ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ACK	Acknowledgement field significant
ARP	Address Resolution Protocol
CDP	Cisco Discovery Protocol
CIFS	Common Internet File System
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IIS	Internet Information Services
IKE	Internet Key Exchange
IP	Internet Protocol
ISO	International Standard Organization
KDC	Key Distribution Centre
L2F	Layer-2 Forwarding
L2TP	Layer-2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
MAC	Medium Access Control
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSTS	Microsoft Terminal Services
NAT	Network Address Translation
NSS	Name Service Switch
PAM	Pluggable Authentication Modules
POP3	Post Office Protocol
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RFC	Request For Comments
RST	Reset the connection
S/MIME	Secure Multipurpose Internet Mail Extension

SHTTP	Secure HTTP
SKIP	Simple Key management for Internet Protocol
SMB	Server Message Blocks
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
SYN	Synchronize sequence numbers
TCP	Transmission Control Protocol
TGT	Ticket Granting Ticket
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network
АИС	Автоматизированная информационная система
АС	Автоматизированная компьютерная система
ЗИ	Защита информации
КИ	Компьютерная информация
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПБ	Политика информационной безопасности
ПИБ	Подсистема информационной безопасности
ПК	Персональный компьютер
ПО	Программное обеспечение
ПРД	Правила разграничения доступа
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
СОИБ	Система обеспечения информационной безопасности
ЦС	Центр сертификации
ЭЦП	Электронно-цифровая подпись

СОДЕРЖАНИЕ

Введение 9

1. Назначение и возможности аппаратно-программных средств защиты информации 11

1.1. Компьютерная система и защита информации 11

1.2. Комплексный подход к защите информации 16

1.3. Что такое СЗИ 19

2. Применение средств криптографической защиты информации 27

2.1. Криптографическая защита информации 27

2.2. Система защиты конфиденциальной информации PGP 35

2.2.1. Основные характеристики системы PGP 35

2.2.2. Инициализация системы PGP на рабочей станции 36

2.2.3. Генерация, импортирование и экспортирование ключей 40

2.2.4. Изменение настроек сервиса PGPkeys. 45

2.2.5. Шифрование и обмен шифрованной информацией 48

2.3. Система защиты конфиденциальной информации «StrongDisk» 54

2.3.1. Основные характеристики системы «StrongDisk» 54

2.3.2. Терминология СКЗИ «StrongDisk» 54

2.3.3. Инициализация системы «StrongDisk» 55

2.3.4. Создание защищенных логических дисков 57

2.3.5. Настройка параметров системы «StrongDisk» 64

2.3.6. Сервисные операции 69

2.3.7. Гарантированное удаление данных 71

2.4. Система защиты корпоративной информации «Secret Disk» 74

2.4.1. Основные характеристики системы «Secret Disk» 74

2.4.2. Инициализация системы «Secret Disk» 74

2.4.3. Создание защищенных логических дисков 75

2.4.4. Работа с защищенными дисками 77

2.4.5. Настройка СКЗИ «Secret Disk» 79

2.4.6. Управление секретными дисками 80

2.4.7. Хранение секретной информации на съемных носителях 82

3. Применение СЗИ от НСД для организации защищенных компьютерных систем 83
3.1. Меры противодействия несанкционированному доступу 83
3.1.1. Идентификация и аутентификация пользователей 83
3.1.2. Ограничение доступа на вход в систему 86
3.1.3. Разграничение доступа 90
3.1.4. Регистрация событий (аудит) 99
3.2. Модель защищенной компьютерной системы 101
3.3. Система защиты информации от несанкционированного доступа «Страж NT» 106
3.3.1. Общие сведения 106
3.3.2. Запуск и регистрация в системе защиты 106
3.3.3. Создание пользователей 108
3.3.4. Реализация мандатной модели разграничения доступа 110
3.3.5. Реализация дискреционной модели разграничения доступа 113
3.3.6. Создание замкнутой программной среды 114
3.3.7. Контроль целостности 116
3.3.8. Организация учета съемных носителей информации 117
3.3.9. Регистрация событий 118
3.3.10. Гарантированное удаление данных 123
3.4. Система защиты информации от несанкционированного доступа «Dallas Lock» 124
3.4.1. Общие сведения 124
3.4.2. Запуск и регистрация в системе защиты 124
3.4.3. Создание пользователей 126
3.4.4. Реализация мандатной модели разграничения доступа 127
3.4.5. Реализация дискреционной модели разграничения доступа 131
3.4.6. Обеспечение замкнутости программной среды 133
3.4.7. Контроль целостности 134
3.4.8. Регистрация событий 136
3.4.9. Печать штампа 137
3.4.10. Гарантированное удаление данных 138
3.4.11. Реализация запрета загрузки ПЭВМ в обход СЗИ 139

3.4. Система защиты информации «Secret NET 5.0-C» 142
3.4.1. Общие сведения 142
3.4.2. Запуск и регистрация в системе защиты 143
3.4.3. Создание учетных записей пользователей 143
3.4.4. Реализация дискреционной модели разграничения доступа 145
3.4.5. Реализация мандатной модели разграничения доступа 147
3.4.6. Режим замкнутой программной среды 153
3.4.7. Контроль целостности 156
3.4.8. Регистрация событий 158
3.4.9. Печать штампа 160
3.4.10. Гарантированное удаление данных 162
3.4.11. Настройка механизма шифрования 163
4. Средства организации виртуальных частных сетей 171
4.1. Задачи, решаемые VPN 171
4.2. Туннелирование в VPN 173
4.3. Уровни защищенных каналов 174
4.4. Защита данных на канальном уровне 176
4.5. Организация VPN средствами протокола PPTP 180
4.5.1. Постановка задачи 180
4.5.2. Установка и настройка VPN 181
4.5.3. Анализ защищенности передаваемой информации 184
4.6. Защита данных на сетевом уровне 185
4.6.1. Протокол SKIP 186
4.6.2. Протокол IPSec 190
4.7. Организация VPN средствами СЗИ VipNet 191
4.7.1. Постановка задачи 191
4.7.2. Настройка сетевых соединений виртуальных машин 192
4.7.3. Установка СЗИ VipNet 193
4.7.4. Настройка СЗИ VipNet 197
4.8. Использование протокола IPSec для защиты сетей 202
4.8.1. Шифрование трафика с использованием протокола IPSec 202
4.8.2. Проверка защиты трафика 203

