макаров В.Ф. Теоретические основы передачи и защиты информации в системах теледоступа в вычислительных ресурсах./Под ред. А.П. Полежаева. - М.: Академия МВД РФ, 1992. - 228 с.
3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006. – 211 с.
4. Расследование неправомерного доступа к компьютерной информации. Учебное пособие. Изд-е 2, дополненное и переработанное / Под.ред. д.ю.н.,

проф. Н.Г. Шурухнова. – М.: Московский Университет МВД России, 2007.
5. Родионов А.Н. Компьютерные преступления и организация борьбы с ними // Системы безопасности. Межотраслевой тематический каталог. М., 2006 г.
6. Теоретические основы развития информационно-телекоммуникационной среды (организационно-правовые и социокультурные аспекты)/Мишин Д.С., Скрыль С.В., Третьяков О.В., Чуев А.В. – Орел: ОрЮИ МВД России, 2005.
7. Уфимцев Ю.С., Ерофеев Е.А. Информационная безопасность России. М.: «Экзамен», 2003 г.

Тема 5.2. Практическое занятие: «Порядок проведения работ по обеспечению информационной безопасности служебных ЛВС»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.
2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:
3.1 Работа с программами: Acronis Privacy Expert Suite, Paragon Encrypted; Password Organizer; Burmies Password.
3.2 Работа с программами защиты информации от несанкционированного доступа Mercury Interactive SiteScore; F-Secure Antivirus for Firewall.

Задания на самоподготовку:
1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:
Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 80 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 5 мин. (подведение итогов)
5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет "Вычислительной техники".
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.

9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Удаление следов работы в Интернете

Едва ли не большинство угроз конфиденциальности работы за компьютером проистекает из интернета. В зависимости от используемого браузера кэш, файлы cookie, журнал истории посещений сайтов, список недавно посещенных страниц, списки автозаполнения форм, пароли хранятся в разных местах.

Использование Мастера удаления вредоносных программ интернет-компонентов

Мастер удаления вредоносных программ интернет-компонентов позволяет вам полностью удалить следы своей работы с интернетом и электронной почтой и с его помощью вы можете:

- очистить кэш интернета - файлы, загружаемые на диск компьютера во время просмотра интернет-сайтов для того, чтобы уменьшить время повторного обращения к ним;
- удалить файлы cookie - небольшие текстовые файлы, которые создаются на компьютере пользователя, когда он посещает какой-либо сайт. Файлы могут содержать имя пользователя и другие данные, которые он вводил, регистрируясь на сайте.
- удалить загружаемые компоненты (элементы ActiveX), которые могут устанавливаться на компьютер пользователя при обращении к некоторым сайтам совершенно незаметно для него.
- очистить журнал истории посещений сайтов
- очистить список адресов сайтов, набранных в адресной строке браузера;
- удалить списки автозаполнения форм, которые сохраняет интернет-браузер в целях быстрого заполнения различных регистрационных анкет;
- удалить сохраняемые в браузере пароли для входа на интернет-сайты, требующие авторизации пользователя;
- гарантированно удалить сообщения электронной почты (в почтовых программах Microsoft Outlook и Outlook Express);
- очистить список контактов и адресную книгу в программе для работы с электронной почтой.

После запуска Мастер произведет поиск следов работы с интернетом на вашем компьютере. Результаты поиска вы сможете увидеть в правой части окна Мастера. По окончании поиска вы можете самостоятельно выбрать, какие из найденных элементов подлежат удалению.

После того как данные, подлежащие удалению, определены, вы можете начать процесс очистки интернет-компонентов.

Учебное упражнение № 1.

Проведите очистку компьютера от следов работы в Интернете и вредоносных программ Интернет-компонеентов при помощи программного пакета Acronis Privacy Expert Suite.

Настройка Мастера удаления вредоносных программ интернет-компонентов

Чтобы настроить параметры работы Мастера удаления вредоносных программ интернет-компонентов, в окне Интернет-компоненты в списке задач выберите пункт Настройка параметров очистки. Некоторые из этих параметров являются общими для нескольких компонентов.

Метод уничтожения данных

Данный параметр определяет, какой метод гарантированного удаления данных будет использован для очистки данного компонента.

Учебное упражнение № 2.

Проведите выбор метода уничтожения данных при помощи программного пакета Acronis Privacy Expert Suite.

Интернет-браузеры

Acronis Privacy Expert Suite автоматически обнаруживает все браузеры установленные на компьютере и поддерживаемые Privacy Expert Suite, и, по умолчанию, очищает все свидетельства работы в интернете, хранящиеся в настройках этих браузеров. Если у вас установлен браузер Internet Explorer, то очищаются структуры, принадлежащие пользователю, зарегистрировавшемуся в системе в текущем сеансе работы.

Браузеры Netscape Navigator и Mozilla поддерживают так называемые персональные профили. Acronis Privacy Expert Suite, без дополнительных настроек, очищает либо так называемый «профиль по умолчанию» (если он единственный), либо профиль пользователя, зарегистрировавшегося в системе в текущем сеансе работы.

Если вам необходимо очищать структуры, связанные только с одним браузером:

1. установите флажок только на его названии (например, Internet Explorer), а остальные флажки снимите;

2. если вы используете одну из версий браузера Netscape Navigator (или Mozilla), дополнительно выберите персональный профиль (щелкнув мышкой на ссылке Профили…).

В качестве значения параметра «Адрес» можно ввести через точку с запятой любые адреса интернета или любые их части, например:

*worldsoccer.com; *formula1.com;

Если вам необходимо:

1. удалить из кэша интернета (списка посещенных адресов) все файлы (списки, элементы), загруженные с определенного адреса (сайта) интернета, введите через точку с запятой адреса интернета или любые их части, например, в виде:

cnn;*formula1*

В результате будут удалены все файлы, загруженные с сайтов www.cnn.com, www.formula1.com.

2. удалить из кэша интернета файлы только определенного типа, загруженные с определенного адреса (сайта) интернета, введите адреса через точку с запятой, например, в виде:

cnn.jpg;*cnn*.gif;*formula1*.jpg;*formula1*.gif

Введя список адресов интернета, вы имеете возможность увидеть файлы (посещенные адреса), соответствующие критериям отбора. Для этого нажмите кнопку Показать адреса. На экране откроется окно с отобранными адресами. Именно эти адреса будут удалены при очистке настраиваемого компонента.

Файлы

Параметр «Файлы» служит для настройки имен удаляемых Acronis Privacy Expert Suite временных файлов (из корзины Windows, а также из системных и пользовательских папок) и представляет собой, по существу, строку поиска.

