

Министерство образования Российской Федерации
Владимирский государственный университет
Кафедра информационных систем
и информационного менеджмента

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
И ЗАЩИТА ИНФОРМАЦИИ**

Методические указания к лабораторным работам

Составители
Р.И. МАКАРОВ
В.В. ВЕРШИНИН

Владимир 2003

УДК 681.3.06

Рецензент
Кандидат технических наук,
доцент Владимирского государственного университета
С.Г. Мосин

Печатается по решению редакционно-издательского совета
Владимирского государственного университета

Информационная безопасность и защита информации. Метод. указания к лабораторным работам / Владим. гос. ун-т; Сост: Р.И. Макаров, В.В. Вершинин. Владимир, 2003. 52 с.

Содержат описание и задания к лабораторным работам по дисциплине «Информационная безопасность и защита информации». Включают работы по изучению и освоению стандартных средств защиты от несанкционированного доступа к компьютеру, используя средства базовой системы ввода/вывода, средств защиты информации, предоставляемых операционной системой Windows, защиты баз данных и особенности разграничения прав при работе в АРМ.

Последние четыре работы посвящены изучению и практической реализации разнообразных криптографических систем, включая криптоанализ (одноключевое шифрование, поточное шифрование, двухключевое асимметричное шифрование).

Предназначены для студентов специальностей 071900, 220100, и других, изучающих дисциплины соответствующего профиля.

Табл. 3. Рис. 24. Библиогр.: 10 назв.

УДК 681.3.06

ПРЕДИСЛОВИЕ

Необходимость и важность обеспечения информационной безопасности объектов информатизации и информационных систем объясняется возросшими требованиями к конфиденциальности данных и их непротиворечивому, постоянному и надежному представлению внутри систем. В сложившихся условиях при проектировании и разработке информационных систем большое внимание необходимо уделять организационным, правовым, техническим и программным средствам, обеспечивающим должный уровень защищенности информации. Поэтому изучение существующих как аппаратных, так и программных средств защиты информации на уровне операционных систем и стандартных утилит представляет особую значимость. В последнее время бурное развитие получили различные криптографические методы, обеспечивающие сокрытие конфиденциальной информации от посторонних лиц. Особенно сильно это развитие происходит с появлением вычислительной техники, теории алгоритмизации и программирования.

Предлагаемый в данных методических указаниях к лабораторным работам по курсу «Информационная безопасность и защита информации» материал ставит целью познакомить студентов с различными аспектами защиты информации в информационных системах.

Первая лабораторная работа посвящена изучению программно-аппаратных средств ЭВМ по защите системы и от неумышленного изменения файлов. Вторая и третья лабораторные работы посвящены изучению средств, предоставляемых различными операционными системами по защите информационных ресурсов. Четвертая лабораторная работа знакомит студентов с методикой организации защиты информации в автоматизированных рабочих местах и разграничением доступа к информационным ресурсам в системах поддержки принятия решения. В пятой и шестой работах рассматривается реализация различных методов шифрования данных для одноключевых блочных и поточных криптографических систем. Седьмая работа посвящена простейшему криптографическому анализу данных. Восьмая работа знакомит со стандартными программами двухключевого шифрования данных и электронной цифровой подписью.

Лабораторная работа № 1

ЗАЩИТА ИНФОРМАЦИИ В ОПЕРАЦИОННОЙ СИСТЕМЕ MS-DOS

1. Цель работы

Цель работы - изучить методы и средства защиты информации в операционной системе MS-DOS и стандартные настройки BIOS Setup.

2. Общие сведения

Операционная система MS DOS относится к тому типу операционных систем, которые не имеют встроенных средств защиты, а также средств разграничения доступа. Для предотвращения несанкционированного доступа к информации, хранящейся на компьютере, работающем под управлением MS DOS, нужно использовать комплекс мер, таких как: установка пароля на вход в систему в SETUP, а также установка специализированных систем контроля доступа, таких как программа System Commander компании V Communications. Под средствами защиты понимается не только предотвращение несанкционированного доступа к информации, но и защита информации от неумышленной порчи, для чего в системе MS DOS предусмотрена команда attrib, изменяющая атрибут файла read only таким образом, что при попытке удалить файл командой del будет выведено сообщение о невозможности совершения данной операции над файлом с атрибутом read only, а при изменении файла при помощи текстового редактора будет выведено сообщение об отказе в доступе к файлу, и изменение произведено не будет, либо будет выведено дополнительное предупреждение.

2.1. Описание средств предотвращения несанкционированного доступа к компьютеру с помощью средств программы BIOS Setup

Рассмотрим Setup, фирмы AMI, (вход по нажатию клавиши Delete при загрузке компьютера). В меню Advanced CMOS Setup необходимо выбрать пункт Password Checking Option, в котором возможны три варианта: Disabled – пароль не запрашивается (смена вариантов клавишами Page Up и Page Down); Setup – пароль требуется только для входа в программу Setup; Always – ввод пароля необходим как для загрузки, так и для входа в программу Setup.

Пункт меню Change Password позволяет изменить текущий пароль. Внимание! Пароль стоит хорошо запомнить, но ни в коем случае не записывать, так как записи на обороте клавиатуры, листочках бумаги становятся

легкой добычей злоумышленников. Если вы, несмотря на это предупреждение, все-таки записываете свои пароли, то хотя бы записывайте их в обратном порядке или добавьте пару цифр в определенные позиции. При выходе из программы Setup необходимо сохранить измененные данные командой Save Settings and Exit. Для снятия пароля в Setup необходимо войти в меню установки пароля, и на приглашение для ввода нового пароля нажать клавишу Enter.

Рассмотрим Setup, фирмы Award, (вход по нажатию клавиши Delete или комбинации Ctrl, Alt и Esc при загрузке компьютера). В меню BIOS Features Setup необходимо выбрать пункт Security Option, в котором возможны два варианта: Setup - пароль требуется только для входа в программу Setup; System - ввод пароля необходим как для загрузки, так и для входа в программу Setup.

В меню Password Settings на приглашение ENTER PASSWORD введите пароль длиной не меньше восьми символов. При выходе из программы Setup необходимо сохранить измененные данные командой Save Settings and Exit.

2.2. Защита файлов от неумышленного изменения при помощи команды MS-DOS *Attrib*

Attrib - изменение и вывод атрибутов файла.

Формат команды:

```
attrib [+r|-r] ([дискковод:] [путь] <имя файла>)
```

Параметры:

+r - устанавливает атрибут "только для чтения";

-r - снимает атрибут "только для чтения".

3. Задания к лабораторной работе

3.1. Изучить общие сведения о защите информации в MS-DOS.

3.2. Выполнить установление/снятие пароля на систему.

3.3. Изменить атрибуты текстового файла.

4. Порядок выполнения работы

4.1. Изучить метод установки пароля в Setup.

4.2. Установить пароль в программе Setup. Войти в систему по паролю.

4.3. Снять пароль в программе Setup.

4.4. Изучить способ изменения атрибута файла read only.

4.5. Создать текстовый файл.

4.6. Занесите в файл информацию, используя текстовый редактор.

4.7. Установить атрибут файла read only.

4.8. Попытаться изменить информацию в текстовом файле.

4.9. Попытаться удалить файл командой MS-DOS del.

4.10. Попытаться удалить файл средствами Norton Commander (или любой другой подобной программы).

5. Содержание отчета

5.1. Цель работы.

5.2. Краткие сведения об основных способах защиты информации в MS-DOS.

5.3. Описание проделанной работы и результаты ее выполнения.

5.4. Выводы по работе.

6. Вопросы для самоподготовки

6.1. Существуют ли стандартные средства MS-DOS для защиты и разграничения доступа?

6.2. Назовите меры для предотвращения несанкционированного доступа к информации, хранящейся на компьютере, работающем под управлением операционной системы MS-DOS.

6.3. Какой из атрибутов файла отвечает за разрешение/запрещение модификации файла?

6.4. Можно ли удалить файл с включенным атрибутом read only, используя команду del?

6.5. Опишите процедуру установки пароля в Setup.

Лабораторная работа № 2

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ И РЕСУРСОВ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS 95/98/ME

1. Цель работы

Цель работы - ознакомление студентов с программными методами защиты информационных ресурсов в локальных одноранговых вычислительных сетях на базе операционной системы Windows 95. Приобретение практических навыков предоставления различного доступа к информации в локальных вычислительных сетях (ЛВС).

2. Общие сведения

Одноранговая вычислительная сеть - это объединение группы компьютеров на постоянной основе, при которой функции рабочей станции и файлового сервера одновременно может выполнять любой из компьютеров,

входящих в эту вычислительную сеть. Для ЛВС с выделенным файловым сервером характерно то, что практически все информационные ресурсы хранятся на одном компьютере (сервере). В одноранговых ЛВС информационные ресурсы могут быть распределены по всем компьютерам. Наиболее распространенный разделяемый ресурс в данной системе - дисковый накопитель. Ресурсом также может являться принтер, подключенный к одному из компьютеров. В одноранговой ЛВС дисковое пространство и файлы любого компьютера могут быть предоставлены в пользование всем пользователям данной ЛВС или ограниченно, в зависимости от прав доступа. Для управления дисковым пространством используют следующие подходы:

1) при форматировании дисковый накопитель разбивают на несколько разделов (например, один для частного использования и один для общего пользования);

2) выделяют отдельные директории для общего пользования (в данном случае невозможно ограничить объем дискового пространства).

Рассмотрим пример предоставления доступа к жесткому диску персонального компьютера в ЛВС на базе операционной системы Windows 95. Для этого нам необходимо, чтобы были установлены все необходимые сетевые устройства (драйвер сетевой карты, IPX/SPX совместимый протокол, служба доступа к файлам и принтерам сетей Microsoft). В сетевых настройках необходимо иметь также в разделе «Доступ к файлам и принтерам» установленный доступ к файлам данного компьютера.

Для предоставления доступа к диску С необходимо:

1) войти двойным щелчком левой кнопки мышки на «Мой компьютер»;

2) выбрать диск С, нажав правую кнопку мышки;

3) в открывшемся меню выбрать «Доступ...» (рис. 1);

4) выбрать сетевое имя диска.

В поле заметки можно указать краткий комментарий для данного диска пользователям сети. Необходимо выбрать тип доступа в зависимости от требований безопасности информации, хранимой на данном диске. При полном типе доступа любой пользователь ЛВС может неограниченно пользоваться данным ресурсом. При типе доступа «Только чтение» аналогично любой пользователь ЛВС может пользоваться данным диском, но не имеет возможности изменять его содержимое. Если доступ определяется паролем, то к диску могут иметь доступ только лица, владеющие данным паролем,

определяющим в свою очередь либо полный доступ, либо доступ только для чтения (рис 2.).

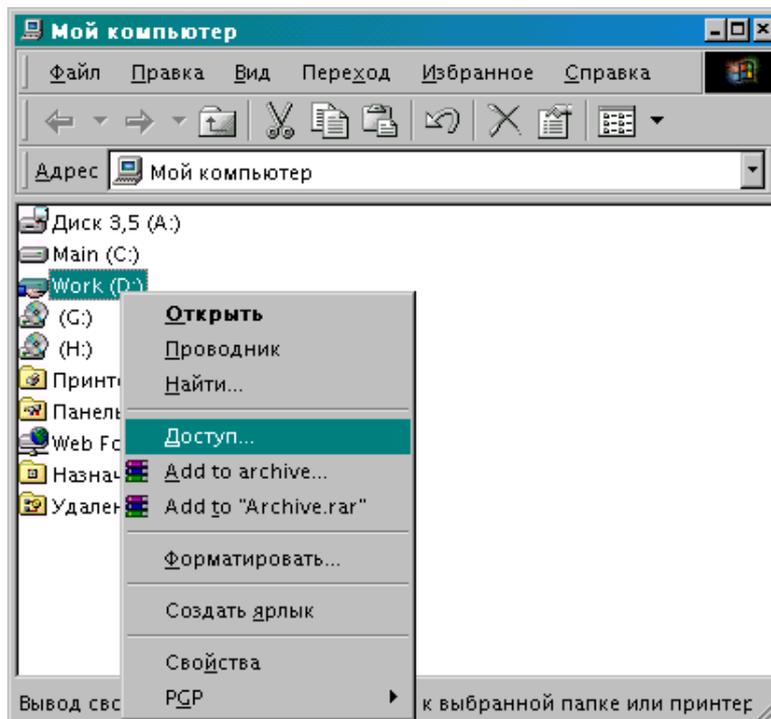


Рис.1. Вызов установки доступа к диску C

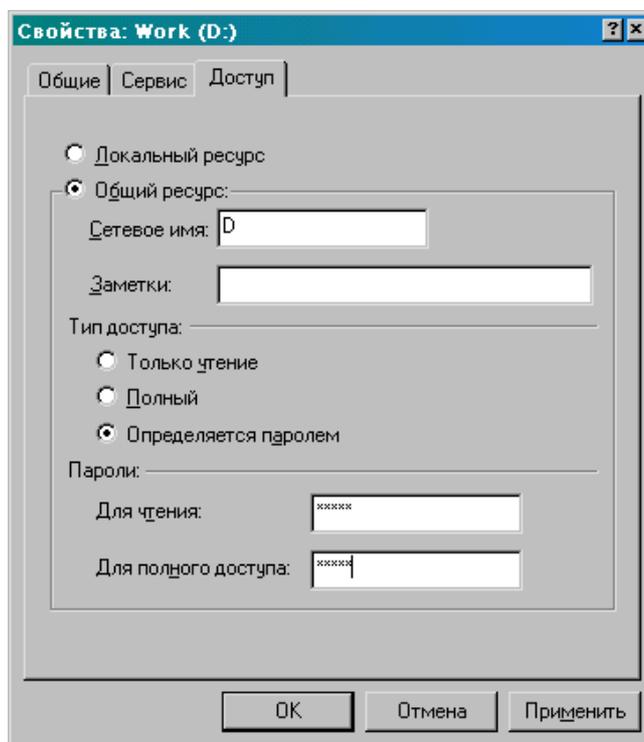


Рис. 2. Выбор варианта доступа к диску

Доступ к сетевому ресурсу может быть временный, либо постоянный. Для установления постоянного доступа необходимо подключить используемый диск в качестве логического диска так, как это показано на рис. 3.

