

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических работ
по дисциплине «Информационные технологии и программирование» для студентов направления
подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной
деятельности)»

Введение

1. Цель и задачи освоения дисциплины:

Целью освоения дисциплины «Основы информационной безопасности» является формирование у будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность» понимания является изучение базовых понятий, таких как методы нарушения конфиденциальности, целостности и доступности информации, причин, видов, каналов утечки и искажения информации, изучение методов и средств обеспечения информационной безопасности.

Задачи дисциплины:

1. заложить терминологический фундамент;
2. научить правильно проводить анализ угроз информационной безопасности;
3. выполнить основные этапы решения задач информационной безопасности;
4. приобрести навыки анализа угроз информационной безопасности;
5. рассмотреть основные общеметодологические принципы теории информационной безопасности;
6. изучить методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации.

2. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы высшего образования

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИД-1ОПК-1 Понимает основные методологические принципы теории информационной безопасности; проблемы государственной и региональной информационной безопасности. ИД-2ОПК-1 Применяет основные методологические принципы теории информационной безопасности. ИД-3ОПК-1 Определяет роль информации, информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства.	Представление презентационного материала по проблемам государственной и региональной информационной безопасности. Раскрывать принципы теории информационной безопасности. Представляет отчет по индивидуальным темам в области информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства.

Тема 1. Понятие национальной безопасности

Практическое занятие №1

Тема: Методы блокирования доступа к персональному компьютеру

ЦЕЛИ ЗАНЯТИЯ:

Отработать практические навыки:

- по ограничению доступа к ПК посредством использования заставки с паролем Windows;
- по оперативному контролю доступа к компьютеру;
- защите компьютера при длительных отлучках.

УЧЕБНЫЕ ВОПРОСЫ:

1. Заставка с паролем для Windows NT/2000/XP. Утилита блокирования доступа Black Magic.
2. Оперативный контроль доступа к компьютеру.
3. Защита компьютера при длительных отлучках.

МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ:

Методическая разработка для проведения занятия

Вводная часть (10-15 мин.)

Проверка наличия готовности учебной группы к занятию (наличие конспектов; учебных пособий; ручек; линеек и т.д.).

Контрольный опрос

1. **Физическая блокировка системы**
2. **Установки пароля BIOS**
3. **Средства оперативного контроля доступа к компьютеру**
4. **Блокирование доступа, использованием специальных утилит**
5. **Заставка с паролем Windows**

Если группа недостаточно подготовлена, то предоставить время на подготовку группы к занятию потом мы начать занятие. При необходимости закончить занятие в часы самоподготовки или выходной день, согласовав это с учебной частью.

II. Основная часть - 150 мин.

1. Заставка с паролем Windows NT/2000/XP. Утилита блокирования доступа Black Magic.

Действия:

1. Щелкните на пункте Настройка (Settings) меню Пуск (Start) и далее выберите пункт Панель управления (Control Panel).
2. Выполните двойной щелчок мышью на апплете Экран (Display). Альтернативно вы можете щелкнуть правой кнопкой мыши на свободной поверхности рабочего стола и выбрать пункт Свойства (Properties). При этом отобразится диалог Свойства: Экран (Display Properties).
3. Щелкните на вкладке **Заставка** (Screen Saver) и выберите из списка **Заставка** (Screen Saver) нужную вам заставку.
4. В поле **Интервал** (Wait) установите время, спустя которое будет запущена заставка.
5. Щелкните на флажке **Защита паролем** (Password Protected).
6. Для заставки будет активизирована защита с паролем, совпадающим с паролем текущего пользователя (в компьютерах с Windows 95/98 далее следует щелкнуть на кнопке **Изменить** (Change) и в отобразившемся диалоге ввести пароль).

Система защиты паролем заставки в системах **Windows NT/2000/XP** прекрасно работает, но имеет следующие недостатки: чтобы ее запустить, следует подождать определенное время или переустановить интервал ожидания запуска заставки.

Пока заставка экрана не будет активирована специальным таймером, ее защита паролем работать не будет. Также следует помнить основной недостаток заставок с паролями: чтобы обойти их защиту, нужно только перезагрузить компьютер, поэтому без установленной входной регистрации пользователей заставки паролями малоэффективны.

Способ активизации заставки без ожидания интервала времени. Если на компьютере установлен пакет *MS Office 97/2000/XP*, то вызов утилиты *osa.exe* за-грузки *MS Office* с ключом *-s* приводит к немедленной активизации заставки. Поместив ярлык вызова утилиты *osa.exe* (которая находится в каталоге программ *MS Office*) и добавив к строке вызова ключ *-s*, мы получим удобное подручное средство защиты системы.

Утилита блокирования доступа **Black Magic**.

Black Magic предоставляет примерно такие же возможности, что и другие утилиты такого рода, но эта утилита не является экранной заставкой в чистом виде, т. е. она не выводит какое-либо изображение на экран. Зато **Black Magic** умеет подавать звуковые сигналы при вводе некорректного пароля (наверное, в расчете, что это кого-то еще способно остановить...)- Для настройки работы **Black Magic** отображается диалог, представленный на Рис. 1.

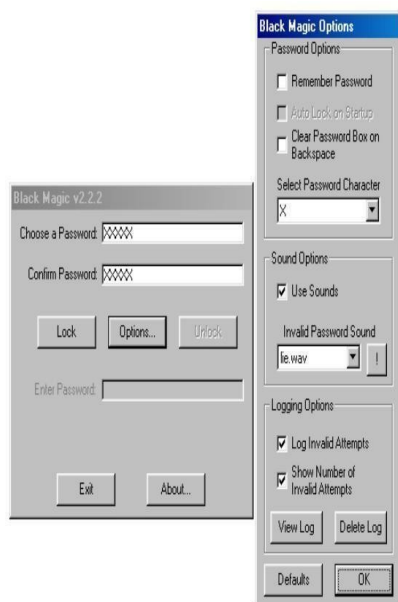


Рис. 1

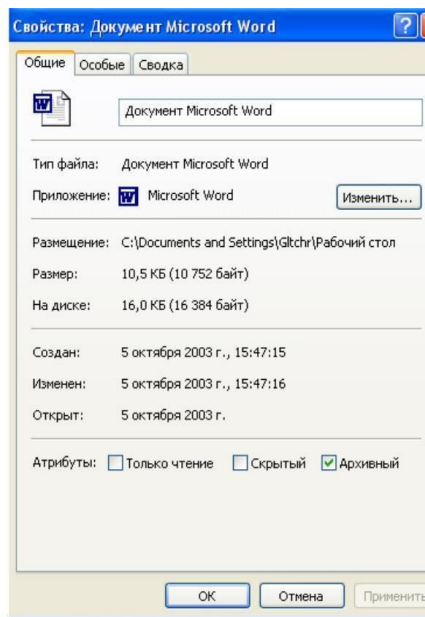


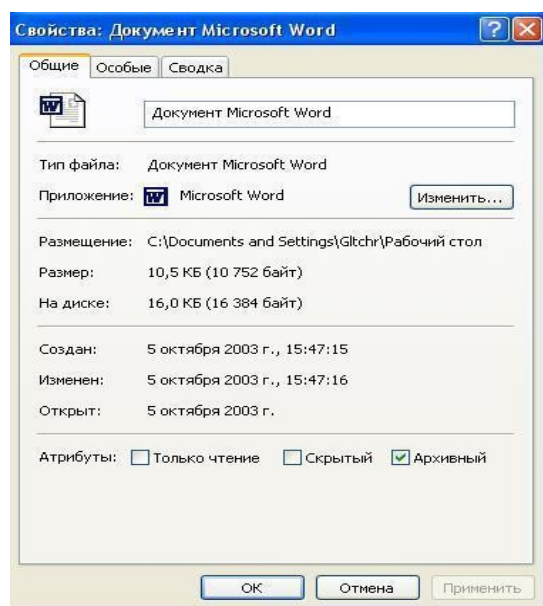
Рис. 2.

2. Оперативный контроль доступа к компьютеру.

Вернувшись на рабочее место, можно поинтересоваться, открывал ли в ваше отсутствие кто-нибудь конкретный файл (скажем, деловое письмо, важный документ и т.д.). Для этого можно воспользоваться средствами проводника

Windows.

1. Создайте любой файл и сохраните.
2. Щелкните правой кнопкой мыши на имени файла в окне проводника, и в отобразившемся контекстном меню выберите пункт Свойства (Properties). В отобразившемся диалоге (см. Рис. 2.) в строке Изменен будет отображено время последней модификации файла.



3. Внесите изменения в файл и снова сохраните.

4. Щелкните правой кнопкой мыши на имени файла в окне проводника, и в отобразившемся контекстном меню выберите пункт Свойства (Properties). В отобразившемся диалоге (см. Рис. 2.) в строке Изменен будет отображено время последней модификации файла.

Это может, по крайней мере, указать, что кто-то в ваше отсутствие внес в файл изменения, после чего можно принять соответствующие меры.

При открытии файла операционная система **Windows** немедленно обновляет информацию об его свойствах. Поэтому свойства подозрительного файла следует проверять *перед* открытием, иначе информация о дате/времени последнего открытия файла заменится той, что относится к открытию файлами.

Проконтролировать несанкционированный доступ к файлам можно также просмотром подменю **Документы** в меню **Пуск** (Start). Если в этом списке вы увидите подозрительное имя файла (например, документа, с которым вы давно или вообще не работали), проверьте свойства этого файла или откройте документ и проверьте его содержание. Наличие незнакомого документа служит указанием на несанкционированный доступ к компьютеру, а время, когда это случилось, можно определить из окна его свойств.

3. Защита компьютера при длительных отлучках.

При длительной отлучке от компьютера, скажем, на период отпуска, выходных дней, просто на ночь, до следующего рабочего дня, в целях защиты данных, прежде чем выключить компьютер, надлежит выполнить такие операции: Создать резервные копии важных файлов данных, воспользовавшись программой архивации.

Скопировать уязвимые данные на гибкий диск или иной съемный носитель и спрятать его в безопасном месте.

Одной из наиболее часто применяемых программ архивации является WinRAR, предназначенная для работы в системах Windows. Программа WinRAR позволяет сжимать архивируемую информацию в многотомные архивные файлы и ограничивать доступ к ним паролем.

Действия.

1. Выберите файл для архивации. Сделайте на нём правый щелчок мышью (Рис. 3.).

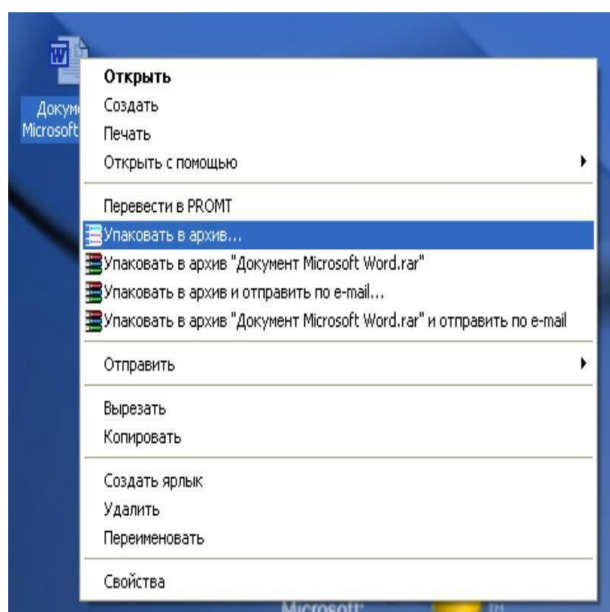


Рис. 3.

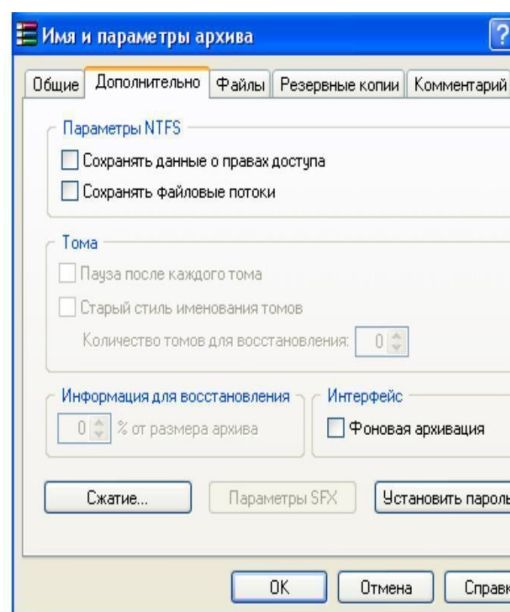


Рис. 4.

2. Выберите упаковать в архив. После того как нажмете ВВОД высветится окно (Рис. 4.).

Функции утилиты Clean Disk Security

Очистка стандартного свободного пространства
Удаление резервных файлов
Очистка списка недавно использованных файлов
Очистка корзины (пустой)
Очистка временной папки (Temp) Windows
Очистка памяти браузера Интернета
Очистка записей Хронологии
Удаление Интернет Cookies
Очистка файла подкачки Windows

3. Выберите установить пароль.
4. Установите пароль и нажмите ОК (Рис. 5).

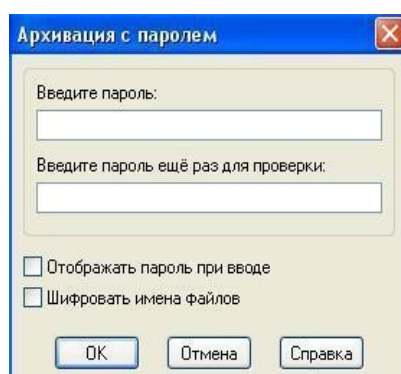


Рис. 5.

Утилита Clean Disk Security 5.01

(<http://www.theabsolute.net/sware/index.html>SCIndisk), удовлетворяет основным требованиям, предъявляемым к средствам очистки носителей секретной информации (и даже несколько их усиливает).

Для очистки исходных файлов и папок можно воспользоваться специальной утилитой очистки, например, Clean Disk Security.

Самые интересные возможности утилиты Clean Disk Security заключаются в методах, применяемых для очистки информации. Как видно на Рис. 6 утилита предоставляет четыре метода очистки:

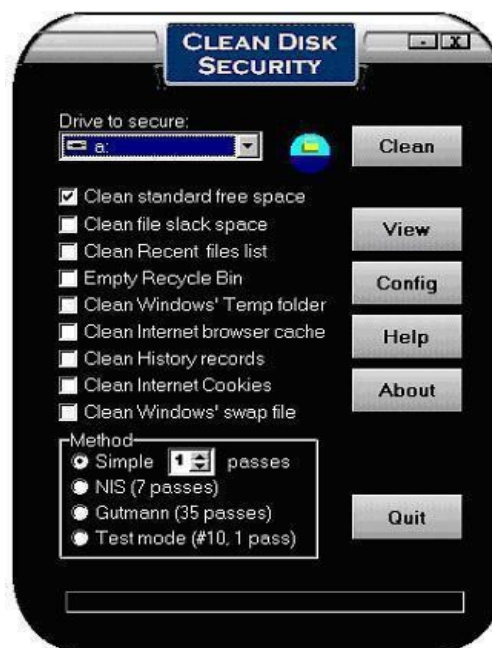


Рис. 6.

Simple (Простой), допускающий выполнение до 6 проходов, во время которых на диск записываются случайно генерируемые символы. Этот метод пригоден для большинства случаев; обычно бывает достаточно 1 прохода.

NIS, поддерживающий до 7 проходов с записью случайно генерируемых символов (т. е. наборов битов определенной длины) и их преобразований. Этот метод описан в оперативном руководстве программы национальной индустриальной безопасности Министерства обороны США.

Gutmann, поддерживающий до 35 проходов с записью случайно генерируемых шаблонов (т. е. последовательностей случайно генерируемых битов). Этот метод предложен Питером Гутманом из департамента компьютерных наук университета г. Окленд. Полная очистка этим методом занимает много времени, но зато обеспечивает защиту от сканирования диска высокоточным оборудованием.

Test mode (Тестовый режим), выполняющий за один проход запись символа #10 кода ASCII.

III. Заключительная часть – (5) мин.

Прием работ.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач. Дать задание для самостоятельной проработки.

Повторить лекции.

Тема 2. Понятие информационной безопасности

Практическое занятие №2

Тема: Защита документов в приложении MS Office. ЦЕЛИ ЗАНЯТИЯ:

1. Отработать практические навыки в обеспечении защиты информации средствами MS Office.
2. Проверить возможности MS Office в обеспечении ИБ (обеспечение конфиденциальности, целостности и доступности).

УЧЕБНЫЕ ВОПРОСЫ:

4. Удаление личных сведений из файла при его сохранении.
5. Шифрование документа MS Office.
6. Шифрование свойств документа MS Office.

МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ:

Методическая разработка для проведения занятия

Вводная часть (10-15 мин.)

Проверка наличия готовности учебной группы к занятию (наличие конспектов; учебных пособий; ручек; линеек и т. д.).

Контрольный опрос. Если группа недостаточно подготовлена, то предоставить время на подготовку группы к занятию, потом начать занятие. При необходимости закончить занятие в часы самоподготовки или выходной день, согласовав это с учебной частью.

II. Основная часть (80 мин).

3. Удаление личных сведений из файла при его сохранении.

Действия:

1. Создайте документ Word и сохраните под именем Doc1 Рабочем столе.
2. Создайте документ Word Рабочем столе под именем Doc2, причем выберите СОХРАНИТЬ КАК Сервис - Параметры безопасности – удалять личные сведения (поставить флажок) - ОК - Сохранить.
3. Выберите последовательно оба файла: двойной щелчок мышью на файле. Затем необходимо щелкнуть правой кнопкой мыши и выбрать пункт Свойства (Properties). При этом отобразится диалог Свойства. Диалоги Doc1 и Doc2 сравнить, а отличия занести в раздел бланка-ОПИСАНИЕ ЭКСПЕРИМЕНТА.

4. Шифрование документа MS Office.

1. Выберите созданный на Рабочем столе документ Word под именем Doc2 откройте его, выберите СОХРАНИТЬ КАК Сервис - Параметры безопасности - Дополнительно – Тип шифрования (для каждого типа активируются различные вкладки – их выписать в бланк) - ОК - Сохранить Doc21, Doc22... соответственно для каждого типа.
2. Для каждого ТИПА ШИФРОВАНИЯ – зафиксировать размер файла.
3. Провести сравнительный анализ размерности от типа шифрования – отразить в выводах по работе.

Doc1 откройте его, выберите сохранить как Сервис - Параметры безопасности – Дополнительно – Тип шифрования RC4 – отметить флажок – шифровать свойства документа - ОК - Сохранить Doc11.

Выберете последовательно три файла Doc1, Doc2 и Doc11: двойной щелчок мышью на файле. Затем необходимо щелкнуть правой кнопкой мыши и выбрать пункт Свойства (Properties). При этом отобразится диалог Свойства. Диалоги Doc1, Doc2 и Doc11 сравнить, а отличия занести

в раздел бланка –описание эксперимента.

Выводы по работе сформулировать на основе цели №2.

III. Заключительная часть – (5) мин.

Контроль усвоения материала (приём отчетов по работе).

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач.

Дать задание для самостоятельной проработки. Повторить лекции.

Контрольный опрос

1. Методы блокирования доступа к ПК.

2. Типы резервного копирования.

3. Схемы архивации.

Тема 3. Государственная информационная политика

Практическое занятие № 3

Тема: Архивация данных утилитой ntbackup.exe

Целевая установка.

Закрепить практические навыки по архивации и восстановлению данных в системах Windows.

Учебные вопросы.

1. Архивация файлов, папок и дисков.
2. Восстановление данных.
3. Отчет о событиях архивации и восстановления.
4. Диск аварийного восстановления.

Материальное обеспечение:

Методическая разработка для проведения занятия

Вводная часть 10-15 мин.

1. Проверить готовность группы, аудитории к занятию.
2. Объявить тему, цели и учебные вопросы занятия.
3. Контроль усвоения теоретического материала.

Основная часть 80 мин.

С помощью утилиты ntbackup.exe данные можно архивировать на любое устройство хранения данных, подсоединенное к локальному компьютеру или к сети, для доступа к которому у пользователя имеются соответствующие права. Для архивации данных проще всего воспользоваться мастером, который поможет выполнить все необходимые действия.

Для самостоятельного выполнения архивации выполните такие действия

1. Запустите утилиту ntbackup.exe системы Windows 2000/XP. Для этого выберите команду меню **Пуск • Программы • Стандартные • Служебные • Архивация данных** (Start • Programs • Accessories • System Tools * Backup). Или же выберите команду **Пуск • Выполнить** (Start • Run), а затем в появившемся диалоговом окне введите команду **ntbackup** и нажмите клавишу **Выполнить**. После запуска утилиты на экране появится диалог, представленный на Рис. 1.

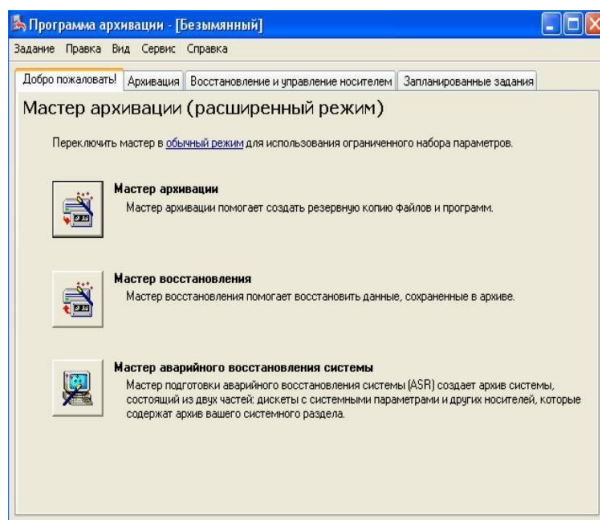


Рис. 1. Диалог
утилиты архивации
ntbackup.exe Архивация и
восстановление данных в
системах Windows 2000 и
Windows XP
аналогичны.

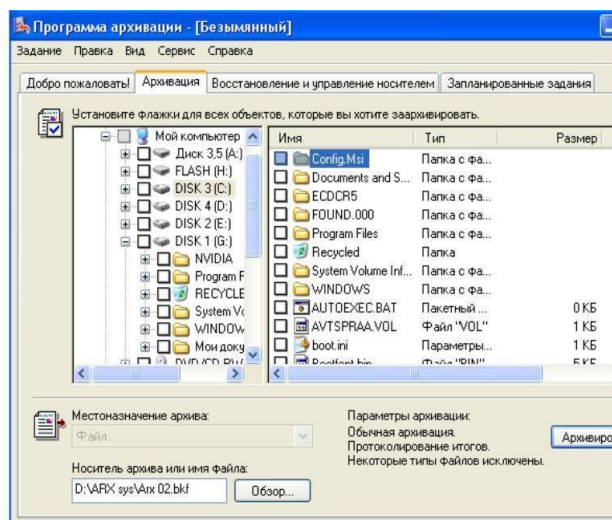


Рис. 2. Вкладка
архивации файлов и папок в
ручном режиме

2. В диалоге на Рис. 1 имеются три кнопки для запуска мастеров архивации, восстановления и создания аварийной дискеты. Архивацию и восстановление можно выполнить самостоятельно, воспользовавшись вкладками **Архивация** (Backup) и **Восстановление** (Restore).

Вопрос 1. Архивация файлов, папок и дисков

1. В диалоге утилиты архивации щелкните на вкладке **Архивация** (Backup); на экране появится диалог, представленный на Рис. 2.
2. Щелчками мыши отметьте в окне на вкладке **Архивация** (Backup) архивируемые файлы и папки, заранее Вами созданные на рабочем столе (средства навигации аналогичны используемым в проводнике Windows).
3. Выберите из раскрывающегося списка **Местоназначение архива** (Backup destination) способ сохранения архивных данных. Может быть выбран или параметр **Файл** (File), или любой накопитель на магнитной ленте, подсоединенный к компьютеру.
4. В поле **Носитель архива или имя файла** (Backup media or file name) укажите место, в котором будут храниться файлы архива. При этом можно воспользоваться кнопкой **Обзор** (Browse) для выбора места обычными средствами навигации по файлам и папкам Windows. (В диалоге на Рис. 2 для архивации выбран файл с базой данных местоназначением **Файл** (File) и хранением архивного файла на логическом диске E в папке Архив X).
5. Щелкните на кнопке **Архивировать** (Start Backup). На экране появится диалог **Сведения о задании архивации** (Backup Job Information), представленный на Рис. 3.

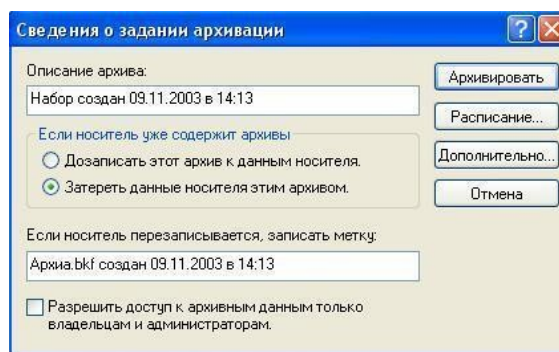


Рис. 3. Диалог запуска архивации

6. В диалоге **Сведения о задании архивации** (Backup Job Information) отметьте флажок. Разрешить доступ архивным данным только владельцам и администраторам (Allow only the owner and the Administrator access to the backup data) для защиты архивных данных от несанкционированного доступа.

7. Диалог **Сведения о задании архивации** (Backup Job Information) содержит несколько кнопок задания режима выполнения архивации. Щелчок на кнопке **Архивация**, в некоторых случаях **Запуск** (Backup), начинает процесс архивации; щелчок на кнопке **Расписание** (Schedule) открывает диалог задания расписания архивации (это же можно сделать на вкладке **Запланированные задания** (Schedule Jobs) диалогового окна **Архивация** (Backup)). Щелчок на кнопке **Дополнительно** (Advanced) открывает диалог **Дополнительные параметры архивации** (Advanced Backup Options), представленный на Рис. 4.