Строка поиска в соответствии с правилами, определенными в операционной системе Windows, может представлять полное имя или любую часть имени файла. Строка поиска может состоять из любых буквенно-цифровых символов, включая точку, а также символов * и ?.

Несколько различных строк поиска удаляемых файлов можно вводить через точку с запятой, например:

*.bak; *.tmp; *.~~~;

И так далее. При этом будут удаляться все файлы, имена которых соответствуют хотя бы одной из введенных строк.

Учебное упражнение № 3.

Проведите выбор удаляемых Интернет-браузеров, адресов и файлов при помощи программного пакета Acronis Privacy Expert Suite.

Автозаполнение форм

Данный пункт позволит вам задать параметры очистки тех значений полей автозаполнения форм, которые вы считаете нужными. Например, вы можете настроить его так, что при каждом запуске Мастера удаления вредоносных программ интернет-компонентов будут везде очищаться те поля, куда введены ваши персональные данные (имя, фамилия, электронная почта и т.п.). При определении значений данного параметра вы можете использовать маски ввода.

Сообщения электронной почты

В данном пункте вы можете указать, в каких почтовых программах следует производить удаление сообщений согласно выбранным критериям.

В настоящее время в программе Acronis Privacy Expert Suite реализована поддержка почтовых программ MS Outlook и Outlook Express.

Очистка отдельных интернет-компонентов

Если вы не хотите уничтожать следы работы с интернетом для всей категории Интернет-компоненты полностью (например, в целях экономии времени), вы можете сделать этого для любого из входящих в данную категорию компонентов по отдельности.

В этом случае все настройки параметров, которые были сделаны для всего Мастера удаления вредоносных программ интернет-компонентов, будут действительны и при очистке отдельных компонентов.

Учебное упражнение № 3.

Проведите очистку автозаполнения форм и электронной почты при помощи программного пакета Acronis Privacy Expert Suite.

Acronis Pop-up Blocker

Во время посещения некоторых интернет-сайтов вам наверняка приходилось сталкиваться с так называемыми «всплывающими окнами» (pop-up windows). Эти окна открываются на экране независимо от желания пользователя дополнительно к основному окну того сайта, на который вы попали. Как правило, «всплывающие окна» содержат навязчивую рекламную информацию. Появление «всплывающих окон» приводит к заметному замедлению скорости интернет-соединения, а также к увеличению интернет-трафика, который оплачивает пользователь.

Acronis Pop-up Blocker активизируется автоматически и предотвращает открытие всех окон браузера Microsoft Internet Explorer, кроме главного, в котором находится страница, интересующая пользователя. С помощью Acronis Pop-up Blocker вы также можете устанавливать фильтрацию содержимого веб-страниц (блокировать анимированные gif-файлы, flash-ролики, а также объекты ActiveX и т.д.) тем самым, избавляя себя от надоедливых баннеров на веб-страницах.

Настройка Acronis Pop-up Blocker

Открыть окно настройки параметров работы Acronis Pop-up Blocker в браузере Microsoft Internet Explorer можно следующими способами:

- Щелкнув на соответствующей пиктограммее панели инструментов браузера;
- Выбрав пункт меню Инструменты - Acronis Pop-up Blocker;
- Из контекстного меню браузера Acronis Pop-up Blocker - Options.

Параметры настройки Acronis Pop-up Blocker

В данном разделе вы можете включить или отключить Acronis Pop-up Blocker. Перемещая ползунок, вы также можете выбрать один из трех уровеней фильтрации содержимого веб-страниц:

- Низкий уровень фильтрации предусматривает только блокировку «всплывающих окон»;
- Средний уровень (рекомендуемый) помимо «всплывающих окон», также блокирует анимированные gif-файлы и элементы ActiveX
- Высокий уровень включает в себя все блокировки среднего уровня, а также добавляет блокировки flash-анимации, аплетов и «всплывающих окон» в слоях.

Щелкнув на кнопке Текущие настройки вы сможете настроить параметры блокировки для выбранного уровня фильтрации.

Список пользователя

Если вы хотите установить определенные правила фильтрации для конкретного сайта, то вам необходимо поместить его в Список пользователя. Для этого щелкните на кнопке Добавить, в появившемся окне введите адрес сайта и установите/снимите флажки напротив необходимых блокировок.

Иногда в процессе очередного посещения сайта вы можете обнаружить, что данный ресурс более не представляет для вас интереса и даже является не желательным для открытия. В этом случае вы можете переместить сайт в список Запрещенных сайтов, щелкнув на кнопке Поместить в Запрещенные сайты.

Запрещенные сайты

При необходимости с помощью Acronis Pop-up Blocker вы можете полностью блокировать доступ к тому или иному сайту, добавив его адрес в список Запрещенные сайты. В этом случае при попытке открыть страницу по данному адресу в строке состояния браузера будет появляться сообщение: «Данный сайт находится в 'Запрещенных сайтах'. Переход по данному адресу заблокирован!». Чтобы внести сайт в список запрещенных сайтов, щелкните на кнопке Добавить и в появившемся окне введите адрес ресурса.

Учебное упражнение № 5.

Проведите настройку компонента Pop-up Blocker - Options программного пакета Acronis Privacy Expert Suite.

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

Список литературы:

1. Еременко В.Т., Чистяков М.В. Теоретические основы создания и

применения профилей протоколов архитектур безопасности. Монография. / Под редакцией Еременко В.Т. – Екатиренбург: Уральский Государственный технический университет, 2000.

2. Макаров В.Ф. Теоретические основы передачи и защиты информации в системах теледоступа в вычислительных ресурсах./Под ред. А.П. Полежаева. - М.: Академия МВД РФ, 1992. - 228 с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006. – 211 с.

4. Расследование неправомерного доступа к компьютерной информации. Учебное пособие. Изд-е 2, дополненное и переработанное / Под.ред. д.ю.н., проф. Н.Г. Шурухнова. – М.: Московский Университет МВД России, 2007.

5. Родионов А.Н. Компьютерные преступления и организация борьбы с ними//Системы безопасности. Межотраслевой тематический каталог. М., 2006г.

6. Теоретические основы развития информационно-телекоммуникационной среды (организационно-правовые и социокультурные аспекты)/Мишин Д.С., Скрыль С.В., Третьяков О.В., Чуев А.В. – Орел: ОрЮИ МВД России, 2005.

7. Уфимцев Ю.С., Ерофеев Е.А. Информационная безопасность России. М.: «Экзамен», 2003 г.

Тема 5.3. Практическое занятие: «Каналы утечки, искажения и порчи информации, циркулирующей в сети»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 4 часа.

2. **Цель занятия**:

- изучить порядок работы с программными продуктами защиты информации в автоматизированных системах обработки данных;
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования компьютерной технологии для защиты информации.