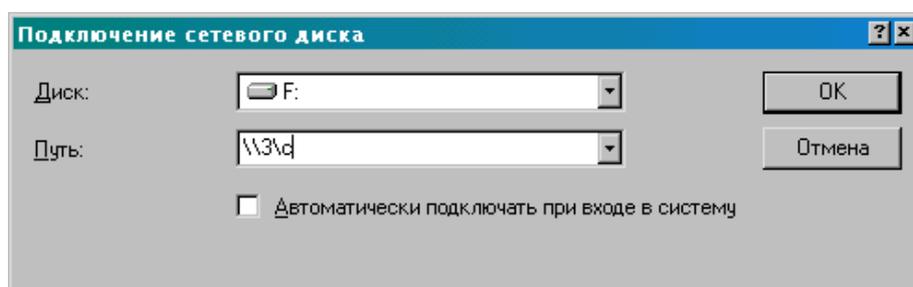


Рис.3. Установление постоянного доступа к диску C на компьютере с сетевым именем «3» в одноранговой ЛВС

Необходимо отметить, что предоставление сетевого доступа к каталогам диска и к принтеру осуществляется аналогичным образом.

Рассматривая правила организации доступа к местным и сетевым ресурсам, мы касались только одного способа управления доступом. Этот метод в Windows 95 получил название «Доступ на уровне ресурсов» (Share-level Access Control). Такой доступ предполагает защиту каждого из общих ресурсов собственным паролем.

Однако Windows 95 предлагает и другой способ управления доступом, который называется «Доступ на уровне пользователей» (User-level Access Control). Суть его весьма проста и понятна уже из названия: для каждого ресурса вы должны поименно указать список всех пользователей, которые имеют право работы с этим ресурсом.

Если мы хотим организовать доступ на уровне пользователей, то сначала необходимо включить этот режим, а уже потом можно будет для каждого ресурса поименно указать список пользователей. Осуществить это можно следующим образом:

1) дважды щелкните на значке «Сеть» и в одноименном окне диалога выберите вкладку «Управление доступом» (Access Control). Внешний вид этой вкладки продемонстрирован на рис. 5;

2) переключатель «Управление доступом к общим ресурсам производится» (Control Access to Shared Resources Using) установите в положение «На уровне пользователей» (User-level Access Control);

3) в поле «Взять список пользователей и групп с сервера» (Obtain List of Users and Groups From) введите имя компьютера, на котором будет храниться соответствующий список. Например, если он должен храниться на компьютере MAIN, то это имя и введите (рис. 4).

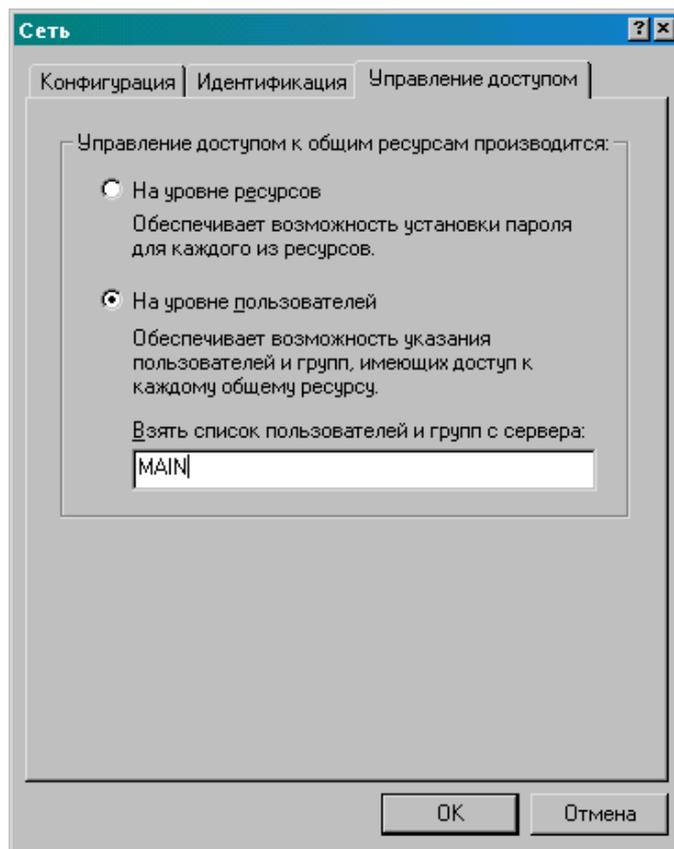


Рис. 4. Установка режима доступа к ресурсу на уровне пользователей

Если вы установили режим доступа на уровне пользователей (User-level Access Control), то это означает, что соответствующим образом изменились свойства каждого ресурса. Теперь вы уже можете установить права для каждого из пользователей сети. Делать это нужно следующим образом:

1) в папке «Мой компьютер» выберите папку, доступ к которой требуется ограничить;

2) откройте окно свойств этой папки, используя для этого команду «Файл» (File) или правую кнопку мыши для вызова контекстного меню;

3) выберите вкладку «Доступ» (Sharing) (рис. 5). Обратите внимание, что в окне приведен список всех пользователей и доменов сети, а также указаны определенные для них права доступа;

4) если список допущенных пользователей еще пуст или вы хотите добавить новых пользователей, то нажмите кнопку «Добавить» (Add);

5) в окне «Добавить пользователей» (Add Users), в списке слева выберите пользователя, домен или группу из нескольких пользователей, которым требуется предоставить доступ к ресурсам вашего компьютера, после чего нажмите одну из трех кнопок, определяющих тип прав доступа (рис. 6).

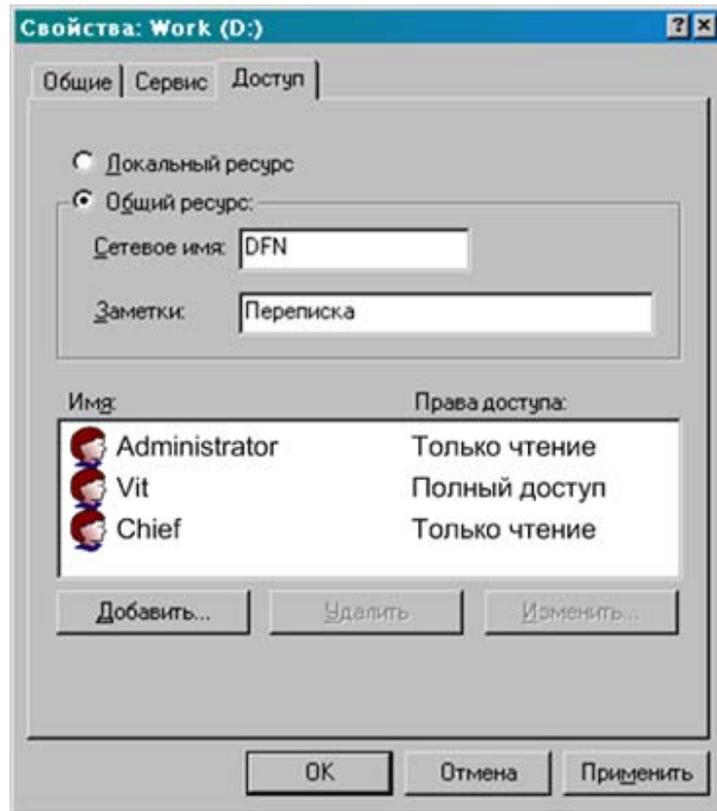


Рис. 5. Вкладка «Доступ» (Sharing) в окне свойств. Установлен режим доступа на уровне пользователей

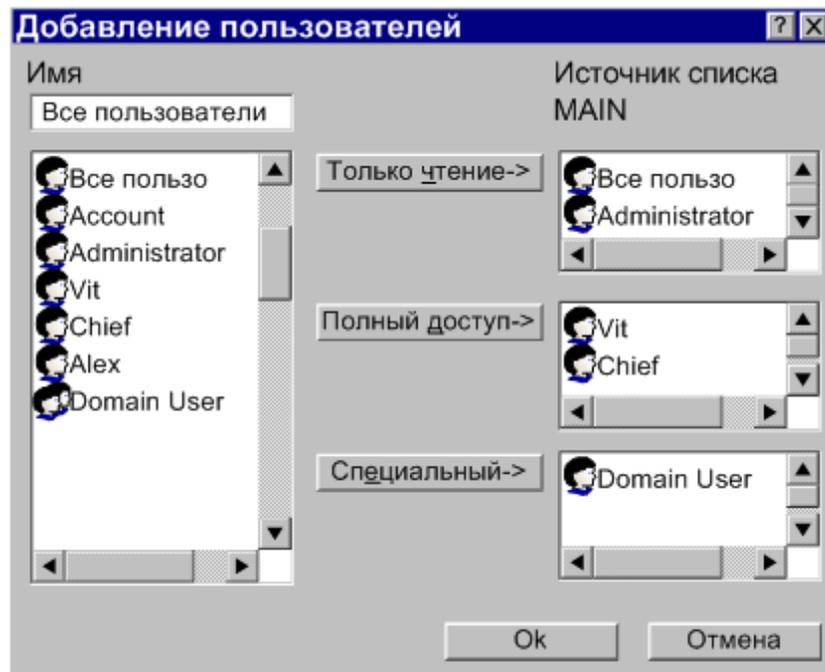


Рис. 6. Добавление новых пользователей

Из рис. 6 видно, что для каждого пользователя можно выбрать следующие права доступа: «Только чтение» (Read Only), «Полный доступ» (Full Access) или «Специальный» (Custom). Если вы устанавливаете права доступа «Специальный», то вам придется настраивать их в окне «Изменение прав доступа» (Change Access Rights).

3. Задания к лабораторной работе

3.1. Изучить подходы к созданию ЛВС и предоставлению доступа через сеть различных информационных ресурсов.

3.2. Познакомиться с возможностями Windows 95 в качестве сетевой операционной системы.

3.3. Создать на одном из компьютеров сетевой доступ к диску со всеми вариантами ограничений.

3.4. Установить постоянный доступ к данному диску на другом компьютере. И проверить ограничения доступа.

3.5. Установить доступ к диску для ряда пользователей с различными вариантами прав.

3.6. Убрать доступ к диску.

3.7. Повторить пункты 3.2, 3.3 и 3.4, но для вновь созданной директории.

4. Порядок выполнения работы

4.1. Проверить готовность компьютеров к проведению данной лабораторной работы.

4.2. Включить 2 или более компьютера и дождаться загрузки операционной системы Windows 95.

4.3. На одном из компьютеров по вышеописанной схеме предоставить в сетевое пользование один из дисковых накопителей по выбору (например, дисковод для гибких дисков).

4.4. На другом компьютере произвести проверочное чтение и запись с данным сетевым ресурсом.

4.5. Прodelать аналогичные шаги 4.3 и 4.4 для различных вариантов защиты данных (с ограничением доступа).

4.6. Повторить шаги 4.3 и 4.4, но для случая установления режима доступа на уровне пользователей.

5. Содержание отчета

5.1. Цель работы.

5.2. Описание действий для предоставления доступа к выбранной директории.

5.3. Описание действий по осуществлению постоянного доступа к выбранной директории.

5.4. Описание действий по осуществлению доступа к ресурсу на уровне пользователей.

5.5. Результаты исследования доступа к ресурсу при различных ограничениях доступа.

5.6. Выводы по работе.

6. Вопросы для самоподготовки

6.1. Отличительные особенности одноранговой ЛВС и ЛВС с выделенным файловым сервером?

6.2. Подходы для выделения дискового пространства компьютера в одноранговой ЛВС.

6.3. Последовательность действий для предоставления ограниченного доступа к дисковому накопителю компьютера в одноранговой ЛВС.

6.4. Последовательность действий для установления постоянного доступа к дисковому накопителю компьютера в одноранговой ЛВС?

6.5. В каких случаях выгоднее использовать режим доступа на уровне ресурсов, а в каких режим доступа на уровне пользователей?

6.6. Недостатки и достоинства защиты информации в одноранговой ЛВС.

Лабораторная работа №3

ИЗУЧЕНИЕ СТАНДАРТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТИ NETWARE

1. Цель работы

Цель работы - изучить методы и средства защиты информации в сети NetWare.

2. Общие сведения

Для получения доступа к сети злоумышленники могут использовать различные методы. Предотвратить доступ таких лиц к локальной сети можно с помощью регистрации пользователей и обеспечения их выхода из сети. Вы можете установить регистрацию пользователя только на определенной рабочей станции и в определенное время. Также необходимо предотвратить раскрытие злоумышленниками паролей и перекрыть все возможные обходные методы вхождения в сеть.

2.1. Механизмы защиты информации

2.1.1 Авторизация доступа к данным в сети. В NetWare реализованы три уровня защиты данных (рис. 7). Под аутентификацией понимается:

- процесс подтверждения подлинности клиента при его подключении к сети;
- процесс установления подлинности пакетов, передаваемых между сервером и рабочей станцией.

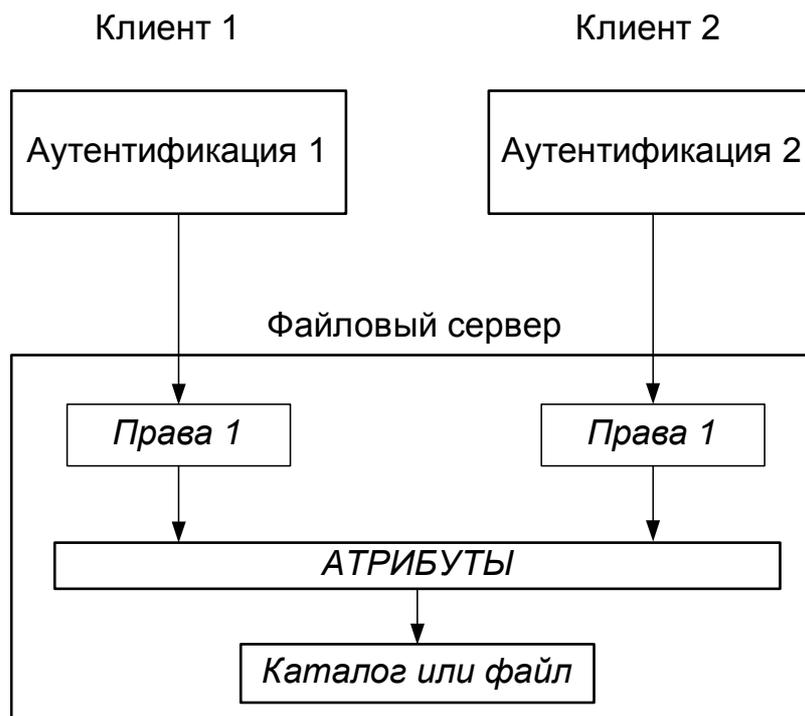


Рис.7. Уровни защиты данных в NetWare

Права по отношению к файлу (каталогу) определяют, какие операции пользователь может выполнить с файлом (каталогом). Администратор может для каждого клиента сети определить права по отношению к любому сетевому файлу или каталогу.