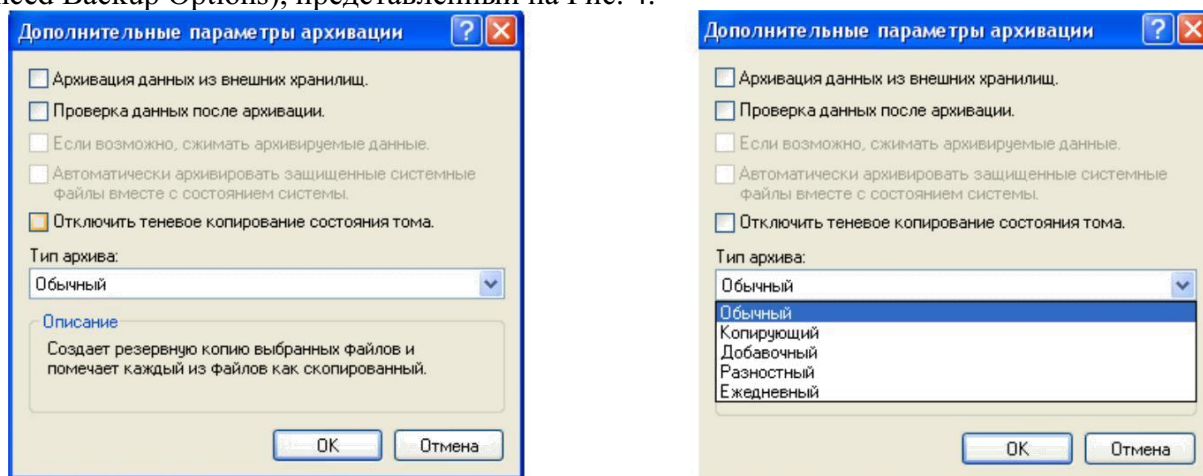


Рис. 4. Диалог дополнительной настройки архивации

8. Щелчком мыши выберите из раскрывающегося списка **Тип архива** (Backup Type) тип, создаваемого архива.

Обычный (Normal). При обычной архивации на архивный носитель копируются все выбранные для архивирования файлы, независимо от состояния их архивного атрибута, и после копирования файлов их архивный бит сбрасывается. Обычную архивацию иногда называют полной архивацией. **Копирующий** (Copy). Как и при обычной архивации, все выбранные файлы копируются на архивный носитель.

Однако в отличие от обычной архивации, состояние архивного бита не изменяется.

Добавочный (Incremental). Архивируются только файлы из выбранного набора с установленным архивным битом. Этим достигается быстрое резервное копирование только тех файлов, которые были модифицированы после выполнения последней добавочной архивации. Архивные биты скопированных файлов сбрасываются. При следующей модификации файла

система Windows 2000 Professional снова установит архивный бит.

Разностный (Differential). Это разновидность добавочной архивации, при которой копируются только файлы, для которых установлен архивный бит. Состояние архивного бита при этом не изменяется. **Ежедневный (Daily).** Копируются только те выбранные файлы, которые были модифицированы в течение дня. Ежедневная архивация полезна для быстрого копирования часто изменяющейся информации.

9. Щелчком мыши отметьте флажок **Проверка данных после архивации** (Verify data after backup), установив режим сравнения исходных и архивированных данных.

10. Щелкните на кнопке ОК и запустите архивацию. На диске будет создан архивный файл с расширением .bkf. По завершении отобразится диалог **Ход архивации** (Backup Progress).

11. Чтобы просмотреть отчет о событиях архивации, щелкните на кнопке **Отчет** (Report) или закройте диалог щелчком на кнопке **Заккрыть** (Close). Кроме того, утилита ntbakup.exe позволяет архивировать системные данные, включающие в себя, помимо прочего, системный реестр и загрузочные файлы Windows 2000 (файлы NTLDR и NTDETECT.COM). Архивация этих данных выполняется описанным выше способом, но при выборе архивируемых объектов в диалоге на вкладке **Архивация** (Backup) следует выбрать объект **Состояние системы**. Далее укажите местоназначение архива в файле с именем system.bkf, расположенном в какой-либо локальной папке компьютера. В процессе архивации реестра будут выполнены специальные действия, поскольку многие открытые в данный момент программы используют реестр. *Открытые файлы обычно пропускаются.* Заметим, что информацию из системных реестров сетевых ресурсов с помощью утилиты ntbakup.exe архивировать нельзя. Это единственное ограничение, не позволяющее использовать утилиту ntbakup.exe в качестве единственного средства архивирования для всей сети. Созданный архив гарантирует восстановление системы после аварии.

Вопрос 2. Восстановление данных

Операция восстановления информации с помощью архива очень похожа на операцию создания архива. Для восстановления данных вначале откройте вкладку

Восстановление (Restore) диалога **Архивация (Backup)**, представленную на Рис. 5.

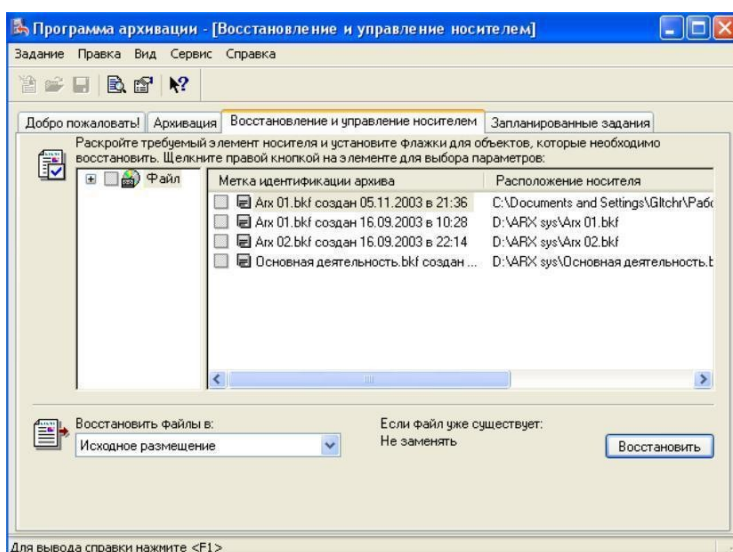


Рис. 5. Вкладка восстановления данных

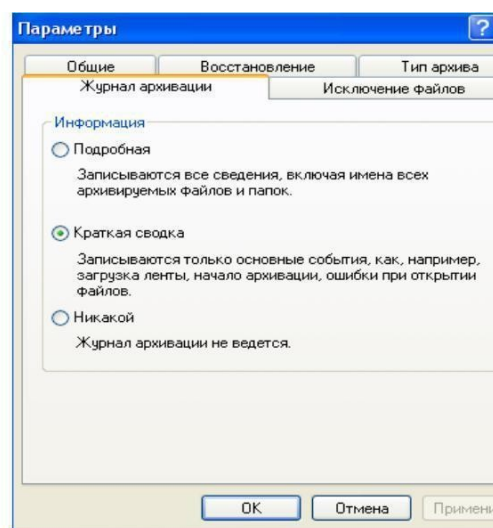


Рис. 6. Задание уровня детализации отчета о событиях архивации и восстановления.

Область диалога **Установите флажки для всех объектов, которые вы хотите восстановить** (Click to select the check box for any drive, folder, or file that you want to restore) позволяет выбрать восстанавливаемый архив. Место для записи восстанавливаемых данных указывается в раскрывающемся списке **Восстановить файлы в:** (Restore files to). При этом существуют следующие возможности. При выборе **Исходное размещение** (Original location) восстановленные данные будут записаны в место их первоначального нахождения.

При выборе **Альтернативное размещение** (Alternate location) восстановленные данные будут записаны в указанную папку с сохранением структуры каталогов архивных данных.

При выборе **Единственную папку** (Single folder) восстановленные данные будут записаны в единственную папку без сохранения структуры каталогов.

При выборе двух последних возможностей в диалоге отображается поле **Альтернативное размещение** (Alternate location) для указания папки восстановления данных и кнопка **Обзор** (Browse) для выбора этого места с помощью навигации по папкам компьютера и его сетевого окружения.

Выполним восстановление архива состоянием системы в папку на локальном компьютере с сохранением структуры каталогов архива.

1. В области. Установите флажки для всех объектов, которые вы хотите восстановить (Click to select the check box for any drive, folder, or file that you want to restore) раскройте архив system.bkf, созданный в предыдущем разделе.

2. В списке. **Восстановить файлы в:** (Restore files to) выберите Альтернативное размещение (Alternate location).

3. Щелкните на кнопке Обзор (Browse); отобразится диалог **Путь восстановления** (Restore path).

4. Средствами навигации диалога **Путь восстановления** (Restore path) выберите папку для размещения восстанавливаемых данных, например, **C:\Restore**.

5. Щелкните на кнопке ОК и закройте диалог **Путь восстановления** (Restore path).

6. Щелкните на кнопке **Восстановить** (Start Restore) и запустите восстановление архивных данных.

При запуске восстановления вначале отображаются несколько диалогов, позволяющих указать путь к архивному файлу и задать дополнительные параметры восстановления. Для нас наиболее интересен флажок **Восстановление безопасности** (Restore security) диалога **Дополнительные параметры восстановления** (Advanced Restore Options).

Установка флажка **Восстановление безопасности** (Restore security) в случае использования файловой системы NTFS приводит к установлению прав доступа, разрешений и аудита файлов и папок NTFS. Это позволит избежать дополнительных усилий по настройке безопасности системы, что особенно важно при восстановлении целых дисков многопользовательских систем.

Вопрос 3. Отчет о событиях архивации и восстановления

Утилита ntbackup.exe позволяет создавать отчеты о ходе процесса архивации и восстановления, причем с различным уровнем детализации. Для задания режима создания отчета с нужным уровнем детализации выберите команду **Сервис • Параметры** (Tools • Options) и в открывшемся диалоге **Параметры** (Options) щелкните на вкладке **Журнал Архивации** (Backup log). На этой вкладке (см. Рис. 6) содержится несколько переключателей, выбор которых задает уровень детализации отчета или позволяет отказаться от ведения журнала событий архивирования. *Журнал* регистрации - полезная вещь, поскольку процедуры архивации и восстановления могут быть весьма длительными, и их желательно выполнять в автоматическом режиме. Чтобы просмотреть отчет, выберите команду **Сервис • Отчет** (Tools • Report) и в отобразившемся диалоге выберите требуемый отчет для просмотра.

Все описанные средства архивации и восстановления работают при условии нормального функционирования операционной системы Windows 2000. Но что, если система будет повреждена и не сможет загрузиться по причине повреждения среды загрузки, системных файлов, системного реестра или загрузочного сектора системного диска? Для этого случая в систему загрузки Windows 2000 Professional встроена подсистема восстановления, которая с помощью диска аварийного восстановления и установочного компакт-диска может оказаться в состоянии восстановить работоспособность системы. Рассмотрим эту возможность.

Вопрос 4. Диск аварийного восстановления

Программа установки Windows 2000 Professional в процессе работы позволяет выбрать параметр создания исходного диска аварийного восстановления. Диск аварийного восстановления можно рассматривать как моментальный снимок системы.

Поскольку по мере работы системы в ней накапливаются изменения, связанные с пополнением компонентов Windows, установкой приложений и добавления новых пользователей, диск аварийного восстановления требуется обновлять, воспользовавшись утилитой ntbackup.exe.

Восстановления в системе Windows XP претерпели некоторые изменения сравнительно с Windows 2000 - создание диска аварийного восстановления в Windows XP сопровождается автоматическим созданием еще одного архива с системными файлами.

Для создания диска аварийного восстановления щелкните на кнопке **Диск аварийного восстановления** (Emergency Repair Disk) в диалоге утилиты ntback-up.exe (см. Рис. 1) и запустите мастера создания аварийного диска.

Обратите внимание на флажок **Архивировать реестр в папку восстановления** (Als restore the registry to the repair directory). Если установить этот флажок, текущие файлы реестра будут сохранены в папку системных _корневой_каталог_repair/RegBack. Это бывает полезно, если требуется восстановить систему в случае сбоя жесткого диска, но такая операция представляет серьезную угрозу для безопасности системы. Дело в том, что при этом копируется, вся база данных диспетчера безопасности SAM (хакинг которой мы обсудим в следующем семестре).

Поскольку в базе SAM хранятся зашифрованные пароли пользователей компьютера доступ к файлу базы SAM - весьма заманчивая цель для хакеров Щелчок на кнопке ОК приводит к запуску программы создания диска аварийного восстановления. В последующее время, если вам не повезет, и система Windows 2000 перестанет загружаться, можно воспользоваться аварийным диском. Для этого загрузите компьютер с помощью установочных дисков Windows 2000, и в процессе исполнения программы установки Windows 2000 в ответ на запрос выберите параметр восстановления поврежденной системы (для этого потребуется нажать клавишу R). Начнется процесс восстановления, которым можно управлять выбором следующих параметров, отображаемых на экране компьютера.

- **Проверка реестра** (Inspecting the Registry).
- **Проверка среды загрузки** (Inspecting the boot environment).
- **Проверка системных файлов Windows 2000** (Checking and verifying the Windows 2000 system files).
- **Проверка загрузочного сектора загрузочного диска** (для компьютеров In-tel или на базе процессора Alpha) (Inspecting the boot sector of the boot disk (Intel computers, NVRAM on Alpha)).

Выберите нужную опцию и выполните проверку, в процессе которой определяется наличие и работоспособность всех необходимых системных файлов. Ход проверки фиксируется в файле setup.log диска аварийного восстановления.

Заключительная часть 5 мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработки учебных задач.

Дать задание для самостоятельной проработки. Повторить лекции.

Тема 4. Стратегия развития информационного общества до 2030

Практическое занятие №4

Тема: Средства пользовательского интерфейса программы PGP *Целевая установка.*

Ознакомиться с основными возможностями интерфейса программы PGP и порядком начала работы.

Учебные вопросы.

1. Средства пользовательского интерфейса.
2. Создание пары ключей.
3. Защита ключей.

Материальное обеспечение:

Методическая разработка для проведения занятия

Вводная часть 10-15 мин.

1. Проверить готовность группы, аудитории к занятию. 2. Объявить тему, цели и учебные вопросы занятия.
2. Контроль усвоения теоретического материала.

Основная часть 70 мин.

Метод, которым пользователь может обратиться к средствам PGP, во многом определяется его предпочтениями. Пользователь может выбрать метод, который в данное время ему наиболее доступен и удобен. Программа PGP работает с данными, генерированными другими приложениями. Поэтому функциональные средства PGP спроектированы так, чтобы пользователь мог обратиться к ним напрямую, изнутри отдельного приложения.

Вопрос 1. Средства пользовательского интерфейса.

Чтобы получить доступ к утилитам PGP (PGPkeys, PGPtools, PGPtray и PGPdisk).

На панели задач щелкните на кнопке Start (Пуск), затем щелкните на пунктах Programs (программы) и PGP и выберите команду из открывшегося подменю.

1. При использовании приложения электронной почты, для которого существует встраиваемый модуль PGP, можно использовать панель PGPmail (см. Рис. 1).



Рис.1

Открыть панель PGPmail можно выбором команды PGPmail из меню, открываемого щелчком на значке PGP в системном лотке или выбором команды меню Пуск • Программы • PGP • PGPmail.

2. Пользователь может шифровать, подписывать, дешифровать и верифицировать файлы текстовых документов, электронных таблиц и видеоклипов непосредственно в окне проводника Windows. Чтобы получить доступ к функциональным средствам PGP из проводника Windows, щелкните правой кнопкой мыши на файле в окне проводника и выберите команду PGP из отобразившегося контекстного меню, либо выделите нужный файл и выберите команду PGP из меню

File (Файл) проводника (см. Рис 2.).

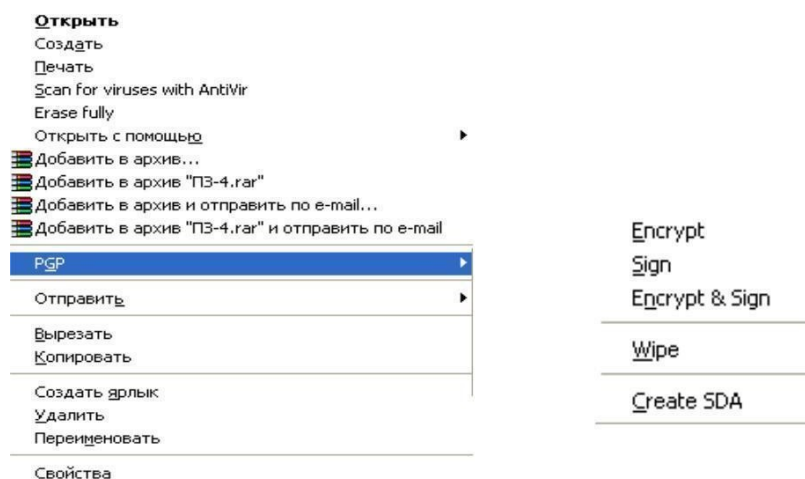


Рис. 2

Набор команд, отображаемый в подменю PGP, зависит от текущего состояния выбранного файла. Если файл еще не шифровался или не подписывался, в меню появляются команды для выполнения функций шифрования и подписания.

Если же файл уже шифровался или подписывался, отображаются команды дешифрования и верификации подписи файла.

Вопрос 2. Создание пары ключей.

Первая задача, работы в PGP заключается в создании новой пары ключей. Генерирование ключей выполняется утилитой PGPkeys с использованием мастера генерации ключей PGP (PGP Key Generation Wizard), который проводит пользователя через пошаговую процедуру генерации ключей.

1. Запустите утилиту PGPkeys. Утилиту PGPkeys можно открыть командой меню Start • Programs • PGP • PGPkeys (Пуск • Программы • PGP • PGPkeys) или выбором команды PGPkeys из меню, отображаемого щелчком на значке PGP в системном лотке (или щелчком на панели инструментов вашего приложения электронной почты).

2. Диалог утилиты PGPkeys (см. Рис. 3) отображает пары открытых и закрытых: ключей, созданных пользователем, а также все открытые ключи других пользователей, добавленных в связку открытых ключей.

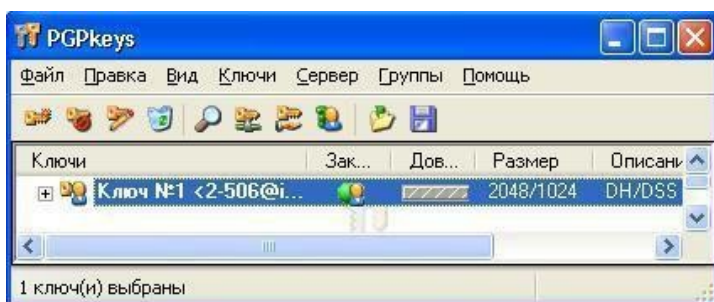
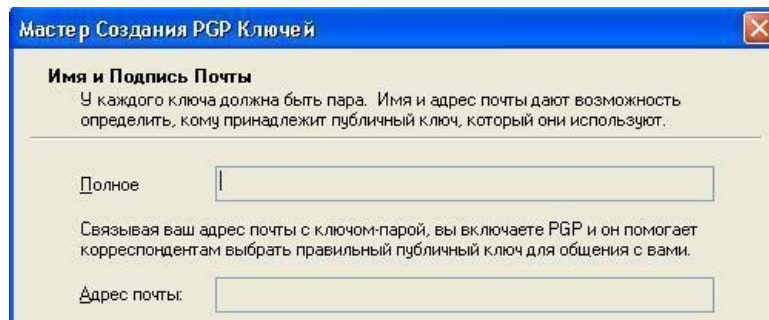


Рис. 3. Диалог управления ключами приложения PGP

3. Выберите команду меню **Keys • New Keys** (Ключи • Новые ключи). Отобразится первый Диалог мастера **Key Generation Wizard** (Мастер генерации ключей) с некоторой вводной информацией. Прочитав информацию, щелкните на кнопке **Далее**, чтобы перейти в следующее



окно мастера. (Если вы хотите создать особый ключ, щелкните на кнопке **Expert** (Эксперт). В отобразившемся окне можно выбрать алгоритм шифрования, тип генерируемого ключа, указать размер ключа и установить срок его действия).

Рис. 4. Указание имени и адреса электронной почты владельца генерируемых ключей

4. В новом диалоге мастера, представленном на Рис. 4, введите свое имя в поле **Полное** (Имя) и свой адрес электронной почты в поле **Email** (Почта). Необязательно вводить свое настоящее имя, и даже адрес вашей электронной почты.

Однако использование настоящего имени облегчает другим людям идентификацию вас как владельца вашего открытого ключа. Чтобы продолжить, щелкните на кнопке **Next** (Далее).

5. В отобразившемся диалоге (см. Рис. 5) мастер создания ключей предлагает ввести текст парольной фразы. В поле **Passphrase** (Парольная фраза) введите строку символов или слов, которые хотите использовать для поддержки эксклюзивного доступа к закрытому ключу. Чтобы подтвердить ввод, нажмите клавишу **Tab**, перейдите в следующее поле, затем введите текст парольной фразы еще раз.

Как правило, в качестве дополнительной меры защиты, вводимые символы не отображаются на экране. Однако если вы уверены, что за вами никто не наблюдает, а вам хотелось бы видеть символы текста пароля по мере ввода, сбросьте флажок **Hide Typing** (Скрыть Букв).

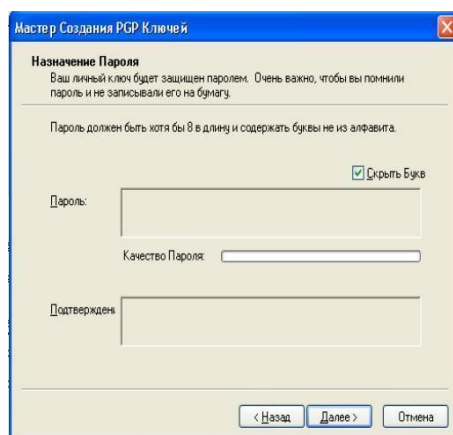


Рис. 5. Задание пароля ключей

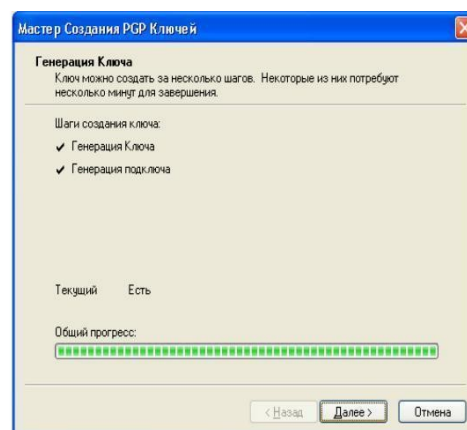


Рис. 6. Диалог отображает ход процесса генерирования ключей

6. Щелкните на кнопке **Далее**, чтобы начать процесс генерирования ключа. В отобразившемся диалоге (см. Рис. 6) полоса прогресса указывает, что мастер занят генерированием нового ключа. Если на предыдущем шаге была введена неудовлетворительная

парольная фраза, перед началом генерирования ключа отобразится предупреждение. Пользователь может либо принять плохую идентификационную фразу, либо ввести более надежную фразу. При этом выполняемые пользователем нажатия клавиш генерируют случайную информацию, которая необходима для создания уникальной пары ключей. Если объем случайной информации не достаточен для построения ключа, отображается диалог PGP Random Data (Случайные данные PGP). Повинуясь инструкциям в диалоге, вводите серию случайных символов нажатиями клавиш, пока полоса продвижения не заполнится полностью.

7. По завершению процесса генерирования ключей отобразится последнее информационное окно мастера. Щелкните на кнопке **Готово**. Программа PGP автоматически вставит закрытый ключ пользователя **MyName** в связку закрытых ключей, а открытый и ключ - в связку открытых ключей, которая отображается в диалоге Рис. 7.

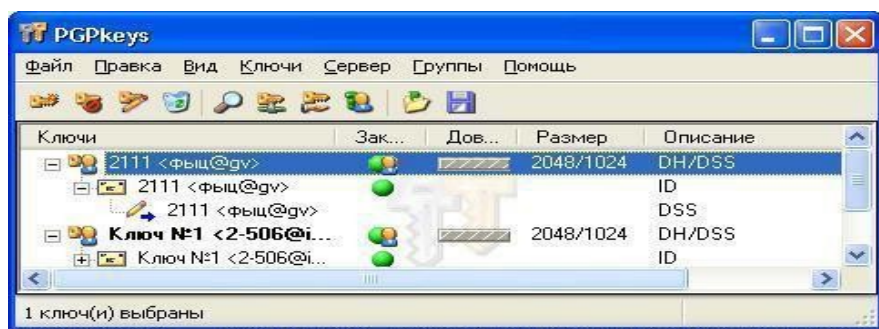


Рис. 7. В связке ключей отображается генерированная пара ключей PGP

8. После генерирования пары ключей можно приступить к использованию утилиты PGPkeys для создания новых пар ключей и распределения всех остальных ключей.

Вопрос 3. Защита ключей.

Кроме создания резервных копий ключей, следует особенно позаботиться о месте хранения своего закрытого ключа. Даже если закрытый ключ защищен паролем, который известен только вам, есть вероятность, что кто-нибудь найдет возможность раскрыть ваш пароль, а затем использовать закрытый ключ для дешифрования вашей электронной почты или подделки цифровой подписи. Для этого существует множество методов.

Чтобы задать имя и местоположение файлов со связками ваших закрытых и открытых ключей, выберите команду меню **Edit • Options** (Правка • Параметр), используйте вкладку Files (Файлы) диалога Options (Параметры).

Заключительная часть 5 мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработки учебных задач.