3. **Учебные вопросы**:

3.1 Работа с программами: S-tools, Burmies Password; Password Organizer; Paragon Encrypted.

3.2 Работа с программами защиты информации от несанкционированного доступа F-Secure Antivirus for Firewall; Mercury Interactive SiteScore.

Задания на самоподготовку:
1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. Рекомендуемый план распределения времени:
Вступительная часть - 5 мин. (характеристика занятия)
Практическая часть - 80 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 5 мин. (подведение итогов)

5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет "Вычислительной техники".
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Стеганографические методы защиты данных

Рассматривая современные подходы к проблеме защиты данных, прослеживается возрастающее внимание к “системам маскировки”, т.е. методам, получившим название «стеганографических» или «стелсографических» методов защиты, которые при применении для защиты данных, помимо чисто технических и программных способов препятствования НСД, создают дополнительно - психологическую проблему отбора данных для анализа.

Таким образом цель стеганографии - скрыть сам факт существования секретного сообщения. Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, которые, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео- или аудио- сигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах). Причем в отличие от криптографии данные методы скрывают сам факт передачи информации.

Основными положениями современной компьютерной стеганографии являются следующие:

1. Методы скрытия должны обеспечивать аутентичность и целостность сообщений.

2. Предполагается, что противнику полностью известны возможные стеганографические методы,

3. Безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого сообщения при внесении в него секретного сообщения в виде неявного изменения физической или логической структуры данных.

Анализ информационных источников компьютерной сети Интернет позволяет сделать вывод что в настоящее время стеганографические системы активно используются для решения следующих основных задач:

- защиты конфиденциальной информации от несанкционированного доступа;
- преодоления систем мониторинга и управления сетевыми ресурсами;
- камуфлирования программного обеспечения;
- защиты авторского права на некоторые виды интеллектуальной собственности.

В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям

1 методы, основанные на использовании специальных свойств компьютерных форматов;

2 методы, основанные на избыточности аудио- и визуальной информации.

Сравнительные характеристики существующих стеганографических методов приведены в таблице. Как видно из таблицы, первое направление основано на использовании специальных свойств компьютерных форматов представления данных, а не на избыточности самих данных. Специальные свойства форматов выбираются с учетом защиты скрываемого сообщения от непосредственного прослушивания, просмотра или прочтения.

На основании анализа материалов таблицы можно сделать вывод, что в настоящее время, основным направлением компьютерной стеганографии является использование избыточности текстовых и мультимедийных файлов, форматов разметки дисковых пространств носителей информации, т.е. особенностей дисковой и файловой структуры данных. [8]

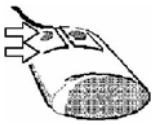
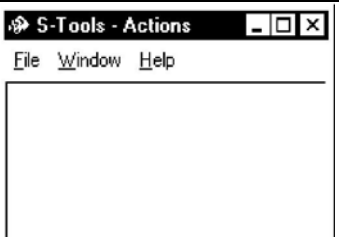
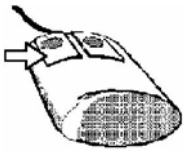
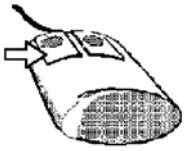
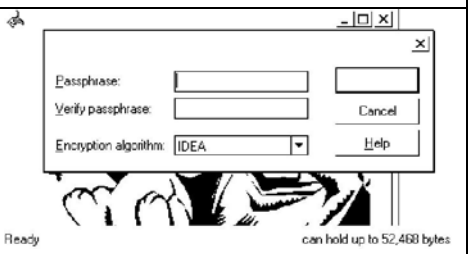
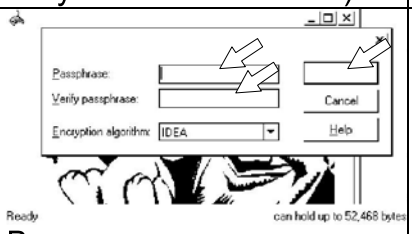
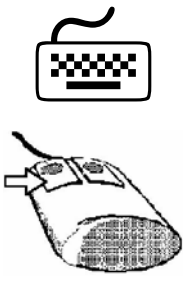
Таблица 1

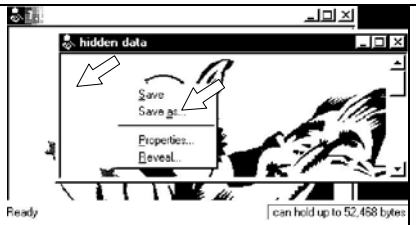
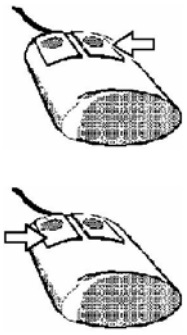
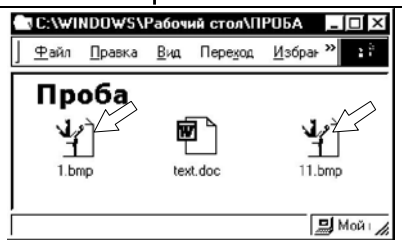
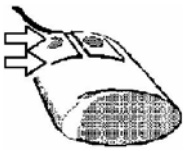
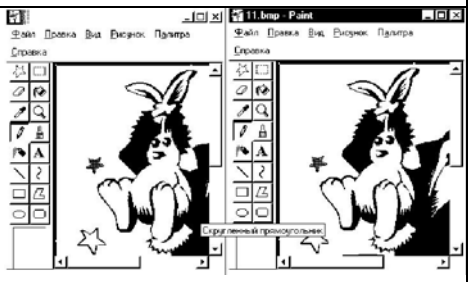
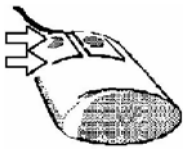
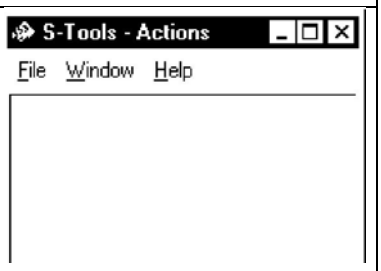
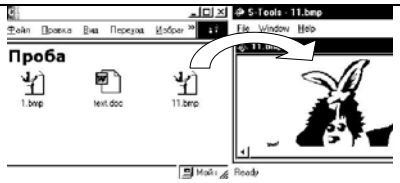
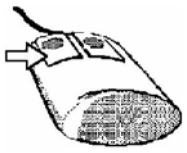
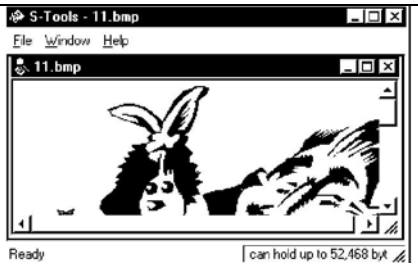
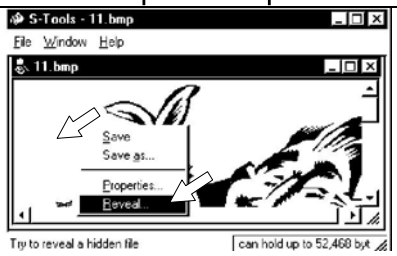
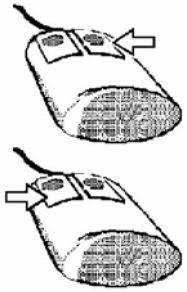
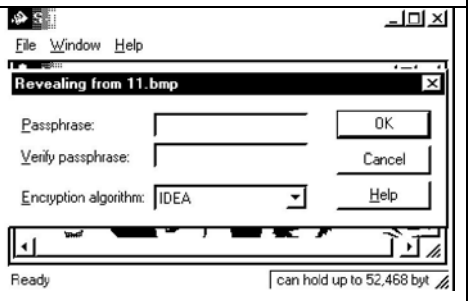
Стеганографические методы защиты [8]