4.8.3. Настройка политики межсетевого экранирования с использованием протокола IPSec 205
4.9. Организация VPN средствами СЗИ StrongNet 208
4.9.1. Описание системы 208
4.9.2. Постановка задачи 208
4.9.3. Генерация и распространение ключевой информации 209
4.9.4. Настройка СЗИ StrongNet 210
4.9.5. Установка защищенного соединения 211
4.10. Защита на транспортном уровне 213
4.11. Организация VPN средствами протокола SSL в Windows Server 2003 215
4.11.1. Активизация IIS 215
4.11.2. Генерация сертификата открытого ключа для web-сервера 217
4.11.3. Настройка SSL-соединения 221
4.12. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP 223
4.12.1. Организация почтового обмена 224
4.12.2. Активизация IIS 224
4.12.3. Установка СКЗИ КриптоПро CSP 225
4.12.4. Установка Центра сертификации в ОС Windows Server 2003 225
4.12.5. Получение сертификатов открытых ключей 225
4.12.6. Организация защищенного обмена электронной почтой 227
Заключение 228
Библиографический список 229
Приложение 231
Рекомендации по проведению практических занятий 231
Организация дисковой памяти. Главная загрузочная запись 232
Электронные идентификаторы 235

ВВЕДЕНИЕ

Государственный стандарт (ГОСТ Р 51275-99 – «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.») описывает весьма внушительное пространство угроз, которые существуют объективно и, реализовавшись, могут нанести ущерб информации, обрабатываемой в компьютерной системе. Кроме несанкционированного доступа злоумышленников, технических разведок извечных конкурентов, злого умысла обиженных сотрудников, сюда присоединяются и вполне «обыденные» угрозы, связанные с разлитым на системный блок кофе, засыпанием на «back space», чисто человеческим любопытством, граничащим с некомпетентностью.

От большого пространства разнообразных опасностей можно уберечься только соответствующим множеством рубежей защиты разнообразных по физическому принципу действия, по объекту, субъекту, способу и степени противодействия угрозам. Большинство опытных пользователей ПЭВМ хорошо знакомы с мерами по защите информации. Отдельные мероприятия сами по себе могут быть очень хороши, но особенно они действенны при соблюдении основных принципов защиты информации, среди которых важнейшими являются системность, комплексность, непрерывность в пространстве и во времени. Системному администратору или администратору безопасности организовать одному надежный заслон ущербу компьютерной информации не только очень сложно, – практически невозможно, хотя бы потому, что информационная безопасность подразумевает, в том числе и целый ряд административно-организационных, технических, кадровых мероприятий. Более того, обилие необходимых и возможных мер защиты компьютерной информации (КИ) затрудняет их комплексирование, планирование и контроль. В этой ситуации на помощь специалистам по защите автоматизированных информационных систем (АИС) приходят специализированные аппаратно-программные средства защиты информации (СЗИ).

Предлагаемое пособие предназначено для специалистов, отвечающих за безопасность информационных объектов, может быть полезным руководителям предприятий, преподавателям и студентам ВУЗов, изучающим современные информационные технологии.

Цель пособия — предоставить читателям возможность изучить методы и средства защиты информации (СЗИ) на примере имеющихся на российском рынке специализированных программно-аппаратных систем. Основной акцент в пособии делается на практическое изучение материала. Известные авторам многочисленные учебные пособия [например, 13, 14, 15, 16, 17, 24, 26] содержат подробное теоретически обоснованное описание методов защиты информации, однако редко рассматривают конкретные специализированные программно-аппаратные средства. Практическая реализация защитных механизмов в этих книгах рассмотрена на уровне операционных систем. С другой стороны, техническая документация, поставляемая с системами защиты, подробно описывая особенности реализации методов защиты в каждой конкретной системе, не всегда дает методику применения этих средств.

В настоящем пособии сделана попытка сформировать общую методику применения готовых программно-аппаратных СЗИ для решения наиболее важных проблем, неизбежно возникающих в процессе защиты информации на предприятиях и в организациях. Вместе с тем пособие не следует воспринимать как руководящий документ по защите информации, в особенности составляющей государственную тайну.

По мере изложения теоретического материала читателям предлагаются практические задания, обозначенные абзацем ***«ВЫПОЛНИТЬ!»***. Выполнение заданий, а также ответы на содержащиеся в них вопросы являются необходимым условием освоения учебного материала.

Предполагаем, что, познакомившись с теоретической частью пособия и выполнив практические задания, читатели смогут, во-первых, обоснованно подойти к выбору того или иного средства защиты и, во-вторых, грамотно использовать выбранное средство в процессе своей творческой деятельности.

Пособие состоит из трех глав, библиографического списка и приложения:

Глава 1. Задачи и методы защиты компьютерной информации от несанкционированного доступа. В главе приведено описание основных методов защиты информации, предназначенных для защиты информации от несанкционированного доступа. Глава содержит постановку задачи для проведения практических занятий в виде стандартных требований к защите компьютерной информации на произвольном предприятии или в учреждении.

Глава 2. Применение СКЗИ. Содержит основные теоретические сведения и практические задания для изучения средств криптографической защиты информации « PGP-8.0», «StrongDisk» и «Secret Disk».

Глава 3. Применение СЗИ от НСД для организации защищенных компьютерных систем. Состоит из трех разделов, в двух из которых приведены основные сведения по применению распространенных средств защиты информации: «Страж NT» и «Dallas Lock». В главе также рассматривается программно-аппаратный комплекс защиты информации «Secret Net 5.0-C», предоставляющий пользователю кроме стандартных мер защиты компьютерных систем от НСД, возможность работы с зашифрованными данными.