Дать задание для самостоятельной проработки. Повторить лекции.

Тема 5. Понятие и виды информации, свойства информации и систем ее обработки
Практическое занятие №5

Тема: Защита файлов и папок с помощью PGP

ЦЕЛИ ЗАНЯТИЯ:

Отработать практические навыки по созданию зашифрованных дисков.

УЧЕБНЫЕ ВОПРОСЫ:

- 1. Шифрование и подписание файлов.**
- 2. Дешифрование и верификация файлов.**
- 3. Создание защищенного диска утилитой PGPdisk.**

МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ:

Методическая разработка для проведения занятия

Вводная часть (10-15 мин.)

Проверка наличия готовности учебной группы к занятию (наличие конспектов; учебных пособий; ручек; линеек и т. д.).

Контрольный опрос

Если группа недостаточно подготовлена, то предоставить время на подготовку группы к занятию потом начать занятие. При необходимости закончить занятие в часы самоподготовки или выходной день, согласовав это с учебной частью.

II. Основная часть (70) мин.

Приложение PGP можно использовать для шифрования и подписания файлов, используемых как вложения электронной почты, а также для шифрования и верификации файлов или вложений, которые были зашифрованы вашими корреспондентами. В этом разделе описаны методики, используемые для выполнения указанных задач.

1. Шифрование и подписание файлов

Для защиты своих файлов и папок следует использовать команды **Encrypt** (Шифрование), **Sign** (Подписание) или **Encrypt and Sign** (Шифрование и подписание), доступные для выбора из меню, отображаемого щелчком на значке PGP в системном лотке, из панели **PGPtools** или меню **File** (Файл) в диалогепроводника Windows. При выборе команды **Encrypt** (Шифрование) или **Encrypt and Sign** (Шифрование и подписание) автоматически отображается диалог **PGP Key Selection** (Выбор ключа PGP) Этот диалог позволяет выбрать открытый ключ получателя для шифруемых вами данных.

Для выбора открытого ключа его следует перетащить из связки ключей его в список **Recipients** (Получатели) В левом нижнем углу диалога можно установить дополнительные параметры шифрования. Параметры, доступные вам, зависят от типа данных, шифруемых в текущий момент. Доступны следующие опции:

Text Output (Текстовый вывод). При отсылке файлов как вложений с помощью некоторых приложений электронной почты вам может понадобиться установить флажок **Text Output** (Текстовый вывод), чтобы сохранить файл как текст ASCII. Иногда это необходимо для отсылки двоичных файлов с помощью устаревших приложений электронной почты. Установка этого флажка увеличивает размер зашифрованного файла примерно на 30 процентов.

Wipe Original (Стереть оригинал). Установите этот флажок для перезаписи исходного документа, который вы шифруете, с тем, чтобы вашу уязвимую информацию не мог прочитать ни один человек, имеющий доступ к вашему жесткому диску.

Secure Viewer (Защита просмотра). Установите этот флажок для защиты текста при дешифровании от атак TEMPEST. При выборе этой опции данные отображаются специальным шрифтом (с размытым контуром и серого цвета), предотвращающим атаку TEMPEST, поскольку такой текст плохо читаем на оборудовании захвата излучений. При дешифровании электронная почта не может быть сохранена в расшифрованном формате. Эта опция доступна только при шифровании текста или текстовых файлов.

Conventional Encrypt (Обычное шифрование). Установите этот флажок чтобы полагаться только на обычную парольную фразу, а не на криптографию с открытыми ключами. Файл шифруется сеансовым ключом, который шифрует(и дешифрует) с помощью парольной фразы, предлагаемой вам на выбор.

Self Decrypting Archive (SDA, Само дешифрующийся архив).

Установите этот флажок, чтобы создать автоматически дешифрующийся исполняемый файл.

При отметке этого флажка файл шифруется с использованием сеансового ключа, который шифрует (и дешифрует) данные с помощью парольной фразы, которую пользователю предлагается указать. Итоговый исполняемый файл может быть дешифрован простым двойным

щелчком и вводом надлежащей парольной фразы. Эта опция особенно удобна при отсылке зашифрованных файлов корреспондентам, у которых не установлена программа PGP. Имейте в виду, в этом случае отправитель и получатель должны использовать одинаковые операционные системы.

Если вы подписываете файлы, вам будет предложено ввести свою парольную фразу. Если после шифрования вы заглянете в папку, где находился исходный файл, вы обнаружите файл с заданным именем и расширением PGP.

2. Дешифрование и верификация файлов

Когда кто-нибудь присылает вам файл с зашифрованными данными, можно дешифровать содержимое и верифицировать любую приложенную подпись, чтобы убедиться, что данные присланы подлинным отправителем, а не подменены. Для шифрования своих файлов и папок используйте команду **Decrypt & Verify** (Дешифрование и верификация), доступную из меню значка PGP в системном лотке, панели инструментов **PGPtools** или меню **File** (Файл) диалога проводника Windows.

Чтобы зашифровать и/или верифицировать данные, которые были зашифрованы для вашего ключа, вы должны располагать своим закрытым ключом и парольной фразой. Если при шифровании файла был установлен флажок **Secure Viewer** (Защита просмотра), дешифрованный текст отображается на защищенном экране PGP специальным шрифтом (размытым и серого цвета), предотвращающим атаку TEMPEST. В противном случае сообщение отобразится в его исходном состоянии.

Чтобы открыть само дешифрующийся архив (архив SDA), щелкните дважды на исполняемом файле (с расширением SDA.EXE). Введите корректный пароль и укажите местоположение, в котором следует сохранить дешифрованный файл.

3. Создание защищенного диска утилитой PGPdisk

Утилита PGPdisk представляет собой несложное приложение шифрования, которое позволяет выделить на свободном дисковом пространстве область для хранения уязвимых данных. Эта область используется для создания файла, называемого диска PGPdisk. Несмотря на то, что он представляет собой единый файл, работа с диском PGPdisk во многом подобна операциям со обычными логическими дисками, создаваемыми на жестком диске компьютера. Диск PGPdisk предоставляет пространство для хранения файлов и приложений, и операции с этими элементами выполняются обычными средствами проводника Windows.

Чтобы использовать приложения и файлы, хранящиеся в диске PGPdisk, его необходимо смонтировать и, указав парольную фразу, открыть к диску доступ. После монтирования диска PGPdisk его можно использовать как обычный логический диск. Вы можете устанавливать в диске приложения, перемещать или сохранять в нем файлы и т. д. После демонтирования диск PGPdisk становится не доступным любому, кто не знает секретной парольной фразы. Программа PGPdisk:

- Позволяет создавать защищенные диски шифрованных данных, которые функционируют в точности так же, как любые диски, которые вы привыкли использовать для хранения своих файлов.
- Обеспечивает быстрое и надежное шифрование данных с минимальным влиянием на время доступа к программам и файлам.
- Сохраняет содержимое каждого защищенного диска в зашифрованном файле, который несложно архивировать и обменивать с коллегами.

Для защиты диска программа PGPdisk предоставляет на выбор два мощных алгоритма шифрования:

- CAST5 (128-битовый). Алгоритм CAST представляет собой 128-битовый блочный шифр. Это мощный алгоритм, соответствующий требованиям военного ведомства, имеющий прочную репутацию криптостойкого алгоритма за его способность противостоять несанкционированному доступу.

- Twofish (256-битовый). Алгоритм Twofish представляет собой новый 256-битовый симметричный блочный шифр, созданный Брюсом Шнейером (Bruce Schneier). Входит в число пяти алгоритмов, включенных Американским национальным институтом стандартов и технологии (NIST) в расширенный стандарт шифрования (Advanced Encryption Standard - AES), пришедший на смену стандарту шифрования данных DES.

Порядок создания диска PGPdisk:

1. Выберите в меню Windows команду Start - Programs - PGP - PGPdisk (Пуск - Программы - PGP - PGPdisk).

2. Отобразится первый диалог мастера PGPdisk Wizard (Мастер PGPdisk). Прочти вводную информацию.

3. Щелкните на кнопке Next (Далее). Отобразится диалог, предлагающий указать местоположение и размер нового диска.

4. Щелкните на кнопке **Browse** (Просмотр), чтобы перейти к целевому каталогу для диска PGPdisk или примите стандартное местоположение.

5. В поле **Choose a Size** (Выбор размера) введите размер пространства, которое хотите зарезервировать для нового диска. Используйте целые числа, без десятичных разрядов. Для увеличения или уменьшения числа, отображаемого в поле, можно использовать кнопки со стрелками. Над полем **Size** (Размер) отображается объем свободного дискового пространства.

6. В правом поле выберите единицы измерения: KB (Кбайт), MB (Мбайт) или GB (Гбайт). Вы можете создать диск любого объема свыше 100 Кбайт. Максимальный допустимый объем диска PGPdisk зависит от версии Windows, а также размера и формата жесткого диска.

7. Щелкните на кнопке **Advanced Options** (Дополнительные параметры),

чтобы указать, где и как хотите смонтировать диск PGPdisk, а также выбрать алгоритм шифрования. Отобразится диалог **Options** (Параметры).

8. Выберите нужные параметры с помощью следующих флажков списков.

Переключатель **On a drive letter** (Буква диска). Выберите букву диска, которой будет отмечаться создаваемый диск PGPdisk после монтирования в дереве дисков и папок окна проводника Windows. Переключатель **As a directory on an NTFS volume** (Как каталог в диске NTFS). Этот параметр доступен только в системах Windows 2000. Установите этот переключатель, если хотите смонтировать новый диск PGPdisk как каталог диска NTFS. Введите в текстовое поле путь к пустому каталогу или щелкните на кнопке **Browse** (Просмотр) и перейдите к нужному местоположению.

9. При вводе пути к несуществующему каталогу диска NTFS, появится запрос необходимости создать каталог с данным именем. Щелкните на кнопке Yes (Да), затем введите свою парольную фразу. В окне Windows Explorer (Проводник Windows) в выбранном вами диске NTFS появится новый каталог.

10. Выберите алгоритм шифрования, который хотите использовать для защиты своих данных: Twofish Cipher Algorithm (256-bit) означает выбор алгоритма

11. Выберите формат файловой системы для нового диска PGPdisk.

- ☐ ☐ Файловая система FAT. Доступна на всех платформах Windows. ☐
- ☐ Файловая система NTFS. Доступна на платформах Windows NT и ☐

Windows 2000 и только для дисков PGPdisk размером не менее 5 Мбайт. Файловая система FAT32. Доступна на платформах Windows 95, Windows 98 и Windows 2000 и только для дисков PGPdisk размером не менее 260Мбайт.

12. Флажок Mount at startup (Монтировать при запуске). Установите этот флажок, чтобы диски PGPdisk монтировались при загрузке. При установке флажка при загрузке операционной системы вам будет предлагаться ввести парольную фразу для доступа к диску PGPdisk.

13. Щелкните на кнопке ОК. Диалог Options (Параметры) закроется.

14. Щелкните на кнопке Next (Далее). Отобразится диалог.

15. Выберите метод защиты нового диска PGPdisk. Можно выбрать один из следующих методов.

16. Public key (Открытый ключ). Если вы предпочтете защищать диск PGPdisk открытым ключом, отобразится список открытых ключей в вашей связке. Выберите ключ, которым хотите защитить диск PGPdisk.

17. Passphrase (Парольная фраза). Если вы предпочитаете защищать свой диск PGPdisk парольной фразой, вы должны также ввести свое пользовательское имя.

В последнем случае для получения доступа к новому диску введите строку слов или символов, которые будут служить вашей парольной фразой. (Эту строку также называют главной парольной фразой диска). Для подтверждения ввода нажмите клавишу **Tab**. перейдите в новое текстовое поле и введите парольную фразу еще раз. Рекомендуемый размер парольной фразы составляет восемь символов.

Как правило, в качестве дополнительного уровня защиты, символы, которые вы вводите для парольной фразы, не видимы на экране. Однако если вы уверены, что никто не подглядывает (как физически, так и по сети), а вы предпочли бы видеть символы парольной фразы во время ввода, сбросьте флажок Hide Typing(Скрыть ввод).

18. Щелкните на кнопке Next (Далее). Полоса прогресса укажет размер диска PGPdisk, инициализированный и форматированный в текущий момент.

19. Щелкните на кнопке Next (Далее), чтобы смонтировать диск PGPdisk. Отобразится завершающий информационный диалог.

20. Щелкните на кнопке Finish (Готово); на экране отобразится диалог проводника Windows с новым диском PGPdisk. Теперь с ним можно работать средствами проводника как с обычным логическим диском.

В диске PGPdisk можно создавать, копировать и удалять файлы и папки точно так же, как в любом другом логическом диске. Подобным образом, другой пользователь, имеющий доступ к диску (на этом же компьютере или по сети), также может получить доступ к данным, хранящимся на диске. Данные в зашифрованном файле, ассоциированном с этим диском, станут недоступными только после демонтирования диска.

III. Заключительная часть – (5) мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач.

Дать задание для самостоятельной проработки. Повторить лекции.

Тема 6. Проблемы информационной войны

Практическое занятие № 6

Тема: **Криптозащита сообщений с помощью PGP**

ЦЕЛИ ЗАНЯТИЯ:

Отработать практические навыки по созданию зашифрованных дисков.

УЧЕБНЫЕ ВОПРОСЫ:

- 1. Шифрование и подписание данных. Дайджест сообщения.**
- 2. Дешифрование и верификация файлов.**

МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ:

Методическая разработка для проведения занятия

Вводная часть (10-15 мин.)

Проверка наличия готовности учебной группы к занятию (наличие конспектов; учебных пособий; ручек; линеек и т.д.).

Контрольный опрос

Если группа недостаточно подготовлена, то предоставить время на подготовку группы к занятию потом начать занятие. При необходимости закончить занятие в часы самоподготовки или выходной день, согласовав это с учебной частью.

II. Основная часть (150) мин.

Приложение PGP можно использовать для шифрования и подписания файлов, используемых как вложения электронной почты, а также для шифрования и верификации файлов или вложений, которые были зашифрованы вашими корреспондентами. В этом разделе описаны методики, используемые для выполнения указанных задач.

Краткие сведения из теории

Для защиты своих файлов и папок следует использовать команды **Encrypt** (Шифрование), **Sign** (Подписание) или **Encrypt and Sign** (Шифрование и подписание), доступные для выбора из меню, отображаемого щелчком на значке PGP в системном лотке, из панели **PGPtools** или меню **File** (Файл) в диалогепроводника Windows. При выборе команды **Encrypt** (Шифрование) или **Encrypt and Sign** (Шифрование и подписание) автоматически отображается диалог **PGP Key Selection** (Выбор ключа PGP) Этот диалог позволяет выбрать открытый ключ получателя для шифруемых вами данных.

Для выбора открытого ключа его следует перетащить из связки ключей его в список **Recipients** (Получатели) В левом нижнем углу диалога можно установить дополнительные параметры шифрования. Параметры, доступные вам, зависят от типа данных, шифруемых в текущий момент. Доступны следующие опции:

Text Output (Текстовый вывод). При отсылке файлов как вложений с помощью некоторых приложений электронной почты вам может понадобиться установить флажок **Text Output** (Текстовый вывод), чтобы сохранить файл как текст ASCII. Иногда это необходимо для отсылки двоичных файлов с помощью устаревших приложений электронной почты. Установка этого флажка увеличивает размер зашифрованного файла примерно на 30 процентов.

☐ **Wipe Original** (Стереть оригинал). Установите этот флажок для перезаписи исходного документа, который вы шифруете, с тем, чтобы вашу уязвимую информацию не мог прочитать ни один человек, имеющий доступ к вашему жесткому диску.

☐ **Secure Viewer** (Защита просмотра). Установите этот флажок для защиты текста при дешифровании от атак TEMPEST. При выборе этой опции данные отображаются специальным шрифтом (с размытым контуром и серого цвета), предотвращающим атаку TEMPEST, поскольку такой текст плохо читаем на оборудовании захвата излучений. При дешифровании электронная почта не может быть сохранена в расшифрованном формате. Эта опция доступна только при шифровании текста или текстовых файлов.

☐ **Conventional Encrypt** (Обычное шифрование). Установите этот флажок чтобы полагаться только на обычную парольную фразу, а не на криптографию с открытыми ключами. Файл шифруется сеансовым ключом, который шифрует(и дешифрует) с помощью парольной фразы, предлагаемой вам на выбор. **Self Decrypting Archive** (SDA, Само дешифрующийся архив).

Установите этот флажок, чтобы создать автоматически дешифрующийся исполняемый файл.

При отметке этого флажка файл шифруется с использованием сеансового ключа, который шифрует (и дешифрует) данные с помощью парольной фразы, которую пользователю предлагается указать. Итоговый исполняемый файл может быть дешифрован простым двойным щелчком и вводом надлежащей парольной фразы. Эта опция особенно удобна при отсылке зашифрованных файлов корреспондентам, у которых не установлена программа PGP. Имейте в виду, в этом случае отправитель и получатель должны использовать одинаковые операционные системы.

Если вы подписываете файлы, вам будет предложено ввести свою парольную фразу. Если после шифрования вы заглянете в папку, где находился исходный файл, вы обнаружите файл с заданным именем и расширением PGP.

Когда кто-нибудь присылает вам файл с зашифрованными данными, можно дешифровать содержимое и верифицировать любую приложенную подпись, чтобы убедиться, что данные присланы подлинным отправителем, а не подменены. Для шифрования своих файлов и папок используйте команду **Decrypt & Verify** (Дешифрование и верификация), доступную из меню значка PGP в системном лотке, панели инструментов **PGPtools** или меню **File** (Файл) диалога проводника Windows.

Чтобы зашифровать и/или верифицировать данные, которые были зашифрованы для вашего ключа, вы должны располагать своим закрытым ключом и парольной фразой. Если при шифровании файла был установлен флажок **Secure Viewer** (Защита просмотра), дешифрованный текст отображается на защищенном экране PGP специальным шрифтом (размытым и серого цвета), предотвращающим атаку TEMPEST. В противном случае сообщение отобразится в его исходном состоянии.

Чтобы открыть само дешифрующийся архив (архив SDA), щелкните дважды на исполняемом файле (с расширением .SDA.EXE). Введите корректный пароль и укажите местоположение, в котором следует сохранить дешифрованный файл.

Содержание работы.

1. Создание дайджеста сообщения программой PGP.
2. Передача открытого сообщения с контролем целостности.
3. Передача открытого сообщения с ЭЦП.

III. Заключительная часть – (5) мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач.

Дать задание для самостоятельной проработки. Повторить лекции.

Тема 7. Компьютерные системы в сфере государственного и муниципального управления

Практическое занятие № 8

Тема: Настройка политики IP-безопасности.

ЦЕЛИ ЗАНЯТИЯ:

Отработать практические навыки по установке политики IP-безопасности в ОС Windows 2000/XP.

УЧЕБНЫЕ ВОПРОСЫ:

- 1. Создание новой политики IP-безопасности.**
- 2. Изменение настроек политики IP-безопасности**

МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ:

Методическая разработка для проведения занятия

Вводная часть (10-15 мин.)

Проверка наличия готовности учебной группы к занятию (наличие конспектов; учебных пособий; ручек; линеек и т.д.).

Контрольный опрос

Если группа недостаточно подготовлена, то предоставить время на подготовку группы к занятию потом начать занятие. При необходимости закончить занятие в часы самоподготовки или выходной день, согласовав это с учебной частью.

II. Основная часть (150 мин).

- 1. Создание новой политики IP-безопасности.**

Система Windows 2000 позволяет создавать новую политику безопасности. Для этого можно воспользоваться мастером политики IP-безопасности. Вот как это делается.

1. Щелкните правой кнопкой мыши на записи **Политики безопасности IP** (IP Security Policies on Local Machine) в левой части консоли MMC (см. Рис. 1) и выберите в контекстном меню команду **Создать политику безопасности IP** (Create IP Security Policy). Эта команда отображает первый информационный диалог **Мастер политики IP-безопасности** (IP Security Policy Wizard); щелкните на кнопке **Далее** (Next).

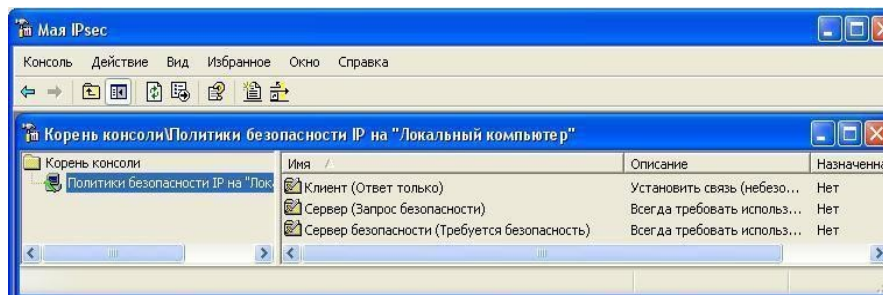


Рис. 1 Оснастка политики безопасности IP

2. В отобразившемся диалоге мастера (см. Рис. 2) укажите название создаваемой политики и укажите ее назначение. Щелкните на кнопке **Далее** (Next).

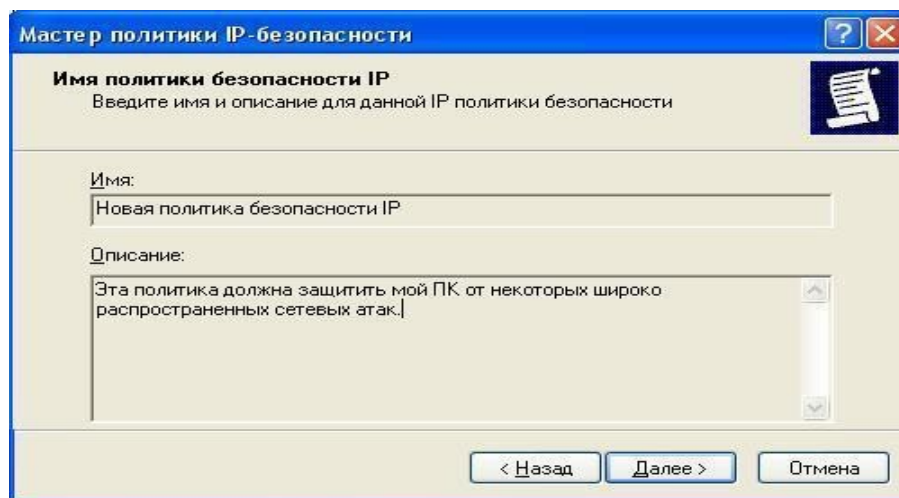


Рис. 2. Указание имени и назначения новой политики IP-безопасности

3. В отобразившемся диалоге (см. Рис. 3) укажите, должна ли новая политика использоваться по умолчанию. Оставьте отметку флажка. **Использовать правило по умолчанию** (Activate the Default Response Rule) и щелкните на кнопке **Далее** (Next).

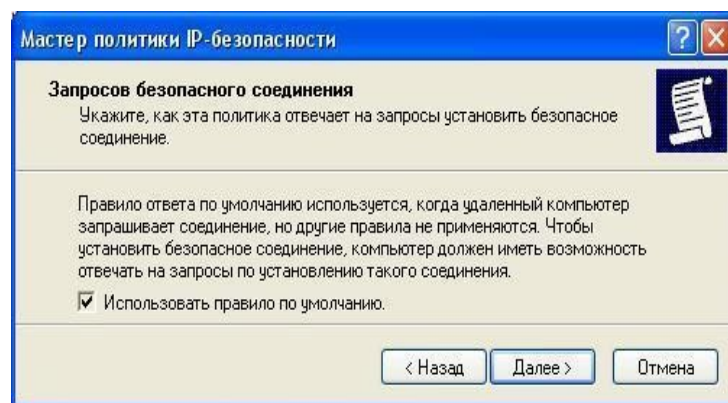


Рис. 3. Установка режима ответа на запросы об установлении безопасного соединения

4. В следующем диалоге мастера (см. Рис. 4) следует выбрать метод проверки подлинности подключаемого компьютера.

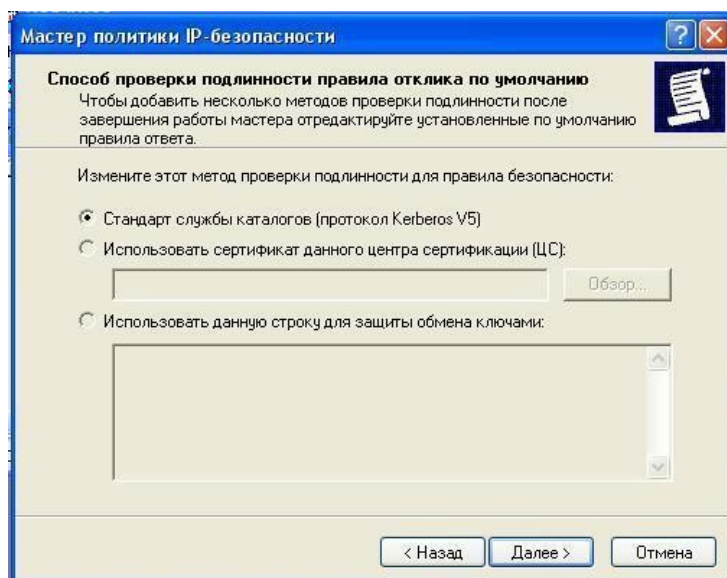


Рис. 4. Выбор метода аутентификации соединения

Мастер позволяет выбрать только один из следующих методов аутентификации.

Стандарт Windows 2000 (Kerberos v5) (Windows 2000 default (Kerberos v5 protocol)). Протокол Kerberos представляет собою стандартную технологию защиты системы Windows 2000. Этот метод годится аутентификации всех компьютеров, поддерживающих протокол **Kerberos v5** и входящих в доверяемый домен.