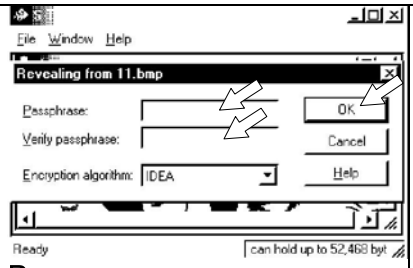
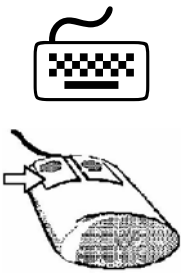
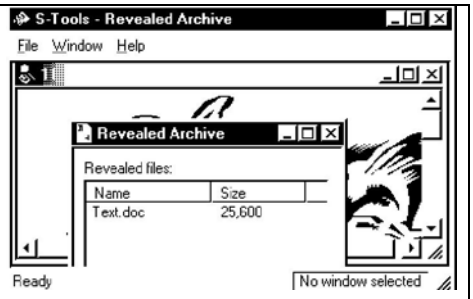
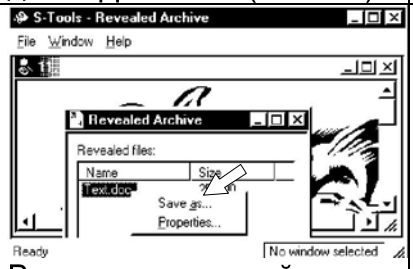
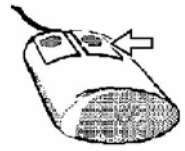
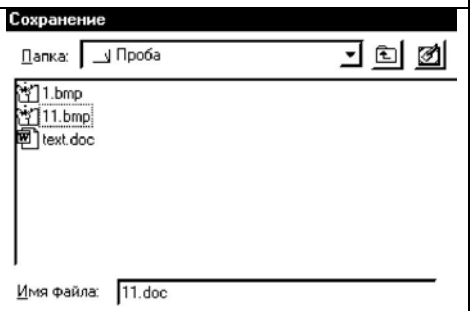
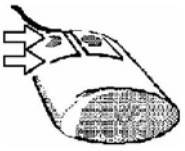
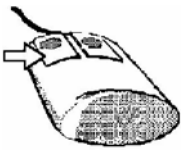
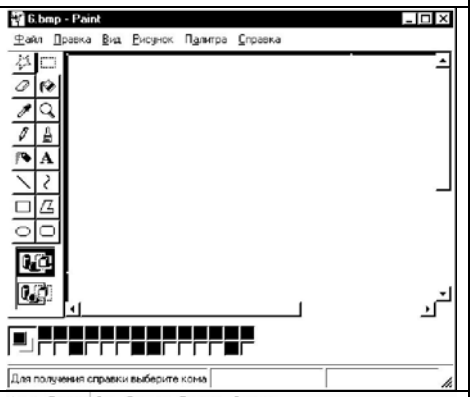
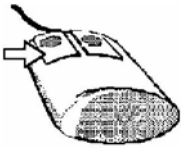
Стенографические методы	**Краткая характеристика методов**	**Недостатки**	**Преимущества**
1.Методы использования скрытых свойств форматов данных			
1.1 Методы использования полей расширения форматов данных	Поля расширения имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой	Низкая степень скрытности, передача небольших ограниченных объемов информации	Простота использования
1.2. Методы удаления идентифицирующего файл заголовка	Скрываемое сообщение шифруется и в результата удаляется идентифицирующий заголовок, оставляя только	1.Проблема скрытия решается только частично, 2.Необходимо	Простота реализации. Многие средства (White Noise Storm,