Глава 4. Средства организации виртуальных частных сетей. Содержит основные теоретические сведения и практические задания для изучения средств криптографической защиты информации «VipNet», «StrongNet», «КриптоПро», а также стандартных средств организации виртуальных частных сетей в операционных системах семейства Windows.

Библиографический список содержит 30 наименований нормативных документов, технической документации и учебных пособий, требующихся для углубленного изучения отдельных тем.

В приложении приводятся рекомендации для преподавателей по проведению практических занятий с использованием технологии виртуальных машин, структура главной загрузочной записи и технические характеристики распространенных электронных идентификаторов.

1. НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

1.1. Компьютерная система и защита информации

Безопасность автоматизированной системы [1] — это состояние АС, определяющее защищенность обрабатываемой информации и ресурсов от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность АС выполнять предписанные функции без нанесения неприемлемого ущерба объектам и субъектам информационных отношений. Пространство угроз весьма велико и разнообразно [2]. Столь же представительно и разнообразно должно быть противодействие угрозам КИ. *Защита информации* [3] — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию — предполагает комплексный и системный подход. Согласно [4], система защиты информации автоматизированной компьютерной системы — совокупность технических, программных и программно-технических средств *защиты информации* и средств *контроля эффективности защиты* информации. Если это определение дополнить организационными действиями, учесть требования (комплексности, системности и др.), то защиту информации можно определить, как комплекс взаимосвязанных мер правового, административного, технического, технологического и специального характера, а также соответствующих им мероприятий, сил, средств и методов, предназначенных для решения задач защиты компьютерной информации. Задачи защиты КИ, требования к системе защиты объективны (порождены практическим опытом эксплуатации АС) и во многом близки и для больших распределенных вычислительных систем и для одиночных ПК, работающих в многопользовательском режиме.

Определить типичные задачи и сформулировать требования к системе защиты информации можно на примере анализа потребностей по обеспечению информационной безопасности некоторой вымышленной организации, ведущей проектирование инженерной документации, составляющей государственную тайну. С таким же успехом можно анализировать потребности коммерческой организации, исследующей товарный рынок и генерирующей прогнозы его развития.

Внедряемая система защиты информации должна обеспечивать надежную, т. е. бесперебойную, устойчивую и правильную работу АС, оперативный доступ сотрудников к информации в соответствии с предоставленными им полномочиями, возможность восстановления информации в случае ее случайной утраты или уничтожения вследствие возникновения аварийных ситуаций и многое другое. В целом система мер по защите информации должна воплощать в жизнь разработанную на предприятии с участием соответствующих специалистов и утвержденную его руководителем *политику информационной безопасности* (ПБ). Политика безопасности организации [1] — совокупность руководящих принципов, правил, процедур и практических приемов в области безо-

пасности, которыми руководствуется организация в своей деятельности. ПБ представляет собой документ, который должен быть доступен всем сотрудникам, и, в первую очередь, отвечающим за обеспечение режима информационной безопасности на предприятии. Этот документ определяет основные цели политики информационной безопасности и область ее применения, а также ее значение как механизма, позволяющего сотрудникам предприятия коллективно использовать информацию. В документе рядовые пользователи и ответственные за безопасность сотрудники должны найти разъяснение мер, принципов, стандартов и конкретных вариантов реализации политики безопасности, требований к ее соблюдению, общих и конкретных обязанностей по обеспечению режима информационной безопасности, включая выполнение правовых и договорных актов.

С тех пор как на рынке услуг безопасности появились специализированные предприятия, берущие на себя организацию защиты информации, возникла необходимость в стандартизации подходов к формированию ПБ. Политика разрабатывается в соответствии с имеющейся нормативной базой, многие ее разделы являются законодательно необходимыми, а положения могут быть формализованы без потери качества документа. На момент написания пособия «свежими» нормативными документами можно считать: ГОСТ 15408–02 «Критерии оценки безопасности информационных технологий» и построенные на его основе руководящие документы Гостехкомиссии (ныне ФСТЭК) России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий»; международный стандарт ISO/IEC 17799 «Информационные технологии. Свод правил по управлению защитой информации». Разработка ПБ — дело творческое, но и в таком деле отказываться от опыта специалистов не разумно. Дельные советы по разработке политики безопасности можно найти, например, в [28]. Там же описаны специализированные программные комплексы, осуществляющие формализованный анализ ПБ на полноту и соответствие требованиям нормативных актов.

Большое внимание политика безопасности обычно уделяет специальным мероприятиям, обеспечивающим защиту информации от *несанкционированного доступа* (НСД) злоумышленника к конфиденциальным данным. Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа. Типичные требования к системе защиты от НСД можно найти в руководящих документах [5, 6], где приводятся классификация средств вычислительной техники (СВТ) и автоматизированных систем (АС) по уровню защищенности от НСД и перечень показателей защищенности. Несмотря на солидный возраст документов (оба разработаны еще в 1992 году), они, дополняя друг друга, содержат исчерпывающий перечень требований по защите компьютерных систем от НСД. В [5], например, для защиты от НСД автоматизированных систем основные защитные меры группируют в четыре подсистемы:

- управления доступом,
- регистрации и учета,
- криптографической,
- обеспечения целостности.

Для различного класса автоматизированных систем документ регламентирует выполнение требований, приведенных в табл. 1.1.