Использовать сертификат данного центра сертификации (Use a certificate front this certificate authority (CA)). В этом методе для аутентификации используются сертификаты (прошлый семестр - криптография). Применение данного метода требует предъявления сертификата открытого ключа, подтверждающий его подлинность. Для использования такого метода необходимо настроить хотя бы один центр сертификации CA, которые мы обсуждали в прошлом семестре - лекция №6. Этот метод идентификации обычно используют для доступа к Интернету или для доступа к компьютерам, на которых не установлен протокол Kerberos v5.

Краткие сведения из лекции №6

Сертификаты открытых ключей

Сертификатом открытого ключа называют набор данных, удостоверяющих подлинность открытого ключа.

Сертифицированный ключ, хранимый в базе данных открытых ключей, содержит не только сам открытый ключ, но и информацию, идентификационную его владельца - имя, адрес проживания и некоторую другую.

Кроме того, ключ должен быть подписан доверенным лицом или организацией, обычно называемой *бюро сертификации* (CA - Certification Authority). Бюро CA подписывает как сам ключ, так информацию об его владельце, тем самым, заверяя, что идентификация лица, предъявившего сертификат, подлинна, и открытый ключ принадлежит именно этому лицу. Любой пользователь сертифицированного ключа перед его применением может проверить подлинность подписи бюро CA.

При организации инфраструктуры PKI для криптосистем с сертифицированными ключами следует решить следующие вопросы. Выбрать лицо, уполномоченное выдавать сертификаты, и определиться, кому их выдавать.

Ясно, что сертификаты могут выдавать только лица, действительно вызывающие доверие, и нужен какой-то механизм фильтрации подозрительных сертификатов. Один из способов решения

такой задачи - создание цепочек или деревьев передачи доверия, например, такого типа: одно центральное бюро СА сертифицирует открытые ключи других доверенных бюро СА, которые сертифицируют бюро СА организации, а бюро СА организации сертифицирует открытые ключи своих работников. Установить процедуру выдачи сертификата бюро СА. □

В идеальном случае, прежде чем бюро СА выдаст какому-либо лицу сертификат, этому лицу придется пройти процедуру идентификации. Кроме того, для защиты от компрометированных ключей, важно использовать какие-то метки времени или признаки срока действия сертификата. Соответствующих нескольким открытым ключам. Эти ключи могут иметь различное предназначение и длину, поэтому их хранение должно быть обеспечено с различной степенью надежности.

Операционная система Windows 2000 версий Server и Advanced Server обеспечивает средства организации инфраструктуры PKI для корпоративных сетей. Это большое достижение, поскольку в прошлом операционные системы Windows NT поддерживали устаревшие версии сервера сертификации, и фактически могли использовать сертификаты только в браузерах Интернета для проверки подлинности посещаемых Web-узлов.

Однако использование такой громоздкой инфраструктуры PKI может оказаться неэффективным, если, скажем, участники переговоров доверяют только своим друзьям или же вообще только самим себе и используют шифрование для частного общения.

В таком случае можно организовать инфраструктуру PKI на основе так называемых *доверительных отношений пользователей*, использованных в популярной программе шифрования PGP.

Доверительные отношения пользователей

В инфраструктуре PKI, опирающейся на доверительные отношения пользователей, подтверждение подлинности ключей возложено на *поручителей*, в роли которых выступают отдельные пользователи PKI, которым доверяют все прочие пользователи.

ПРИМЕР

Допустим, Джон и Боб доверяют Элен; тогда Элен для сертификации своего открытого ключа может попросить у Джона и Боба подписать свой ключ. После такого подписания Элен для Доказательства другому пользователю, например Джеку, подлинности своего ключа, Может предъявить ему подписи Джона и Боба, и, если Джек доверяет Джону и Бобу, он будет доверять и Элен.

Перед подписанием чужих открытых ключей поручителям, чтобы пресечь попытки подмены ключей, приходится как-то идентифицировать владельцев ключей, требуя скажем, личной встречи или связываясь с ними по телефону.

Преимущество

Отсутствие официального бюро СА, которому должны доверять все

Недостатки

отсутствие у такой подписи юридической силы; □

- возможно возникновение ситуации, когда два переговорщика не будут иметь общих поручителей. □

Использовать данную строку для защиты обмена ключами (Use This string to protect the key exchange (preshared key)). В этом методе аутентификация проводится на основе предварительно оговоренного секретного ключа. В качестве ключа можно использовать слово или фразу, заранее оговоренную обоими пользователями. Microsoft не рекомендует использовать этот метод, поскольку ключ хранится в политике IPsec в открытом виде и для его защиты следует ограничить доступ к политике IPsec.

5. Выберите метод и щелкните на кнопке **Далее** (Next); отобразится завершающий

диалог мастера с флажком, предлагающим открыть окно свойств созданной политики. Оставьте флажок на месте и щелкните на кнопке **Готово** (Finish). Отобразится диалог настройки свойств политики IP-безопасности (см. Рис. 5).

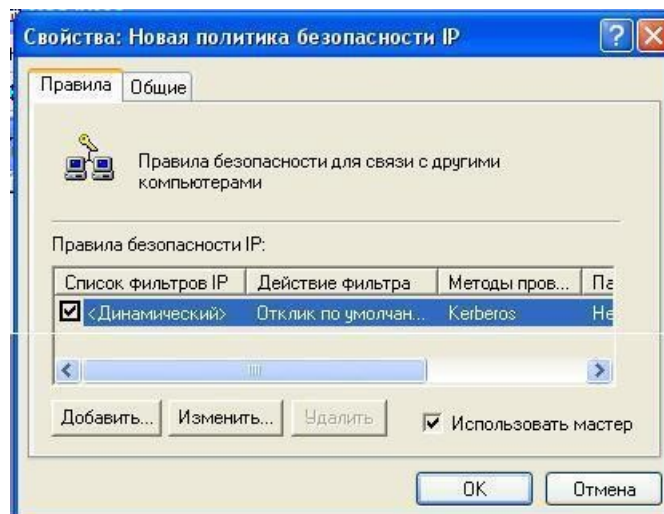


Рис. 5. Диалог настройки параметров политики IP-безопасности

2. Изменение настроек политики IP-безопасности

Для изменения настроек политики IP-безопасности можно либо щелкнуть на кнопке **Изменить** (Edit) и откорректировать параметры в отобразившемся диалоге, либо воспользоваться мастером, который автоматически запускается при отмеченном флажке **Использовать мастер** (Use Add Wizard).

Этот мастер позволяет упростить процедуры настройки, которые достаточно сложны и требуют углубленного понимания принципов функционирования политики IP-безопасности. – Рекомендуется поэкспериментировать.

Полученный результат в системе Windows 2000 необходимо просмотреть с помощью программы ipsecmon, предназначенной для мониторинга защищенных соединений IP.

Для просмотра диалога монитора IP-безопасности, введите в диалог **Запуск программы** (Run) команду ipsecmon и просмотрите отобразившийся диалог. Средства IP-безопасности представляют собою мощную, современную технологию защиты, призванную стать основным инструментом защиты сетевых соединений. Однако запуск и настройка IPsec требуют профессиональной подготовки и знаний в области организации сетей TCP/IP на основе компьютеров Windows 2000, и, в принципе, технология IP-безопасности предназначена для защиты больших и сложных корпоративных сетей. Для более простых сетей существуют более простые способы защиты сетевых коммуникаций, которые, тем не менее, не уступают по эффективности технологии IPsec. Один из таких способов состоит в применении приложения PGP, которое мы уже рассматривали в лекциях 7 и 8 прошлого семестра.

III. Заключительная часть – (5) мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач.

Дать задание для самостоятельной проработки. Повторить лекции.

III. Заключительная часть – (5) мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач.

Дать задание для самостоятельной проработки. Повторить лекции.

Лабораторное занятие №

Тема: Установка политики IP-безопасности. ЦЕЛИ ЗАНЯТИЯ:

Отработать практические навыки по установке политики IP-безопасности в ОС Windows 2000/XP.

УЧЕБНЫЕ ВОПРОСЫ:

1. **Установка политики IP-безопасности. КОНТРОЛЬНЫЕ ВОПРОСЫ:**

1. Семиуровневая модель взаимодействия компьютеров.
2. Адресация персональных компьютеров в сети Интернет.
3. Протокол TCP/IP.
4. Базовые протоколы прикладного уровня модели TCP/IP.
5. Средства Winsock. Протокол NetBT. Разрешение имен хостов.
6. Базовые протоколы межсетевого уровня модели TCP/IP.

МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ:

Вводная часть (10-15 мин.)

Проверка наличия готовности учебной группы к занятию (наличие конспектов; учебных пособий; ручек; линеек и т.д.).

Контрольный опрос

Если группа недостаточно подготовлена, то предоставить время на подготовку группы к занятию потом начать занятие. При необходимости закончить занятие в часы самоподготовки или выходной день, согласовав это с учебной частью.

II. Основная часть (150 мин).

Политику IP-безопасности можно установить для локального компьютера, домена или для всех доменов активного каталога. В системе Windows2000/XP политика IP-безопасности устанавливается с помощью оснастки

Управление политикой безопасности IP (IP Security Policy) в консоли MMC (Microsoft Management Console).

Для открытия оснастки **Управление политикой безопасности IP** необходимо выполнить следующие шаги.

1. Щелкните указателем мыши на кнопке **Пуск (Start)**; на экране появится главное Windows 2000.
2. Выберите из меню пункт **Выполнить (Run)**; на экране отобразится диалог **Выполнить (Run)**.
3. Введите **mmc /a** и далее нажмите клавишу **ОК**. Отобразится диалог консоли **MMC**.
4. Щелкните на меню **Консоль (Console)** и выберите пункт **Добавить/Удалить оснастку (Add/Remove Snap-in)**.
5. В появившемся на экране диалоге **Добавить/Удалить оснастку (Add/Remove Snap in)** щелкните на кнопке **Добавить (Add)**. Отобразится диалог **Добавить изолированную оснастку (Add Standalone Snap-in)**.
6. Прокрутите список **Доступные изолированные оснастки (Available Standalone Snap-ins)** и выберите оснастку **Управление политикой безопасности IP (IP Security Policy Management)**.
7. Щелкните на кнопке **Добавить (Add)**; на экране появится диалог **Выбор компьютера (Select Computer)** (см. Рис. 1).

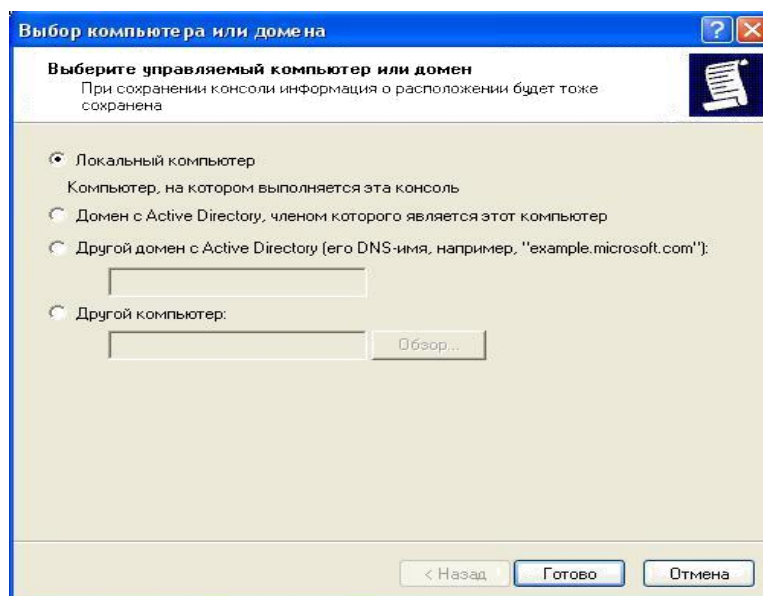


Рис. 1. Диалог выбора компьютера для применения политики IP-безопасности

8. Оставьте без изменения установленный по умолчанию переключатель **Локальный компьютер** (Local computer) и щелкните на кнопке **Готово** (Finish). Остальные возможности позволяют управлять политикой IP-безопасности для домена с данным компьютером, других доменов или других компьютеров домена.

9. Щелкните на кнопке **Заккрыть** (Close) для закрытия диалога **Выбор изолированной оснастки**.

10. Щелкните на кнопке ОК для закрытия диалога **Добавить/Удалить оснастку** (Add Standalone Snap-in). В диалоге консоли **ММС** отобразится добавленная оснастка (Рис. 2).

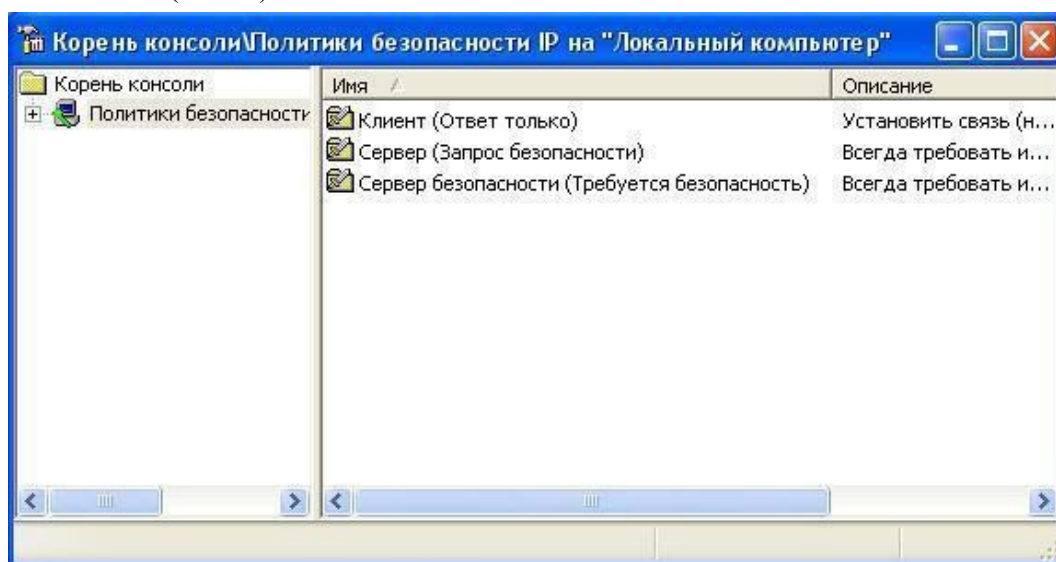


Рис. 2. Оснастка политики безопасности IP

11. Щелкните на меню **Консоль** (Console) и далее на пункте **Сохранить** (Save). В отобразившемся диалоге сохранения файлов введите имя созданной консоли, скажем **MyIPsec**, и щелкните на кнопке **ОК**.

В правой части диалога Рис. 2 отображены три установленных по умолчанию политики IP-безопасности. Эти политики сгруппированы в соответствии с функциональным предназначением компьютеров. **Клиент (Только ответ)** (Client (Respond Only)). Компьютеры с такой политикой IPsec могут только отвечать (но не запрашивать) на запросы установления защищенного соединения.

Сервер (запрос безопасности) (Server (Request Security)). Компьютеры с такой политикой запрашивают защиту устанавливаемого соединения, однако в случае неудачи согласования безопасности устанавливают незащищенное соединение. Такая политика полезна при наличии в сети устаревших компьютеров.

Безопасность сервера (требовать безопасность) (Secure Server (Require Security)). Компьютеры, поддерживающие эту политику, не взаимодействуют с компьютерами, не поддерживающими защищенное соединение. Если при установлении соединения согласование безопасности закончится неудачей или если подсоединяемый компьютер не поддерживает IPsec, соединение не устанавливается.

12. Чтобы задействовать нужную политику IP-безопасности, щелкните правой кнопкой мыши на нужной записи в правой части диалога консоли (см. Рис. 2) и в отобразившемся контекстном меню выберите команду **Назначить** (Assign). Для отключения назначенной политики щелкните правой кнопкой мыши на строке назначенной политики и выберите в контекстном меню команду **Снять** (Un-assign).

III. Заключительная часть – (5) мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач.

Дать задание для самостоятельной проработки. Повторить лекции.

Тема 8. Современная постановка задачи защиты информации. Организационно-правовое обеспечение информационной безопасности

Практическое занятие № 9

Тема: Настройка параметров безопасности Web-браузера.

ЦЕЛИ ЗАНЯТИЯ:

Отработать практические навыки по настройке параметров безопасности Web-браузера ОС Windows 2000/XP.

УЧЕБНЫЕ ВОПРОСЫ:

3. Настройка параметров безопасности Web-браузера.

МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ:

Методическая разработка для проведения занятия

Вводная часть (10-15 мин.)

Проверка наличия готовности учебной группы к занятию (наличие конспектов; учебных пособий; ручек; линеек и т.д.).

Контрольный опрос

Если группа недостаточно подготовлена, то предоставить время на подготовку группы к занятию потом начать занятие. При необходимости закончить занятие в часы самоподготовки или выходной день, согласовав это с учебной частью.

II. Основная часть (70 мин).

Для настройки параметров безопасности браузера IE версий 5 и 6 выполнит такую пошаговую процедуру.

Запустите приложение IE 5 и выберите команду меню **Сервис - Свойства обозревателя (Tools - Internet Options)**.

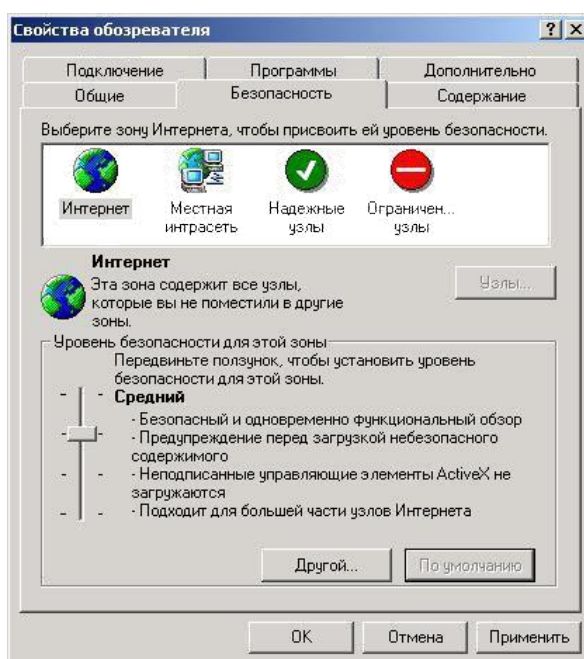


Рис. 1. Диалог настройки системы безопасности браузера IE 5

В отобразившемся диалоге **Свойства обозревателя** (Internet выберите вкладку **Безопасность** (Security), представленную на Рис. 1.

Для настройки параметров безопасности Интернета щелкните на пиктограмме Интернет (Internet) сверху вкладки **Безопасность** (Security), и либовоспользуйтесь предварительно настроенными уровнями безопасности, либосоздайте свои правила безопасности.

Для выбора предварительно настроенного уровня безопасности передвиньте ползунковый регулятор в разделе **Уровень безопасности для этой зоны** (Security level for this zone) в нужную позицию; по умолчанию для браузера IE 5 установлен средний уровень, пригодный для посещения большинства сайтов. Для ручной настройки правил безопасности щелкните на кнопка (Custom level). Отобразится диалог **Правила безопасности** (SecuritySettings), представленный на Рис. 2.

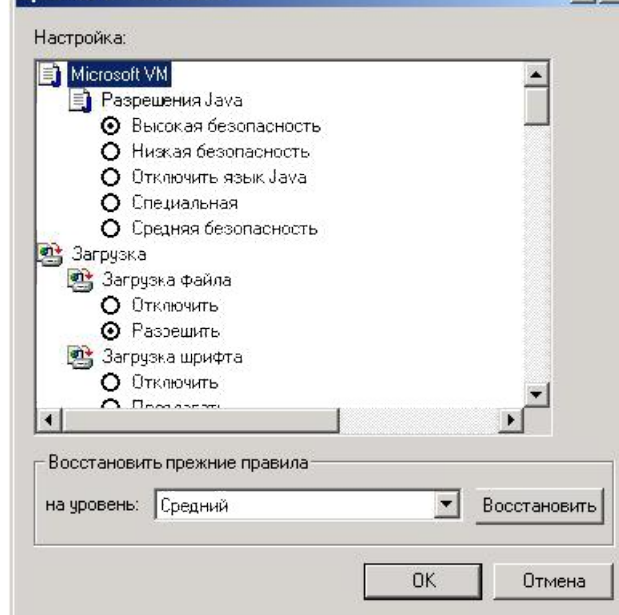


Рис. 2. Диалог настройки параметров безопасности Интернета

Правила безопасности (Security Settings) для большинства параметров можно выбрать три значения - **Отключить** (Disable), **предлагать** (Prompt) и **разрешить** (Enable), означающие, соответственно, блокирование операции, предварительное отображение сообщения и разрешение операции. Просмотрите список параметров и выберите для них подходящие значения. Диалог **Правила безопасности** (Security Settings) предоставляет в разделе

Восстановить прежние правила (Reset custom settings) список на уровень (Resetto) и кнопку. **Восстановить** (Reset). **Вы** можете выбрать один из уровней безопасности и откорректировать его параметры. Щелкните на кнопке **ОК** и вернитесь в диалог **Свойства обозревателя** (Internet Options), которое теперь выглядит так, как показано на Рис. 3.

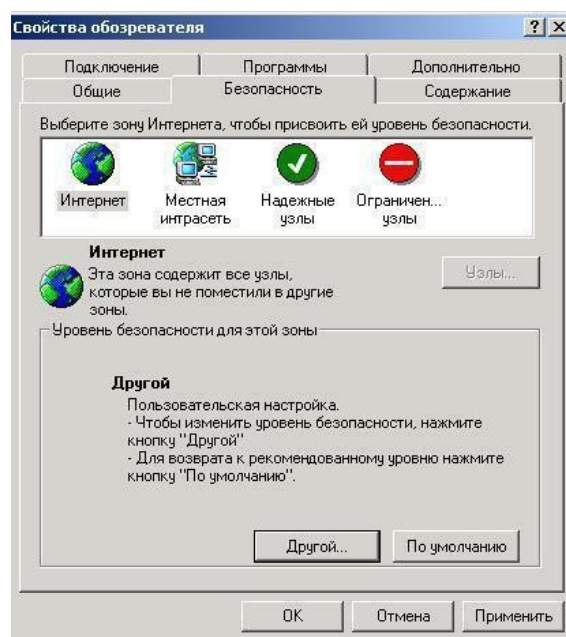


Рис. 3. Теперь вкладка настройки безопасности отображает пользовательские настройки

Если требуется, вы можете создать списки узлов, которые вы считаете небезопасными и, наоборот, которым вы доверяете, воспользовавшись вкладкой **Безопасность** (Security). Для создания списка надежных узлов выполните следующие действия. Выберите пиктограмму **Надежные узлы** (Trusted sites) сверху вкладки.

Безопасность (Security) и щелкните на кнопке **Узлы** (Sites). Отобразится диалог **Надежные узлы** (Trusted sites), представленный на Рис. 4.

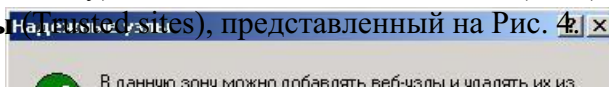


Рис. 4. Диалог создания списка надежных узлов

Которые обеспечивают для связи сокет SSL (Secure Sockets Layer - про-

токол защищенных сокетов). Для задания такого режима установите флажок. **Для всех узлов этой зоны требуется проверка серверов (https)** (Require server verification (https:) for all sites in this zone). Теперь в создаваемый список сайтов могут войти только те, которые поддерживают протокол HTTPS.

Сокеты SSL гарантируют безопасную передачу данных по Интернету, используя криптографическую систему с открытым ключом, шифрующую передаваемые данные надежным алгоритмом. Серверы Интернета, поддерживающие сокет SSL, используют протокол HTTPS (Hyper Text Transmission Protocol, Secure -протокол защищенной передачи гипертекстов); соответственно, адреса URL таких серверов начинаются с записи https://.

Введите адрес добавляемого сайта в поле **Добавить узел в зону** (Add this Web-sites to the zone) и щелкните на кнопке **Добавить** (Add). Адрес сайта отобразится в списке **Веб-узлы** (Web sites).

При щелчке на поле **Добавить узел в зону** (Add this Web-sites to zone) в поле отобразится список посещенных узлов, адреса которых хранятся в кэше памяти браузера. При необходимости их можно выбирать и пополнять список узлов зоны.

Для удаления сайта из списка **Веб-узлы** (Web sites) выберите адрес сайта из списка **Веб-узлы** (Web sites) и щелкните на кнопке **Удалить**

После создания списка надежных Web-сайтов щелкните на кнопке **ОК** и вернитесь во вкладку **Безопасность**

С помощью тех же методов, что и для зоны Интернета, настройте параметры безопасности зоны надежных Web-сайтов.

Для создания списка ненадежных сайтов выполните следующие действия.

На вкладке **Безопасность** (Security) диалога **Свойства обозревателя** (Internet Options) щелкните на пиктограмме **Ограниченные узлы** (Restricted sites).

1. Щелкните мышью на кнопке **Узлы** (Sites); отобразится диалог **Ограниченные узлы** (Restricted sites), представленный на Рис. 5.