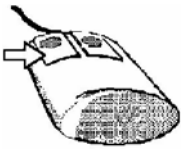
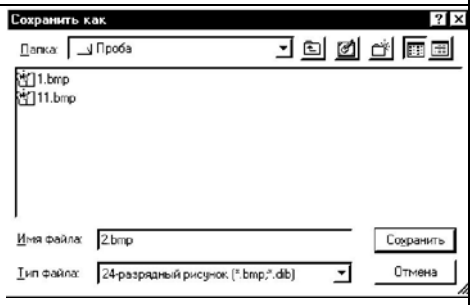
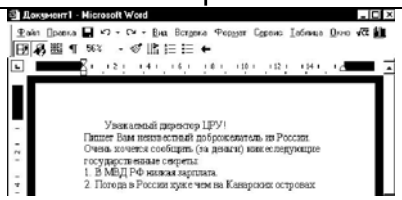
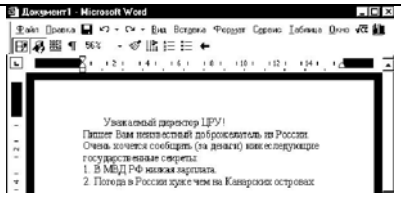
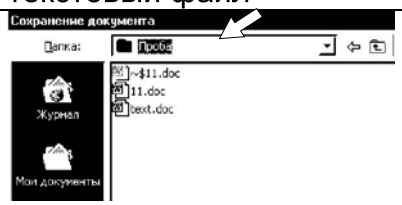
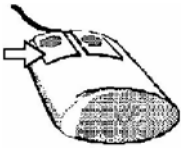
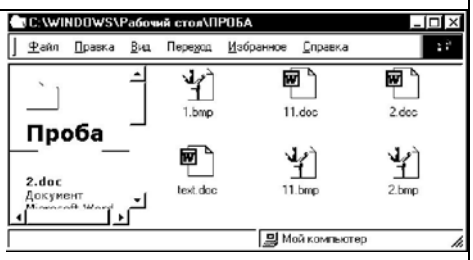
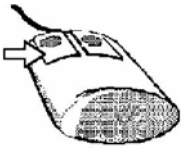
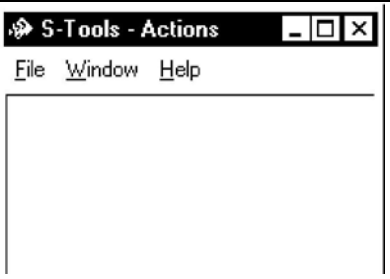
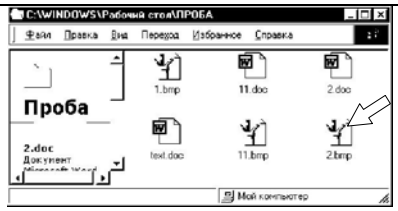
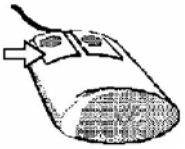
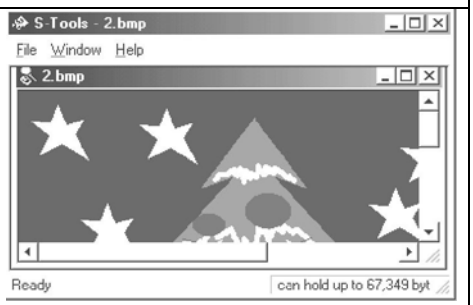
Стенографические методы	Краткая характеристика методов	Недостатки	Преимущества
	шифрованное данные. Получатель заранее знает о передаче сообщения и имеет недостающий заголовок	заранее передать часть информации получателю	S-Tools) обеспечивают реализацию этого метода с PGP шифроалгоритмом
2. Методы специального форматирования текстовых файлов			
2.1. Методы использования известного смещения слов, предложений, абзацев донного	Методы основаны на изменении положения; строк и расстановки слов в предложении, что обеспечивается вставками дополнительных пробелов между словами	1. Слабая производительность метода, передача небольших объемов информации 2.Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение реализации метода
2.2. Методы выбора определенных позиций букв (нулевой шифр)	Акростих - частный случай этою метода (например, начальные буквы каждой строки образуют сообщение		
2.3. Методы использования имитирующих функций (mimic-function)	Метод основан на генерации текстов и является обобщением акростиха. Для тайного сообщения генерируется осмысленный текст, скрывающий само сообщение	1. Слабая производительность метода, передача небольших объемов информации 2. Низкая степень скрытности	Результирующий текст не является подозрительным для систем мониторинга
3. Методы скрытия в изменениях разметки гибких дисков			
3.1. Метод изменеия порядка следования и номера загрузочного сектора	Нетрадиционная разметка дискет не дает возможность обратиться к дискете, без специального драйвера	Низкая степень защиты, риск потери данных при ощибочном восстановлении BOOT-сектора	Простота использования Имеется несколько драйверов изменения начальной загрузки (Например PU1700)
3.2. Метод записи в нулевую дорожку.	Информация записывается в обычно неиспользуемых местах ГМД (например, в нулевой дорожке)	1. Слабая производительность метода, передача небольших объемов информации 2. Низкая степень скрытности	Простота использование. Имеется опубликованное программное обеспечение реализации данного метода
4. Методы использования избыточности мультимедиа-файлов			
4.1. Методы использования избыточности шифровых фотографий, цифрового звука и цифрового видео	Младшие разряды цифровых отсчетов содержит очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и дает возможность скрытия конфиденциальной информации	1.Искажаются статистические характеристики цифровых потоков, требуется коррекция статистических характеристик	Возможность скрытой передачи большого объема информации. Возможность зашиты товарной марки, регистрационных номеров и т.п.

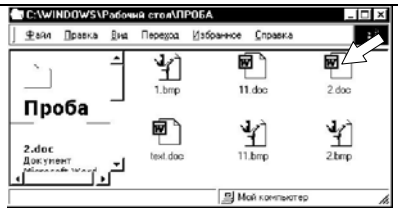
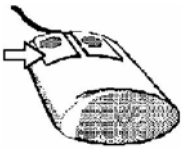
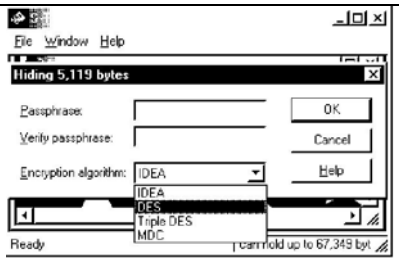
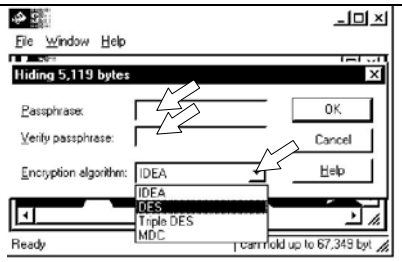
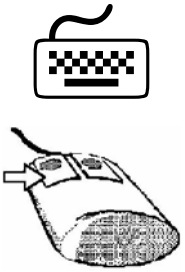
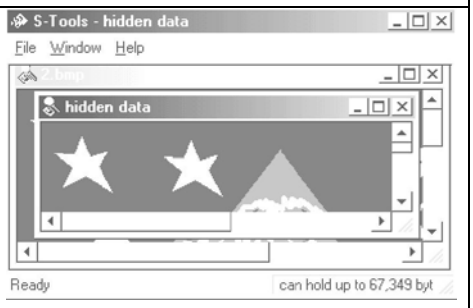
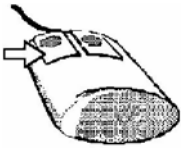
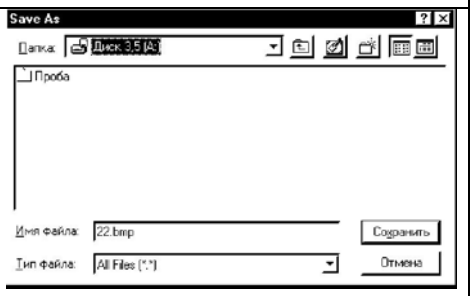
Программа стеганографического закрытия информации “S-tools” [8]

№ п/п	Шаг выполнения и вид экрана до выполнения операции	Действие	Вид экрана после выполнения операции
1.	**Закрытие текстовой информации в графическом файле**		
1.1	 Запустите программу ”S-Tool”		
1.2	 В папке «Проба» выделите рисунок 1.bmp и перетащите его в окно программы ”S-Tool” (не отпуская кнопки мыши)		
1.3	 В папке «Проба» выделите текстовый фаил text.doc и перетащите его в окно программы ”S-Tool” (не отпуская кнопки мыши)		
1.4	 Введите пароль для шифрования файла (123456) и подтвердите его (123456)		