Атрибуты определяют некоторые системные свойства файлов (каталогов). Они могут быть назначены администратором для любого сетевого файла или каталога. Например, чтобы записать данные в файл, клиент должен:

- знать свой идентификатор и пароль для подключения к сети;
- иметь право записи данных в этот файл;
- файл должен иметь атрибут, разрешающий запись данных.

Следует отметить, что атрибуты файла (каталога) имеют более высокий приоритет, чем права пользователей по отношению к этому файлу.

2.1.2 Аутентификация пользователя при подключении к сети. Подключение к сети выполняется с помощью утилиты logfn.exe. Эта программа передаёт на сервер идентификатор, введённый пользователем (рис. 8).

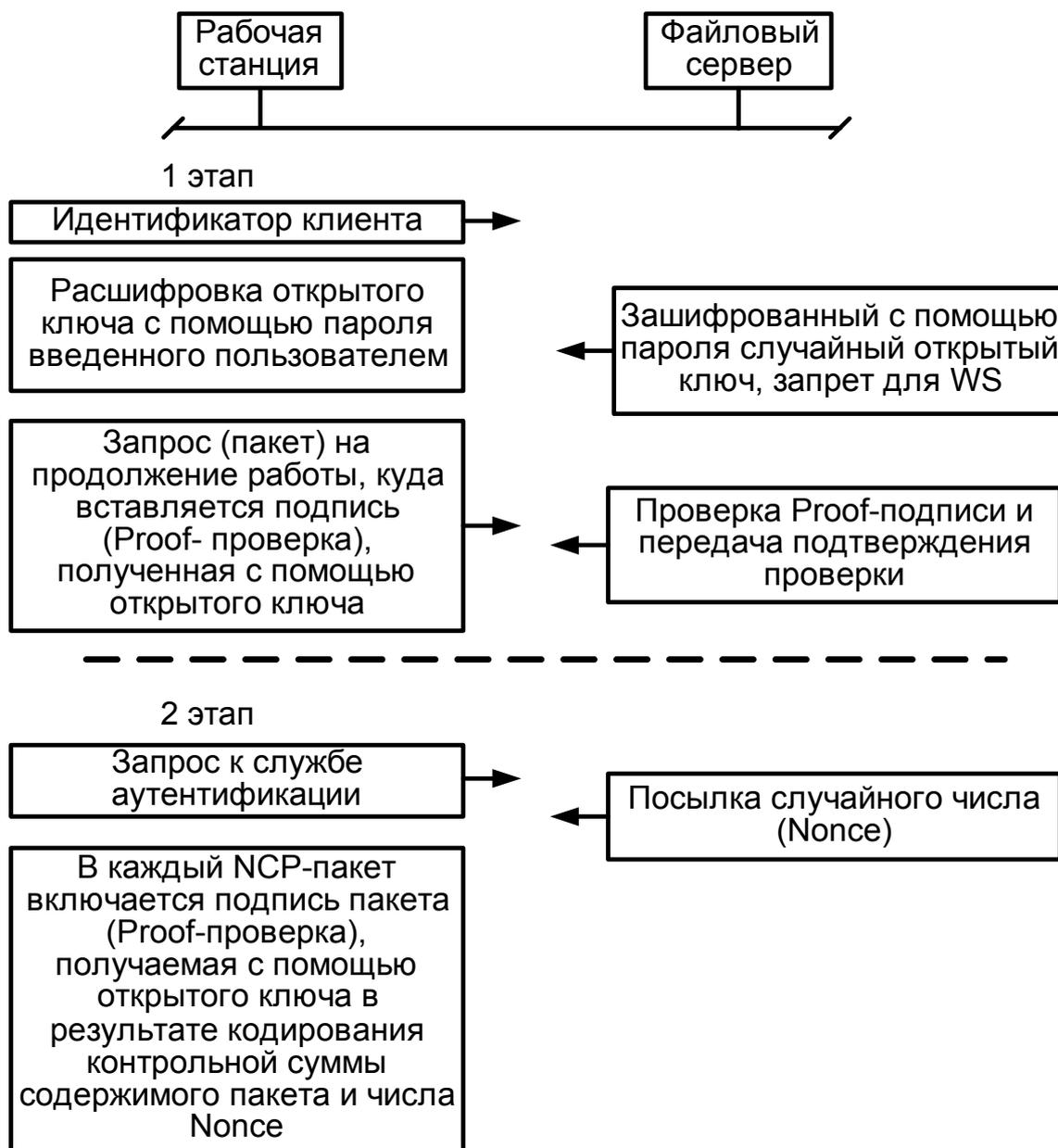


Рис. 8. Аутентификация клиента

По этому идентификатору NetWare выполняет поиск соответствующего объекта пользователя в системной базе данных сетевых ресурсов. Если в базе данных хранится значение пароля для этого клиента, то NetWare посылает на рабочую станцию зашифрованный с помощью пароля открытый ключ (симметричное шифрование). На рабочей станции этот ключ расшифровывается с помощью пароля, введённого пользователем, и ис-

пользуется для получения подписи запроса (пакета) к серверу о продолжении работы. Сервер расшифровывает эту подпись с помощью закрытого ключа (асимметричное шифрование), проверяет её и посылает подтверждение на рабочую станцию. В дальнейшем каждый NCP-пакет снабжается подписью, получаемой в результате кодирования открытым ключом контрольной суммы содержимого пакета и случайного числа Nonce. Это число генерируется для каждого сеанса. Поэтому подписи пакетов не повторяются для разных сеансов, даже если пользователь выполняет те же самые действия.

2.1.3 Права пользователей. В NetWare существует следующая иерархия прав: администратор, менеджер группы, группа пользователей, пользователь.

В NetWare v.4.0 за всей сетью наблюдает администратор (по крайней мере, первоначально). Он может создавать пользователей с правами супервизора для управления разделами каталога, относящимися к конкретному подразделению или отделу фирмы. Супервизор управляет сервером и пользователями в подразделении. Администратор может также привлекать супервизоров к установке дополнительных серверов в сети.

Администратор - это пользователь, который регистрируется с именем ADMIN. Пароль администратора - это ключ ко всей системе. Для него следует обеспечить особую секретность. Администратор имеет полномочия супервизора при доступе к корню дерева каталога, то есть обладает наивысшим уровнем доступа. Администратор может выполнять задачи, связанные с созданием, изменением или удалением объектов. Пользователь, задающий в дереве каталога первый NetWare-сервер, задает пароль ADMIN, имея, таким образом, все административные права.

Менеджеры групп обладают различным уровнем доступа к сети. Доступ к объединенной сети осуществляется путем регистрации в сети, а доступ к ресурсам управляется полномочиями доступа пользователя к объектам, каталогам и файлам.

Группы пользователей представляют собой наборы объектов пользователей. Они облегчают управление сетью и применение электронной почты. Ограничения, пароли, полномочия и другие характеристики могут назначаться супервизорами сразу для всей группы. Групповые объекты имеют имена и могут включать в себя пользователей из различных подразделений. Когда объект пользователя добавляется к группе, он получает полномочия этой группы. Таким образом, можно заранее создать группы для пользователей, проектов или администрирования, а затем просто добавлять при необходимости пользователей в нужные группы.

Пользователи могут получить доступ к сети, как только администратор или супервизор создадут для них пользовательский объект, который содержит его имя и пароль. Имена пользователей могут быть длиной до 47 символов, однако рекомендуется использовать формат, комбинирующий инициалы и фамилию пользователя. После создания объекта пользователя администратор или супервизор предоставляют ему права доступа к файловой системе.

2.1.4. Полномочия доступа и защита. Полномочия доступа и защита имеют для операционной системы жизненно важное значение. При правильном управлении защитой предотвращение потери или порчи данных из-за действий неуполномоченных пользователей и их секретность будут обеспечены. Первая "линия обороны" против неуполномоченных пользователей - это регистрация в системе с помощью пароля. Кроме того, назначение полномочий доступа к файлам позволяет ограничить доступ пользователей к файловой системе. Полномочия доступа позволяют также управлять использованием различных ресурсов сети. Полномочия доступа в NetWare группируются следующим образом:

- полномочия доступа к объектам управляют доступом к объектам системных ресурсов;
- полномочия владения управляют тем, кто может просматривать и изменять характеристики объектов;
- полномочия SMS управляют доступом к объектам в приложениях SMS (Storage Management System);
- полномочия доступа к каталогам определяют, кто может обращаться к каталогам на томах (дисках) и файлам в них;
- права доступа к файлам обеспечивают контроль доступа к файлам в каталогах на пофайловой основе.

2.1.5. Права и фильтры. Фильтр наследуемых полномочий IRF (Inherited Rights Filter) определяет, какие полномочия пользователи могут наследовать из порождающих каталогов и объектов-контейнеров. Вы можете использовать IRF для отмены некоторых или всех полномочий пользователя, наследуемых из порождающего (родительского) каталога или объекта.

Права и фильтры (маски) наследуемых прав назначаются администратором сети с помощью утилит NetWare. Но назначение прав для каждого пользователя по отношению ко всем требуемым файлам и каталогам - это утомительная задача. В NetWare предлагается механизм наследования прав:

- *Опекун (Trustees)* - это пользователь (или группа пользователей, или другой объект), которому администратор с помощью утилиты (например, FILER) явно назначает права по отношению к какому-либо файлу или каталогу. Такие права называются опекунами назначениями.

- *Фильтр наследуемых прав (IRF - Inherited Rights Filter)* - это свойство файла (каталога), определяющее, какие права данный файл (каталог) может унаследовать от родительского каталога. Фильтр назначается администратором с помощью утилиты (например, filer).

- *Наследуемые права* - права, передаваемые (распространяемые) от родительского каталога.

- *Эффективные права* - права, которыми пользователь реально обладает по отношению к файлу или каталогу.

2.1.6 *Атрибуты файлов и каталогов.* Ниже приводятся обозначение и краткое описание видов доступа к файлам и каталогам.

Таблица 1

Список возможных прав по отношению к каталогу или файлу

Право	Обозначение	Описание
Supervisor	S	Предоставляет все права по отношению к каталогу или файлу, включая возможность назначения этого права другим пользователям. Не блокируется фильтром наследуемых прав IRF. Это право не может быть удалено ниже по дереву каталогов.
Read	R	Чтение существующего файла (просмотр содержимого текстового файла, просмотр записи в файле базы данных и т.д.)
Write	W	Запись в существующий файл (добавление, удаление частей текста, редактирование записей базы данных)
Create	C	Создание в каталоге новых файлов (и запись в них) и подкаталогов. На уровне файлов позволяет восстанавливать файл, если он был ошибочно удален
Erase	E	Удаление существующих файлов и каталогов
Modify	M	Изменение имен и атрибутов (файлов и каталогов), но не содержимого файлов
File Scan	F	Просмотр в каталоге имен файлов и подкаталогов. По отношению к файлу - возможность видеть структуру каталогов от корневого уровня до этого файла (путь доступа)
Access Control	A	Возможность предоставлять другим пользователям все права, кроме Supervisor. Возможность изменять фильтр наследуемых прав IRF.

2.2. Работа с NetWare

2.2.1 *Подключение пользователей к системе.* Войдите в сеть как супервизор и запустите программу syscon.exe. В появившемся меню, показанном на рис. 9, выберите строку «User Information». Вы увидите список имеющихся пользователей, состоящий из двух строк - GUEST и SUPERVISOR.

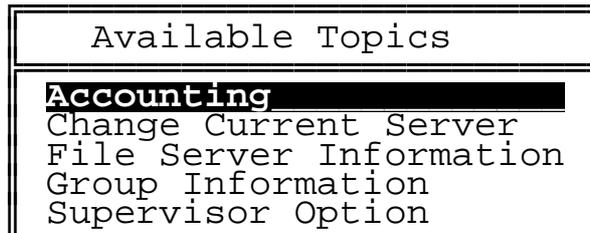


Рис. 9. Главное меню программы syscon.exe

Нажмите клавишу <Insert> и введите имя нового пользователя. После ввода имени появится окно, в котором вам будет предложено создать для этого пользователя индивидуальный каталог на диске SYS с именем, совпадающим с именем пользователя. Если вы не собираетесь создавать такой каталог, нажмите клавишу <Esc>. Для создания каталога нажмите клавишу <Enter>. В любом случае в списке «User Names» появится новый пользователь (рис. 10.).

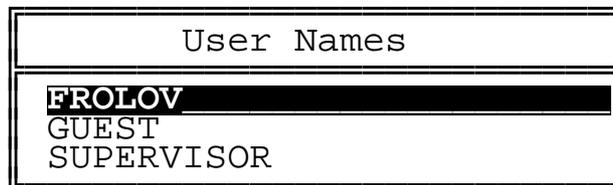


Рис. 10. Отображение имени нового пользователя в списке «User Names»

Выберите его и нажмите клавишу <Enter>. Появится окно «User Information», напоминающее окно «Group Information». С помощью этого окна вы можете установить для созданного пользователя различные атрибуты, права и ограничения. Детали вы узнаете позже. Прежде всего, создайте еще одного пользователя и наделите его правами супервизора (на тот случай, если вы забудете пароль супервизора). Для этого выберите строку «Security Equivalence». В появившемся списке нет пользователя SUPERVISOR. Вместо этого там находится «бесправная» группа «EVERYONE». Ничего страшного, просто нажмите клавишу <Insert>. Из полного списка пользователей и групп, появившегося вслед за этим на экране (рис. 11), выберите пользователя SUPERVISOR и нажмите клавишу <Enter>.