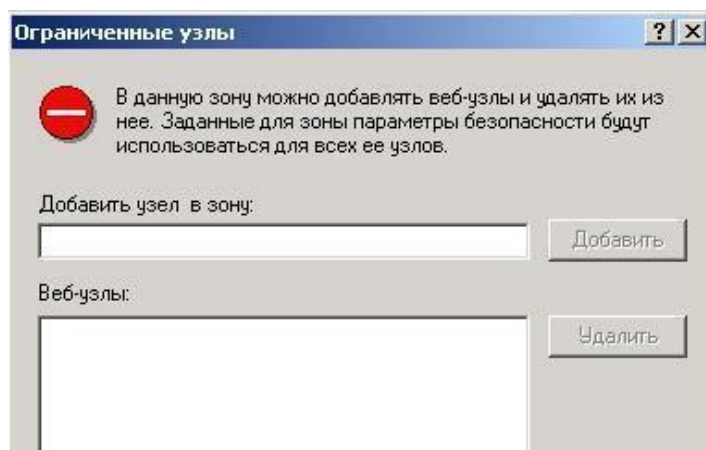


Рис. 5. Диалог пополнения списка ненадежных Web-сайтов

Введите в поле. **Добавить узел в зону** (Add this Web site to the zone) адрес ненадежного Web-сайта и щелкните на кнопке **Добавить** (Add). Введенный адрес отобразится в списке **Веб-узлы** (Web sites). сайта из списка ненадежных узлов выберите адрес узла из списка **Веб-узлы** (Web sites) и щелкните мышью на кнопке **Удалить** (Delete)

С помощью тех же методов, что и для зоны Интернета, настройте параметры безопасности зоны ненадежных Web-сайтов.

Вывод

Выполнив настройку параметров безопасности браузера можно значительно уменьшить угрозы, связанные с загрузкой из Web документов HTML со злонамеренными сценариями и апплетами, поскольку, исследования показывают, что большинство уязвимостей браузера проявляется лишь при установлении низкого уровня безопасности.

III. Заключительная часть – (5) мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач.

Дать задание для самостоятельной проработки. Повторить лекции.

III. Заключительная часть – (5) мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач.

Дать задание для самостоятельной проработки. Повторить лекции.

Тема 9. Анализ угроз информационной безопасности
Практическое занятие №10

Тема: **Инструменты управления, настройка брандмауэров.**

ЦЕЛИ ЗАНЯТИЯ:

Отработать практические навыки по настройке инструментов управления работы брандмауэров.

УЧЕБНЫЕ ВОПРОСЫ:

- 1. Настройка параметров системы выявления вторжений.**
- 2. Настройка параметров брандмауэра.**

МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ:

Методическая разработка для проведения занятия

Вводная часть (10-15 мин.)

Проверка наличия готовности учебной группы к занятию (наличие конспектов; учебных пособий; ручек; линеек и т.д.).

Контрольный опрос

Если группа недостаточно подготовлена, то предоставить время на подготовку группы к занятию потом начать занятие. При необходимости закончить занятие в часы самоподготовки или выходной день, согласовав это с учебной частью.

II. Основная часть (150 мин).

1. Настройка параметров системы выявления вторжений. Установка приложения.

Инсталляция приложения BlackICE Defender не вызывает никаких проблем, и после ее выполнения на панели задач появляется значок, означающий функционирование приложения. Для запуска приложения BlackICE щелкните на значке, после чего отобразится диалог.

Закрытие диалога не останавливает работу программы BlackICE - для этого необходимо выполнить команду **Tools - Stop BlackICE Engine** (Инструменты - Остановить исполнение BlackICE). После остановки значок приложения BlackICE на панели инструментов отображается перечеркнутым красной линией.

При обнаружении атаки приложение BlackICE автоматически блокирует доступ хакерского компьютера к защищаемому компьютеру. Однако не все выявленные программой события появления подозрительных пакетов (или, как говорят, события безопасности) являются настоящей атакой - подчас, сложности обнаружения атак приводят к ложному срабатыванию системы IDS. Для управления степенью "тревожности" приложения BlackICE пользователю предоставляется возможность настройки параметров защиты, позволяющих определить "параноидальное" и "доверчивое" поведение системы IDS.

Настройка параметров.

1. Выберите команду **Tools - Edit BlackICE Settings** (Инструменты- Настройка параметров BlackICE). Отобразится диалог **BlackICE Settings** (Параметры BlackICE) с множеством вкладок. Выберите вкладку **Firewall** (Брандмауэр).

2. В зависимости от своих предпочтений выберите одну из четырех позиций переключателя в группе Protection Level (Уровень безопасности): Paranoid (Параноидальный) - блокировка всего подозрительного трафика, Nervous (Нервный) - блокировка большей части подозрительного трафика, Cautious (Осторожный) - блокирование небольшой части подозрительного трафика, Trusting (Доверчивый) - разрешение всего входящего трафика.

Три флажка внизу вкладки Firewall (Брандмауэр) позволяют задать следующие режимы: **Enable Auto-Blocking** (Разрешить автоматическое блокирование) – отметка этого флажка приведет к автоматическому блокированию всех попыток атак компьютера. Рекомендуем оставить отметку этого флажка (режим задан по умолчанию). **Allow Internet file sharing** (Разрешить общий доступ к файлам из Интернета) - разрешает общий доступ к файлам и папкам компьютера всем остальным компьютерам локальной сети и из Интернета. Не отмечайте этот флажок.

Allow NetBIOS Neighborhood (Разрешить запросы соседей NetBIOS) - позволяет обращаться к защищаемому компьютеру из локальной сети по его IP- адресу и отображаться в

папке Network Neighborhood (Соседние компьютеры) проводника Windows. Не отмечайте этот флажок - в главе 13 будет показано, насколько опасными могут быть сеансы связи по протоколу NetBIOS.

Управление блокированием атак

Приложение BlackICE Defender не выполняет автоматического блокирования узлов, инициировавших атаку на компьютер. Режим автоматического блокирования, заданный в параметрах настройки, выполняет блокирование только активных в текущий момент хостов, представляющих прямую угрозу компьютеру. Однако пользователь может вручную указать приложению BlackICE правило обработки запросов, подозрительных на попытку вторжения. Для этого выполните следующие операции.

1. Откройте вкладку **Intruders** (Вторжения) главного диалога BlackICE и щелкните на строке сообщения о вторжении правой кнопкой мыши, отобразив контекстное меню.

2. Выберите нужную команду из контекстного меню:

Для блокирования вторжения выберите команду **Block Intruder** (Блокировать вторжение), и в отобразившемся контекстном меню выберите период времени блокирования - **For a Hour** (На час), **For a Day** (На день), **For a Month** (На месяц), **Forever** (Навсегда).

Для разрешения доступа выберите команду **Trust Intruder** (Разрешить вторжение) и в отобразившемся подменю выберите время действия разрешения.

С помощью других команд контекстного меню можно выполнить операции **Cut** (Вырезать), **Copy** (Копировать), **Delete** (Удалить) над выделенной строкой (или строками). Можно, также, выбрать все строки командой **Select All** (Выбрать все), найти нужную строку командой **Find** (Поиск) нужной строки и напечатать выделенные строки командой **Print** (Печать).

События безопасности и предыстория

На вкладке **Events** (События) приложение BlackICE отображает сообщения обо всех выявленных событиях безопасности, подозрительных на попытки вторжения.

Каждая строка содержит сведения о событии: в столбце **Time** (Время) указано время возникновения события, в столбце **Event** (Событие) - краткое описание события, в столбце **Intruder** (Злоумышленник) - IP-адрес хоста, с которого пришел подозрительный пакет, а в столбце **Count** (Счетчик) указано число попыток вторжений. В списке внизу диалога приводится краткое описание вторжения - в данном случае, сообщается о возможной попытке взлома DNS-сервера.

Вкладка **History** (Предыстория), содержит графическое представление событий безопасности и сетевого трафика, поступающего на данный локальный компьютер.

Переключатели в разделе **Interval** (Интервал) позволяют указать промежуток времени наблюдения событий и трафика, отображаемых на графиках. Предысторию выявленных вторжений можно также просмотреть в диалоге **BlackICE Advanced Firewall Settings** (Дополнительные параметры брандмауэра BlackICE) дополнительных свойств брандмауэра, открываемого выбором команды **меню Tools - Advanced Firewall Settings** (Инструменты - Дополнительные параметры брандмауэра).

Кнопка **Options** (Параметры) внизу диалога **BlackICE Advanced Firewall Settings** (Дополнительные параметры брандмауэра BlackICE) позволяет установить режим выдачи предупреждений перед исчерпанием времени блокирования атаки. Другие кнопки - **Add** (Добавить), **Delete** (Удалить) и **Modify** (Изменить) позволяют, соответственно, добавить, удалить и модифицировать описание и параметры выделенной атаки.

III. Заключительная часть – (5) мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач.

Дать задание для самостоятельной проработки. Повторить лекции

Тема 10. Причины, виды и каналы утечки информации.

Тема 11. Стратегии защиты информации. Методы обеспечения информационной безопасности. Способы и средства защиты информации

Тема 12. Киберугрозы. Киберденьги. Криптовалюта Bitcoin. Понятие электронных денег.

Тема 13. Цифровая экономика.

Практическое занятие №11

Тема: Использование ключей PGP.

ЦЕЛИ ЗАНЯТИЯ:

Отработать практические навыки по настройке использования ключей PGP.

УЧЕБНЫЕ ВОПРОСЫ:

- 3. Включение ключа в сообщение е-почты.**
- 4. Проверка подлинности ключа.**
- 5. Подписание ключа.**
- 6. Шифрование е-сообщений.**

МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ:

Методическая разработка для проведения занятия

Вводная часть (10-15 мин.)

Проверка наличия готовности учебной группы к занятию (наличие конспектов; учебных пособий; ручек; линеек и т. д.).

Контрольный опрос

Если группа недостаточно подготовлена, то предоставить время на подготовку группы к занятию потом начать занятие. При необходимости закончить занятие в часы самоподготовки или выходной день, согласовав это с учебной частью.

II. Основная часть (70 мин).

- 1. Включение ключа в сообщение е-почты.**

Порядок действий.

1. Откройте утилиту PGPkey.
2. Создайте ключ, как указано в ЛР4.
3. Присоедините файл ключа к почтовому сообщению.

2. Проверка подлинности ключа.

Порядок действий.

1. Откройте утилиту PGPkey и выделите ключ, который необходимо проверить.
2. Выберите команду СВОЙСТВА в меню keys.
3. Необходимо проверить совпадение набора слов в текстовом поле ЦИФРОВОЙ ОТПЕЧАТОК с оригиналом, например, переданным по телефону. ИЛИ
4. Проверить совпадение набора 20 16-тиричных символов поле ЦИФРОВОЙ ОТПЕЧАТОК с оригиналом, например, переданным по телефону.

3. Подписание ключа.

1. Откройте утилиту PGPkey и выделите ключ который необходимо подписать.
2. Выберите команду Sing в меню keys или щёлкните на значке Sing на панели PGPkey.
3. В отобразившемся диалоге Sing Keys в текстовом поле отобразиться открытый ключ и его цифровой отпечаток.
4. Щелкните на More Choices (дополнительно) отобразиться диалог, в котором необходимо конфигурировать параметры подписи см. лекцию 18.

4. Шифрование e-сообщений.

Создать сообщение, зашифровать и подписать средствами PGP.

III. Заключительная часть – (5) мин.

Контроль усвоения материала.

Дать оценку подготовленности группы к занятию, оценить полноту и качество отработанных задач.

Дать задание для самостоятельной проработки. Повторить лекции

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Основы информационной безопасности»
для студентов направления подготовки
10.03.01 Информационная безопасность
Направленность (профиль)
«Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)»

1. Общие сведения о дисциплине

Цель дисциплины «Основы информационной безопасности» — заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучение методов и средств обеспечения информационной безопасности, методов нарушения конфиденциальности, целостности и доступности информации.

Для выполнения задач достаточно базовых знаний из курсов математического анализа, линейной алгебры, дискретной математики.

Виды занятий и способы контроля

В соответствии с учебными планами направления подготовки бакалавров 10.03.01 дисциплина «Основы информационной безопасности» включает следующие виды занятий:

1. лекции
2. практические занятия;
3. самостоятельная работа студентов.

Составляющие дисциплину, и разбираются примеры практических задач. Практические занятия направлены на закрепление лекционного материала. Самостоятельная работа студентов заключается в подготовке к практическим и лекционным занятиям и выполнении домашних заданий, выдаваемых преподавателем по каждому из разделов дисциплины.

В целях лучшего понимания сути представления и обработки информации при защите рекомендуется использовать гипотетическую модель информации, что позволит использовать архитектурные особенности, свойственные конкретным моделям анализа. Примеры следует выбирать так, чтобы вычисления были не слишком громоздкими. Следует рассматривать задачи, возникающие в самых различных отраслях и показать динамику решения задач: как подойти к решению конкретной проблемы, какие ограничения возникают в рамках данного решения и какие результаты получаются в конечном счете. В идеальном случае процесс обучения должен происходить следующим образом: студент слушает лекции, читает учебную литературу, работает дома и на практических занятиях. Студенту рекомендуется иметь доступ к компьютеру во время самостоятельной работы для выполнения индивидуальных заданий.

Подготовка к каждой работе производится во внеаудиторное время. В самостоятельную работу входит выполнение индивидуальных заданий. Преподаватель принимает решение о допуске студента к практической работе по

результатам собеседования. Студенты знакомятся с общими сведениями, порядком выполнения работы, пишут необходимые пояснения в соответствии с полученным вариантом задания. При защите работы студент отвечает преподавателю на контрольные вопросы,

представляет теоретическую часть решения задачи, практический расчет.

Учебно-методические материалы по дисциплине

Основная литература

1. Семкин С.Н., Семкин А.Н. Основы информационной безопасности объектов обработки информации. Научно-практическое пособие. – Орел: 2000. – 300с.
2. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: "Инкомбук", 1997. – 540с.
3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. М.: Энергоатомиздат –1994
4. Хоффман Л.Дж. Современные методы защиты информации / Пер. с англ. - М.: Советское радио, 1980
5. Грушко А.А., Тимонина Е.Е. Теоретические основы защиты информации. Изд-во агентства "Яхтсмен", 1996
6. Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.: ил.

Дополнительная литература

1. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов / П.Ю.Белкин, О.О. Михальский, А.С. Першаков и др. – М.: Радио и связь, 2000. – 168 с.: ил.
2. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Уч. пособие для вузов /Проскурин В.Г., Крутов С.В., Мацкевич И.В. – М.: радио и связь, 2000. – 168с
3. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ – Санкт- Петербург, 2000. – 384 с.: ил.
4. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика. Электроинформ 1997
5. Гайкович В.Ю., Першин А.Ю. Безопасность электронных банковских систем. М.: Единая Европа, 1994

4. Введение

Теория защиты информации определяется как система основных идей, относящихся к защите информации, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

Составные части теории являются:

1. полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты;

2. систематизированные результаты анализа развития теоретических исследований и разработок, а также опыта практического решения задач защиты;

3. научно обоснованная постановка задачи защиты информации в современных системах ее обработки, полно и адекватно учитывающая текущие и перспективные концепции построения систем и технологий обработки, потребности в защите информации и объективные предпосылки их удовлетворения;

4. общие стратегические установки на организацию защиты информации, учитывающие все многообразие потенциально возможных условий защиты;

5. методы, необходимые для адекватного и наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные прикладные методы решения;

6. методологическая и инструментальная база, содержащая необходимые методы и инструментальные средства для решения любой совокупности задач защиты в рамках любой выбранной стратегической установки;

7. научно обоснованные предложения по организации и обеспечению работ по защите информации;

8. научно обоснованный прогноз перспективных направлений развития теории и практики защиты информации.

Информационная безопасность определяется способностью государства, общества, личности:

1. обеспечивать с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;

2. противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;

3. вырабатывать личностные и групповые навыки и умения безопасного поведения;

4. поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

5. Обеспечение противодействия информационному оружию

Рисунок 1

Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
ОПК-1 ИД-1 ОПК-1 ИД-2 ОПК-1 ИД-3	Самостоятельное изучение литературы	Лабораторные работы	16.00	2.00	18.00
ОПК-1 ИД-1 ОПК-1 ИД-2 ОПК-1 ИД-3	Подготовка к экзамену	Изучение лекций	16.00	2.00	18.00
Итого			32.00	4.00	36.00

4.1 Современная постановка задачи защиты информации

Комплексность — решение в рамках единой концепции двух или более разноплановых задач (целевая комплексность), или использование для решения одной и той же задачи разноплановых инструментальных средств (инструментальная комплексность), или то и другое (всеобщая комплексность).

Целевая комплексность означает, что система информационной безопасности должна строиться следующим образом:

1. защита информации, информационных ресурсов и систем личности, общества государства от внешних и внутренних угроз;
2. защита личности, общества и государства от негативного информационного воздействия.

Инструментальная комплексность подразумевает интеграцию всех видов и направлений ИБ для достижения поставленных целей. В рамках прежнего представления о защите информации практически независимо развивались четыре вида защиты: организационная (режим секретности), техническая (противодействие техническим средствам разведки), криптографическая и обеспечение компьютерной безопасности. При этом имело место дублирование решаемых задач.

Структурная комплексность предполагает обеспечение требуемого уровня защиты во всех элементах системы обработки информации.

Функциональная комплексность означает, что методы защиты должны быть направлены на все, выполняемые функции системы обработки информации. *Временная комплексность* предполагает непрерывность осуществления мероприятий по защите информации как в процессе непосредственной ее обработки, так и на всех этапах жизненного цикла объекта

обработки информации.

Требования к системе защиты информации:

1. Система защиты информации должна быть представлена как нечто целое. Целостность системы будет выражаться в наличии единой цели ее функционирования, информационных связей между элементами системы, иерархичности построения подсистемы управления системой защиты информации.

2. Система защиты информации должна обеспечивать безопасность информации, средств информации и защиту интересов участников информационных отношений и невозможности несанкционированного доступа злоумышленника к защищаемой информации.

3. Система защиты информации в целом, применяемые методы и средства защиты должны быть по возможности "прозрачными" для законного пользователя, не создавать ему больших дополнительных неудобств, связанных с процедурами доступа к информации.

4. Система защиты информации должна обеспечивать оценку угроз внешних дестабилизирующих факторов и защиту от них.

5. Угрозы информации

Угроза информации – возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию.

Виды угроз. Основные нарушения:

1. Физической целостности (уничтожение, разрушение элементов).
2. Логической целостности (разрушение логических связей).
3. Содержания (изменение блоков информации, внешнее навязывание ложной информации).
4. Конфиденциальности (разрушение защиты, уменьшение степени защищенности информации).
5. Прав собственности на информацию (несанкционированное копирование, использование).

Три наиболее выраженные угрозы:

1. подверженность физическому искажению или уничтожению;
2. возможность несанкционированной (случайной или злоумышленной) модификации;
3. опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

Характер происхождения угроз

Умышленные факторы:

1.1. хищение носителей информации;

1.2. подключение к каналам связи;

1.3. перехват ЭМИ;

1.4. несанкционированный доступ;

1.5. разглашение информации;

1.6. копирование данных.

2. Естественные факторы:

2.1. несчастные случаи (пожары, аварии, взрывы);

2.2. стихийные бедствия (ураганы, наводнения, землетрясения);

2.3. ошибки в процессе обработки информации (ошибки пользователя, оператора, сбои аппаратуры).

Источники угроз

Понимается непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию.

люди;

технические устройства; модели, алгоритмы, программы;

технологические схемы обработки; внешняя среда.

Предпосылки появления угроз

1. объективные (количественная или качественная недостаточность элементов системы) — причины, не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

2. субъективные — причины, непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

Несанкционированный доступ — получение лицами в обход системы защиты с помощью программных, технических и других средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации.

Разглашение информации ее обладателем есть умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к не вызванному служебной необходимостью оглашению охраняемых сведений, в также передача таких сведений по открытым техническим каналам или обработка на не категорированных ЭВМ.

Утечку информации в общем плане можно рассматривать как бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена.

Система защиты информации — совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

5.1 Классы каналов несанкционированного получения информации:

1.1. Хищение носителей информации.

1.2. Копирование информации с носителей (материально-вещественных, магнитных и т.д.).

1.3. Подслушивание разговоров (в том числе аудиозапись).

1.4. Установка закладных устройств в помещение и съем информации с их помощью.

1.5. Выведывание информации обслуживающего персонала на объекте.

1.6. Фотографирование или видеосъемка носителей информации внутри помещения.

1.7. Снятие информации с устройств электронной памяти.

1.8. Установка закладных устройств в СОИ.

1.9. Ввод программных продуктов, позволяющих злоумышленнику получать информацию.

1.10. Копирование информации с технических устройств отображения (фотографирование с мониторов и др.)

3.1. Получение информации по акустическим каналам (в системах вентиляции, теплоснабжения, а также с помощью направленных микрофонов).

1. Получение информации по виброакустическим каналам (с использованием акустических датчиков, лазерных устройств).

2. Использование технических средств оптической разведки (биноклей, подзорных труб и т.д.).

3. Использование технических средств оптико-электронной разведки (внешних телекамер, приборов ночного видения и т.д.).

4. Осмотр отходов и мусора.

5. Выведывание информации у обслуживающего персонала за пределами объекта.

6. Изучение выходящей за пределы объекта открытой информации (публикаций, рекламных проспектов и т.д.).

7. Электромагнитные излучения СОИ (ПЭМИ, паразитная генерация усилительных

каскадов, паразитная модуляция высокочастотных генераторов низкочастотным сигналом, содержащим конфиденциальную информацию).

8. Электромагнитные излучения линий связи.
9. Подключения к линиям связи.
10. Снятие наводок электрических сигналов с линий связи.
11. Снятие наводок с системы питания.
12. Снятие наводок с системы заземления.
13. Снятие наводок с системы теплоснабжения.
14. Использование высокочастотного навязывания.
15. Снятие с линий, выходящих за пределы объекта сигналов образованных на технических средствах за счет акустоэлектрических преобразований.

16. Снятие излучений оптоволоконных линий связи.
17. Подключение к базам данных и ПЭВМ по компьютерным сетям.

1.11 Причины нарушения целостности информации

1.1. Субъективные преднамеренные.

☐ Диверсия (организация пожаров, взрывов, повреждений электропитания и др.).

☐ Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации).

Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействия на психику личности психотропным оружием).

1.2. Субъективные непреднамеренные.

1. Отказы обслуживающего персонала (гибель, длительный выход из строя).
2. Сбои людей (временный выход из строя).
3. Ошибки людей.

2.1. Объективные непреднамеренные.

1. Отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

2. Сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

3. Стихийные бедствия (наводнения, землетрясения, ураганы).

4. Несчастные случаи (пожары, взрывы, аварии).

5. Электромагнитная несовместимость.

6. Методы и модели оценки уязвимости информации

Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в автоматизированных системах обработки данных средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторам и нежелательного их воздействия на защищаемую информацию. Модель уязвимости информации в автоматизированных системах обработки данных в общем виде показано (рисунок 4).

Данная модель (рис.4 - Общая модель воздействия на информацию) детализируется при изучении конкретных видов уязвимости информации: нарушения физической или логической целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размножения.

При детализации общей модели основное внимание акцентируется на том, что подавляющее большинство нарушений физической целостности информации имеет место в процессе ее обработки на различных участках технологических маршрутов. При этом целостность информации зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход. Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов автоматизированных систем обработки данных), которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений автоматизированной системы обработки данных и их оборудования. Что касается злоумышленных действий, то они связаны, главным образом, с несанкционированным доступом к ресурсам автоматизированной системы обработки данных. При этом наибольшую опасность представляет занесение вирусов.

В соответствии с изложенным общая модель процесса нарушения физической целостности информации на объекте автоматизированной системы обработки данных может быть представлена (рисунок 5 Общая модель процесса нарушения физической целостности информации).

С точки зрения несанкционированного получения информации принципиально важным является то обстоятельство, что в современных автоматизированных системах обработки данных оно возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей. Воздействие случайных факторов непосредственно не ведет к несанкционированному получению информации, оно лишь способствует появлению каналов несанкционированного получения информации, которыми может воспользоваться злоумышленник. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных для самого общего случая представлена:

Злоумышленные действия

Внешняя неконтролируемая зона

Зона контролируемой территории

Зона помещений

Зона ресурсов

Зона баз данных

Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных

Выделенные зоны определяются следующим образом:

1. внешняя неконтролируемая зона — территория вокруг автоматизированной системы обработки данных, на которой персоналом и средствами автоматизированной системой обработки данных не применяются никакие средства и не осуществляется никакие мероприятия для защиты информации;
2. зона контролируемой территории — территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных;
3. зона помещений автоматизированной системы обработки данных внутренне пространство тех помещений, в которых расположена система;
4. зона ресурсов автоматизированной системы обработки данных — та часть помещений, откуда возможен непосредственный доступ к ресурсам системы;
5. зона баз данных — та часть ресурсов системы, с которых возможен непосредственный доступ к защищаемым данным.

Злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон. При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий: нарушитель должен получить доступ в соответствующую зону; во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий канал несанкционированного получения информации; соответствующий канал несанкционированного получения информации должен быть доступен нарушителю соответствующей категории; в канале несанкционированного получения информации в момент доступа к нему нарушителя должна находиться защищаемая информация.

Рассмотрим далее трансформацию общей модели уязвимости с точки зрения несанкционированного размножения информации. Принципиальными особенностями этого процесса являются:

1. любое несанкционированное размножение есть злоумышленное действие;
2. несанкционированное размножение может осуществляться в организациях-разработчиках компонентов автоматизированной системы обработки данных, непосредственно в автоматизированной системе обработки данных и сторонних организациях, причем последние могут получать носитель, с которого делается попытка снять копию как законным, так и

незаконным путем.

Попытки несанкционированного размножения информации у разработчика и в автоматизированной системе обработки данных есть один из видов злоумышленных действий с целью несанкционированного ее получения и поэтому имитируются приведенной моделью. Если же носитель с защищаемой информацией каким-либо путем (законным или незаконным) попал в стороннюю организацию, то для его несанкционированного копирования могут использоваться любые средства и методы, включая и такие, которые носят характер научных исследований и опытно- конструкторских разработок.

В процессе развития теории и практики защиты информации сформировалось три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.

2.1 Эмпирический подход к оценке уязвимости информации.