Таблица 1.1

Требования по защите информации от НСД для АС

Подсистемы и требования	Классы АС								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом 1.1. Идентификация. Проверка подлинности и контроль доступа объектов:									
− в систему	+	+	+	+	+	+	+	+	+
− к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ				+		+	+	+	+
− к программам				+		+	+	+	+
− к томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
1.2. Управление потоками информации				+			+	+	+
2. Подсистема регистрации и учета									
− 2.1. Регистрация и учет: − входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+	+	+	+	+
− выдачи печатных (графических) выходных документов		+		+		+	+	+	+
− запуска/завершения программ и процессов (заданий, задач)				+		+	+	+	+
− доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи				+		+	+	+	+
− доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, каталогам, файлам, записям, полям записей				+		+	+	+	+
− изменения полномочий субъектов доступа							+	+	+
− создаваемых защищаемых объектов доступа				+			+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3.Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних носителей		+		+		+	+	+	+
2.4. Сигнализация попыток нарушения							+	+	+

Окончание табл. 1.1

Подсистемы и требования	Классы АС								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
3. Криптографическая подсистема									
3.1. Шифрование конфиденциальной информации				+				+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группа субъектов) на различных ключах									+
3.3. Использование аттестованных (сертифицированных) криптографических средств				+				+	+
4. Подсистема обеспечения целостности									
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС				+			+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты		+		+			+	+	+

Руководящий документ [6] для различных классов СВТ устанавливает требования к показателям защищенности, приведенным в табл. 1.2.

Таблица 1.2

Требования к показателям защищенности СВТ от НСД

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	–	–	+	=	=	=
Очистка памяти	–	+	+	+	=	=
Изоляция модулей	–	–	+	=	+	=
Маркировка документов	–	–	+	=	=	=
Защита ввода и вывода на отчуждаемый физический носитель информации	–	–	+	=	=	=
Сопоставление пользователя с устройством	–	–	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	–	+	+	+	+	+

Окончание табл. 1.2

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Регистрация	–	+	+	+	=	=
Взаимодействие пользователя с комплексом средств защиты (КСЗ)	–	–	–	+	=	=
Надежное восстановление	–	–	–	+	=	=
Целостность КСЗ	–	+	+	+	=	=
Контроль модификации	–	–	–	–	+	=
Контроль дистрибуции	–	–	–	–	+	=
Гарантии архитектуры	–	–	–	–	–	+
Тестирование	+	+	+	+	+	+
Руководство для пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

« – » — нет требований к данному классу;
« + » — новые или дополнительные требования;
« = » — требования совпадают с требованиями к СВТ предыдущего класса.

Наборы требований к показателям защищенности, приведенные в табл. 1.1 и табл. 1.2, являются минимально необходимыми для соответствующих классов АС и СВТ. По мнению авторов, вполне достаточным для многих конкретных ситуаций является приведенный ниже набор требований к защите компьютерной системы:

1. Только зарегистрированные в АС пользователи и только в разрешенное для каждого из них время могут включить компьютер (загрузить операционную систему);
2. Без регистрации никто не должен получать доступ к конфиденциальной информации и информации, хранящейся на защищаемых носителях;
3. Пользователь, обрабатывающий конфиденциальные данные, должен иметь возможность удостовериться в «чистоте» («легитимности») компьютерной системы, а именно в неизменности системного и прикладного программного обеспечения, пользовательских данных, в отсутствии вредоносных программ;
4. Пользователи должны получать доступ только к той информации и с теми возможностями по ее обработке, которые соответствуют их функциональным обязанностям;
5. Пользователям при обработке защищаемой информации разрешается применение только тех программных средств, которые необходимы им для выполнения своих функциональных обязанностей;
6. Для хранения конфиденциальных данных должны использоваться только учтенные носители информации; возможность копирования информации на внешние или сетевые носители определяется уровнем конфиденциальности информации, уровнем допуска сотрудника и уровнем конфиденциальности носителя;

7. Конфиденциальная информация, обрабатываемая полномочным пользователем, в том числе ее фрагменты в виде «технологического мусора», без соответствующего разрешения не должна прямо или косвенно быть доступна иному субъекту;
8. В целях профилактики и расследования возможных инцидентов, а также в качестве сдерживающего фактора автоматически должна вестись регистрация в специальных электронных журналах наиболее важных событий, связанных с доступом пользователей к защищаемой информации и компьютерной системе в целом;
9. При печати документов на бумажные носители автоматически должен фиксироваться факт распечатки в специальном журнале и автоматически выводиться соответствующий штамп на сам документ;
10. В компьютерной системе должен быть администратор безопасности, который обязан воплощать в жизнь политику безопасности и, следовательно, имеет право устанавливать порядок доступа пользователей к АС и документам, разрешения (ограничения), пароли и т. д.;

Все перечисленные требования должны обеспечиваться средствами самой компьютерной системы автоматически. Каждый сотрудник предприятия должен быть *вынужден* гарантированно выполнять требования политики безопасности, а не только под воздействием силы приказов и распоряжений начальников. На предприятии должен быть организован такой режим функционирования АС, который просто не позволит пользователю работать с конфиденциальными данными в незащищенном режиме.

Перечисленные выше требования защиты АС от НСД вытекают из опыта, здравого смысла и давно существующего порядка работы с конфиденциальной информацией (на бумажных или электронных носителях). Этот набор требований далеко не полон, не противоречит официальным руководящим документам, однако он не затрагивает специальных вопросов проектирования комплекса защиты информации, параметров функциональности средств и механизмов защиты, разработки необходимой документации, тестирования СЗИ, контроля защищенности АС.

1.2. Комплексный подход к защите информации

Как указывалось выше, система защиты компьютерной информации — это комплекс мер, а также соответствующих им мероприятий, сил, средств и методов. На страницах многочисленных изданий по компьютерной тематике можно детально познакомиться с основными мерами и методами защиты информации. В любой книге по информационной безопасности можно встретить примерно такой «джентльменский» набор:

- ограничение физического доступа к АС,
- идентификация и аутентификация пользователей,
- ограничение доступа на вход в систему,
- разграничение доступа,
- регистрация событий (аудит),

- криптографическая защита,
- контроль целостности,
- управление политикой безопасности,
- уничтожение остаточной информации,
- антивирусная защита,
- резервирование данных,
- сетевая защита,
- защита от утечки и перехвата информации по техническим каналам.