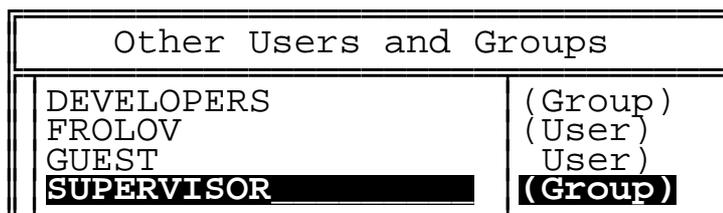


Рис. 11. Полный список имеющихся групп и пользователей

Теперь SUPERVISOR появится в списке «Security Equivalence». Выберите его и нажмите клавишу <Esc>. Вы создали пользователя с правами супервизора. Обязательно задайте пароль для него и для пользователя с именем SUPERVISOR. Для этого выберите строку «Change Password» и введите пароль два раза. Запишите пароль и храните где-нибудь в безопасном месте, так как, если вы забудете пароли для всех пользователей с правами супервизора, вам скорее всего придется заново переустанавливать Novell NetWare. Для каждого пользователя вы можете записать полное имя, если выберете строку «Full Name» из меню «User Information».

С помощью строки «Groups Belonged To» вы можете задать группу, к которой принадлежит данный пользователь.

Выбрав строку «Managed Users And Groups», вы сможете указать, какими пользователями и группами управляет данный пользователь. А с помощью строки «Managers» вы можете узнать, кто может управлять самим пользователем. Можно также сменить своего «менеджера». Разумеется, для выполнения всех перечисленных действий у вас должны быть соответствующие права - либо вы должны быть супервизором, либо должны управлять данным пользователем или группой, в которую он входит.

Учтите, что «назначить» руководителя группы может только супервизор. Для этого, запустив программу syscon.exe, необходимо выбрать из меню «Available Topics» строку «Supervisor Options». Появившееся меню (рис.12) открывает для супервизора много полезных возможностей.

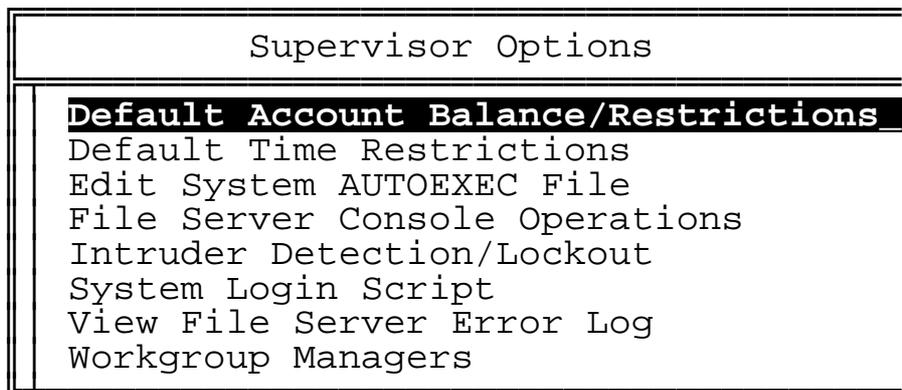


Рис. 12. Меню «Supervisor Options»

В частности, выбрав строку «Workgroup Managers», супервизор может назначить руководителя группы. Руководитель группы может самостоятельно подключать к файл-серверу новых пользователей и определять их права. Причем руководителем группы может быть не только пользователь, но и группа пользователей.

2.2.2. *Определение прав пользователей.* Для того, чтобы пользователь мог управлять работой сервера (имел доступ к соответствующим командам), он должен иметь права оператора консоли. Супервизор обладает такими правами и может предоставить их другим пользователям. Для этого ему надо выбрать строку «File Server Console Operator».

Выберите из меню «Supervisor Options» строку «Default Account Balance/Restrictions». На экране появится одноименная диалоговая панель (рис. 13).

Default Account Balance/Restrictions	
Account has expiration date: -----	No
Date account expire: -----	
Limit Concurrent Connections: -----	No
Maximum Connections: -----	0
Create Home Directory for User: ----	Yes
Require Password: -----	No
Minimum Password Length: -----	0
Force Periodic Password Changes: ---	No
Days Between Forced Changes: ----	0
Limit Grace Logins: -----	0
Grace Logins Allowed: -----	0
Require Unique Passwords: -----	No
Account Balance: -----	0
Allow Unlimited Credit: -----	No
Low Balance Limit: -----	0

Рис 13. Диалоговая панель строки «Default Account Balance/Restrictions»

При помощи этой панели вы можете повлиять на процедуру создания новых пользователей, а также задать ограничения, назначаемые для вновь создаваемых пользователей по умолчанию. Например, установив в поле «Create Home Directory for User» значение «No», вы отмените выдачу запроса на создание персонального каталога пользователя.

Если предъявляются повышенные требования к защите от несанкционированного доступа к ресурсам файл-сервера, укажите значение «Yes» в поле «Require Password». В этом случае для каждого вновь создаваемого пользователя будет необходимо указывать пароль.

Можно также указать минимальную длину пароля (поле «Minimum Password length»), потребовать периодическую смену пароля (поле «Force Periodic Password Changes»), причем период времени (в днях), в течение которого действует пароль, задается в поле «Days Between Forced Changes».

Есть и другая возможность ограничения доступа. Выбрав в меню «Supervisor Options» строку «Default Time Restrictions», вы сможете задать допустимое время подключения к сети в виде графика на каждый день не-

дели. Созданный график будет действовать по умолчанию для всех вновь создаваемых пользователей. Разумеется, такой график вы можете создать и для отдельных пользователей, а также для групп пользователей. Выбрав в меню «Supervisor Options» строку «Intruder Detection/Lockout», системный администратор может задать такой режим работы файл-сервера, при котором фиксируются все попытки подбора паролей пользователей.

По умолчанию при включенном режиме фиксации пользователю разрешается вводить неправильный пароль не более 7 раз в течение получаса. Если же этот лимит будет превышен, возможность подключения к сети для данного пользователя блокируется на 15 минут. Вы можете изменить указанные значения в соответствии с вашими требованиями.

Еще одна интересная возможность, доступная системному администратору, - просмотр журнала ошибок, который ведется на каждом файл-сервере. Для просмотра журнала ошибок выберите из меню «Supervisor Options» строку «View File Server Error Log». На экране появится содержимое журнала. В этот журнал записываются все ошибки, возникающие при работе операционной системы Novell NetWare, а также связанные с неправильными действиями пользователей (в том числе с преднамеренными попытками получения доступа к защищенным системным ресурсам, подбора паролей и т. д.).

2.2.3. Создание групп пользователей. После того как вы подключили пользователей, можно объединить их в группы. По умолчанию все вновь подключаемые пользователи приписываются к группе «EVERYONE». Как мы уже говорили, эта группа создается автоматически сразу после установки операционной системы Novell NetWare. Для создания новых групп войдите в сеть как супервизор. Из каталога SYS:PUBLIC запустите программу syscon.exe. С помощью этой программы вы будете выполнять практически всю работу по управлению пользователями и правами доступа.

Из меню «Available Topics» выберите строку «Group Information». В появившемся окне «Group Names» вы увидите список имен имеющихся групп.

Вы можете образовать новую группу пользователей, если нажмете клавишу <Insert> и введете имя новой группы. Если вы ошиблись, имя группы можно изменить, если ее высветить и нажать клавишу <F3>. Вы сможете отредактировать имя группы. Для удаления группы ее надо высветить и нажать клавишу <Delete>.

Для группы можно задать различные характеристики. Создайте

группу с любым именем, выберете ее и нажмите клавишу <Enter> . На экране появится меню «Group Information».

С помощью этого меню можно задать полное имя группы, определить списки пользователей, которые управляются данной группой или сами управляют ей, изменить состав группы, определить права группы по доступу к файлам и каталогам, расположенным на дисках файл-сервера.

Для изменения полного имени группы выберите в меню «Group Information» поле «Full Name» и введите имя. В полном имени группы можно отразить выполняемые этой группой функции, например: «Администраторы лаборатории А/25-007». Выбрав в меню «Group Information» строчку «Managed Users And Groups», вы сможете добавить в группу или удалить из нее подчиненных пользователей или подчиненные группы. Добавление выполняется клавишей <Insert>, удаление - клавишей <Delete>.

Для того, чтобы определить пользователей, управляющих группой, выберите строку «Managers». С помощью клавиши <Insert> вы можете добавить в появившийся список отдельных пользователей или группы. Добавленные пользователи и группы пользователей получают права по управлению группой, в частности, они смогут включать в группу новых пользователей и определять их права.

Выбрав строку «Member List», вы увидите список пользователей, входящих в группу. Вы сможете добавлять в этот список пользователей из числа имеющихся. С помощью клавиши <Delete> можно удалить пользователя из группы.

Выбрав строку «Other Information», вы сможете определить, обладает ли данная группа правами оператора консоли файл-сервера, а также сможете узнать идентификатор группы «Group To».

Очень важны строки «Trustee Directory Assignments» и «Trustee File Assignments», выбирая эти строки из меню «Group Information», вы сможете определить права группы пользователей по доступу к каталогам и файлам файл-сервера.

2.2.4 Определение прав доступа к дискам файл-сервера. После того как вы создали группы пользователей и подключили самих пользователей, вам следует определить права доступа к каталогам и файлам файл-сервера Novell NetWare.

Запустите программу syscon.exe. Сначала определите права доступа для групп пользователей. Для этого выберите из меню строку «Group Information», выберите нужную группу и нажмите <Enter>. Далее из меню «Group Information» выберите строку «Trustee Directory Assignments». На

экране появится список, в левой части которого находятся пути к каталогам, в правой - обозначен разрешенный вид доступа к соответствующему каталогу. Для вновь созданной группы список пуст. Нажмите клавишу <Insert>. Появится окно, озаглавленное «Directory In Which Trustee Should Be Added». Вы сможете указать в этом окне путь к каталогу, для которого необходимо определить доступ, например: sys:\users\frolov\alexandr\letters. Если вы вместо того, чтобы вводить путь к каталогу, нажмете еще раз клавишу <Insert>, появится список доступных вам файл-серверов.

Выберите файл-сервер и нажмите <Enter>. Появится список томов, расположенных на этом сервере. Выберите нужный том и из появившегося списка каталогов (рис. 14) выберите нужный вам каталог. Затем нажмите клавиши <Esc> и <Enter>. В списке "Trustee Directory Assignments" появится строка (рис. 15).

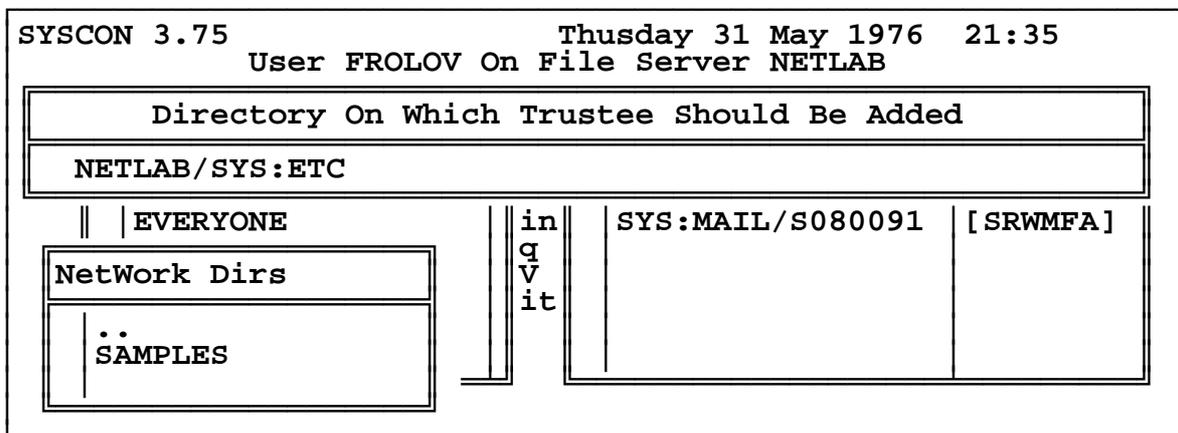


Рис. 14. Список каталогов, расположенных на выбранном сетевом томе

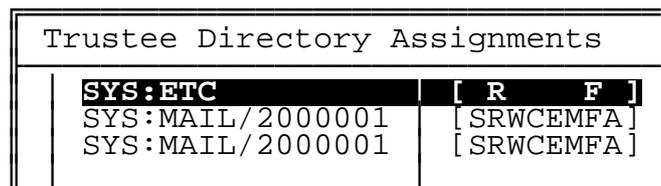


Рис.15. Новые права доступа, добавленные для каталога SYS:ETC

Слева будет путь к каталогу, справа - строка следующего вида: [R F]. Буквами «R» и «F» обозначается вид доступа, разрешенный группе для данного каталога: чтение файлов (Read); поиск файлов в каталоге (File Scan); запись файлов (Write). Нажав клавишу <Delete>, можно удалить строку из списка. При этом права на доступ к каталогу будут ликвидированы. Нажмите клавишу <Insert>. Появится меню, в котором будут представлены виды доступа к выбранному каталогу, не предоставленные для данной группы (рис. 16).

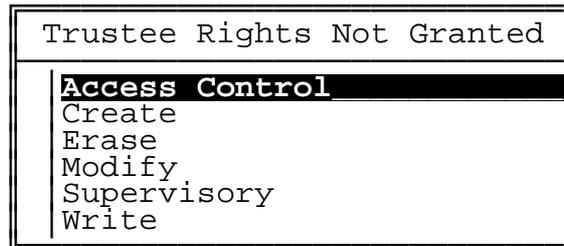


Рис. 16. Виды доступа, которые можно добавить

Для определения прав доступа к отдельным файлам выберите строку «Trustee File Assignments». После этого выберите сервер и каталог, содержащий нужный файл, аналогично тому, как это вы делали при определении прав доступа к каталогу. Затем в появившемся окне «Enter a file for editing trustees, or press <Insert> for a list of files» введите имя файла или (что лучше) нажмите клавишу <Insert> для выбора файла из списка. Выбор подтвердите нажатием клавиши <Enter>. Учтите, что, если содержимое файла на сервере изменится, вам придется заново предоставлять к нему доступ со стороны пользователей. Вам следует задать для каталога SYS:PUBLIC права на просмотр содержимого и чтение (т. е. права, задаваемые по умолчанию). Это нужно для того, чтобы пользователи могли запускать сетевые утилиты из каталога SYS:PUBLIC.

Иногда пользователям не нужны сетевые утилиты. Например, они могут просто работать с единственным томом SYS. Если это так, вы можете совсем не предоставлять некоторым пользователям доступ к каталогу SYS:PUBLIC.