Сущность эмпирического подхода заключается в том, что на основе длительного сбора и обработки данных о реальных проявлениях угроз информации и о размерах того ущерба, который при этом имел место, чисто эмпирическим путем устанавливаются зависимости между потенциально возможным ущербом и коэффициентами, характеризующими частоту проявления соответствующей угрозы и значения имевшего при ее проявлении размера ущерба.

Наиболее характерным примером моделей рассматриваемой разновидности являются модели, разработанные специалистами американской фирмы IBM. Рассмотрим развиваемые этих моделях подходы.

Исходной посылкой при разработке моделей является почти очевидное предположение: с одной стороны, при нарушении защищенности информации наносит некоторый ущерб, с другой, обеспечение защиты информации сопряжено с расходом средств. Полная ожидаемая стоимость защиты может быть выражена суммой расходов на защиту и на потерь от ее нарушения. Совершенно очевидно, что оптимальным решением было бы выделение на защиту информации средств в размере $C_{опт}$, поскольку при этом обеспечивается минимизация общей стоимости защиты информации.

Для того, чтобы воспользоваться данным подходом к решению проблемы, необходимо, во-первых, знать (или уметь определять) ожидаемые потери при нарушении защищенности информации, а во-вторых, в зависимость между уровнем защищенности и средствами, затрачиваемыми на защиту информации.

Решение первого вопроса, т.е. оценки ожидаемых потерь при нарушении защищенности информации, принципиально может быть получено лишь тогда, когда речь идет о защите промышленной, коммерческой и им подобной тайны, хотя и здесь встречаются весьма серьезные трудности. Что касается оценки уровня потерь при нарушении статуса защищенности информации, содержащей государственную, военную и им подобную тайну, то здесь до настоящего времени строгие подходы к их получению не найдены. Данное обстоятельство существенно сужает возможную область использования моделей, основанных на рассматриваемых подходах.

Для определения уровня затрат, обеспечивающих требуемый уровень защищенности информации, необходимо по крайней мере знать, во-первых, полный перечень угроз информации, во-вторых, потенциальную опасность для информации для каждой из угроз и, в третьих, размеры затрат, необходимых для нейтрализации каждой из угроз.

$$10^{(S_i V_i - 4)}$$

Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту состоит в том, что этот уровень должен быть равен уровню ожидаемых потерь при нарушении защищенности, достаточно определить только уровень потерь. Специалистами фирмы IBM предложена следующая эмпирическая зависимость ожидаемых потерь от i -й угрозы информации:

Где S_i — коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы; V_i — коэффициент, характеризующий значение возможного ущерба при ее возникновении. Предложенные специалистами значения коэффициентов:

Значения коэффициента S_i

Таким образом, если бы удалось собрать достаточное количество фактических данных о проявлениях угроз и их последствиях, то рассмотренную модель можно было бы использовать для решения достаточно широкого круга задач защиты информации, причем, нетрудно видеть, что модель позволяет не только находить нужные решения, но и оценивать их точность. По России такая статистика в настоящее время практически отсутствует. В США же, например, сбору и обработке указанных данных большое внимание уделяет целый ряд учреждений (Стенфордский исследовательский институт и др.). В результате уже получены достаточно представительные данные по целому ряду угроз, которые могут быть положены в основу ориентировочных расчетов и для других стран.

2.2 Система с полным перекрытием

Естественным продолжением моделей оценки угроз автоматизированных систем обработки данных являются модели нейтрализации этих угроз, т.е. модели защиты. Наиболее общей моделью защиты является модель так называемой *системы с полным перекрытием*.

При построении данной модели в качестве исходной взята естественная посылка, состоящая в том, что в механизме защиты должно содержаться по крайней мере одно средство для перекрытия любого потенциально возможного канала утечки информации. Методика формального описания такой системы заключается в следующем:

1. составляется полный перечень объектов O системы, подлежащих защите;
2. составляется полный перечень потенциально возможных угроз T информации, т.е. возможных вариантов злоумышленных действий;
3. составленные таким образом множества объединяются в двудольный граф с соблюдением условия: ребро $\langle t_i, o_j \rangle$ существует только тогда, когда угрозой t_i является реальной

для объекта o_j ;

4. для каждого ребра в графе определяется количественная мера соответствующей угрозы для соответствующего объекта;
 5. формируется множество M средств защиты информации в вычислительной системе;
 6. определяется количественная мера возможности противодействия
- превышает уровень угрозы, то соответствующее ребро графа исключается. Очевидно, что если множество M такое, что устраняются все ребра графа, то такая система является системой с полным перекрытием.

Одной из разновидностей теоретически строгих моделей являются модели систем разграничения доступа к ресурсам автоматизированной системы обработки данных

В самом общем виде существо этих моделей может быть представлено следующим образом. Автоматизированная система обработки данных является системой множественного доступа, т.е. к одним и тем же ее ресурсам (техническим средствам, программам, массивам данных) имеет законное право обращаться некоторое число пользователей (абонентов). Если какие-либо из указанных ресурсов являются защищаемыми, то доступ к ним должен осуществляться лишь при предъявлении соответствующих полномочий. Система разграничения доступа и должна стать тем механизмом, который регулирует такой доступ. Требования к этому механизму на содержательном уровне состоят в том, что, с одной стороны, не должен быть разрешен доступ пользователям (или их процессам), не имеющим на это полномочий, а с другой — не должно быть отказано в доступе пользователям (или их процессам), имеющим соответствующие полномочия.

7. Рекомендации по использованию моделей оценки уязвимости информации

Как правило, модели позволяют определять текущие и прогнозировать будущие значения всех показателей уязвимости информации для любых компонентов автоматизированной системы обработки данных, любой их комбинации и для любых условий жизнедеятельности автоматизированной системы обработки данных. Некоторые замечания по использованию: 1) практически все модели строятся в предположении независимости тех случайных событий, совокупности которых образуют сложные процессы защиты информации в современных автоматизированных системах обработки данных; 2) для обеспечения работы моделей необходимы большие объемы таких исходных данных, подавляющее большинство которых в настоящее время отсутствует, а формирование сопряжено с большими трудностями.

Определим замечание первое — допущение независимости случайных событий, происходящих в системах защиты информации. Основными событиями, имитируемыми в моделях определения показателей уязвимости, являются: проявление дестабилизирующих факторов, воздействие проявившихся дестабилизирующих факторов на защищаемую информацию и воздействие используемых средств защиты на дестабилизирующие факторы. При этом обычно делаются следующие допущения:

1. потенциальные возможности проявления каждого дестабилизирующего фактора не зависят от проявления других;
2. каждый из злоумышленников действует независимо от других, т.е. не учитываются возможности формирования коалиции злоумышленников;
3. негативное воздействие на информацию каждого из проявившихся дестабилизирующих факторов не зависит от такого же воздействия других проявившихся факторов;
4. негативное воздействие дестабилизирующих факторов на информацию в одном каком-либо компоненте автоматизированной системы обработки данных может привести лишь к поступлению на входы связанных с ним компонентов информации с нарушенной защищенностью и не оказывает влияния на такое же воздействие на информацию в самих этих компонентах;
5. каждое из используемых средств защиты оказывает нейтрализующее воздействие на

В действительности же события, перечисленные выше являются зависимыми, хотя степень зависимости различна: от незначительной, которой вполне можно пренебречь, до существенной, которую следует учитывать. Однако для решения данной задачи в настоящее время нет необходимых предпосылок, поэтому остаются лишь методы экспертных оценок.

Второе замечание касается обеспечения моделей необходимыми исходными данными. Ранее уже неоднократно отмечалось, что для практического использования моделей определения показателей уязвимости необходимы большие объемы разнообразных данных, причем подавляющее большинство из них в настоящее время отсутствует.

Сформулируем теперь рекомендации по использованию моделей, разработанных в рамках рассмотренных ранее допущений, имея в виду, что это использование, обеспечивая решение задач анализа, синтеза, и управления в системах защиты информации, не должно приводить к существенным погрешностям.

Первая и основная рекомендация сводится к тому, что моделями должны пользоваться квалифицированные специалисты-профессионалы в области защиты информации, которые могли бы в каждой конкретной ситуации выбрать наиболее эффективную модель и критически оценить степень адекватности получаемых решений.

Вторая рекомендация заключается в том, что модели надо использовать не просто для получения конкретных значений показателей уязвимости, а для оценки поведения этих значений при варьировании существенно значимыми исходными данными в возможных диапазонах их изменений. В этом плане модели определения значений показателей уязвимости могут служить весьма ценным инструментом при проведении деловых игр по защите информации.

Третья рекомендация сводится к тому, что для оценки адекватности моделей, исходных данных и получаемых решений надо возможно шире привлекать квалифицированных и экспертов.

Четвертая рекомендация заключается в том, что для эффективного использования моделей надо непрерывно проявлять заботу об исходных данных, необходимых для обеспечения моделей

при решении задач защиты. Существенно важным при этом является то обстоятельство, что подавляющее количество исходных данных обладает высокой степенью неопределенности. Поэтому надо не просто формировать необходимые данные, а перманентно их оценивать и уточнять.

Методы определения требований к защите информации

В самом общем виде и на чисто прагматическом уровне требования к защите могут быть определены как предотвращение угроз информации, по крайней мере тех из них, проявление которых может привести в существенно значимым последствиям. Но поскольку, как рассматривалось раньше защита информации есть случайный процесс (показатели уязвимости носят вероятностный характер), то и требования к защите должны выражаться терминами и понятиями теории вероятностей.

По аналогии с требованиями к надежности технических систем, обоснованными в классической теории систем, требования к защите могут быть сформулированы в виде условия:

$P_z \geq P_{zt}$

где P_z — вероятность защищенности информации, а P_{zt} — требуемый уровень защищенности. С требованиями, выраженными в таком виде, можно оперировать с использованием методов классической теории систем при решении задач защиты всех классов: анализа, синтеза и управления.

Однако на предыдущих лекциях рассматривалось, что решение проблем защиты информации сопряжено с исследованиями и разработкой таких систем и процессов, в которых и конкретные методы, и общая идеология классической теории могут быть применены лишь с большими оговорками. Для повышения степени адекватности применяемых моделей реальным процессам необходим переход от концепции создания инструментальных средств получения необходимых решений на инженерной основе к концепции создания методологического базиса и инструментальных средств для динамического оптимального управления соответствующими процессами.

С учетом данного подхода в самом общем виде и на содержательном уровне требования к защите информации могут быть сформулированы в следующем виде.

Конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации, определяются совокупностью следующих факторов:

1. характером обрабатываемой информации;
2. объемом обрабатываемой информации;
3. продолжительностью пребывания информации в автоматизированной системе обработки данных;
4. структурой автоматизированной системы обработки данных;
5. видом защищаемой информации;

6. технологией обработки информации;
7. организацией информационно-вычислительного процесса в автоматизированной системе обработки данных;
8. этапом жизненного цикла автоматизированной системы обработки данных.

По характеру (с точки зрения требуемой защиты) информацию можно разделить на общедоступную, конфиденциальную, служебную, секретную и совершенно секретную.

Соответствующими рекомендации по предъявлению требований к защите могут быть следующими:

1. При обработке общедоступной информации никаких специальных мер защиты от несанкционированного доступа не требуются.

2. Требования к защите конфиденциальной информации определяет пользователь, устанавливающий статус конфиденциальности.

3. При обработке служебной информации к ней должен быть обеспечен свободный доступ пользователям учреждения-владельца этой информации (по общему списку); доступ же пользователей, не включенных в общий список, должен осуществляться по разовым санкциям, выдаваемым пользователями, включенным в список.

4. При обработке секретной информации в зависимости от ее объема и характера

а. может быть предъявлен один из следующих вариантов требований:

5. персональное разграничение — для каждого элемента информации составляется список пользователей, имеющих к нему право доступа;

6. коллективное разграничение — структура баз защищаемых данных организуется в соответствии со структурой подразделений, участвующих в обработке защищаемой информации; пользователи каждого подразделения имеют право доступа к только к "своим" данным.

- При обработке совершенно секретной информации список лиц, имеющих право доступа, должен составляться для каждого самостоятельного элемента информации с указанием дней и времени доступа, а также перечня разрешенных процедур.

Требования, обуславливаемые размещением *объемов защищаемой информации*, могут заключаться в следующем.

При обработке информации, размещенной только в ОЗУ, должны обеспечиваться требуемые уровень защиты и надежность в центральном вычислителе и на коммуникациях ввода-вывода данных. При обработке информации, размещенной на одном внешнем носителе, дополнительно к предыдущему должна обеспечиваться защита в соответствующем устройстве ВЗУ и коммуникациях, связывающих это устройство с процессором.

При обработке информации, размещенной на нескольких внешних носителях, дополнительно к предыдущему должна обеспечиваться необходимая изоляция друг от друга

данных, размещенных на различных носителях при одновременной их обработке.

При обработке информации, размещенной на очень большом количестве носителей, дополнительно к предыдущему должна обеспечиваться защита в хранилищах носителей и на коммуникациях, связывающих хранилища с помещениями, в которых установлены ВЗУ.

точки зрения *продолжительности пребывания защищаемой информации*

Информация разового использования подлежит защите в процессе подготовки, ввода, решения задач и выдачи результатов решения. После этого защищаемая информация должна быть уничтожена во всех устройствах автоматизированной системы обработки данных.

Информация временного хранения дополнительно к предыдущему подлежит защите в течение объявленного времени хранения, после чего должна быть уничтожена во всех устройствах автоматизированной системы обработки данных и на всех носителях, используемых для ее хранения. Продолжительность хранения задается или длиной промежутка времени, или числом сеансов решения соответствующих функциональных задач.

Информация длительного хранения подлежит постоянной защите, уничтожение ее должно выполняться по определенным командам.

Требования, определяемые *структурой* автоматизированной системы обработки данных, могут быть сформулированы в следующем виде.

Информация должна защищаться во всех структурных элементах автоматизированной системы обработки данных, причем специфические требования к защите информации в структурных элементах различного типа сводятся к следующему.

1. в терминалах пользователей:

— защищаемая информация может находиться только во время сеанса решения задач, после чего подлежит уничтожению;

— устройства отображения и фиксации информации должны располагаться так, чтобы исключить возможность просмотра отображаемой (выдаваемой) информации со стороны;

— информация, имеющая ограничительный гриф, должна выдаваться (отображаться) совместно с этим грифом;

— должны быть предусмотрены возможности быстрого (аварийного) уничтожения информации, находящейся в терминале (в том числе и на устройствах отображения).

при выдаче информации в линии связи должны осуществляться:

1) проверка адреса выдачи информации;

2) маскировка (закрытие) содержания защищаемой информации, выдаваемой в линии связи, проходящей по неконтролируемой территории;

• должны быть предусмотрены возможности аварийного уничтожения информации как в ОЗУ, так и в ВЗУ, а также подачи команды на аварийное уничтожение информации в сопряженных с УГВВ терминалах.

3. В аппаратуре и линиях связи:

- защищаемая информация должна находиться только в течение сеанса; в ЗУ аппаратуры связи могут храниться только служебные части передаваемых сообщений;
- линии связи, по которым защищаемая информация передается в явном виде, должны находиться под непрерывным контролем во время передачи информации;
- перед началом каждого сеанса передачи защищаемой информации должна осуществляться проверка адреса выдачи данных;
- при передаче большого объема защищаемой информации проверка адреса передачи должна периодически производиться в процессе передачи (через заданный промежуток времени или после передачи заданного числа знаков сообщения);
- при наличии в составе аппаратуры связи процессоров и ЗУ должна вестись регистрация данных обо всех сеансах передачи защищаемой информации;
- должны быть предусмотрены возможности аварийного уничтожения информации, находящейся в аппаратуре связи.

1. устройства отображения и фиксации информации должны располагаться так, чтобы исключить возможность просмотра отображаемой (выдаваемой) информации со стороны;

2. информация, имеющая ограничительный гриф, должна выдаваться (отображаться) совместно с этим грифом;

3. при обработке защищаемой информации должно осуществляться установление подлинности всех участвующих в обработке устройств и пользователей, и ведение протоколов их работы;

4. всякое обращение к защищаемой информации должно проверяться на санкционированность;

5. при обмене защищаемой информации, осуществляемом с использованием линий связи, должна осуществляться проверка адреса корреспондента;

5. должны быть предусмотрены возможности аварийного уничтожения всей информации, находящейся в центральном вычислителе, и подачи команды на аварийное уничтожение информации в сопряженных устройствах.

6. Во внешних запоминающих устройствах:

7. сменные носители информации должны находиться на устройствах управления в течение минимального времени, определяемого технологией автоматизированной обработки информации;

8. устройства управления ВЗУ, на которых установлены носители с защищаемой информацией, должны иметь замки, предупреждающие несанкционированное изъятие или замену носителя;

9. должны быть предусмотрены возможности автономного аварийного уничтожения

информации на носителях, находящихся на устройствах ВЗУ.

10. В хранилище носителей:

11. все носители, содержащие защищаемую информацию, должны иметь четкую и однозначную маркировку, которая, однако, не должна раскрывать содержания записанной на них информации;

12. носители, содержащие защищаемую информацию, должны храниться таким образом, чтобы исключались возможности несанкционированного доступа к ним;

13. при выдаче и приемке носителей должна осуществляться проверка личности получающего (сдающего) и его санкции на получение (сдачу) этих носителей;

14. должны быть предусмотрены возможности аварийного уничтожения информации на носителях, находящихся в

15. а специальных регистрационных журналах должны фиксироваться время обработки информации, исполнители, идентификаторы использованных носителей и возможно другие необходимые данные;

16. распределение работ между операторами должно быть таким, чтобы минимизировать осведомленность их о содержании обрабатываемой информации;

17. должны быть предусмотрены возможности аварийного уничтожения информации, находящейся в подразделениях подготовки данных.

18. Требования к защите информации, обуславливаемые территориальной распределенностью автоматизированной системы обработки данных, заключаются в следующем:

а. В компактных автоматизированных системах обработки данных (размещенных в одном помещении) достаточно организовать и обеспечить требуемый уровень защиты в пределах того помещения, в котором размещены элементы автоматизированной системы обработки данных;

б. В слабо распределённых автоматизированных системах обработки данных (размещенных в нескольких помещениях, но на одной и той же территории)

дополнительно к предыдущему должна быть обеспечена требуемая защита информации в линиях связи, с помощью которых сопрягаются элементы автоматизированной системы

обработки данных, расположенные в различных помещениях, для чего должны быть или постоянный контроль за этими линиями связи, или исключена передача по ним защищаемой информации в явном виде;

в сильно распределённых автоматизированных системах обработки данных (размещенных на нескольких территориях) дополнительно к предыдущему должна быть обеспечена требуемая защита информации в линиях связи большой протяженности, что может быть достигнуто предупреждением передачи по ним защищаемой информации в открытом виде.

Требования, обуславливаемые *видом защищаемой информации*, могут быть сформулированы в таком виде.

1. К защите документальной информации предъявляются следующие требования: - должна обеспечиваться защита как оригиналов документов, так и сведений о них, накапливаемых и обрабатываемых в автоматизированной системе обработки данных; - применяемые средства и методы защиты должны выбираться с учетом необходимости обеспечения доступа пользователям различных категорий:

- 1) персонала делопроизводства и библиотеки оригиналов;
- 2) специалистов подразделения первичной обработки документов;

2. специалистов функциональных подразделений автоматизируемых органов. 11. При обработке фактографической быстроменяющейся информации должны учитываться требования:

3. применяемые средства и методы защиты не должны существенно влиять на оперативность обрабатываемой информации;

4. □ применяемые средства и методы защиты должны выбираться с учетом обеспечения доступа к защищаемой информации строго ограниченного круга лиц. К защите фактографической исходной информации предъявляются требования: каждому пользователю должны быть обеспечены возможности формирования требований к защите создаваемых им массивов данных в пределах предусмотренных в автоматизированной системе обработки данных возможностей защиты; - в системе защиты должны быть предусмотрены средства, выбираемые и используемые пользователями для защиты своих массивов по своему усмотрению.

К защите фактографической регламентной информации предъявляются требования: применяемые средства и методы защиты должны быть рассчитаны на длительную и надежную защиту информации; должен обеспечиваться доступ (в пределах полномочий) широкого круга пользователей; повышенное значение приобретают процедуры идентификации, опознавания, проверки полномочий, регистрации обращений и контроля выдачи.

Требования, обуславливаемые *технологическими* *схемами автоматизированной обработки информации*, сводятся к тому, что активном состоянии автоматизированной системы обработки данных должна обеспечиваться защита на всех технологических участках автоматизированной обработки информации и во всех режимах.

С точки зрения *организации вычислительного процесса в автоматизированной системе обработки данных* требуемая защита должна обеспечиваться при любом уровне автоматизации обработки информации, при всех способах взаимодействия пользователей со средствами автоматизации и при всех режимах работы комплексов средств автоматизации.

Специфические требования к защите для различных уровней автоматизации обработки информации состоят в следующем:

1. прием потока запросов и входной информации;
2. формирование пакетов и очередей запросов;
3. диспетчирование в ходе выполнения запросов;
4. регулирование входного потока информации.

В зависимости от способа взаимодействия пользователя с комплексом средств автоматизации предъявляются следующие специфические требования:

- при автоматизированном вводе информации должны быть обеспечены условия, исключающие несанкционированное попадание информации одного пользователя (абонента) в массив другого, причем должны быть обеспечены возможности фиксирования и документального закрепления момента передачи информации пользователя банку данных автоматизированной системы обработки данных и содержания этой информации;

- при неавтоматизированном вводе должна быть обеспечена защита на неавтоматизированных коммуникациях "Пользователь — автоматизированная система обработки данных", на участках подготовки данных и при вводе с местных устройств группового ввода-вывода;

- при пакетном выполнении запросов пользователей должно исключаться размещение в одном и том же пакете запросов на обработку информации различных ограничительных грифов;

1. при обработке запросов пользователей в реальном масштабе времени данные, поступившие от пользователей, и данные, подготовленные для выдачи пользователям, в ЗУ автоматизированной системы обработки данных должны группироваться с ограничительным грифом, при этом в каждой группе должен быть обеспечен уровень защиты, соответствующий ограничительному грифу данных группы. Зависимости от режимов функционирования комплексов средств автоматизации предъявляются следующие специфические требования:

2. в однопрограммном режиме работы в процессе выполнения программы должны предупреждаться:

3. несанкционированное обращение к программам;

4. несанкционированный ввод данных для решаемой задачи;

5. несанкционированное прерывание выполняемой программы;

6. несанкционированная выдача результатов решения;

7. в мультипрограммном режиме сформулированные раньше требования относятся к каждой из выполняемых программ и дополнительно должно быть исключено несанкционированное использование данных одной программы другой;

8. в мультипроцессорном режиме сформулированные выше требования должны обеспечиваться одновременно во всех участвующих в решении задачи процессорах, кроме того, должно быть исключено несанкционированное вклинивание в вычислительный процесс при распараллеливании и при диспетчеризации мультипроцессорного выполнения программ.

Требования, обуславливаемые *этапом жизненного цикла* автоматизированной системы обработки данных, формулируются так:

1. на этапе создания автоматизированной системы обработки данных должно быть обеспечено соответствие возможностей защиты требованиям к защите информации, сформулированным в задании на проектирование, кроме того, должно быть исключено несанкционированное включение элементов (блоков) в компоненты автоматизированной системы обработки данных (особенно системы защиты);

2. на этапе функционирования автоматизированной системы обработки данных в пассивном ее состоянии должна быть обеспечена надежная защита хранящейся информации и исключены возможности несанкционированных изменений компонентов системы;

3. на этапе функционирования автоматизированной системы обработки данных в активном ее состоянии дополнительно к сформулированным раньше требованиям должна быть обеспечена надежная защита информации во всех режимах автоматизированной ее обработки.

Так могут быть представлены общие рекомендации по формированию требований к защите

информации. Нетрудно видеть, что приведенные раньше требования хотя и содержат полезную информацию, но недостаточны для выбора методов и средств защиты информации в конкретной автоматизированной системе обработки данных.

Последовательность решения задачи должна быть следующей:

1. разработка методов оценки параметров защищаемой информации;
2. формирование перечня и классификация факторов, влияющих на требуемый уровень защиты информации;
3. структуризация возможных значений факторов;
4. структуризация поля потенциально возможных вариантов сочетаний значений факторов (вариантов условий защиты);
5. оптимальное деление поля возможных вариантов на типовые классы;
6. структурированное описание требований к защите в пределах выделенных классов.

1. Анализ существующих методик определения требований к защите информации

Проблема определений к защите информации в автоматизированных системах ее обработки возникла практически одновременно с самой проблемой защиты, т.е. когда средства ЭВТ стали применяться для обработки конфиденциальной информации. При этом оказалось, что для ее решения нет сколько-нибудь адекватного аналога, поскольку в условиях бумажной информатики вопросы защиты информации решались преимущественно организационными средствами. Система защиты строилась таким образом, чтобы возможности несанкционированного получения защищаемой информации практически были исключены. В условиях же автоматизированной обработки существует большое количество таких каналов несанкционированного получения информации, которые не могут быть перекрыты без применения специфических технических и программно-аппаратных средств. Соответственно возникла необходимость определения требований к системам защиты, содержащим указанные средства. Задача оказалась достаточно сложной, в силу чего регулярная методика ее решения до настоящего времени не разработана.

В сложившейся ситуации наиболее подходящим оказался подход, основанный на выделении некоторого количества типовых систем защиты с четким обозначением тех механизмов защиты, которые должна содержать каждая из типовых систем, и разработке рекомендаций по их использованию.

1.1 Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США"

Наиболее известным документом, четко определяющим критерии, по которым должна оцениваться защищенность вычислительных систем, и те механизмы защиты, которые должны использоваться в системах обработки секретной (конфиденциальной — в более общей постановке) информации, является так называемая "Оранжевая книга", представляющая собой стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах

министерства обороны США" (Trusted Computer Systems Evaluation Criteria — TCSEC), принятый в 1983 году. Его принятию предшествовали пятнадцатилетние исследования, проводившиеся специально созданной рабочей группой и национальным бюро стандартов США.