Программно-аппаратные средства защиты информации, о которых идет речь в данном пособии, призваны реализовывать несколько мер и соответствующих им методов по противодействию злоумышленнику при возможности его физического доступа к компьютерам автоматизированной системы.

Мы уже отмечали, что защита информации предполагает комплексный и системный подход. Только взаимообусловленный, основанный на тщательном анализе самой компьютерной системы, комплекс защитных мер может обеспечить достаточный уровень безопасности обрабатываемой в АИС информации. Любое происшествие или успешная атака являются, как правило, следствием совокупности причин, реализацией нескольких угроз.

Перечисленные требования в системе защиты КИ способны противостоять большинству угроз компьютерной информации, связанных с несанкционированным доступом злоумышленника на программном и аппаратном уровнях. Было бы интересно определить, насколько предложенный выше набор защитных методов соответствует этим требованиям. Проследить это соответствие можно с помощью табл. 1.3. В таблице не учитываются методы защиты, которые не связаны непосредственно с выполнением указанных требований: антивирусная защита, резервирование данных, сетевая защита, защита от утечки и перехвата информации по техническим каналам.

В таблице символом ✓ обозначено, какие требования позволяет обеспечить тот или иной метод защиты. Из таблицы видно, что нет требований, которые не обеспечиваются ни одним из рассмотренных выше методов защиты. Хотя бы один из методов защиты реализует каждое из требований.

Наиболее важные требования обеспечиваются выполнением одновременно нескольких методов. В этом проявляется комплексный подход к защите компьютерной информации. Необходимость комплексного и системного подхода наглядно иллюстрируется на примере требования 2 — без регистрации никто не должен получать доступ к конфиденциальной информации. Методы, обеспечивающие выполнение этого требования, взаимосвязаны. Без достоверной аутентификации субъекта АИС не допустима загрузка операционной системы. Без идентификации и аутентификации пользователя также не имеют смысла регистрация сеанса его работы и реализация той или иной модели разграничения доступа.

Таблица 1.3

Требования к системе защиты информации и меры по их реализации

Требования к системе защиты компьютерной системы	Методы защиты информации							
	идентификация и аутентификация	ограничение доступа на вход в систему	разграничение доступа	регистрация событий (аудит)	криптографическая защита	контроль целостности	управление политикой безопасности	уничтожение «технологического мусора»
1. Только зарегистрированные пользователи в разрешенное время могут загрузить ОС	✓	✓					✓	
2. Без регистрации никто не должен получать доступ к конфиденциальной информации	✓	✓	✓		✓		✓	✓
3. Пользователь должен быть уверен в «чистоте» компьютерной системы		✓	✓			✓	✓	
4. Пользователи должны получать доступ только к той информации и с теми возможностями, которые соответствуют их функциональным обязанностям			✓				✓	
5. Пользователям разрешается применение только необходимых для обработки информации программных средств			✓				✓	
6. Для хранения конфиденциальных данных должны использоваться только учтенные носители			✓				✓	
7. Конфиденциальная информация, в том числе ее фрагменты в виде «технологического мусора», не должна быть доступна иному субъекту	✓	✓	✓		✓		✓	✓
8. В АИС автоматически должна вестись регистрация наиболее важных событий	✓	✓		✓			✓	
9. При печати документов на бумажные носители автоматически должны фиксироваться факт распечатки в специальном журнале и выводиться штамп на сам документ				✓			✓	
10. В АИС должен быть администратор безопасности, который обязан воплощать в жизнь политику безопасности							✓	

В то же время, если злоумышленник получит физический доступ, например, к жесткому диску, то с помощью низкоуровневых дисковых редакторов он сумеет считать приватные данные в обход системы разграничения доступа. Противодействием атакам наиболее подготовленных злоумышленников может стать криптографическая защита информации. С другой стороны, правомерность обращения субъекта к самим программам шифрования, процесс ввода ключевой (аутентифицирующей) информации, блокирование вредоносных программ — перехватчиков паролей, находятся под контролем систем ограничения и разграничения доступа. Таким образом, криптографическое преобразование конфиденциальных данных только в тесной взаимосвязи с механизмами ограничения и разграничения доступа способны гарантировать надежную защиту компьютерной информации от НСД. Этот же комплект методов защиты противодействует «программной» утечке конфиденциальной информации, обусловленной несовершенством операционных систем, в том числе наличием «технологического мусора» (требование 7).

Не менее показательным является требование аудита критических событий в АИС. На первый взгляд это требование может показаться обособленным и независимым от других требований и методов, их реализующих. Однако каким образом регистрировать, например, попытки несанкционированного входа в систему, если вход в нее не ограничен? Безусловно, само знание факта злоумышленных (подозрительных) действий в АИС важно для их пресечения. Фиксация конкретного лица, совершившего эти действия, позволит расследовать правонарушения и вести их профилактику более эффективно. Как выявлять злоумышленников, если в системе не ведутся идентификация и аутентификация пользователей?

Система защиты информации АИС — совокупность разнообразных средств и методов, взаимообусловливающих и дополняющих друг друга. Разумная, взвешенная, комплексная их реализация — непростая и творческая задача. Программно-аппаратные средства защиты информации помогают решить ее более целенаправленно и эффективно.

Осуществляя построение и эксплуатацию защищенной компьютерной системы, необходимо базироваться на принятой в организации политике безопасности, на представлении методов защиты компьютерной информации, с помощью которых могут быть реализованы требования политики безопасности, и на этой основе выбирать, устанавливать и администрировать специализированные программно-аппаратные средства защиты информации.

1.3. Что такое СЗИ

Средства защиты информации (СЗИ) — технические, криптографические, программные и другие средства, предназначенные для реализации совокупности взаимосвязанных требований безопасности АС, а также средства контроля эффективности защиты информации. СЗИ являются надстройкой над

программно-аппаратной средой защищаемой компьютерной системы и самостоятельно или совместно со встроенными возможностями операционных систем и аппаратных устройств АС реализуют некоторый набор защитных механизмов.