Некоторые почтовые программы требуют, чтобы все пользователи имели доступ к каталогу SYS:MAIL на создание в нем файлов и запись (C и W). Доступ к этому каталогу должен быть организован по принципу почтового ящика - в него можно положить письмо, но нельзя взять или посмотреть содержимое ящика.

Обычные пользователи и администраторы групп не должны иметь никакого доступа к каталогу SYS:SYSTEM. Там находятся модули сетевой операционной системы и утилиты супервизора.

Не следует предоставлять пользователям доступ к корневым каталогам томов сервера. Предоставляйте пользователям доступ к каждому каталогу в отдельности. В этом случае создаваемые супервизором новые каталоги не будут доступны никому. Создав каталог, супервизор (или администратор группы, если он может создавать каталоги) может предоставить отдельным группам или пользователям доступ к нему. При этом он может

быть уверен в том, что другие группы или пользователи не имеют никакого доступа к вновь созданному каталогу

3. Задания к лабораторной работе

Для предложенной ситуации определить группу(ы) пользователей, менеджера(ов) и установить им права для работы в системе.

3.1 Сеть университета

Существуют два преподавателя. У каждого преподавателя есть группа студентов. Студенты выполняют контрольное тестирование, т.е. могут только прочитать тексты вопросов. Преподаватель определяет состав вопросов и разрешает допуск студента к файлу.

3.2 Сеть складов

В центральном оптовом складе существуют два управляющих, каждому из которых подчиняются по два отдела. Работники отделов могут просматривать базу данных товаров и заносить сведения в базу данных клиентов. Управляющий определяет для каждого отдела, с какими базами данных может работать отдел, и сам работает со всеми базами данных без ограничения доступа.

3.3 Сеть туристического агентства

Турагентство имеет каталог туров, с которым могут знакомиться клиенты. Консультанты оформляют заявки клиентов на участие в туре, модифицируя файл заявок. Каталог составляет менеджер агентства, он же контролирует работу консультантов (предоставляет права доступа консультантам). И существует бухгалтерия, которая может удалять заявку из файла по истечении определенного времени, определяемого менеджером.

4. Порядок выполнения работы

- 4.1. Получить вариант у преподавателя.
- 4.2. Изучить варианты заданий и выполнить анализ задания.
- 4.3. Создать пользователей.
- 4.4. Определить их права.
- 4.5. Объединить пользователей в группы.
- 4.6. Создать пользователей, являющихся менеджерами групп.
- 4.7. Определить права доступа к дискам файл-сервера.

5. Содержание отчета

- 5.1. Цель работы.
- 5.2. Сведения об основных способах защиты информации в NetWare.
- 5.3. Маршрут активизации защиты в NetWare.

5.4. Результаты анализа задания.

5.5. Результаты выполнения работы (схемы защиты с объектами и разрешениями).

5.6. Выводы по работе.

6. Вопросы для самоподготовки

6.1. Известные механизмы защиты информации в NetWare.

6.2. Назовите уровни защиты.

6.3. Охарактеризуйте первый, второй и третий уровни защиты.

6.4. Иерархия прав. Администратор. Его права и обязанности.

6.5. Менеджеры групп, группы пользователей. Пользователи. Права.

6.6. Назначение полномочий доступа. Группы полномочий.

6.7. Понятие фильтра наследуемых прав? Правила использования? Механизмы наследования прав, предлагаемых в NetWare.

6.8. Атрибуты файлов и каталогов.

6.9. Назовите основные этапы подключения пользователей к сети.

6.10. Назовите основные этапы определения прав пользователей.

6.11. Назовите основные этапы создания групп пользователей.

6.12. Основные этапы определения прав доступа к дискам файл-сервера.

Лабораторная работа № 4

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

1. Цель работы

Познакомиться с методикой организации защиты информации в автоматизированных рабочих местах (АРМ) и способами разграничения доступа к информационным ресурсам системы.

2. Общие сведения

Система поддержки принятия решений (СППР) конфигурируется под решаемую задачу в режиме configdb.exe. Меню пользователя создается с помощью элемента базы данных (БД) «Список элементов». Элемент «Список элементов» содержит в себе три отдельных списка, в которых сгруппированы вызываемые элементы под названием «Список предобъектов», «Список доступных объектов» и «Список постобъектов». «Список доступных объектов» образует пункты меню пользователя, вызываемые в режиме диалога dialogdb.exe.

Элементы списка предобъектов инициируются компьютером автоматически перед первым обращением к какому либо элементу БД из списка доступных объектов. В список предобъектов включаются элементы БД, которые должны выполняться без вызова пользователя до вызова пунктов меню в режиме диалога.

В список постобъектов заносятся элементы БД, которые инициируются компьютером после завершения диалога и выхода из меню пользователя. Сюда заносятся элементы БД, выполняемые без участия пользователя.

Каждая запись списка содержит два поля: <имя файла> <уровень доступа>. Установкой уровня доступа разграничивается доступ пользователей к элементам списка. Корневым списком, образующим меню пользователя, является «Список элементов», имеющий идентификатор ROOT. СППР позволяет разрабатывать меню пользователя иерархической структуры. Каждый пункт меню может состоять из подпунктов, а подпункты, в свою очередь, из других подпунктов и т.д. Иерархичность структуры меню обеспечивается за счет включения в список доступных объектов в качестве элементов других списков и т.д. Уровень вложенности списков не ограничивается.

Программное обеспечение СППР требует распределения оперативной памяти компьютера под функциональные программы системы и БД. Память, занимаемая функциональными программами, относительно стабильна, а выделяемая под локальную базу данных - зависит от количества элементов и их размерностей.

2.1 Установка комплекса

Проводится в режиме конфигурирования (configdb.exe). Для настройки выбирается пункт меню «Настройка». Выбрав пункт «Разное» из меню следующего уровня задаются параметры настройки:

1) путь к данным, хранящимся в БД (например, AWS*.aws). Задание пути к файлам и расширения имен файлов позволяет указывать при обращении к элементам БД только имя файла дескриптора элемента;

2) список пользователей задает имя файла для хранения списка фамилий, уровня доступа и паролей пользователей (password.aws);

3) имя файла первого элемента БД, с которого начинается работа компоненты dialogdb.exe (например, root.aws);

4) имя файла для хранения системного журнала (svcllog.aws), максимальное количество записей;

5) отмена звукового сигнала при выдаче на экран сообщений об ошибках (N);

6) атрибуты цветов различных элементов изображения на экране.

В подпункте «Пользователи» меню «Настройка» указывается фамилия пользователя, уровень доступа от 0 (самый высокий) до 255 (самый низкий) и пароль из четырех любых символов. В результате проведения инсталляции в активном каталоге либо создается, либо изменяется файл `config.aws`, в котором храниться информация о настройке.

2.2. Конфигурирование базы данных

Включает в себя создание новых элементов БД, коррекцию и удаление существующих элементов. При работе в режиме `configdb.exe` в пункте меню «Элементы БД» администратор базы данных может просмотреть имена, типы, имена файлов дескрипторов существующих элементов БД, корректировать информацию, определяющую сущность элементов БД, удалять файлы дескрипторов с диска, а также выполнять функции, определенные для нормальной работы комплекса, без запуска компоненты `dialogdb.exe`. Для просмотра списка элементов БД выбирается пункт меню «Оглавление БД». Здесь можно просмотреть списки элементов одного или несколько выбранных типов.

3. Задание к лабораторной работе

3.1. Выполнить инсталляцию комплекса. Ввести свою фамилию в список пользователей, задав уровень доступа и пароль.

3.2. Составить схему меню пользователя исследуемой системы. Выявить подпункты меню, не требующие диалога с пользователем.

3.3. Предложить проект упрощенного варианта меню пользователя. Согласовать его с преподавателем.

3.4. Создать разработанный вариант меню пользователя для СППР и проверить удобство работы пользователя с системой с вновь созданным меню.

3.5. Создать элемент аутентификации пользователя для организации доступа к системе поддержки принятия решений.

3.6. Выделить типы данных с конфиденциальной информацией. Определить группу пользователей и организовать разграниченный доступ к данным.

3.7. Испытать систему защиты на тестовых примерах.

4. Порядок выполнения работы

4.1. Войти в режим диалога. Нажав клавишу F1 вызвать «Помощь». Ознакомиться с общими положениями по работе с комплексом, работой с

элементами БД в режиме просмотра БД, а также с сообщениями об ошибках.

4.2. В режиме конфигурирования выбрать пункт меню «Настройка». В подпункте «Пользователи» набрать свою фамилию, установить уровень доступа и записать пароль для входа в систему.

4.3. Составить схему меню исследуемой системы в режиме configdb.exe элемента ROOT. Перейти в режим dialogdb.exe. Выполнить все пункты меню и отметить те пункты, выполнение которых не требует диалога с пользователем.

4.4. Составить схему упрощенного варианта меню пользователя. Согласовать схему с преподавателем.

4.5. Разработать структуру элемента БД типа «Список элементов», заполнив в нем три типа списков: «Список предобъектов», «Список доступных объектов», «Список постобъектов». Эти списки должны содержать все элементы исходного списка элементов ROOT. Структуру предлагаемого списка элементов согласовать с преподавателем.

4.6. В режиме configdb.exe внести корректировку в элемент БД ROOT в соответствии с предложенным проектом меню пользователя.

4.7. Программным путем разграничить доступ к выделенным файлам с информацией ограниченного пользования.

4.8. Перейти в режим dialogdb.exe и испытать работу системы. Продемонстрировать результаты конфигурирования системы преподавателю. Восстановить исходное меню системы.

4.9. Завершить работу, выйти из СППР, отключить компьютер в соответствии с инструкцией пользователя.

5. Содержание отчета

5.1. Цель работы.

5.2. Схема исходного меню пользователя. Состав элементов БД типа «Список элементов» ROOT.

5.3. Схема разработанного варианта меню пользователя и содержание созданного элемента «Список элементов».

5.4. Таблица распределения ресурсов оперативной памяти компьютера под компоненты программного комплекса СППР и ее базу данных.

5.5. Схема защиты и разграничения доступа, выбранная в работе. Используемые в работе средства MS DOS и персонального компьютера.

5.6. Оценка прочности защиты и разграничения доступа к информации.

5.7. Выводы по работе.

6. Вопросы для самоподготовки

6.1. Особенности построения информационных СППР. Выполняемые функции, используемые информационные технологии, используемые средства защиты и аппаратно-программная реализация.

6.2. Технология создания меню пользователя в исследуемой СППР. Используемые методы защиты информации в СППР промышленных предприятий.

6.3. Состав программного комплекса исследуемой СППР. Механизмы защиты и разграничения доступа к информации. Распределение ресурсов оперативной памяти.

6.4. Организационные, аппаратные и программные меры защиты в информационных системах. Прочность мер защиты.

6.5. Понятие идентификации и аутентификации в информационных системах, их реализация.

6.6. Понятие инсталляции и конфигурирования системы, ее содержание.

Лабораторная работа № 5

ОДНОКЛЮЧЕВЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ

1. Цель работы

Изучить простейшие алгоритмы блочного шифрования данных в одноключевых криптографических системах (КС). Исследовать скорость шифрования данных.

2. Общие сведения

Одноключевые КС можно представить единой схемой, представленной на рис. 17.

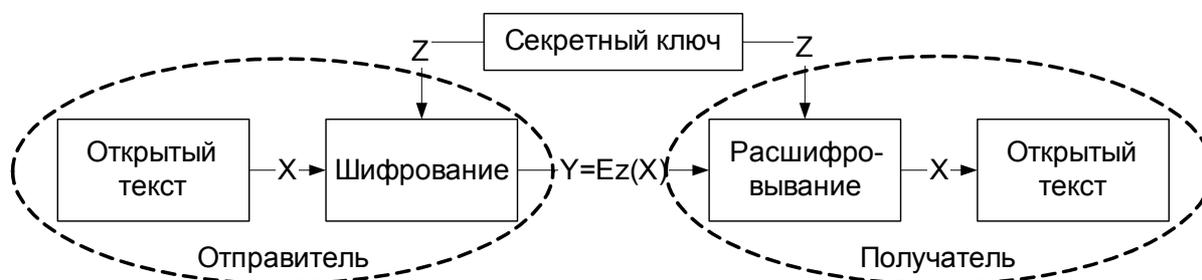


Рис. 17. Структурная схема одноключевой КС

На рисунке приняты следующие обозначения: X – открытый текст; Y – шифротекст; Ez(X) – функция шифрования; Z – ключ шифрования.

Далее вкратце опишем существующие методы шифрования характерные для одноключевых КС:

1) простая (одноалфавитная) подстановка. Способ шифрования, когда каждый символ (принадлежащий одному алфавиту) открытого текста заменяется символом из другого алфавита. Например, буквы заменяются цифрами, символами и т.д.;

2) многоалфавитная подстановка. Несколько подстановок шифров, например, в зависимости от номера буквы в открытом тексте. Впервые использовал Леон Баптиста в 1568 г. Также использовалась объединенной Армией во время гражданской войны в Америке, до сих пор используется в текстовом редакторе WordPerfect;

3) шифрование с использованием двоичного кода. Двоичное представление буквы складывается по модулю два с двоичным ключом. Результатом сложения является шифротекст (рис. 18). В данном случае длина ключа равна четырем, но в общем случае она может быть произвольной;

4) шифр Цезаря – циклический сдвиг на 3 вправо по модулю 26 (26 – количество букв в латинском алфавите). В общем случае сдвиг может производиться на большее число позиций h. В шифре Цезаря связь между исходным алфавитом и алфавитом шифротекста имеет вид

$$F(h_i) = [F(m_i) + h] \text{ mod } K,$$

где K – количество знаков в алфавитах; m_i – знак исходного текста, принадлежащего алфавиту A, h_i – знак исходного текста, принадлежащего алфавиту шифротекста B;

5) многоалфавитные шифры – шифр Вижинера, шифр Энигма, цилиндр Джефферсона и другие.