Стандартом предусмотрено шесть фундаментальных требований, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии — в каждой группе по два требования следующего содержания.

1. Стратегия.

Требование 1 — стратегия обеспечения безопасности: необходимо иметь явную и хорошо определенную стратегию обеспечения безопасности.

Требование 2 — маркировка: управляющие доступом метки должны быть связаны с объектами.

2. Подотчетность.

Требование 3 — идентификация: индивидуальные субъекты должны идентифицироваться.

Требование 4 — подотчетность: контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

3. Гарантии.

Требование 5 — гарантии: вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет достаточного уровня гарантий того, что система обеспечивает выполнение изложенных выше требований (с первого по четвертое).

Требование 6 — постоянная защита: гарантировано защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от "взламывания" и/или несанкционированного внесения изменений.

В зависимости от конкретных значений, которым отвечают автоматизированные системы, они разделены на четыре группы (D, C, B, A), которые названы так:

D — минимальная защита;

C — индивидуальная защита; B — мандатная защита;

A — верифицированная защита.

Группы систем делятся на классы, причем все системы, относимые к группе D, образуют один класс (D), к группе C — два класса (C1 и C2), к группе B

— три класса (B1, B2 и B3), к группе A — один класс (A1 с выделением части систем вне класса).

Ниже рассмотрим названия и краткую характеристику перечисленных классов:

D — минимальная защита — системы, подвергнутые оцениванию, но не отвечающие

требованиям более высоких классов;

C1 — защита, основанная на индивидуальных мерах — системы, обеспечивающие разделение пользователей и данных. Они содержат внушающие доверие средства, способные реализовать ограничения подоступу, накладываемые на индивидуальной основе, т.е. позволяющие пользователям иметь надежную защиту их информации и не дающие другим пользователям считывать или разрушать их данные. Допускается кооперирование пользователей по уровням секретности;

C2 — защита, основанная на управляемом доступе — системы, осуществляющие не только разделение пользователей как в системах C1, но и разделение их по осуществляемым действиям;

B1 — защита, основанная на присваивании имен отдельным средствам безопасности — системы, располагающие всеми возможностями систем класса C, и дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным (включая и выдаваемые за пределы системы) и средства мандатного управления доступом ко всем поименованным субъектам и объектам;

B2 — структурированная защита — системы, построенные на основе ясно определенной и формально задокументированной модели, с мандатным управлением доступом ко всем субъектам и объектам, располагающие усиленными средствами тестирования и средствами управления со стороны администратора системы;

B3 — домены безопасности — системы, монитор обращений которых контролирует все запросы на доступ субъектов к объектам, не допускающие несанкционированных изменений. Объем монитора должен быть небольшим вместе с тем, чтобы его состояние и работу можно было сравнительно легко контролировать и тестировать. Кроме того должны быть предусмотрены: сигнализация о всех попытках несанкционированных действий и восстановление работоспособности системы;

A1 — верификационный проект — системы, функционально эквивалентные системам класса B3, но верификация которых осуществлена строго формальными методами. Управление системой осуществляется по строго определенным процедурам. Обязательно введение администратора безопасности.

1.2 Руководящий документ Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации"

Аналогичный подход реализован и в руководящем документе Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации", выпущенном в 1992 году. В данном документе выделено девять классов защищенности автоматизированных систем от несанкционированного доступа к информации, а для каждого класса определен минимальный состав необходимых механизмов защиты и требования к содержанию защитных функций каждого из механизмов в каждом из классов систем.

Классы систем разделены на три группы, причем основным критерием деления на группы

приняты специфические особенности обработки информации, а именно:

Третья группа — системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности. К группе отнесены два класса, обозначенные 3Б и 3А;

Вторая группа — системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности. К группе отнесены два класса, обозначенные 2Б и 2А;

Первая группа — многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют различные права на доступ к информации. К группе отнесено пять классов: 1Д, 1Г, 1В, 1Б и 1А.

Требования к защите растут от систем класса 3Б к классу 1А.

Все механизмы защиты разделены на четыре подсистемы следующего назначения:

Содержание средств для каждой группы систем приведено в документе. Приведенная в руководящем документе Гостехкомиссии методика распространяется на защиту от несанкционированного доступа к информации, находящейся непосредственно в ЗУ ЭВМ и на сменных машиночитаемых носителях. Значительно раньше (1978г.) Гостехкомиссией были выпущены руководящие документы, определяющие требования к защите информации в автоматизированных системах от утечки по побочным электромагнитным излучениям и наводкам. При разработке названных требований учитывались следующие факторы:

доля грифовой информации в общем объеме обрабатываемой;

интенсивность обработки грифовой информации, выражаемая относительной долей времени ее обработки в течение суток;

условия расположения аппаратуры автоматизированной системы.

Наличие рассмотренных методик и закрепление их в официальных документах создает достаточно надежную базу для защиты информации на регулярной основе. Однако нетрудно видеть, что с точки зрения современной постановки задачи защиты информации имеющиеся методики являются недостаточными по ряду причин, а именно:

методики ориентированы на защиту информации только в средствах ЭВТ, в то время как имеет место устойчивая тенденция органического сращивания автоматизированных и традиционных технологий обработки информации;

учитываются далеко не все факторы, оказывающие существенное влияние на уязвимость информации, а поэтому и подлежащие учету при определении требований к защите;

в научном плане они обоснованы недостаточно (за исключением требований к защите информации от утечки по техническим каналам).

10. Классы защищенности средств вычислительной техники от несанкционированного доступа

В части 2 руководящих документов ГТК устанавливается классификация средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Под средствами вычислительной техники понимаются совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Показатели защищенности содержат требования средств вычислительной техники от несанкционированного доступа к информации и применяются к общесистемным программным средствам и операционным системам (с учетом архитектуры компьютера). Конкретные перечни показателей определяются классы защищенности средств вычислительной техники и описываются совокупностью требований. Совокупность всех средств защиты составляет комплекс средств защиты.

Примечание: "-" — нет требований к данному классу; "+" - новые или дополнительные требования; "=" — требования совпадают с требованиями к средствам вычислительной техники предыдущего класса.

10.1 Факторы, влияющие на требуемый уровень защиты информации Группа 1 — обуславливаемые характером обрабатываемой информации:

- 1.1. Степень секретности.
- 1.2. Объемы.
- 1.3. Интенсивность обработки.

Группа 2 — обуславливаемые архитектурой автоматизированной системы обработки данных:

1. Геометрические размеры.
2. Территориальная распределенность.
3. Структурированность компонентов.

Группа 3 — обуславливаемые условиями функционирования автоматизированной системы обработки данных:

1. Расположение в населенном пункте.
2. Расположение на территории объекта.
3. Обустроенность.

Группа 4 — обуславливаемые технологией обработки информации.

- 4.1. Масштаб.
- 4.2. Стабильность.
- 4.3. Доступность.

4.4. Структурированность.

Группа 5 — обуславливаемые организацией работы автоматизированной системы обработки данных:

1. Общая постановка дела.
2. Укомплектованность кадрами.
3. Уровень подготовки и воспитания кадров.
4. Уровень дисциплины.

11. Функции и задачи защиты информации

11.1 Общие положения

Одно из фундаментальных положений системно-концептуального подхода к защите информации состоит в том, что предполагается разработка такой концепции, в рамках которой имелись бы (по крайней мере потенциально) возможности гарантированной защиты информации для самого общего случая архитектурного построения автоматизированной системы обработки данных, технологии и условий их функционирования. Для того, чтобы множество функций соответствовало своему назначению, оно должно удовлетворять требованию полноты, причем под полнотой множества функции понимается свойство, состоящее в том, что при надлежащем обеспечении соответствующего уровня (соответствующей степени) осуществления каждой из функций множества гарантировано может быть достигнут требуемый уровень защищенности информации.

Защита информации в современных автоматизированных системах обработки данных может быть эффективной лишь в том случае, если она будет осуществляться как непрерывный и управляемый процесс. Для этого должны быть предусмотрены, с одной стороны, **механизмы непосредственной защиты информации**, а с другой — **механизмы управления механизмами непосредственной защиты**. Соответственно этому и множество функций защиты должно состоять из двух подмножеств: первого, содержащего функции непосредственно защиты, и второго, содержащего функции управления механизмами защиты.

Обеспечение регулярного осуществления функций защиты достигается тем, что в автоматизированных системах обработки данных регулярно решаются специальные задачи защиты. При этом задачей защиты информации называются организованные возможности средств, методов и мероприятий, реализуемых в автоматизированных системах обработки данных с целью осуществления функций защиты. Основное концептуальное требование к задачам защиты состоит в надежном обеспечении заданного уровня осуществления каждой из полного множества функций защиты. Сущность этого требования заключается в следующем.

Множество функций защиты должно быть полным в том смысле, что регулярное их осуществление обеспечивает условия для надежной защиты информации в системном плане. При этом варьируя усилиями и ресурсами, вкладываемыми в осуществление различных функций,

можно стремиться к такому положению, когда требуемый уровень защиты информации будет достигаться при минимальных затратах, или к положению, когда при заданных затратах будет достигаться максимальный уровень защиты. Иными словами, полнота множества функций защиты и взаимозависимости различных функций создают предпосылки для оптимального построения системы защиты информации в автоматизированных системах обработки данных. Практическая реализация этой возможности может быть обеспечена лишь в том случае, если множество задач защиты будет репрезентативным в том смысле, что будет позволять обеспечивать любой заданный уровень осуществления каждой функции защиты, и притом с минимизацией расходов на осуществление как каждой функции отдельно, так и их совокупности. Таким образом, задачи защиты информации являются инструментом практической реализации функций защиты в соответствии с объективными потребностями защиты.

11.2 Методы формирования функций защиты.

Требование полноты множества функций защиты применительно к двум отмеченным видам интерпретируются следующим образом:

Множество функций обеспечения защиты должно быть таким, чтобы осуществлением их в различных комбинациях и с различными усилиями в любой ситуации при функционировании автоматизированных систем обработки данных могли быть созданы все условия, необходимые для надежной защиты информации.

Множество функций управления должно создавать все предпосылки для оптимальной реализации функций обеспечения в любых условиях.

Вместе с тем принципиально важно подчеркнуть, что регулярных (а тем более формальных) методов решения проблемы не существует (по крайней мере в настоящее время). Вынужденно приходится использовать методы неформальные. Таким образом, формирование функций защиты приходится осуществлять в ситуации, когда требования к формированию являются абсолютными а методы которые могут быть при этом использованы весьма относительно структурно логический анализ экспертные оценки и просто здравый смысл компетентных специалистов

Совершенно очевидно, что множество функций защиты информации должно быть таким чтобы надлежащим их осуществлением можно было оказывать желаемое воздействие на любую ситуацию которая потенциально возможна в процессе организации и обеспечения защиты информации Последовательность и содержание структурно логического анализа ситуаций потенциально возможных в процессе защиты информации можно представить в следующем виде

Для того чтобы защищенность информации могла быть нарушена должны существовать (иметь место) такие условия при которых могут проявиться

Событие 1 —защита информации обеспечена, поскольку даже при условии проявления дестабилизирующих факторов предотвращено их воздействие на защищаемую информацию или ликвидированы последствия такого воздействия.

Событие 2 — защита информации нарушена поскольку не удалось предотвратить воздействие дестабилизирующих факторов на информацию, однако это воздействие локализовано.

Событие 3 — защита информации разрушена, поскольку воздействие дестабилизирующих факторов на информацию не только не предотвращено, но даже не локализовано.

Рисунок 6

Формирование множества задач осуществляется на основе анализа объективных возможностей реализации поставленных целей защиты. Такое множество задач может состоять из ряда классов задач, включающих содержащие однородные в функциональном отношении задачи.

Класс задач — однородное в функциональном отношении множество задач, обеспечивающих полную или частичную реализацию одной или нескольких целей.

11.3 Классы задач защиты информации

Учитывая, что основными целями обеспечения информационной безопасности являются обеспечение защиты: системы от обнаружения и от информационного воздействия, а также содержания информации выделяются задачи соответствующих видов.

Одной из первичных целей противника является обнаружение объекта,обработывающего конфиденциальную информацию, и выявление сведений о его предназначении. Поэтому к первому виду задач можно отнести задачи **уменьшения степени распознавания объектов**. К этому виду относятся следующие классы задач.

Класс 1.1 Скрытие информации о средствах, комплексах, объектах и системах обработки информации. Эти задачи могут подразделяться на технические и организационные.

Организационные задачи по скрытию информации об объектах направлены на недопущение разглашения этих сведений сотрудниками и утечки их по агентурным каналам.

Технические задачи направлены на устранение или ослабление технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них. При этом скрытие осуществляется уменьшением электромагнитной, временной, структурной и признаковой доступности, а также ослаблением адекватности между структурой, топологией и характером функционирования средств, комплексов, объектов, систем обработки информации и управления.

Решение этой задачи представляет реализацию комплекса организационно-технических мероприятий и мер, обеспечивающих выполнение основного требования к средствам, комплексам и системам обработки информации —разведзащищенности и направлено на

достижение одной из главных целей —исключение или существенное затруднение технической разведке поиска,определения местоположения, радионаблюдения источников радиоизлучения, классификации и идентификации объектов техническойразведкой по выявленным демаскирующим признакам.

Решение задачи по снижению электромагнитной доступности затрудняет как энергетическое обнаружение, так и определение координат района расположения источников радиоизлучения, а также увеличивает время выявления демаскирующих признаков, уменьшает точность измерения параметров и сигналов средств радиоизлучения.

Снижение временной доступности радиоизлучающих средств предполагает сокращение времени их работы на излучение при передаче информации и увеличение длительности паузы между сеансами обработки информации. Для уменьшения структурной и признаковой доступности информации реализуются организационно-технические мероприятия, ослабляющие демаскирующие признаки и создающие так называемый "серый фон".

Технические задачи скрытия должны решаться, например, для подвижных объектов (автомобилей), оборудованных радиосвязью.

Класс 1.2. Дезинформация противника.

К этому классу относятся задачи, заключающиеся в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности, положении дел на предприятии и т. д.

Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по внешнему виду или проявлениям похожих на интересующих соперника объекты, и др.

Роль дезинформации подчеркивал А.Ф.Вивиани, специалист в области контршпионажа: "На нас обрушивается, валится, извергается огромное количество информации. Она бывает фальшивой, но выглядит правдоподобно; бывает правдивой, а на самом деле хитроумно перекроена, дабы производить впечатление фальшивой; бывает отчасти фальшивой и отчасти правдивой. Все зависит от выбранного способа так называемой дезинформации, цель которой — заставить вас верить, желать, думать, принимать решения в направлении, выгодном для тех, кому зачем-то нужно на нас воздействовать..."

Техническая дезинформация на объекте защиты представляет комплекс организационных мероприятий и технических мер, направленных на введение в

заблуждение технической разведки относительно истинных целей систем обработки информации, намерений органов управления.

Частными задачами технической дезинформации являются:

☐ искажение демаскирующих признаков реальных объектов и систем, соответствующих признакам ложных объектов;

☐ создание (имитация) ложной обстановки, объектов, систем, комплексов путем воспроизведения демаскирующих признаков реальных объектов, структур систем, ситуаций, действий, функций и т. д.

☐ передача, обработка, хранение в системах обработки ложной информации.

В общем виде эти задачи могут быть сгруппированы в частные задачи радиоимитации, радиодезинформации, демонстративных действий.

Класс 1.3. Легендирование.

Объединяет задачи по обеспечению получения злоумышленником искаженного представления о характере и предназначении объекта, когда наличие объекта и направленность работ на нем полностью не скрываются, а маскируются действительное предназначение и характер мероприятий.

На практике, учитывая очень высокую степень развития современных средств ведения разведки, является чрезвычайно сложным полноекрытие информации об объектах. Так, современные средства фоторазведки позволяют делать из космоса снимки объектов с разрешающей способностью несколько десятков сантиметров.

Поэтому наряду с рассмотренным видом задач, не менее важными, а по содержанию более объемными являются задачи **защиты содержания обрабатываемой, хранимой и передаваемой информации**. К этому виду относятся следующие классы задач.

Класс 2.1. Введение избыточности элементов системы.

Под избыточностью понимается включение в состав элементов системы обработки информации дополнительных компонентов, обеспечивающих реализацию заданного множества целей защиты, с учетом воздействий внешних и внутренних дестабилизирующих факторов.

Решение этой задачи включает реализацию комплекса организационных мероприятий, технических, программных и других мер, обеспечивающих организационную, аппаратную, программно-аппаратную, временную избыточности.

Организационная избыточность осуществляется за счет введения дополнительной численности обслуживающего персонала, его обучения, организации и обеспечения режима сохранения государственной тайны и другой конфиденциальной информации, определения порядка передачи информации различной степени важности, выбора мест размещения средств комплексов обработки и т.п.

Аппаратурная избыточность осуществляется за счет введения дополнительных технических устройств, обеспечивающих защиту информации.

Программно-аппаратная избыточность предполагает использование дополнительных программных, аппаратных и комбинированных средств защиты в системе обработки информации.

Информационная избыточность осуществляется за счет создания дополнительных информационных массивов, банков данных.

Временная избыточность предполагает выделение дополнительного времени для

проведения обработки информации и др.

Класс 2.2. Резервирование элементов системы.

Резервирование, в отличие от задачи введения избыточности предполагает не введение дополнительных элементов, обеспечивающих защиту информации, а их исключение и перевод в резерв на случай возникновения необходимости обработки дополнительного массива информации, повышения статуса защищенности информации, возникновения непредвиденных ситуаций. Такое резервирование может быть горячим и холодным.

При горячем резервировании элементы находятся в рабочем состоянии после дополнительных операций включения и подготовки к работе, а при холодном элементы переводятся в рабочее состояние после дополнительных операций. Класс 2.3. Регулирование доступа к элементам системы и защищаемой информации.

Регулирование доступа к средствам, комплексам и системам обработки информации (на территорию, в помещение, к техническим средствам, к программам, к базам данных и т.п.) предполагает реализацию идентификации, проверки подлинности и контроля доступа, регистрацию субъекта, учет носителей информации в системе ее обработки.

Кроме того, к данному классу относятся задачи по установлению и регулированию контролируемых зон вокруг технических средств обработки информации, за пределами которых становятся невозможными выделение и регистрация с помощью технических средств разведки сигналов, содержащих конфиденциальную информацию. Такие сигналы могут возникать, например, за счет появления вокруг функционирующих средств обработки информации побочных электромагнитных излучений или наводок в проводах, выходящих за пределы контролируемой зоны.

Класс 2.4. Регулирование использования элементов системы и защищаемой информации.

Регулирование использования заключается в осуществлении запрашиваемых процедур (операций) при условии предъявления некоторых заранее обусловленных полномочий.

Для решения данного класса задач относительно конфиденциальной информации могут осуществляться такие операции, как ее дробление и ранжирование.

Дробление (расчленение) информации на части с таким условием, что знание какой-то одной части информации (например, знание одной операции технологии производства какого-то продукта) не позволяет восстановить всю картину, всю технологию в целом.

Ранжирование включает, во-первых, деление засекречиваемой информации по степени секретности и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций.

Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности информации и определяется матрицей доступа.

Примером данного класса задач является доступ сотрудников к обслуживанию специальной техники только при наличии соответствующего разрешения.

Класс 2.5. Маскировка информации.

Маскировка информации заключается в преобразовании данных, исключающем доступ посторонних лиц к содержанию информации и обеспечивающем доступ разрешенным пользователям при предъявлении ими специального ключа преобразования. Решение этой задачи осуществляется на основе криптографических, некриптографических и смежных с ними (кодирование, ортогональные преобразования) преобразований.

Класс 2.6. Регистрация сведений.

Регистрация предполагает фиксацию всех сведений о фактах, событиях, возникающих в процессе функционирования средств и систем обработки информации, относящихся к защите информации, на основании которых осуществляется решение задач оценки состояния безопасности информации с целью повышения эффективности и управления механизмами защиты.

Класс 2.7. Уничтожение информации.

Решение задачи уничтожения информации представляется как процедура своевременного полного или частичного вывода из системы обработки элементов информации, компонентов системы, не представляющих практической, исторической, научной ценности, а так же если их дальнейшее нахождение в системе обработки снижает безопасность информации.

Необходимо отметить, что для различных классов информационно-телекоммуникационных систем уничтожение информации будет иметь определенную специфику. Так, для систем автоматизированной обработки информации типичной процедурой является уничтожение остаточной информации в элементах оперативного запоминающего устройства, отдельных магнитных носителях, программных модулях, контрольных распечатках, выданных документах после решения соответствующей задачи обработки информации.

Для криптографических систем такой задачей может быть своевременное уничтожение носителей ключевой информации для шифрования данных в целях повышения криптостойкости (способности аппаратуры шифрования противостоять вскрытию секрета шифра).

Одной из разновидностей уничтожения информации является так называемое аварийное уничтожение, осуществляемое при явной угрозе злоумышленного доступа к информации повышенной важности.

Класс 2.8. Обеспечение сигнализации.

Решение задачи обеспечения сигнализации состоит в реализации процедуры сбора, генерирования, передачи, отображения и хранения сигналов о состоянии механизмов защиты с целью обеспечения регулярного управления ими, а также объектами и процессами обработки информации. Этот класс задач обеспечивает обратную связь в системе управления, чем достигается обеспечение активности системы защиты. В основном такие задачи решаются с помощью технических средств сигнализации.

Класс 2.9. Обеспечение реагирования.

Получив по каналам обратной связи информацию о состоянии системы защиты, в

соответствии с законами управления орган управления должен при необходимости выработать управленческое решение, т.е. отреагировать на полученный сигнал. Реагирование на проявление дестабилизирующих факторов является признаком активности системы защиты информации, реализации которого направлена на предотвращение или снижение степени воздействия факторов на информацию.

Класс 2.10. Управление системой защиты информации.

Этот класс объединяет широкий круг задач, связанных с контролем правильности функционирования механизмов обработки и защиты информации, оценкой внутренних и внешних угроз, планированием защиты и т.д. При этом понятие "контроль" рассматривается в узком смысле и сводится к проверкам эффективности реализации технических и, в частности, аппаратных мер защиты: соответствия элементов системы заданному их составу, текущего состояния элементов системы, работоспособности элементов системы, правильности функционирования элементов системы, отсутствия несанкционированных устройств и систем съема информации.

Класс 2.11. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности.

Приведенный ранее анализ угроз информации показал, что одной наиболее значимых причин нарушения ее целостности является ошибки и сбои в работе персонала. В связи с этим к рассматриваемому классу относятся задачи достижения необходимого уровня теоретической подготовки и практических навыков в работе (подготовка персонала), а также задачи формирования высокой психофизиологической устойчивости к воздействию дестабилизирующих факторов и моральной устойчивости к разглашению конфиденциальных сведений (подбор, оценка персонала, стимулирование его деятельности и др.).

К третьему виду относятся **задачи защиты информации от информационного воздействия**. К ним можно отнести следующие классы задач.

Класс 3.1. Защита от информационного воздействия на технические средства обработки.

Информационное воздействие на технические средства обработки, хранения передачи информации может быть направлено:

на уничтожение информации (например, электронное подавление средств связи);

искажение или модификацию информации и логических связей (внедрение компьютерных вирусов);

внедрение ложной информации в систему.

Таким образом, данный класс включает задачи реализации технических средств и организационно-технических мероприятий по защите от рассмотренных направлений воздействия.

Класс 3.2. Защита от информационного воздействия на общество.

Задачи предполагают разработку и реализацию методов защиты от негативного воздействия через средства массовой информации на общественное сознание людей. Целями

такого воздействия могут быть, например, навязывание общественного мнения (пропаганда), решение экономических вопросов (реклама), разрушение национальных традиций и культуры (навязывание со стороны других государств чуждых культурных ценностей) и др.

Класс 3.3. Защита от информационного воздействия на психику человека. Включает широкий круг задач, направленных как непосредственно на защиту от технических средств воздействия на психику (психотронного оружия), так и на определение и формирование у человека высокой стрессоустойчивости, высоких моральных качеств и т.д., позволяющих противостоять такому воздействию.

Рассмотрев содержание вышеперечисленных классов, можно сделать вывод, что под задачей защиты информации понимаются организованные возможности средств, методов и мероприятий, используемых на объекте обработки информации с целью осуществления функций защиты.

11.4 Функции защиты

Под *функцией защиты* понимается множество действий, реализаций, проведение функционально однородных мероприятий, осуществляемых на объектах обработки конфиденциальной информации различными средствами, способами и методами с целью обеспечения заданных уровней защищенности информации. Множество функций обеспечения защиты в различных их комбинациях должно создавать условия для обеспечения надежной защиты независимо от условий внешних воздействий, внутренних неопределенностей систем обработки и защиты информации.

Состояния и функции системы защиты информации.

зависимости от событий потенциальных воздействий угроз и мер, снижающих их влияние, система защиты переходит в определенные состояния, соответствующим событиям.

Состояние 1 — защита информации обеспечена, если при наличии условий, способствующих появлению угроз, их воздействие на защищаемую информацию предотвращено или ликвидированы последствия такого воздействия.

Состояние 2 — защита информации нарушена, если невозможно предотвратить воздействие на нее угроз, однако оно обнаружено и локализовано.