К сожалению, СЗИ, реализующих полный комплект подсистем безопасности, который удовлетворял бы требованиям руководящих документов [1–9], на сегодняшний день не существует. Представленные на рынке информационной безопасности и описываемые в данном пособии средства, как правило, располагают ограниченным (неполным) комплектом методов защиты и имеют свою «специализацию». Типичный набор функциональных подсистем, которым разработчики комплексных СЗИ наделяют свои изделия, приведен на рис. 1.1.

Рис. 1.1. Защитные подсистемы СЗИ

Классифицировать средства защиты можно по разным признакам. Однако основным критерием, по которому принято подразделять средства защиты информации, является их функциональность. Обычно по критерию функциональности выделяют три класса СЗИ (рис. 1.2). *Средства криптографической защиты (СКЗИ)* — средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности [7]. *Средства защиты от несанкционированного доступа (СЗИ НСД)* — средства, реализующие комплекс организационных мер и программно-технических средств защиты от несанкционированного доступа к информации в автоматизированных системах [7]. В отдельный класс СЗИ можно выделить *средства защиты информации сетевого действия*.

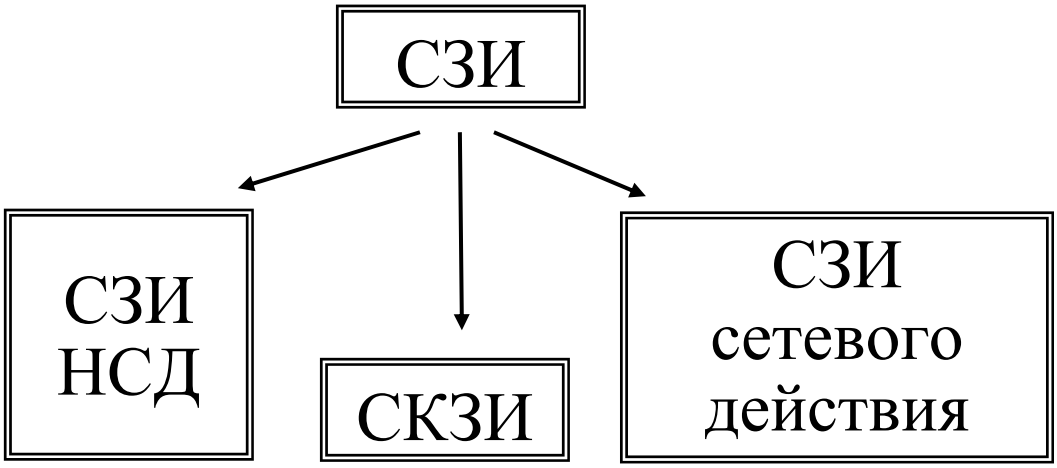


Рис. 1.2. СЗИ различного назначения

Мы уже не раз отмечали, что СЗИ предназначены для защиты АС от несанкционированного доступа злоумышленника. «СЗИ от НСД» носят общее название, однако в первую очередь подразумевают организацию доверенной загрузки компьютерной системы. Такие СЗИ, как правило, имеют аппаратную составляющую и обеспечивают идентификацию и аутентификацию пользователей, проверку целостности критичных системных файлов и аппаратных средств до загрузки операционной системы. К этому классу средств защиты можно отнести программно-аппаратные комплексы «Страж NT», «Dallas Lock», «Secret NET 5.0-C», «Аккорд-NT/2000». Основными функциональными «обязанностями» этих СЗИ являются:

- организация доверенной загрузки с возможностью идентификации и аутентификации пользователей при помощи ключевых дискет, электронных ключей Touch memory, USB-ключей eToken R2, eToken Pro, Guardant и т. п., включая авторизацию пользователей во временной области;
- контроль целостности системных областей жесткого диска, назначенных администратором безопасности системы;
- контроль целостности конфигурации аппаратных средств;

- регистрацию событий доступа в энергонезависимой памяти.

Рис. 1.3. СЗИ «Страж NT»

Разработчики этого класса СЗИ заявляют свои продукты как «комплексы» защиты АС от НСД и оснащают их дополнительными функциональными возможностями, реализующими меры защиты в работающей компьютерной системе:

- дискреционная и мандатная модели разграничения доступа пользователей к защищаемым ресурсам и прикладным программам;
- создание для пользователей замкнутой программной среды;
- контроль потоков защищаемой информации;
- очистка освобождаемой памяти и дискового пространства;
- контроль целостности запускаемых программ и баз данных;
- аудит доступа к защищаемым ресурсам;
- управление вводом-выводом на отчуждаемые носители.

Некоторые из комплексных СЗИ от НСД позволяют осуществлять криптографическую защиту конфиденциальной информации.

СЗИ «Страж NT» (рис. 1.3) разработано научно-исследовательским институтом проблем управления, информатизации и моделирования Академии военных наук (ЗАО «НИИ УИМ АВН»). Аппаратная часть комплекса предназначена для идентификации пользователей на основе электронных ключей Touch Memory. В то же время идентификация пользователей в «Страж NT» может осуществляться за счет использования ключевых дискет, которые создают-

ся самим средством для каждого пользователя. В качестве средства аутентификации применяется пароль. Средство обеспечивает доверенную загрузку путем модификации главной загрузочной записи жесткого диска.

Изделие «Dallas Lock» (рис. 1.4), разработанное ООО «Конфидент», — это комплексное средство защиты, в котором доверенная загрузка осуществляется путем аутентификации пользователей на основе электронных идентификаторов Touch Memory. При инициализации системы на компьютере модифицируется главная загрузочная запись жесткого диска. СЗИ «Dallas Lock» позволяет осуществлять защиту приватных данных путем шифрования указанной области данных на жестком диске компьютера (например, загрузочной записи логического раздела диска).