1.5	 Вызовите контекстное меню результатов работы программы и сохраните результат (Save as) в папке ПРОБА как 11.bmp		
1.6	 Откройте файлы 11.bmp и 1.bmp и сравните их		
2.	**Извлечение текстового файла из файла контейнера**		
2.1	 Запустите программу ”S-Tool”		
2.2	 Выделите и перетащите из папки ПРОБА файл контейнер “11.bmp”		
2.3	 Вызовите меню управления, дешифруйте файл 11.bmp (Reveal)		

2.4	 Введите пароль дешифрования (123456)		
2.5	 Выделите искомый текстовый файл и вызвав контекстное меню (save as) сохраните в папке ПРОБА под именем 11.doc		
2.6	 Откройте файл 11.doc		
3.	**Подготовка данных для сокрытия в программе S-Tools**		
3.1	 Запустите графический редактор “Paint Brush” (Пуск / Программы / стандартные / Paint)		
3.2	 В графическом редакторе создайте		

	картинку - поздравление с ближайшим праздником		
3.3	 Сохраните рисунок в папке ПРОБА под именем 2.bmp		
3.4	 Создайте в редакторе “Word” небольшой текстовый файл		
3.5	 Сохраните текст в папке ПРОБА под именем 2.doc		
3.6	 Запустите программу ”S-Tool”		
3.7	 Переместите созданный графический файл (2.bmp) в окно программы “S-Tools”		

3.8	 Переместите созданный текстовый файл (2.bmp) в окно программы “S-Tools”		
3.9	 Выберите стандарт шифрования как “DES” и введите пароль 2000		
3.10	 Вызовите меню управления и сохраните результат как 22.bmp на дискету		
4.	Поменяйтесь с товарищами дискетами и попробуйте расшифровать сообщение. (см. п/п 2.2 – 2.6)		

III. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

Список литературы:

1. Еременко В.Т., Чистяков М.В. Теоретические основы создания и применения профилей протоколов архитектур безопасности. Монография. / Под редакцией Еременко В.Т. – Екатиренбург: Уральский Государственный технический университет, 2000.

2. Макаров В.Ф. Теоретические основы передачи и защиты информации в системах теледоступа в вычислительных ресурсах./Под ред. А.П. Полежаева. -

М.: Академия МВД РФ, 1992. - 228 с.

3. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006. – 211 с.

4. Расследование неправомерного доступа к компьютерной информации. Учебное пособие. Изд-е 2, дополненное и переработанное / Под.ред. д.ю.н., проф. Н.Г. Шурухнова. – М.: Московский Университет МВД России, 2007.

5. Родионов А.Н. Компьютерные преступления и организация борьбы с ними//Системы безопасности. Межотраслевой тематический каталог. М., 2006г.

6. Теоретические основы развития информационно-телекоммуникационной среды (организационно-правовые и социокультурные аспекты)/Мишин Д.С., Скрыль С.В., Третьяков О.В., Чуев А.В. – Орел: ОрЮИ МВД России, 2005.

7. Уфимцев Ю.С., Ерофеев Е.А. Информационная безопасность России. М.: «Экзамен», 2003 г.

8. Программные методы защиты информации в компьютерных сетях Часть 1/ Учебно-методические материалы Для слушателей Академии МВД России, 2006.

Тема 5.4. Практическое занятие: «Методы и средства дистанционного съема компьютерной информации»

I. МЕТОДИЧЕСКАЯ ХАРАКТЕРИСТИКА ЗАНЯТИЯ

1. **Продолжительность занятия** 2 часа.
2. **Цель занятия**:

- ознакомить слушателей с основными понятиями и принципами организации защиты информации в вычислительных сетях;
- способствовать развитию научно-технического кругозора, формировать у обучаемых практические навыки использования современных средств обеспечения информационной безопасности.

3. **Учебные вопросы**:

3.1 Изучение технических характеристик и параметров устройств обеспечивающих съема компьютерной информации через ПЭМИН

Задания на самоподготовку:

1. Изучить рекомендованные по теме учебные материалы.
2. Подготовить алгоритм выполнения заданий, выносимых на практическое занятие.

4. **Рекомендуемый план распределения времени**:

Вступительная часть - 5 мин. (характеристика занятия)

Практическая часть - 80 мин. (инструктаж, выполнение практических заданий)
Заключительная часть - 5 мин. (подведение итогов)
5. **Метод проведения**: индивидуальная работа, учебно-тренировочные упражнения.
6. **Место проведения**: кабинет "Вычислительной техники".
7. **Исходные материалы**: УММ, рекомендуемая литература, конспект лекции.
8. **Итоговые документы**: записи в тетрадях основного содержания учебного материала, оценка преподавателем ответов на контрольные вопросы.
9. **Материальное обеспечение**: ПЭВМ.

II.ПРАКТИЧЕСКАЯ РАБОТА.

Устройства защиты телефонных линий и телефонных переговоров от прослушивания.

Предотвращение несанкционированного прослушивания телефонных переговоров остаётся одной из наиболее актуальных задач в области защиты информации от её утечки по техническим каналам. Это объясняется широким использованием средств телефонной связи для ведения переговоров, сравнительно высокой доступностью телефонного тракта для средств разведки потенциального противника, незначительной стоимостью оборудования, необходимого для обеспечения прослушивания в случае отсутствия в телефонном тракте каких-либо средств защиты информации.

Известны различные методы организации подобного канала утечки информации: контактное подключение к телефонной линии, индуктивный съем сигналов, передающихся по телефонной линии, высокочастотное навязывание и др. Наиболее уязвимым звеном телефонного тракта были и остаются абонентские линии интересующих злоумышленника физических лиц и организаций.

"Цикада-М" устройство защиты телефонных переговоров

Сертификат Гостехкомиссии России (ФСТЭК России)

Предназначено для защиты телефонных переговоров на участке линии от абонента до ГАТС. Принцип действия прибора основан на маскировке спектра речи широкополосной шумовой помехой и компенсации постоянного напряжения линии. Прибор формирует синфазную и дифференциальную шумовую помеху как при «положенной», так и при «поднятой» трубке

защищаемого телефонного аппарата. Прибор предназначен для эксплуатации как на городских, так и на местных телефонных линиях.

Прибор обеспечивает эффективное противодействие следующим средствам несанкционированного съема информации:

- телефонным радиопередатчикам с питанием от линии и с внешним питанием, включенным в линию последовательно, параллельно или через индуктивные датчики;
- аппаратуре магнитной записи, подключаемой к линии через контактные адаптеры или индуктивные датчики;
- микрофонам и радиомикрофонам с питанием от линии и аналогичной аппаратуре (в том числе, параллельным ТА), использующей линию в качестве канала передачи информации или в качестве источника электропитания;
- аппаратуре «ВЧ-навязывания».