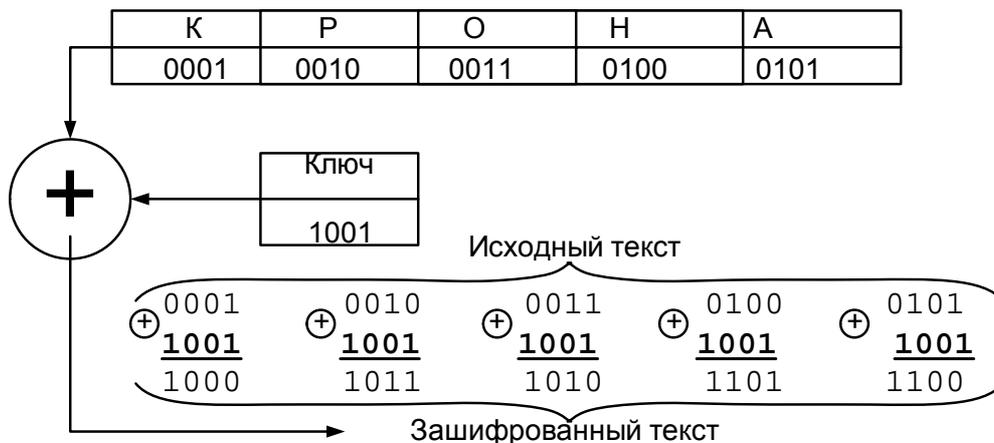


Рис. 18. Шифрование с использованием двоичного кода

Рассмотрим суть алгоритма шифра Вижинера. Совокупность всех алфавитов, сведенных в одну таблицу, образует так называемую шифровальную таблицу Вижинера (рис. 19). Это есть множество (для русского алфавита) из 33 алфавитов, циклически сдвинутых друг относительно друга на одну букву (подобно шифру Цезаря).

А	Б	В	Г	Д	...	Э	Ю	Я
Б	В	Г	Д	Е	...	Ю	Я	А
В	Г	Д	Е	Ё	...	Я	А	Б
Г	Д	Е	Ё	Ж	...	А	Б	В
Д	Е	Ё	Ж	З	...	Б	В	Г
Е	Ё	Ж	З	И	...	В	Г	Д
...
Я	А	Б	В	Г	...	Ь	Э	Ю

Рис.19. Шифровальная таблица Вижинера для русского алфавита

При шифровании исходное сообщение разбивается на блоки длиной равной длине ключевого слова. Например, если исходное сообщение «баба где деда», и ключевое слово «где», то разбиение будет выглядеть следующим образом:

где где где где

баб агд еде да

Далее в таблице выбирается строка с алфавитом, начинающимся с первой буквы ключевого слова (буквы «Г»). В этом алфавите выбирается та буква, которая стоит напротив буквы исходного сообщения (буквы «Б») нормального алфавита (первая строка таблицы) и получаем букву «Д» (рис. 19). Следующая буква находится на пересечении строки таблицы, начинающейся со второй буквы ключевого слова (буквы «Д») и столбца, начинающегося со второй буквы открытого текста (буква «А») в итоге получается буква «Д». Зашифрованное сообщение для исходного текста будет таким:

ддё гзи изй жд

б) группа шифров с использованием перестановок

Такие алгоритмы шифрования переупорядочивают группу текста регулярным образом в соответствии с выбранным ключом (правилом) перестановки. При этом часто использовались специальные таблицы, которые давали простые шифрующие процедуры (ключи), согласно которым производились перестановки букв в сообщении. Ключом у таких таблиц служили размеры таблицы, фраза, задающая перестановку или другие специальные особенности таблицы:

а) пример простейшего шифра перестановки представлен на рис. 20. Например, шифруем сообщение «ЮСТАС АЛЕКСУ ВСТРЕЧАЙТЕ СВЯЗНОГО». Для этого текст сообщения записывается по столбцам, после чего считывается построчно и записывается группами, например, по 5 цифр. Последнее не относится к процессу шифрования и нужно лишь для удобства записи шифрограммы. Для расшифровки такого текста необходимо знать ключ – размер таблицы;

Ю	А	У	Е	Е	Н
С	Л	В	Ч	С	О
Т	Е	С	А	В	Г
А	К	Т	Й	Я	О
С	С	Р	Т	З	Ъ

ЮАУЕЕ НСЛВЧ СОТЕС АВГАК ТЙЯОС СРТЗЪ

Рис. 20. Шифрование перестановкой

б) другой способ шифрования с использованием таблиц заключается в том, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной равной длине строки таблицы. Например, используя ключ «246136», производится перестановка букв исходного сообщения открытого текста. Первая буква ключа «2» указывает на то, что в очередном шифрованном блоке первой буквой будет вторая буква из исходного текста. Вторая цифра ключа «4» говорит о том, что второй буквой в шифре будет четвертая буква из исходного блока текста и т.д. Подобная перестановка выполняется внутри каждого блока, рис. 21. Для упрощения запоминания ключа обычно используют ключевое слово. В данном случае это слово «КОРЕНЬ».

Открытый текст	ЗАСЕДА	НИЕСОС	ТОИТСЯ	ЗАВТРА	ЮСТАСЪ
	123456	123456	123456	123456	123456
Ключевое слово	корень				
Ключ	246136				
Зашифрованный текст	АЕДЗСА	ИСОНЕС	ОТСТИЯ	ФТРЗВА	САСЮТЬ
	123456	123456	123456	123456	123456

Рис. 21. Шифрование с перестановкой столбцов при использовании ключа

в) шифр простой перестановки с использованием свойств таблиц, называемых магическими квадратами, использовался еще в средние века.

13	8	12	1
2	11	7	14
3	10	6	15
16	5	9	4

При этом буквы исходного сообщения записываются в обычном порядке, а считываются из нее в порядке нумерации клеток таблицы.

3. Варианты индивидуального задания

- 3.1. Шифры простой подстановки
- 3.2. Шифр Цезаря с циклическим сдвигом на n букв
- 3.3. Одноалфавитная подстановка, когда одной букве может соответствовать несколько букв шифротекста.
- 3.4. Шифр Вижинера.
- 3.5. Шифрование с использованием двоичного кода (сложение по модулю 2).
- 3.6. Шифрование перестановкой с использованием таблиц $m \times n$.
- 3.7. Шифрование перестановками с использованием таблиц $m \times n$ и с использованием ключа для перестановки строк.
- 3.8. Шифрование перестановками с использованием таблиц $m \times n$ и с использованием ключа для перестановки строк и столбцов.
- 3.9. Шифр простой перестановки с использованием свойств таблиц (магические квадраты).

4. Порядок выполнения работы

В качестве языка программирования при выполнении работы может быть выбран Pascal или C++.

- 4.1. Получить у преподавателя вариант индивидуального задания.
- 4.2. Ознакомиться с простейшими методами шифрования текста.
- 4.3. Реализовать выбранный алгоритм шифрования (дешифрования).
- 4.4. Исследовать скорость работы алгоритма в зависимости от длины ключа и длины шифруемого сообщения.

5. Содержание отчета

- 5.1. Цель работы.
- 5.2. Вариант индивидуального задания.
- 5.3. Описание алгоритма реализации.
- 5.4. Рабочие примеры выполнения программы (пример шифрования и дешифрования).
- 5.5. Результаты исследований быстродействия алгоритма шифрования/дешифрования с анализом результатов.
- 5.6. Листинги программ.
- 5.7. Выводы по работе.

6. Вопросы для самоподготовки

- 6.1. Общая схема работы одноключевых КС.
- 6.2. Особенности использования одноключевых КС.
- 6.3. Назначение и использование функций шифрования и дешифрования.
- 6.4. Назначение ключа шифрования/дешифрования в КС.

Лабораторная работа № 6

ПОТОЧНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ

1. Цель работы

Изучить алгоритмы поточного шифрования, основанные на различных способах формирования псевдослучайных последовательностей (ПСП).

2. Общие сведения

Впервые поточное шифрование использовалось в так называемом одноразовом блокноте (шифр Вернама). При шифровании использовалась уникальная абсолютно случайная ключевая последовательность. При этом символы открытого текста складывались по модулю два с символами последовательности. Такие шифры обладают абсолютной криптостойкостью, так как не существует механизма повторного воспроизведения содержимого блокнота. Ключевая последовательность доставляется абоненту отдельно от шифротекста. Такое шифрование имеет ряд неудобств при работе. Впоследствии абсолютно случайная ключевая последовательность была заменена ПСП, которая формируется с использованием регистров сдвига с линейной обратной связью (РСЛОС).

РСЛОС состоит из двух частей: регистра сдвига и последовательно-стью ответвления (рис. 22).

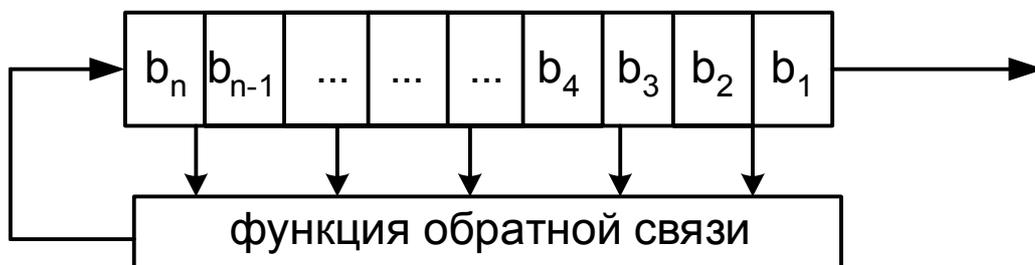


Рис.22. Регистр сдвига с линейной обратной связью

В этой схеме регистр сдвига есть последовательность битов. Как только нам нужен следующий бит, все биты регистра сдвига сдвигаются направо и РСЛОС выдает наименее значимый бит. При этом наибольший значимый бит вычисляется через функцию обратной связи (часто XOR) от прочих битов регистра, согласно последовательности ответвления. Последовательность ответвления может быть разной и в каждом конкретном случае определяется самой схемой регистра. Теоретически, n -битный РСЛОС может сгенерировать псевдослучайную последовательность длиной $2^n - 1$ бит перед заикливанием. Для этого регистр сдвига должен побывать во всех $2^n - 1$ внутренних состояниях (количество состояний именно $2^n - 1$, а не 2^n , так как регистр сдвига, состоящий из нулей, вызовет бесконечную последовательность нулей, что не очень удачно).

В поточных шифрах ключевая последовательность формируется независимо от последовательности символов открытого текста и каждый символ этого текста шифруется независимо от других символов, а ключом Z является начальная установка генератора ПСП и сами регистры. Процесс шифрования и расшифровывания при этом описывается выражениями:

$$y_i = x_i \oplus F_i(Z) \text{ – шифрование; } x_i = y_i \oplus F_i(Z) \text{ – расшифровывание,}$$

где y_i , x_i – двоичные символы зашифрованного и открытого текста, $F_i(Z)$ – i -й символ ПСП, вырабатываемый генератором с функцией обратной связи F и начальным состоянием Z . То есть, процесс шифрования определяется способом построения ПСП:

- а) метод комбинирования ПСП;
- б) метод функциональных отображений.

Метод комбинирования ПСП заключается в построении комбинированных схем, представляющих собой совокупность регистров сдвига с линейными обратными связями. Примерами таких схем являются схема Джеффа (рис. 23а) и схема Брюса (рис. 23б).

Отличие этих двух схем состоит в использовании для формирования ПСП различных логических устройств. Так, в схеме Джеффа применяется операция логического умножения и сложения по модулю 2. Схема Брюса использует пороговое устройство, работающее по правилу: на выходе 1, если порог превышен, иначе 0:

$$O = \begin{cases} 1, & \text{если порог превышен} \\ 0, & \text{иначе} \end{cases}$$

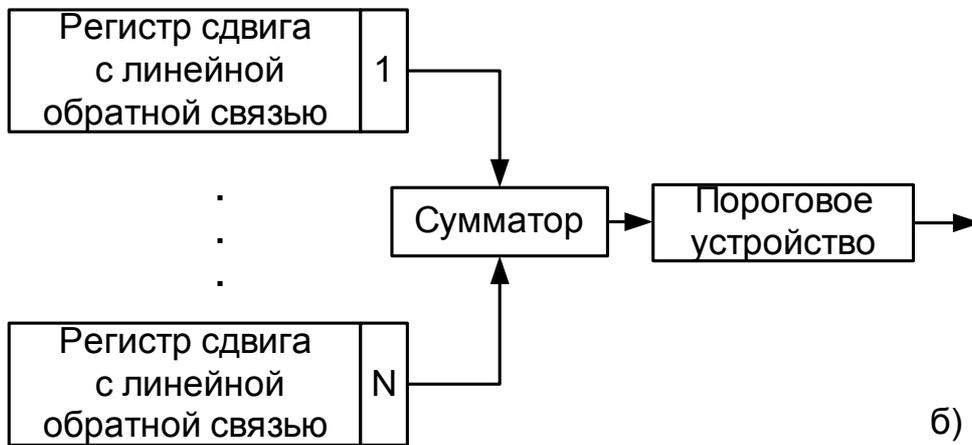
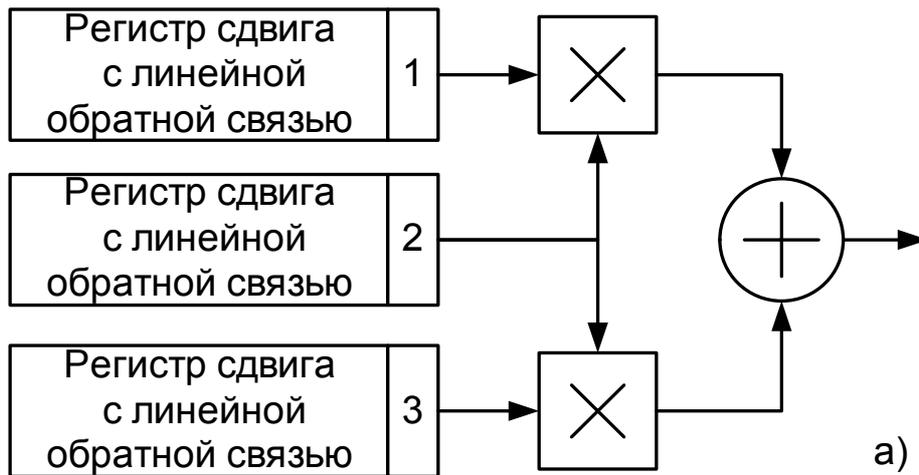


Рис. 23. Методы комбинирования ПСП: (а) схема Джеффа; (б) схема Брюса

Метод функциональных отображений является более сложным. Пусть дано некоторое векторное пространство $GF(2^m)$ с числом координат m в каждом векторе, причем каждая координата вектора принадлежит множеству скалярных величин $GF(2)=\{0, 1\}$. Очевидно, что общее число векторов, принадлежащих пространству равно 2^m . Пусть задано некоторое функциональное отображение f , которое каждому вектору из пространства $GF(2^m)$ ставит в соответствие вектор из пространства $GF(2^k)$. При этом обязательным является выполнение условия $k \leq m$. Далее пусть задано некоторое функциональное отображение g , которое каждому вектору из $GF(2^k)$ ставит в соответствие скаляр из множества $GF(2)$. В этом случае получим ПСП с использованием вышеприведенных функциональных отображений. Например, ПСП, полученная по схеме, изображенной на рис. 24 ($m=4, k=2$) по методу двухступенчатых отображений.