Рис. 1.4. СЗИ «Dallas Lock»

Комплексное средство защиты информации «Secret Net 2000» (рис. 1.5) разработано ЗАО НИП «ИНФОРМЗАЩИТА» (г. Москва). При аутентификации пользователей СЗИ может работать с различными электронными картами памяти (iButton, eToken, Smart Card, Proximity Card). Программная часть «Secret Net 2000» представляет собой надстройку над стандартной системой безопасности MS Windows и начинает работать после загрузки основных модулей операционной системы. Для обеспечения корректной доверенной загрузки СЗИ «Secret Net 2000» необходимо использовать совместно с аппаратными средствами, например, электронным замком «Соболь-PCI» (рис. 1.6).

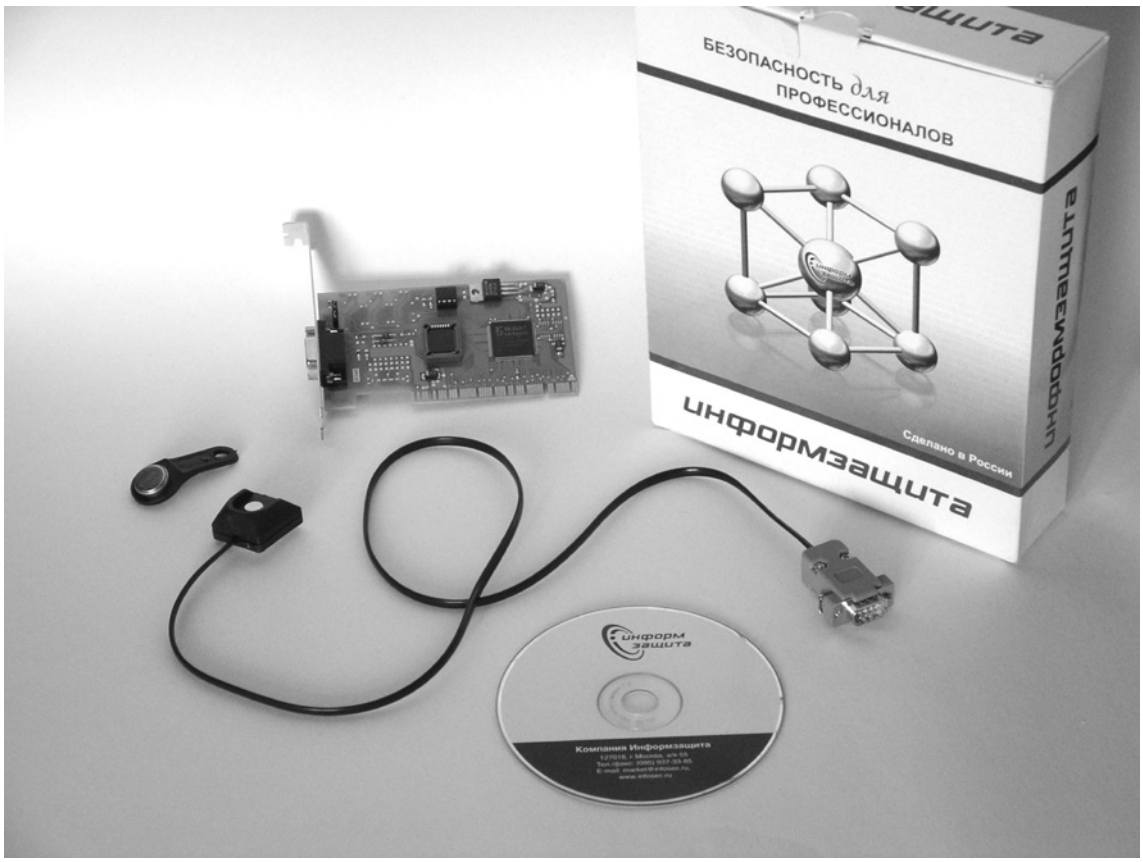


Рис. 1.5. СЗИ «Secret Net 2000»

Аппаратный модуль доверенной загрузки (АМДЗ) СЗИ «Аккорд-NT/2000» (рис. 1.7), разработанный ОКБ САПР, имеет плату расширения, вставляемую в PCI-слот защищаемого компьютера. СЗИ перехватывает управление компьютером после выполнения BIOS процедуры POST. В качестве идентификаторов выступают электронные ключи Touch memory. Поставляемый в комплекте СЗИ считыватель этих устройств работает непосредственно с аппаратным модулем, а не подключается к стандартным портам ПЭВМ. Контрольные суммы проверяемых на целостность системных областей ОС и аппаратных средств хранятся в энергонезависимой памяти аппаратного модуля.

В последнее время на российском рынке стали появляться средства комплексной защиты информации, сочетающие в себе функции СЗИ от НСД и СКЗИ. Одним из таких средств является модификация комплекса «Аккорд» — «Аккорд-СБ», представляющее собой программно-аппаратный комплекс, включающий и аппаратный модуль доверенной загрузки, и аппаратный модуль криптографической защиты. Аппаратно-программный комплекс защиты информации «Secret Net 5.0» кроме широкого арсенала средств защиты от несанкционированного доступа предоставляет пользователю возможность создавать зашифрованные каталоги для хранения персональных данных.