Состояние 3 — защиты информации разрушена, если результаты воздействий на нее угроз не только не предотвращены, но и не локализованы. Множество функций защиты информации определяется следующей последовательностью действий, обеспечивающей выполнение конечной цели — достижение требуемого уровня информационной безопасности. Прежде всего, необходимо попытаться предупредить возникновение условий, благоприятствующих появлению угроз информации. Выполнение этой функции в связи с большим количеством таких угроз и случайным характером их проявлений имеет вероятность, близкую к нулю. Поэтому следующим

шагом должно быть своевременное обнаружение проявившихся угроз и предупреждение их воздействия на информацию. Если все-таки такое воздействие произошло, необходимо вовремя его обнаружить и локализовать с целью недопущения распространения этого воздействия на всю конфиденциальную информацию, обрабатываемую на объекте. И последней функцией защиты должна быть ликвидация последствий указанного воздействия для восстановления требуемого состояния безопасности информации. Рассмотрим эти функции несколько подробнее.

Функция 1 — предупреждение проявления угроз. Реализация этой функции носит упреждающую цель и должна способствовать такому архитектурно-функциональному построению современных систем обработки и защиты информации, которое обеспечивало бы минимальные возможности появления дестабилизирующих факторов в различных условиях функционирования систем. Например, для предупреждения возможности установки в помещении закладных устройств необходимо с помощью технических средств и организационных мероприятий обеспечить невозможность несанкционированного доступа в него.

Функция 2 — обнаружение проявившихся угроз и предупреждение их воздействия на информацию. Основными целями реализации функции осуществляется комплекс мероприятий, в результате которых проявившиеся угрозы будут обнаружены до их воздействия на защищаемую информацию, а также недопущение воздействий этих угроз на защищаемую информацию в условиях их проявления и обнаружения. Так для нейтрализации закладных устройств необходимо регулярно проводить спецпроверки помещений, устанавливать системы их автоматического поиска, а для предупреждения их воздействия на конфиденциальную информацию использовать устройства защиты типа генераторов объемного зашумления, позволяющих создавать вокруг устройств обработки информации шумовое поле.

Функция 3 — обнаружение воздействия угроз на защищаемую информацию и локализация этого воздействия. Содержание функции направлено на непрерывный контроль средств, комплексов, систем обработки, защиты информации и различных компонентов защищаемой информации с целью своевременного обнаружения фактов воздействия на их угрозы. Своевременное обнаружение предполагает обеспечение реальной возможности локализации воздействия на информацию, т.е. минимизацию возможного нарушения ее целостности и защищенности и недопущение распространения этого воздействия за пределы допустимых размеров. В компьютерных системах, например, эту функцию реализуют аппаратно-программные средства контроля и регистрации попыток несанкционированного доступа в систему или к информации (цифровая подпись).

Функция 4 — ликвидация последствий воздействия угроз. Функция предусматривает проведение мероприятий защиты в отношении обнаруженного и локализованного воздействия угроз на информацию с целью обеспечения защиты и локализованного воздействия угроз на информацию с целью обеспечения защиты и дальнейшей обработки информации без результатов воздействий, т.е. осуществляется восстановление системы обработки, защиты информации и

состояния защищаемой информации применением соответствующего множества средств, способов и мероприятий защиты

"+" - восстановление работоспособности системы "-" - работоспособности системы не возобновлена.

12. Стратегии защиты информации

Стратегия — это общая, рассчитанная на перспективу руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов.

Организация защиты информации в самом общем виде может быть определена как поиск оптимального компромисса между потребностями в защите и необходимыми для этих целей ресурсами.

Потребности в защите обуславливаются, прежде всего, важностью и объемами защищаемой информации, а также условиями ее хранения, обработки и использования. Эти условия определяются уровнем (качеством) структурно-организационного построения объекта обработки информации, уровнем организации технологических схем обработки, местом и условиями расположения объекта и его компонентов и другими параметрами.

Размер ресурсов на защиту информации может быть ограничен определенным пределом либо определяется условием обязательного достижения требуемого уровня защиты. В первом случае защита должна быть организована так, чтобы при выделенных ресурсах обеспечивался максимально возможный уровень защиты, а во втором — чтобы требуемый уровень защиты обеспечивался при минимальном расходовании ресурсов.

Сформулированные задачи есть не что иное, как прямая и обратная постановки оптимизационных задач. Существует две проблемы, затрудняющие формальное решение.

Первая — процессы защиты информации находятся в значительной зависимости от большого числа случайных и трудно предсказуемых факторов, таких как поведение злоумышленника, воздействие природных явлений, сбои и ошибки в процессе функционирования элементов системы обработки информации и др.

Вторая — среди средств защиты весьма заметное место занимают организационные меры, связанные с действием человека.

Обоснование числа и содержания необходимых стратегий будем осуществлять по двум критериям: требуемому уровню защиты и степени свободы действий при организации защиты. Значения первого критерия лучше всего выразить множеством тех угроз, относительно которых должна быть обеспечена защита:

от наиболее опасных из известных (ранее появившихся) угроз; от всех известных угроз;

от всех потенциально возможных угроз.

Второй критерий выбора стратегий защиты сводится к тому, что организаторы и исполнители процессов защиты имеют относительно полную свободу распоряжения методами и средствами защиты и некоторую степень свободы вмешательства в архитектурное построение системы обработки информации, а также в организацию и обеспечение технологии ее функционирования. По этому аспекту удобно выделить три различные степени свободы:

1. никакое вмешательство в систему обработки информации не допускается. Такое требование может быть предъявлено к уже функционирующим системам обработки информации и нарушение процесса их функционирования для установки механизмов защиты не разрешается;

2. к архитектурному построению системы обработки информации и технологии ее функционирования допускается предъявлять требования неконцептуального характера. Другими словами, допускается приостановка процесса функционирования системы обработки информации для установки некоторых механизмов защиты;

3. требования любого уровня, обусловленные потребностями защиты информации, принимаются в качестве обязательных условий при построении системы обработки информации, организации и обеспечения их функционирования.

Так, выбирая оборонительную стратегию, подразумевают, что при недопущении вмешательства в процесс функционирования системы обработки информации можно нейтрализовать лишь наиболее опасные угрозы. Например, данная стратегия, применяемая для существующего объекта, может включать разработку организационных мер использование технических средств по ограничению несанкционированного допуска к объекту. Упреждающая стратегия предполагает тщательное исследование возможных гроз системы обработки информации и разработку мер по их нейтрализации еще на стадии проектирования и изготовления системы. При этом нет смысла на данном этапе рассматривать ограниченное множество подобных угроз.

13. Способы и средства защиты информации

Множество и разнообразие возможных средств защиты информации определяется, прежде всего, возможными способами воздействия на дестабилизирующие факторы или порождающие их причины, причем воздействия в направлении, способствующем повышению значений показателей защищенности или (по крайней мере) сохранению прежних (ранее достигнутых) их значений.

Рассмотрим содержание представленных способов и средств обеспечения безопасности.

Препятствие заключается в создании на пути возникновения или распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры. Типичными примерами препятствий являются блокировки, не позволяющие техническому устройству или программе выйти за опасные границы; создание физических препятствий на пути злоумышленников, экранирование помещений и технических средств и т.п.

Управление есть определение на каждом шаге функционирования систем обработки информации таких управляющих воздействий на элементы системы, следствием которых будет решение (или содействие решению) одной или нескольких задач защиты информации. Например, управление доступом на объект включает следующие функции защиты:

1. идентификацию лиц, претендующих на доступ, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
2. опознавание (установление подлинности) объекта или субъекта по предъявленному идентификатору;
3. проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
4. регистрацию (протоколирование) обращений к защищаемым ресурсам;
5. реагирование (сигнализация, отключение, задержка работ, отказ в процессе) при попытках несанкционированных действий.

Маскировка предполагает такие преобразования информации, вследствие которых она становится недоступной для злоумышленников или такой доступ существенно затрудняется, а также комплекс мероприятий по уменьшению степени распознавания самого объекта. К маскировке относятся криптографические методы преобразования информации, скрытие объекта, дезинформация и легендирование, а также меры по созданию шумовых полей, маскирующих информационные сигналы.

Регламентация как способ защиты информации заключается в разработке и реализации в процессе функционирования объекта комплекса мероприятий, создающих такие условия, при которых существенно затрудняются проявление и воздействие угроз. К регламентации относится разработка таких правил обращения с конфиденциальной информацией и средствами ее обработки, которые позволили бы максимально затруднить получение этой информации злоумышленником.

Принуждение — такой метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение есть способ защиты информации, при котором пользователи и персонал объекта внутренне (т.е. материальными, моральными, этическими, психологическими и другими мотивами) побуждаются к соблюдению всех правил обработки информации.

Как отдельный, применяемый при ведении активных действий противоборствующими сторонами, можно выделить такой способ, как *нападение*. При этом подразумевается как применение информационного оружия при ведении информационной войны, так и непосредственное физическое уничтожение противника (при ведении боевых действий) или его средств разведки.

Рассмотренные способы обеспечения защиты информации реализуются с применением

различных методов и средств. При этом различают формальные и неформальные средства. К формальным относятся такие средства, которые выполняют свои функции по защите информации формально, т.е. преимущественно без участия человека. К неформальным относятся средства, основу которых составляет целенаправленная деятельность людей. Формальные средства делятся на физические, аппаратные и программные.

Физические средства — механические, электрические, электромеханические и т.п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

Аппаратные средства — различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации. Например, для защиты от утечки по техническим каналам используются генераторы шума.

Физические и аппаратные средства объединяются в класс *технических средств защиты информации*.

Программные средства — специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения автоматизированных систем с целью решения задач защиты информации.

Это могут быть различные программы по криптографическому преобразованию данных, контролю доступа, защиты от вирусов и др.

Неформальные средства делятся на организационные, законодательные и морально-этические.

Организационные средства — специально предусматриваемые в технологии функционирования объекта организационно-технические мероприятия для решения задач защиты информации, осуществляемые в виде целенаправленной деятельности людей.

Законодательные средства — существующие в стране или специально издаваемые нормативно-правовые акты, с помощью которых регламентируются права и обязанности, связанные с обеспечением защиты информации, всех лиц и подразделений, имеющих отношение к функционированию системы, а также устанавливается ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации.

Морально-этические нормы — сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе. Именно человек, сотрудник предприятия или учреждения, допущенный к секретам и накапливающий в своей памяти колоссальные объемы информации, в том числе секретной, нередко становится источником утечки этой информации или по его вине соперник получает возможность несанкционированного доступа к носителям защищаемой информации.

Морально-нравственные методы защиты информации предполагают прежде всего

воспитание сотрудника, допущенного к секретам, то есть проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично), и обучение сотрудника, осведомленного в сведениях, составляющих охраняемую тайну, правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Интересный подход к формированию множества способов защиты предлагает член-корреспондент Академии криптографии РФ Расторгуев С.П. В основу названной им "абсолютной системы защиты", обладающей всеми возможными способами защиты, положены основные принципы защиты, реализуемые в живой природе. Развивая этот подход, можно выделить следующие основные способы защиты животного мира в сравнении с рассмотренными способами защиты информации:

1. Пассивная защита. Перекрывает все возможные каналы воздействия угроз и предполагает "одевание брони" на себя и создание территориальных препятствий. Налицо полное соответствие такому способу защиты информации, как препятствие.

2. Изменение местоположения. Желание спрятаться можно соотнести с таким способом, как скрытие.

3. Изменение собственной внешности, мимикрия — слияние с ландшафтом и т.п. Цель — представиться объектом неинтересным или незаметным для нападающей стороны. Аналогичную функцию защиты информации реализуют ее маскировкой.

4. Нападение с целью уничтожения нападающего. Выше был рассмотрен соответствующий способ защиты информации.

5. Воспитание навыков безопасности у потомства, доведение этих навыков до уровня инстинкта. Для систем защиты информации аналогичные навыки у обслуживающего персонала формируются принуждением и побуждением.

6. Выработка определенных правил жизнедеятельности, способствующих выживанию и сохранению рода. К таким правилам, выработанным природой, можно отнести мирное существование особей одного вида, жизнь в стаях (стадах) и т.д. Другими словами, природа регламентирует необходимые для безопасности правила жизни.

Таким образом, анализ присущих животному миру защитных свойств, положенный в основу так называемой "абсолютной системы защиты", показывает, что все они соответствуют рассмотренным способам защиты информации, что подтверждает полноту их формирования.

14. Архитектура систем защиты информации

14.1 Требования к архитектуре СЗИ

Система защиты информации (СЗИ) в самом общем виде может быть определена как

организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) на объекте обработки информации (ООИ) для решения в ней выбранных задач защиты.

Введением понятия СЗИ определяется тот факт, что все ресурсы, выделяемые для защиты информации должны объединяться в единую, целостную систему, которая является функционально самостоятельной подсистемой любого ООИ.

Важнейшим концептуальным требованием к СЗИ является требование адаптируемости, т.е. способности к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования ООИ. Важность требования адаптируемости обуславливается, с одной стороны, тем, что перечисленные факторы могут существенно изменяться, а с другой, тем, что процессы защиты информации относятся к слабоструктурированным, т.е. имеющим высокий уровень неопределенности. Управление же слабоструктурированными процессами может быть эффективным лишь при условии адаптируемости системы управления.

Помимо общего концептуального требования к СЗИ предъявляется еще целый ряд более конкретных, целевых требований, которые могут быть разделены:

1. на функциональные;
2. эргономические;
3. экономические;
4. технические;
5. организационные.

Сформированная к настоящему времени система включает следующий перечень общеметодологических принципов

1. концептуальное единство;
2. адекватность требованиям;
3. гибкость (адаптируемость);
4. функциональная самостоятельность;
5. удобство использования;
6. минимизация предоставляемых прав;
7. полнота контроля;
8. адекватность реагирования;
9. экономичность.

Концептуальное единство означает, что архитектура, технология, организация и

обеспечение функционирования как СЗИ в целом, так и составных компонентов должны рассматриваться и реализовываться в строгом соответствии с основными положениями единой концепции защиты информации.

Адекватность требованиям означает, что СЗИ должна строиться в строгом соответствии с требованиями к защите, которые, в свою очередь определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации.

Гибкость (адаптируемость) системы защиты означает такое построение и такую организацию ее функционирования, при которых функции защиты осуществлялись бы достаточно эффективно при изменении в некотором диапазоне структуры объекта обработки информации, технологических схем или условий функционирования каких-либо ее компонентов.

Функциональная самостоятельность предполагает, что СЗИ должна быть самостоятельной обеспечивающей подсистемой системы обработки информации и при осуществлении функций защиты не должна зависеть от других подсистем.

Удобство использования означает, что СЗИ не должна создавать дополнительных неудобств для пользователей и персонала объекта обработки информации.

Минимизация предоставляемых прав означает, что каждому пользователю и каждому лицу из состава персонала объекта обработки информации должны предоставляться лишь те полномочия на доступ к ресурсам объекта обработки информации и находящейся в ней информации, которые ему действительно необходимы для выполнения своих функций в процессе автоматизированной обработки информации. При этом предоставляемые права должны быть определены и установленным порядком утверждены заблаговременно.

Полнота контроля предполагает, что все процедуры автоматизированной обработки защищаемой информации должны контролироваться системой защиты в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах.

Активность реагирования означает, что СЗИ должна реагировать на любые попытки несанкционированных действий. Характер реагирования может быть различным и включает: просьбу повторить действие; отключение структурного элемента, с которого осуществлено несанкционированное действие; исключение нарушителя из числа зарегистрированных пользователей; подача специального сигнала и др.

Экономичность СЗИ означает, что при условии соблюдения основных требований всех предыдущих принципов расходы на СЗИ должны быть минимальными.

14.2 Построение СЗИ

Функциональным построением любой системы называется организованная совокупность тех функций, для регулярного осуществления которых она создается.

Под *организационным построением* понимается общая организация системы, адекватно

отражающая концептуальные подходы к ее созданию. Организационно СЗИ состоит из трех механизмов:

1. обеспечения защиты информации;
2. управления механизмами защиты;
3. общей организации работы системы.

В механизмах обеспечения защиты выделяются два организационных компонента: постоянные и переменные. При этом под постоянными понимаются такие механизмы, которые встраиваются в компоненты объекта обработки информации в процессе создания СЗИ и находятся в рабочем состоянии в течение всего времени функционирования соответствующих компонентов. Переменные же механизмы являются автономными, использование их для решения задач защиты информации предполагает предварительное осуществление операций ввода в состав используемых механизмов. Встроенные и переменные механизмы могут иметь в своем составе технические, программные и организационные средства обеспечения защиты.

Соответственно составу механизмов обеспечения защиты информации, очевидно, должны быть организованы механизмы управления ими.

Механизмы общей организации работы СЗИ предназначены для системной увязки и координации работы всех компонентов СЗИ.

В понятие "организационное построение" СЗИ входит также распределение элементов этой системы по организационно-структурным элементам объекта обработки информации. Исходя из этого, в организационном построении СЗИ должны быть предусмотрены подсистемы защиты на объектах (структурных компонентах) объекта обработки информации со своими специфическими механизмами защиты и некоторое управляющее звено, которое имеет название **ядро СЗИ**.

Ядро средства защиты информации

Ядро системы защиты предназначено для объединения всех подсистем СЗИ в единую целостную систему, организации обеспечения управления ее функционированием.

Ядро может включать организационные и технические составляющие. *Организационная составляющая* представляет собой совокупность специально выделенных для обеспечения ЗИ сотрудников, выполняющих свои функции в соответствии с разработанными правилами, а также нормативную базу, регламентирующую выполнение этих функций.

Техническая составляющая обеспечивает техническую поддержку организационной составляющей и представляет собой совокупность технических средств отображения состояний элементов СЗИ, контроля доступа к ним, управления их включением и т.д. Чаще всего эти средства объединены в соответствующий пульт управления СЗИ.

Ядро СЗИ обладает следующими функциями:

Включение компонентов СЗИ в работу при поступлении запросов на обработку защищаемой информации и блокирование бесконтрольного доступа к ней:

оборудование объекта средствами охранной сигнализации;

организация хранения носителей защищаемой информации в отдельных хранилищах (документация, шифры, магнитные носители и т.д.).

включение блокирующих устройств, регулирующих доступ к элементам СЗИ при предъявлении соответствующих полномочий и средств сигнализации.

2) Организация и обеспечение проверок правильности функционирования СЗИ:

аппаратных средств — по тестовым программам и организационно; физических средств — организационно (плановые проверки средств

охранной сигнализации, сигнализации о повышении давления в кабелях ит.д.);

программных средств — по специальным контрольным суммам (нацеленность) и по другим идентифицирующим признакам.

14.4 Ресурсы средства защиты информации

Ресурсы информационно-вычислительной системы, необходимые для создания и поддержания функционирования СЗИ, как и любой другой автоматизированной системы, объединяются в техническое, математическое, программное, информационное и лингвистическое обеспечение.

техническое обеспечение — совокупность технических средств, необходимых для технической поддержки решения всех тех задач защиты информации, решение которых может потребоваться в процессе функционирования СЗИ;

математическое обеспечение — совокупность математических методов, моделей и алгоритмов, необходимых для оценки уровня защищенности информации и решения других задач защиты;

программное обеспечение — совокупность программ, реализующих программные средства защиты, а также программ, необходимых для решения задач управления механизмами защиты. К ним должны быть отнесены также сервисные и вспомогательные программы СЗИ;

информационное обеспечение — совокупность систем классификации и кодирования данных о защите информации, массивы данных СЗИ, а также входные и выходные документы СЗИ;

лингвистическое обеспечение — совокупность языковых средств, необходимых для обеспечения взаимодействия компонентов СЗИ между собой, с компонентами объекта обработки информации и с внешней средой.

14.5 Организационное построение

Организационное построение СЗИ в самом общем случае может быть представлено совокупностью следующих рубежей защиты:

территории, занимаемой объектом обработки информации; зданий, расположенных на

территории;

помещений внутри здания, в которых расположены ресурсы объекта обработки информации и защищаемая информация;

ресурсов, используемых для обработки и хранения информации и самой защищаемой информации;

линий связи, проходящих в пределах одного и того же здания;

линий (каналов) связи, проходящих между различными зданиями, расположенными на одной и той же охраняемой территории;

линий (каналов) связи, соединяющих с другими объектами вне охраняемой территории.

Таким образом, можно провести организационное построение системы защиты информации с помощью приведенной на рис. 8 семирубежной модели защиты информации. В наиболее общем случае необходимо в зависимости от выбранной стратегии защиты сформулировать требования к ядру средства защиты информации и ресурсам средства защиты информации, а также использовать критерии построения средства защиты информации, изложенные в данной главе.

Необходимо отметить, что построение средств защиты информации должно проводиться в соответствии с нормативно-правовой документацией, принятой в Российской Федерации. Большинство видов деятельности в сфере защиты информации необходимы лицензии. Так, для работы с государственной тайной требуется лицензия Федеральной службы безопасности, для работы с криптографическими средствами — лицензия Федерального агентства правительственной связи и информации, технические средства должны быть аттестованы Государственной технической комиссией и др.

15. Индивидуальные задания

Индивидуальные задания состоят из двух частей, взаимосвязанных друг с другом по объекту защиты информации. Объект необходимо исследовать таким образом, чтобы можно было применить все основные элементы защиты информации, т.е. определяя местоположение, внешние и внутренние характеристики с учетом естественных событий. Однако уточнение характеристик не должно приводить к абсолютной конкретизации объекта, т.к. в этом случае будет затруднен анализ объекта.

Первое задание

Для выполнения первой части необходимо для выбранного определенного объекта защиты информации необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

виды угроз;

характер происхождения угроз;

классы каналов несанкционированного получения информации; источники появления угроз;

причины нарушения целостности информации; потенциально возможные злоумышленных действий;

определить класс защиты информации.

Второе задание

Для выполнения второго задания предложить анализ увеличения защищенности объекта защиты информации по следующим разделам:

определить требования к защите информации; классифицировать автоматизированную систему;

определить факторы, влияющие на требуемый уровень защиты информации;

выбрать или разработать способы и средства защиты информации; построить архитектуру систем защиты информации;

сформулировать рекомендации по увеличению уровня защищенности.

Наименование объекта защиты информации:

1. Единично стоящий компьютер в бухгалтерии.

2. Сервер в бухгалтерии.

3. Почтовый сервер. Веб-сервер.

4. Компьютерная сеть материальной группы.

5. Одноранговая локальная сеть без выхода в Интернет.

6. Одноранговая локальная сеть с выходом в Интернет.

7. Сеть с выделенным сервером без выхода в Интернет.

8. Сеть с выделенным сервером с выхода в Интернет.

9. Телефонная база данных (содержащая и информацию ограниченного пользования)

в твердой копии и на электронных носителях.

10. Телефонная сеть.

11. Средства телекоммуникации (радиотелефоны, мобильные телефоны, пейджеры).

12. Банковские операции (внесение денег на счет и снятие).

13. Операции с банковскими пластиковыми карточками.

14. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.

15. Компьютер, хранящий конфиденциальную информацию о разработках предприятия.

16. Материалы для служебного пользования на твердых носителях в производстве.

17. Материалы для служебного пользования на твердых носителях на закрытом предприятии.

18. Материалы для служебного пользования на твердых носителях в архиве.

- 19.Материалы для служебного пользования на твердых носителях в налоговой инспекции.
- 20.Комната для переговоров по сделкам на охраняемой территории.
- 21.Комната для переговоров по сделкам на неохраняемой территории.
22. Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носителии др.).
- 23.Судебные материалы (твердая копия).
- 24.Паспортный стол РОВД.
25. Материалы по владельцам автомобилей (твердая копия, фотографии, электронные носители и др.).
26. Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.).
- 27.Сведения по тоталитарным сектам и другим общественно-вредным организациям.
- 28.Сведения по общественно-полезным организациям (красный крести др.).
- 29.Партийные списки и руководящие документы.

Вопросы

1. Теория защиты информации. Основные направления.
2. Обеспечение информационной безопасности и направления защиты.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная).
4. Требования к системе защиты информации.
5. Угрозы информации.
6. Виды угроз. Основные нарушения.
7. Характер происхождения угроз.
8. Источники угроз. Предпосылки появления угроз.
9. Система защиты информации.
10. Классы каналов несанкционированного получения информации.
11. Причины нарушения целостности информации.
12. Методы и модели оценки уязвимости информации.
13. Общая модель воздействия на информацию.
14. Общая модель процесса нарушения физической целостности информации.
15. Структурированная схема потенциально возможных злоумышленныхдействий в автоматизированных системах обработки данных.
16. Методологические подходы к оценке уязвимости информации.
17. Модель защиты системы с полным перекрытием.
18. Рекомендации по использованию моделей оценки уязвимости информации.

19. Допущения в моделях оценки уязвимости информации.
20. Методы определения требований к защите информации.
21. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
22. Классификация требований к средствам защиты информации.
23. Требования к защите, определяемые структурой автоматизированной системы обработки данных
24. Требования к защите, обуславливаемые видом защищаемой информации.
25. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации.
26. Анализ существующих методик определения требований к защите информации.
27. Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США". Основные положения.
28. Руководящем документе Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации", выпущенном в 1992 году. Часть 1.
29. Классы защищенности средств вычислительной техники от несанкционированного доступа.
30. Факторы, влияющие на требуемый уровень защиты информации.
31. Функции и задачи защиты информации. Основные положения механизмов непосредственной защиты и механизмы управления механизмами непосредственной защиты.
32. Методы формирования функций защиты.
33. События, возникающие при формировании функций защиты.
34. Классы задач функций защиты.
35. Класс задач функций защиты 1 — уменьшение степени распознавания объектов
36. Класс задач функций защиты 2 — защита содержания обрабатываемой, хранимой и передаваемой информации.
37. Класс задач функций защиты 3 — защита информации от информационного воздействия.
38. Функции защиты информации.
39. Стратегии защиты информации.
40. Способы и средства защиты информации.
41. Способы "абсолютной системы защиты".

- 42. Архитектура систем защиты информации. Требования.
- 43. Общеметодологических принципов архитектуры системы защиты информации.
- 44. Построение средств защиты информации.
- 45. Ядро системы защиты.
- 46. Семи рубежная модель защиты.