Метод ступенчатого отображения $GF(2^m) \rightarrow GF(2^k) \rightarrow GF(2)$ впервые был использован при построении последовательностей Гордона-Милса-Велга. Для порождения векторного пространства $GF(2^m)$ использовались регистры сдвига с линейными обратными связями.

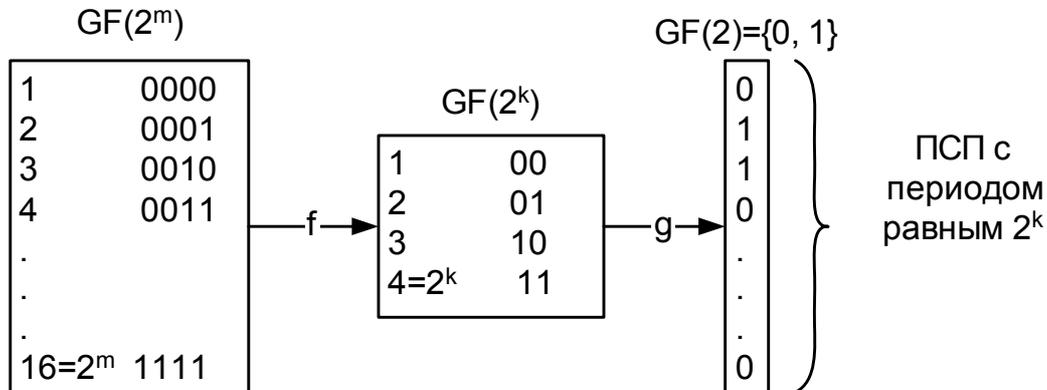


Рис. 24. Принцип формирования ПСП по методу двухступенчатых отображений

3. Задания к лабораторной работе

Замечания:

а) функции обратной связи задаются студентом самостоятельно. Вид функций предварительно согласовывается с преподавателем;

б) в случае, если для формирования ПСП используется схема Брюса, значение порогового регистра выбирается студентом по согласованию с преподавателем.

3.1. Разрядность РСЛОС 6. Формирование ПСП по схеме Джеффа.

3.2. Разрядность РСЛОС 4. Формирование ПСП по схеме Джеффа.

3.3. Разрядность РСЛОС 9. Формирование ПСП по схеме Джеффа.

3.4. Разрядность РСЛОС 7. Формирование ПСП по схеме Джеффа.

3.5. Разрядность РСЛОС 6. Формирование ПСП по схеме Брюса. Количество регистров 6.

3.6. Разрядность РСЛОС 4. Формирование ПСП по схеме Брюса. Количество регистров 10.

3.7. Разрядность РСЛОС 8. Формирование ПСП по схеме Брюса. Количество регистров 8.

3.8. Формирование ПСП по методу двухступенчатых отображений для $m=6$ и $k=4$.

3.9. Формирование ПСП по методу двухступенчатых отображений для $m=8$ и $k=4$.

3.10. Формирование ПСП по методу двухступенчатых отображений для $m=10$ и $k=4$.

4. Порядок выполнения работы

В качестве языка программирования при выполнении работы может быть выбран Pascal или C++.

4.1. Ознакомиться с методами и схемами поточного шифрования.

4.2. Получить у преподавателя вариант индивидуального задания.

4.3. Реализовать свой РСЛОС в соответствии с вариантом индивидуального задания.

4.4. Реализовать алгоритм шифрования (дешифрования), использовать шифр Вернама. В качестве генератора ключевой последовательности использовать ПСП. При этом шифрование должно осуществляться непосредственно при вводе пользователем символов с клавиатуры. Во время ввода отображать формируемую ПСП и результат дешифрования.

4.5. Исследовать период формируемой ПСП.

5. Содержание отчета

5.1. Цель работы.

5.2. Вариант индивидуального задания.

5.3. Описание алгоритма реализации и структуры использованных РСЛОС.

5.4. Начальные значения регистров.

5.5. Результаты выполнения программы (шифрование и дешифрование).

5.6. Начальный фрагмент сформированной ПСП.

5.7. Результаты исследования периода ПСП, формируемой РСЛОС.

5.8. Листинги программ.

5.9. Выводы по работе.

6. Вопросы для самоподготовки

6.1. Общая схема поточного шифрования. Назначение.

6.2. Шифр Вернама. Особенности использования.

6.3. РСЛОС. Назначение и принцип функционирования.

6.4. Формирование ПСП по схеме Джеффа.

6.5. Формирование ПСП по схеме Брюса.

6.6. Формирование ПСП по методу n ступенчатых отображений.

6.7. Понятие ПСП. Назначение.

6.8. Период ПСП. Надежность поточного шифрования от длины ПСП.

6.9. Влияние структуры функции обратной связи на период (длину) ПСП.

Лабораторная работа № 7

ПРОСТЕЙШИЙ КРИПТОАНАЛИЗ ШИФРОТЕКСТА

1. Цель работы

Изучить простейшие способы криптографического анализа и дешифрации сообщений, полученных с использованием методов подстановки и перестановки.

2. Общие сведения

Для простейших шифров, например, подстановок и перестановок, при криптоанализе можно применять статистическое распределение символов в алфавите. Например, в шифре моноалфавитной замены количество возможных перестановок букв алфавита (для английского языка) равно $26! \approx 4 \cdot 10^{26}$, однако данный шифр не является стойким. Это обусловлено тем, что:

1) в шифротексте сохраняются статистические зависимости символов и сочетаний символов исходного текста (табл. 2), что особенно важно, и в большинстве случаев именно благодаря этому предоставляется возможность провести удачный криптоанализ;

2) перемешанный алфавит может быть установлен постепенным подбором.

Хотя конкретное значение частоты встречаемости букв зависит от текста сообщения, и отранжированная по частоте последовательность меняется в целом незначительно. Поэтому подсчет частоты встречаемости букв в шифротексте позволяет достаточно точно определить наиболее и наименее часто используемые символы перемешанного алфавита. Остальные буквы устанавливаются методом проб и ошибок на основе избыточности исходного текста. Существенную помощь может оказать анализ наиболее часто встречающихся сочетаний букв (THE, FROM, IS, ПРИБ ОТ, НА, и т.д.) - см. таблицу 3. На основе анализа частоты встречаемости букв в шифротексте может быть даже установлено, на каком языке написано исходное сообщение.

Для шифра полиалфавитной замены одинаковым буквам исходного сообщения соответствуют разные буквы шифротекста, поэтому непосредственный анализ частоты встречаемости букв успеха не принесет. Существенно облегчит криптоанализ определение количества используемых при шифровании алфавитов. Эта задача решается различными способами, один

из которых заключается в том, что в исходном сообщении (при его достаточной длине) весьма вероятно появление одинаковых буквенных сочетаний, интервал между которыми кратен числу используемых «перемешанных» алфавитов. В этом случае в шифротексте появятся также одинаковые буквенные сочетания. Для шифра полиалфавитной замены с пятью алфавитами можно привести следующий пример (текст: THERE IS NO OTHER MATTER):

Сообщение: THEREISNOOTHERMATTER

Шифротекст: MBJSRBMSPB**MBJS**ZTNYFE

10 букв

После определения количества используемых алфавитов осуществляется вскрытие каждого из них в отдельности так же, как при анализе шифра моноалфавитной замены.

Криптоанализ шифра Вижинера может осуществляться различными методами, применимыми к полиалфавитным шифрам в целом. Особенно эффективен метод, основанный на поиске «вероятного слова». Его суть заключается в выборе слова, с высокой вероятностью присутствующего в исходном «открытом» сообщении. Далее из номера символа криптограммы вычитается номер буквы данного слова по модулю числа символов в алфавите. При этом рассматриваются все варианты их взаимного расположения. Если при каком-либо варианте размещения в результате вычитания будет получено слово естественного языка (или фрагмент слова), то с высокой степенью достоверности можно полагать, что обнаружено именно ключевое слово. После этого легко дешифруется все сообщение.

Пример (вероятное слово ANALYSIS):

Криптограмма – FWТАКТRRNМЕХМЕТWASF . . .

ANALYSIS

Результат вычитания:

FJTPMBJZ

ANALYSIS

WGAZVZYV

ANALYSIS

TNKTTZFU

ANALYSIS

AXTGТУЕМ

ANALYSIS

KGRGRULF

ANALYSIS

TERCOMP – ключевое слово COMPUTER.

Описанная процедура основывается на существенной избыточности, присущей текстам на естественном языке.

Таким образом, если в качестве ключа используется текст на естественном языке, то получаемая криптограмма не является надежной. Однако, если в качестве ключа используется случайная последовательность символов, шифр становится более надежным.

Таблица 2

Частота встречаемости букв в различных алфавитах

Русский алфавит		Английский алфавит		Немецкий алфавит	
<i>a</i>	8,36	<i>a</i>	8,17	<i>a</i>	5,40
<i>б</i>	1,61	<i>b</i>	1,49	<i>b</i>	1,89
<i>в</i>	3,96	<i>c</i>	2,78	<i>c</i>	3,15
<i>г</i>	1,42	<i>d</i>	4,25	<i>d</i>	5,17
<i>д</i>	3,39	<i>e</i>	12,70	<i>e</i>	18,10
<i>е</i>	8,27	<i>f</i>	2,23	<i>f</i>	1,60
<i>ж</i>	0,87	<i>g</i>	2,02	<i>g</i>	3,15
<i>з</i>	1,72	<i>h</i>	6,09	<i>h</i>	5,14
<i>и</i>	8,79	<i>i</i>	6,97	<i>i</i>	7,52
<i>к</i>	3,47	<i>j</i>	0,15	<i>j</i>	0,19
<i>л</i>	4,45	<i>k</i>	0,77	<i>k</i>	1,13
<i>м</i>	4,12	<i>l</i>	4,03	<i>l</i>	3,45
<i>н</i>	6,06	<i>m</i>	2,41	<i>m</i>	2,51
<i>о</i>	11,74	<i>n</i>	6,75	<i>n</i>	10,42
<i>п</i>	3,00	<i>o</i>	7,51	<i>o</i>	2,24
<i>р</i>	4,45	<i>p</i>	1,93	<i>p</i>	0,59
<i>с</i>	5,76	<i>q</i>	0,10	<i>q</i>	0,01
<i>т</i>	6,01	<i>r</i>	5,99	<i>r</i>	8,08
<i>у</i>	2,29	<i>s</i>	6,33	<i>s</i>	6,35
<i>ф</i>	0,14	<i>t</i>	9,06	<i>t</i>	5,57
<i>х</i>	0,85	<i>u</i>	2,76	<i>u</i>	4,10
<i>ц</i>	0,22	<i>v</i>	0,98	<i>v</i>	0,87
<i>ч</i>	1,69	<i>w</i>	2,36	<i>w</i>	1,67
<i>ш</i>	0,90	<i>x</i>	0,15	<i>x</i>	0,01
<i>щ</i>	0,49	<i>y</i>	1,97	<i>y</i>	0,02
<i>ъ</i>	0,05	<i>z</i>	0,07	<i>z</i>	1,67
<i>ы</i>	1,50				
<i>ь</i>	0,49				
<i>э</i>	0,16				
<i>ю</i>	0,68				
<i>я</i>	1,69				

Таблица 3

Встречаемость двух- и трехбуквенных слов, отранжированная по убыванию

Ранг	Английский алфавит		Немецкий алфавит		Ранг	Английский алфавит		Немецкий алфавит	
1	<i>TH</i>	<i>THE</i>	<i>EN</i>	<i>EIN</i>	16	<i>ND</i>	<i>INT</i>	<i>NE</i>	<i>UNG</i>
2	<i>HE</i>	<i>ING</i>	<i>ER</i>	<i>ICH</i>	17	<i>OU</i>	<i>HIS</i>	<i>SE</i>	<i>DAS</i>
3	<i>IN</i>	<i>AND</i>	<i>CH</i>	<i>NDE</i>	18	<i>EA</i>	<i>STH</i>	<i>NG</i>	<i>HEN</i>
4	<i>ER</i>	<i>HER</i>	<i>ND</i>	<i>DIE</i>	19	<i>NG</i>	<i>ERS</i>	<i>RE</i>	<i>IND</i>
5	<i>AN</i>	<i>ERE</i>	<i>EI</i>	<i>UND</i>	20	<i>AS</i>	<i>VER</i>	<i>AU</i>	<i>ENW</i>
6	<i>RE</i>	<i>ENT</i>	<i>DE</i>	<i>DER</i>	21	<i>OR</i>	<i>TTH</i>	<i>DI</i>	<i>ENS</i>
7	<i>ED</i>	<i>THA</i>	<i>IN</i>	<i>CHE</i>	22	<i>TI</i>	<i>TER</i>	<i>BE</i>	<i>IES</i>

Таблица 3 (окончание)

Ранг	Английский алфавит		Немецкий алфавит		Ранг	Английский алфавит		Немецкий алфавит	
8	<i>ON</i>	<i>NTH</i>	<i>ES</i>	<i>END</i>	23	<i>IS</i>	<i>HES</i>	<i>SS</i>	<i>STE</i>
9	<i>ES</i>	<i>WAS</i>	<i>TE</i>	<i>GEN</i>	24	<i>ET</i>	<i>EDT</i>	<i>NS</i>	<i>TEN</i>
10	<i>ST</i>	<i>ETH</i>	<i>IE</i>	<i>SCH</i>	25	<i>IT</i>	<i>EST</i>	<i>AN</i>	<i>ERE</i>
11	<i>EN</i>	<i>FOR</i>	<i>UN</i>	<i>CHT</i>	26	<i>AT</i>	<i>THI</i>	<i>SI</i>	<i>LIC</i>
12	<i>AT</i>	<i>DTH</i>	<i>GE</i>	<i>DEN</i>	27	<i>TE</i>	<i>HAD</i>	<i>UE</i>	<i>ACH</i>
13	<i>TO</i>	<i>HAT</i>	<i>ST</i>	<i>INE</i>	28	<i>SE</i>	<i>OTH</i>	<i>DA</i>	<i>NDI</i>
14	<i>NT</i>	<i>SHE</i>	<i>IC</i>	<i>NGE</i>	29	<i>HI</i>	<i>ALL</i>	<i>AS</i>	<i>SSE</i>
15	<i>HA</i>	<i>ION</i>	<i>HE</i>	<i>NUN</i>	30	<i>OF</i>	<i>ATI</i>	<i>NI</i>	<i>AUS</i>

3. Задания к лабораторной работе

Известно, что шифротекст получен с использованием одного из перечисленных ниже методов шифрования. На основе частотного анализа букв шифротекста определить, на каком языке он был написан (русский/английский). Используя обратный, самостоятельно разработанный алгоритм выполнить дешифрование сообщения, при условии, что ключ не известен.