Технические характеристики:

- подавление устройств последовательного съема;
- подавление устройств параллельного съема;
- блокирование устройств съема с питанием от ТЛ;
- сигнализация использования параллельных ТА;
- габариты: 155 х 60 х 200 мм.

"SI-2002" устройство защиты 4-х телефонных линий

Устройство защиты «SI-2002» позволяет одновременно защищать телефонные переговоры по 4-м линиям на участке: от абонента до АТС. Принцип действия прибора основан на маскировке спектра речи широкополосной шумовой помехой.

телефонным радиопередатчикам, включенным в линию последовательно и параллельно (в том числе с индукционными датчиками и внешним питанием);

аппаратуре магнитной записи, подключаемой к линии с помощью контактных или индукционных датчиков;

Устройство защиты телефонных переговоров "Референт"

Предназначен для защиты принимаемых телефонных сообщений на участке: от абонента до абонента. При приеме сообщений от удаленного абонента съем информации на протяжении всего телефонного канала становится невозможным.

Оригинальный метод защиты основан на том, что сигнал помехи распростанятся на всем протяжении канла связи (от абонента до абонента).

Особенности:

- невозможность компенсации помехи и выделения речевого сигнала современными средствами шумоочистки;
- речь, замаскированная одним «Щитом» не может быть размаскирована другим, в т.ч. одновременно подключенным к линии связи;
- возможность приема конфиденциальных сообщений абонента, использующего таксофон или мобильную связь (включая транкинговую и GSM);
- необходимость установки устройства «Щит» только у принимающего абонента.

Устройства защиты от утечки информации по электросети:

Электрическая силовая сеть, цепи заземления и цепи электропитания являются средой распространения информативных сигналов в соответствующих технических каналах утечки защищаемой информации.

Электрическая сеть может содержать информативные высокочастотные сигналы от подключенных устройств обработки информации (ПЭВМ) или использоваться злоумышленниками для передачи сигналов от специально внедренных средств съема информации.

Информационные сигналы в цепи заземления образуются за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны, в том числе нулевого провода сети электропитания.

Появление информационных сигналов в цепях электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором выпрямителя, а также при неравномерной нагрузке на выпрямитель, приводящей к изменению потребляемого тока по закону изменения информационного сигнала.

Для предотвращения утечки информации по этим каналам необходимо применять соответствующие технические средства защиты.

Фильтр сетевой помехоподавляющий ФСП-1Ф-7А

Сертификат Гостехкомиссии России
(ФСТЭК России)

Предназначен для предотвращения утечки информации по цепям электропитания, а также для защиты средств оргтехники от внешних помех.

Технические характеристики:

- номинальный ток: 7А;
- количество защищаемых фаз: 1 фаза (2 провода);
- вносимое затухание: 60 дБ;
- диапазон подавляемых частот: 0,1 - 1000 МГц;
- масса: 1,4 кг.

Фильтр сетевой помехоподавляющий ФСПК-10

Сертификат Гостехкомиссии России
(ФСТЭК России)

Предназначен для предотвращения утечки информации по цепям электропитания, а также для защиты средств оргтехники от внешних помех.

Технические характеристики:

- номинальный ток: 10А;
- количество защищаемых фаз: 1 фаза (2 провода);
- вносимое затухание: 60 дБ;
- диапазон подавляемых частот: 0,1 - 1000 МГц;
- масса: 5,5 кг.

Фильтр сетевой помехоподавляющий ФСПК-200

Сертификат Гостехкомиссии России
(ФСТЭК России)

Предназначен для предотвращения утечки информации по цепям электропитания, а также для защиты средств оргтехники от внешних помех.

Конструктивно состоит из двух блоков:
Технические характеристики:

- номинальный ток: 200А;
- количество защищаемых фаз: 3 фазы (4 провода);
- вносимое затухание: 60 дБ;
- диапазон подавляемых частот: 0,1 - 1000 МГц;
- масса: 36 кг.

Фильтр сетевой ЛФС-10-3Ф

Предназначен для предотвращения утечки информации по цепям электропитания, а также для защиты средств оргтехники от внешних помех.

Технические характеристики:

- номинальный ток: 10А;
- количество защищаемых фаз: 3 фаза (4 провода);
- вносимое затухание: 60 дБ;
- диапазон подавляемых частот: 0,1 - 1000 МГц;
- масса: 2,5 кг.

"Соната-РС1" генератор шума по сети 220В

Сертификат Гостехкомиссии России (ФСТЭК России)

Предназначен для защиты от утечки информации за пределы выдлененного помещения по сети 220 В и линиям заземления. Принцип действия основан на постановке широкополосной шумоподобной помехи в защищаемых линиях.

Позволяет нейтрализовать:

- аппаратуру, использующую сеть электропитания в качестве канала передачи информации;
- аппаратуру, позволяющую получать информацию, содержащуюся в колебаниях тока (напряжения) электропитания средств вычислительной техники, оргтехники и т.п.;
- аппаратуру, позволяющую получать информацию, содержащуюся в токах, протекающих в экранирующей оплетке кабелей локальных вычислительных сетей, в заземляющих проводниках и т.п.

Устройства защиты от утечки информации по каналам ПЭМИН

Сертификат Гостехкомиссии России (ФСТЭК России)

Генератор шума "Гном-3" предназначен для защиты информации от утечки, обусловленной побочными электромагнитными излучениями и наводками ПЭВМ и других средств обработки информации.

Генератор имеет внешнюю гибкую рамочную антенну (в комплект поставки не входит), которая устанавливается стационарно в защищаемом помещении. Антенна представляет из себя три рамки размером 3 х 5 метров, расположенные во взаимено перпендикулярных плоскостях.

В основном, данный генератор исмользуется для защиты залов вычислительной техники общей площадью до 50 м2.

Технические характеристики:

- диапазон рабочих частот: 0,1 - 1000 МГц;
- спектральная плотность шума: 45-75 дБ;
- индикация работы: световая.

“Гном-3М”

Генератор шума "Гном-3М" предназначен для защиты информации от утечки, обусловленной побочными электромагнитными излучениями и наводками ПЭВМ и других средств обработки информации. В отличие от генератора "Гном-3" позволяет зашумлять сеть электропитания.

Генератор имеет внешнюю гибкую рамочную антенну (в комплект поставки не входит), которая устанавливается стационарно в защищаемом помещении. Антенна представляет из себя три рамки размером 3 х 5 метров, расположенные во взаимено перпендикулярных плоскостях.