- 3.1. Шифры простой подстановки.
- 3.2. Шифр Цезаря с циклическим сдвигом.
- 3.3. Шифр Вижинера.
- 3.4. Шифрование с использованием двоичного кода (сложение по модулю 2).
- 3.5. Шифрование перестановкой с использованием таблиц.
- 3.6. Шифрование перестановками с использованием таблиц и с использованием ключа для перестановки строк.
- 3.7. Шифрование перестановками с использованием таблиц и с использованием ключа для перестановки строк и столбцов.
- 3.8. Шифр простой перестановки с использованием свойств таблиц (магические квадраты).

4. Порядок выполнения работы

- 4.1. Получить у преподавателя вариант индивидуального задания;
- 4.2. Ознакомиться с основами криптографического анализа;
- 4.3. Взять шифротекст, при условии, что известен метод, которым выполнялось шифрование. Для более успешного криптоанализа рекомендуется:
 - а) при формировании шифротекста не брать ключи большого размера, во избежание долгих вычислений;
 - б) исходный текст брать достаточного объема (не менее 500 символов);
 - в) организовать работу программы с использованием файловых операций.

На основании сведений о том, каким алгоритмом был получен шифротекст, произвести криптоанализ сообщения. При этом необходимо:

- а) производить частотный анализ текста;
- б) вычислять частоту встречаемости двух- и трехбуквенных слов в шифротексте и дешифрованном тексте при текущем значении ключа;
- в) производить подсчет времени затраченного на криптоанализ.

5. Содержание отчета

- 5.1. Цель работы.
- 5.2. Вариант индивидуального задания.
- 5.3. Описание алгоритма криптоанализа.
- 5.4. Результаты работы алгоритма (шифротекст и дешифрованный текст).
- 5.5. Результаты подсчета частоты встречаемости букв алфавита.
- 5.6. Зависимость вычислительных затрат на криптоанализ от сложности используемого ключа для выбранного метода.
- 5.7. Листинги программ.
- 5.7. Выводы по работе.

6. Вопросы для самоподготовки

- 6.1. Понятие криптоанализа.
- 6.2. Понятие криптостойкости метода шифрования.
- 6.3. Способы и методы проведения криптоанализа.

Лабораторная работа № 8

ИССЛЕДОВАНИЕ СРЕДСТВ ДВУХКЛЮЧЕВОГО ШИФРОВАНИЯ ДАННЫХ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ PGP

1. Цель работы

Изучить средства двухключевого шифрования данных и электронной цифровой подписи информации с использованием утилит Pretty Good Privacy (PGP) Version 6.5.8. фирмы Network Associates Inc.

2 Общие сведения

2.1. Pretty good privacy (PGP)

Очень сильное средство криптографической защиты. Сила PGP не в том, что никто не знает, как ее взломать иначе как используя «лобовую

атаку» (это не сила, а условие существования хорошей программы для шифровки), а в превосходно продуманном и чрезвычайно мощном механизме обработки ключей, скорости, удобстве и широте распространения. Существуют десятки не менее сильных алгоритмов шифровки, чем тот, который используется в PGP, но популярность и бесплатное распространение сделали PGP фактическим стандартом для электронной переписки во всем мире.

Обычные средства криптографии (с одним ключом для шифрования и дешифрования) предполагали, что стороны, вступающие в переписку, должны были вначале обменяться секретным ключом или паролем, если хотите, с использованием некоего секретного канала (дупло, личная встреча и т.д.), для того, чтобы начать обмен зашифрованными сообщениями. Получается замкнутый круг: чтобы передать секретный ключ, нужен секретный канал. Чтобы создать секретный канал, нужен ключ. Разработанная Филипом Циммерманном программа PGP относится к классу систем с двумя ключами, публичным и секретным. Это означает, что вы можете сообщить о своем публичном ключе всему свету, при этом пользователи программы смогут отправлять вам зашифрованные сообщения, которые никто, кроме вас, расшифровать не сможет. Вы же их расшифровываете с помощью вашего второго, секретного ключа.

Свой публичный ключ можно разместить на Web странице или послать его электронной почтой своему другу. Например, публичный ключ может выглядеть следующим образом:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: PGPfreeware 6.5.8 for non-commercial use  
<http://www.pgp.com>  
Dn/eDkk1z63JM6JsAhvNaP0EAJ8vIuc08NMCHX1lUuQDvwooxC5o4  
A1lbOEYZi4KkPyG75AhwN3FP0qcuqSvkZFrohDp0nx+uS0Ab8aiVP  
+s7417UbIRHBZQR9vHfZQjqbLys==/2MP  
-----END PGP PUBLIC KEY BLOCK-----
```

Ваш корреспондент зашифрует сообщение с использованием вашего публичного ключа и отправит его вам. Прочсть его сможете только вы с использованием секретного ключа. Даже сам отправитель не сможет расшифровать адресованное вам сообщение, хотя он сам написал его 5 минут назад. И самое приятное. На сегодня даже самым мощным компьютерам в ЦРУ и ФСБ требуются века, чтобы расшифровать сообщение, зашифрованное с помощью PGP! Программа PGP широко доступна в сети. В связи с ограничениями на экспорт криптографической продукции, действующими в США, резиденты и нерезиденты США должны использовать разные места для загрузки программы.

2.2. Уязвимые места PGP

Ни одна система защиты данных не является неуязвимой. PGP можно обойти целым рядом способов. Защищая данные, вы должны задать себе вопрос: является ли информация, которую вы пытаетесь защитить, более ценной для атакующего, чем стоимость атаки? Ответ на этот вопрос приведет вас к тому, чтобы защититься от дешевых способов атаки и не беспокоиться о возможности более дорогой атаки.

2.3. Скомпрометированные пароль и закрытый ключ

Наверное, самую простую атаку можно осуществить, если вы оставите где-нибудь записанный пароль, защищающий ваш закрытый ключ. Если кто-нибудь получит его, а затем получит доступ к файлу с вашим закрытым ключом, он сможет читать адресованные вам зашифрованные сообщения и ставить от вашего имени цифровую подпись. Вот некоторые рекомендации по защите пароля:

- не используйте очевидные фразы, которые легко угадать, например, имена своих детей или супруги;
- используйте в пароле пробелы и комбинации цифр, символов и букв. Если ваш пароль будет состоять из одного слова, его очень просто отгадать, заставив компьютер перебрать все слова в словаре. Именно поэтому фраза в качестве пароля гораздо лучше, чем слово;
- используйте творческий подход. Придумайте фразу, которую легко запомнить, но трудно угадать: такая фраза может быть составлена из бессмысленных выражений или очень редких литературных цитат;
- используйте максимально длинные пароли - чем длиннее пароль, тем труднее его угадать;
- при генерации ключей ВСЕГДА выбирайте максимальный размер ключа. В DOS версии на вопрос о размере ключа ответьте: 2048 (вместо выбора предлагаемых трех вариантов). В Windows версии выбирайте ключ размером 4096 и более.

2.4. Интернет-ресурсы PGP

В сети Интернет можно найти огромное количество связанной с PGP информации. Неплохие ее каталоги расположены на страницах:

- PGP Inc. (www.pgp.com);
- международный сервер PGP (www.pgpi.com);
- конференция пользователей PGP (pgp.rivertown.net);

3. Задания к лабораторной работе

Для того, чтобы лучше усвоить механизмы двухключевого несимметричного шифрования и электронной цифровой подписи, дополнительно необходимо выполнить следующие операции:

1. Каждому из участников создать еще одну пару ключей. Не передавать открытый ключ другому участнику. Выполнить шифрование файлов/электронную цифровую подпись с анализом результата.

2. Создать пару ключей, но с ограниченным сроком действия (указывается в мастере создания нового ключа). Выполнить шифрование файлов/электронную цифровую подпись с анализом результата для случая, когда срок действия ключей истек.

3. Выполнить шифрование и электронную цифровую подпись файлов в случае, когда получатель не доверяет ключу отправителя (в свойствах соответствующего открытого ключа установить Untrusting).

4. Порядок выполнения работы

Работу предлагается выполнять минимум по два человека и с разных компьютеров подключенных к локальной сети. Далее первого человека назовем участник А, второго - В.

4.1. Через меню «Пуск» или через «C:\Program Files\PGP\» запустить программу PGPTools.

4.2. Кнопкой PGPKeys запустить менеджер управления ключами.

4.3. В появившемся окне через меню «Keys/New Key» каждому участнику (отдельно А и отдельно В) создать пару ключей.

4.4. Каждому участнику А и В через меню «Keys/Export» сохранить открытый ключ в текстовом файле. Рекомендуется делать это на сетевой диск для доступа с другого компьютера.

4.5. Участнику А в списке ключей найти свой и перейти к нему. Затем через меню «Keys/Import» импортировать открытый ключ участника В.

4.6. Перейти к ключу В. Через меню «Keys/Sign» подписать ключ пользователя В для пользователя А. Через меню «Keys/Properties» перейти к свойствам импортированного ключа. В появившемся диалоге в разделе «Trust Model» ползунок установить в крайнее правое положение (Trusted). Что означает, что А полностью доверяет ключу В.

4.7. Участнику В последовательность 6,5 необходимо выполнить у себя на компьютере по отношению к А.

4.8. Перейти к панели PGPTools. Участнику А по кнопке «Encrypt» зашифровать файлы для пользователя В. Шифрованные файлы также реко-

мендуется сохранять на сетевом диске, либо в общедоступном для А и В каталоге.

4.9. Участнику В расшифровать файлы, которые для него зашифровал А.

4.10. В панели PGPTools участнику А по кнопке «Sign» подписать файлы для В.

4.11. Участнику В проверить файлы, которые ему передал А с использованием цифровой подписи.

4.12. А и В поменяться местами и повторить последовательность шагов 4.7-4.11.

5. Содержание отчета

5.1. Цель работы.

5.2. Описание последовательности действий подделанных при выполнении работы.

5.3. Результаты выполнения работы.

5.4. Свой открытый и закрытый ключи.

5.5. Выводы по работе.

6. Вопросы для самоподготовки

6.1. Общая схема двухключевых КС.

6.2. Виды ключей в двухключевых КС. Назначение.

6.3. Электронная цифровая подпись и шифрование. Понятие.

6.4. Особенности использования ключей при шифровании и электронной цифровой подписи.

6.5. Период действия ключа. Особенности.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Лорин Г., Дейтел Х.М. Операционные системы. – М.: ФиС, 1984 – 392 с.
2. Олифер В.Г. Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2001 г. – 544 с.
3. Кастер Х. Основы Windows NT и NTFS. – М.: Издательский отдел «Русская редакция», 1996 г. – 235 с.
4. Фролов А.В., Фролов Г.В. Сети компьютеров в вашем офисе. – М.: "Диалог-МИФИ", 1995. – 272 с.
5. Соколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. – СПб.: ООО издательство «Полигон», 2000. – 272 с.

6. Максимов Ю.Н., Сонников В.Г., Петров В.Г. и др. Технические методы и средства защиты информации. – СПб.: ООО Издательство «Полигон», 2000. – 315 с.
7. Макаров Р.И. Методы и средства защиты информации: Курс лекций. – ВлГУ, Владимир, 2002. – 136 с.
8. Мельников В.В. Защита информации в компьютерных системах. М.: ФиС, 1997. – 368 с.
9. Защита информации в персональных ЭВМ. А.В. Спесивцев, В.А. Вегнер, А.Ю. Крутяков и др. – М.: РиС, 1992. – 286 с.
10. Герасимов В.А. Защита информации в автоматизированных системах обработки данных. – М., Энергоатомиздат, 1994.

ОГЛАВЛЕНИЕ

Предисловие.....	3
Лабораторная работа № 1. ЗАЩИТА ИНФОРМАЦИИ В ОПЕРАЦИОННОЙ СИСТЕМЕ MS-DOS.....	4
Лабораторная работа № 2. ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ И РЕСУРСОВ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS 95/98/ME.....	6
Лабораторная работа №3. ИЗУЧЕНИЕ СТАНДАРТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТИ NETWARE.....	13
Лабораторная работа № 4. ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ.....	27
Лабораторная работа № 5. ОДНОКЛЮЧЕВЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ.....	31
Лабораторная работа № 6. ПОТОЧНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ.....	36
Лабораторная работа № 7. ПРОСТЕЙШИЙ КРИПТОАНАЛИЗ ШИФРОТЕКСТА.....	41
Лабораторная работа № 8. ИССЛЕДОВАНИЕ СРЕДСТВ ДВУХКЛЮЧЕВОГО ШИФРОВАНИЯ ДАННЫХ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ RGP45	
Список рекомендуемой литературы.....	49

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ
Методические указания к лабораторным работам

Составители
МАКАРОВ Руслан Ильич
ВЕРШИНИН Виталий Васильевич

Ответственный за выпуск – зав. кафедрой профессор А.В. Костров

Редактор Е.В. Невская
Компьютерная верстка и дизайн обложки В.В. Вершинин

ЛР №020275. Подписано в печать 25.07.03.
Формат 60x84/16. Бумага для множит. техники. Гарнитура Таймс.
Печать офсетная. Усл. печ. л. 3,02 Уч.-изд. л. 3,23 Тираж 50 экз.

Заказ
Редакционно-издательский комплекс
Владимирского государственного университета
60000, Владимир, ул. Горького, 87.