Генератор шума "Гном-3" предназначен для защиты информации от утечки, обусловленной побочными электромагнитными излучениями и наводками ПЭВМ и других средств обработки информации.

Генератор имеет внешнюю гибкую рамочную антенну (в комплект поставки не входит), которая устанавливается стационарно в защищаемом помещении. Антенна представляет из себя три рамки размером 3 х 5 метров, расположенные во взаимено перпендикулярных плоскостях.

Технические характеристики:

- диапазон рабочих частот: 0,1 - 1000 МГц;
- спектральная плотность шума: 45-75 дБ;
- индикация работы: световая.

“ГШ-1000М”

Сертификат Гостехкомиссии России (ФСТЭК России)

Генератор шума ГШ-1000М предназначен для защиты информации от утечки, обусловленной побочными электромагнитными излучениями и наводками ПЭВМ и других средств обработки информации.

Генератор имеет внешнюю жесткую рамочную антенну диаметром 60 см.

Может применяться для защиты не более одного автоматизированного рабочего места.

Технические характеристики:

- диапазон рабочих частот: 0,1 - 1000 МГц;
- спектральная плотность шума: 45-75 дБ;
- индикация работы: световая, звуковая.

“ГШ-К-1000М”

Генератор шума ГШ-К-1000М предназначен для защиты информации от утечки, обусловленной побочными электромагнитными излучениями и наводками ПЭВМ и других средств обработки информации.

Генератор является бескорпусным и устанавливается в PCI слот системного блока ПЭВМ. Генератор имеет внешнюю гибкую рамочную антенну диаметром 50 см.

Может применяться для защиты не более одного автоматизированного рабочего места.

Технические характеристики:

- диапазон рабочих частот: 0,1 - 1000 МГц;
- спектральная плотность шума: 45-75 дБ;
- индикация работы: световая, звуковая.

“ГШ-2500М”

Генератор шума "ГШ-2500М" предназначен для защиты информации от утечки, обусловленной побочными электромагнитными излучениями и наводками ПЭВМ и других средств обработки информации.

Генератор имеет внешнюю жесткую рамочную антенну диаметром 60 см.

Может применяться для защиты не более одного автоматизированного рабочего места.

Технические характеристики:

- диапазон рабочих частот: 0,1 - 2500 МГц;
- спектральная плотность шума: 45-75 дБ;
- индикация работы: световая, звуковая.

“ГШ-1000У”

Предназначен для маскировки побочных информативных электромагнитных излучений и наводок персональных компьютеров, компьютерных сетей и комплексов на объектах вычислительной техники 1, 2 и 3 категорий в диапазоне частот 0,1-1800 МГц путем формирования и излучения в окружающее пространство маскирующего электромагнитного поля шума (ЭМПШ). Дополнительно имеет 4 независимых коаксиальных выхода некоррелированного напряжения шума, к которым можно подключать:

- устройства ввода маскирующего напряжения шума (например, ответвитель "Дух") в сети электропитания, заземления, инженерные коммуникации и т.д.;
- дополнительные выносные антенны.

В состав генератора шума входит пять независимых генераторов шума, один из которых нагружен на антенну в виде кольца, а четыре имеют коаксиальные выходы СР-50-73 ФВ для подключения внешних устройств. Независимые генераторы шума могут включаться в любом сочетании по условиям конкретного объекта информатизации. На каждом из четырех коаксиальных 50 Ом выходах генератора шума сформирован широкополосный шумовой сигнал высокой спектральной плотности напряжения. К этим выходам могут быть подключены внешние устройства: дополнительные антенны для улучшения пространственных и поляризационных характеристик излучаемого ЭМПШ, внешние токосъемники, ответвители для ввода напряжения шума в сети питания, заземления, ВТСС, инженерные коммуникации для маскировки информативных наводок создаваемых средствами вычислительной техники. Спектральная плотность напряжения сигнала шума достаточна для обеспечения защиты обрабатываемой средствами вычислительной техники информации от несанкционированного доступа при использовании различных внешних устройств. При использовании в качестве внешних устройств ответвителей "Дух" для ввода напряжения шума в сети питания, заземления, ВТСС, инженерные коммуникации, которые могут входить в комплект поставки генератора по желанию Заказчика, их можно размещать в удаленных точках защищаемого помещения, соединяя с генератором радиочастотным кабелем. Возможная длина кабеля зависит от вносимых им потерь и, как правило, не для дешевого общеупотребительного кабеля, не менее 10 м. Это же относится и к использованию внешних антенн.

Технические характеристики:

- диапазон частот: 0,1-1800 МГц;
- нормализованный коэффициент качества напряжения шума К, формируемого генератором не менее 0,8;
- электропитание генератора осуществляется от сети переменного тока напряжением 220 ±22 В и частотой 50 Гц;
- габаритные размеры:

- блок генератора с излучающей антенной - 650х650х50 мм;
- блок питания - 155х85х55 мм.

- масса:
  - блок генератора с излучающей антенной не более - 0,9 кг;
  - блок питания не более - 0,9 кг.

IV. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

При подведении итогов преподаватель анализирует степень реализации поставленных целей занятия, выставляет слушателям оценки за выполнение практических заданий и ответы на контрольные вопросы, выдаёт задания на самостоятельную подготовку.

Список литературы:

1. Макаров В.Ф. Теоретические основы передачи и защиты информации в системах теледоступа в вычислительных ресурсах./Под ред. А.П. Полежаева. - М.: Академия МВД РФ, 1992. - 228 с.

2. Методологические аспекты формирования информационной инфраструктуры общества и борьбы с преступлениями в сфере информационных технологий: Монография / Д.С. Мишин, С.Л. Паньков, О.В. Третьяков – Орел: Орловский юридический институт МВД РФ, 2006. – 211 с.

3. Теоретические основы развития информационно-телекоммуникационной среды (организационно-правовые и социокультурные аспекты)/Мишин Д.С., Скрыль С.В., Третьяков О.В., Чуев А.В. – Орел: ОрЮИ МВД России, 2005.

4. Уфимцев Ю.С., Ерофеев Е.А. Информационная безопасность России. М.: «Экзамен», 2003 г.

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Основы информационной безопасности в органах внутренних дел

Составители:
Мишин Дмитрий Станиславович, к.ю.н.
Подчерняев Николай Григорьевич, к.т.н., доцент

Свидетельство о государственной аккредитации
Рег. № 0440 от 22.12.06 г.
Подписано в печать _____ г. Формат 60x90$^{1}/_{16}$.
Учет.-изд.л. - _____. Тираж _____. Заказ № _____.

Орловский юридический институт МВД РФ.
302027, Орел, Игнатова, 2.