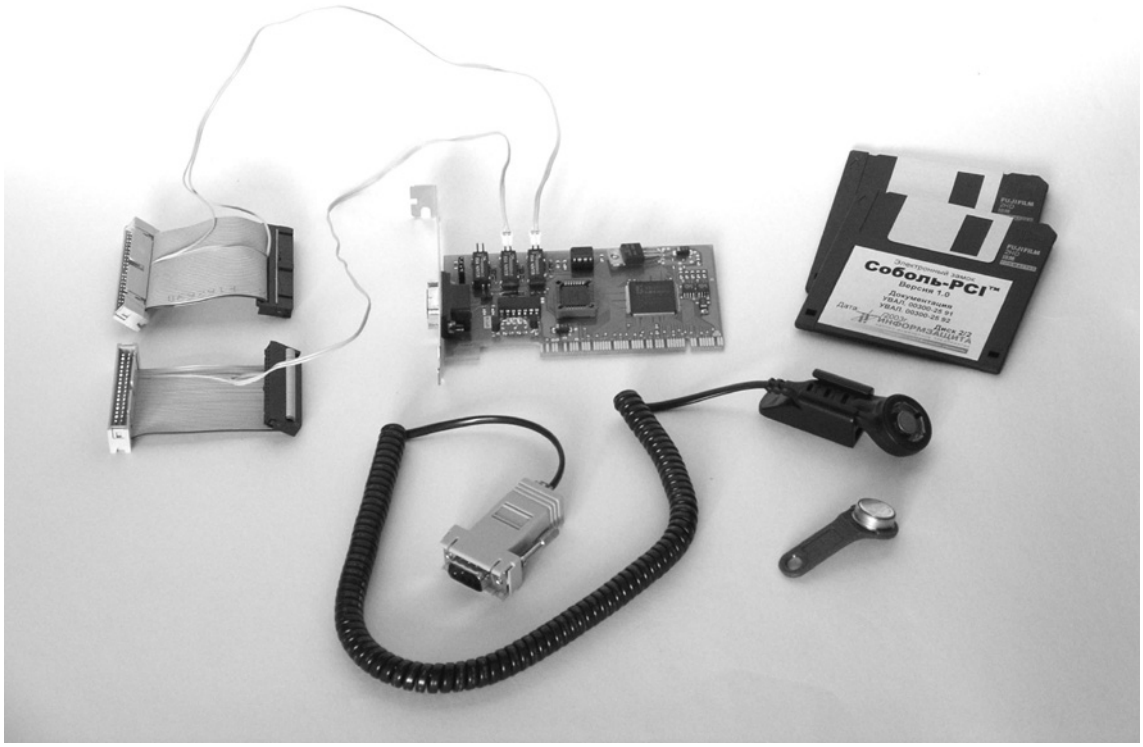


Рис. 1.6. СЗИ электронный замок «Соболь-PCI»

Рис. 1.7. СЗИ «Аккорд-NT/2000»

Сетевая защита в компьютерных системах реализуется двумя основными способами: с использованием межсетевых экранов и путем организации виртуальных частных сетей. Под межсетевыми экранами понимают локальное или функционально-распределенное аппаратно-программное (программное) средство, реализующее контроль над информацией, поступающей в ЛВС и/или выходящей из ЛВС (рис. 1.8).

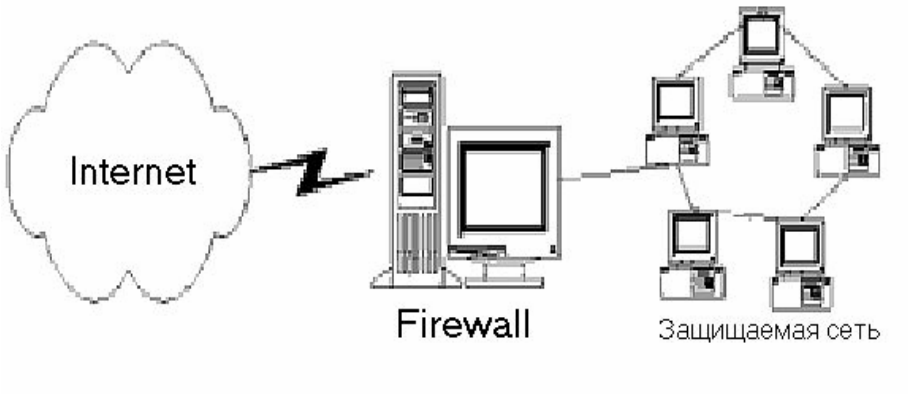


Рис. 1.8. Защита ЛВС с помощью межсетевых экранов

Виртуальные частные сети (Virtual Private Network VPN) — это технология, объединяющая доверенные сети, узлы и пользователей через открытые сети, к которым нет доверия.

Средства защиты сетевого действия (программные или аппаратно-программные) устанавливаются на тех компьютерах в составе локальной вычислительной сети, обмен информацией между которыми в открытом режиме нецелесообразен. СЗИ этого класса основываются на криптографических методах защиты с использованием механизма открытых ключей. Если компьютер работает в незащищенном режиме, то в составе ЛВС он присутствует как равноправная рабочая станция. Перевод компьютера в защищенный режим означает шифрование всего входящего/исходящего трафика, включая адресную и служебную информацию, или только пакетированных данных. ПЭВМ, на которых не установлено соответствующее программное (аппаратно-программное) обеспечение просто не «видят» в сети станции, работающие под управлением сетевых СЗИ.

Классическим примером комплексного средства защиты, включающего в себя функцию организации VPN, является распространенное отечественное аппаратно-программное средство сетевой защиты ViPNet, разработанное компанией «ИнфоТеКС» (Информационные Технологии и ТелеКоммуникационные Системы, г. Москва). Сетевые решения и технология ViPNet позволяют:

- защищать передачу данных, файлов, видеоинформации и переговоры, информационные ресурсы пользователя и корпоративной сети при работе с любыми приложениями Интернет/Интранет;
- создавать в открытой глобальной сети Интернет закрытые корпоративные Интранет-сети.

2. ПРИМЕНЕНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Криптографическая защита информации

Криптографическое преобразование информации, по мнению некоторых специалистов, является самой важной мерой ее защиты. Конечно, с этим можно соглашаться или не соглашаться. Скептики говорят, что никакая криптография не способна защитить информацию от утечки по техническим каналам, от ошибочных действий персонала, аварий или выхода из строя жесткого диска. Однако когда речь идет о защите важной, критичной информации от НСД, а угрозой является реальный человек — злоумышленник и существует вероятность физического доступа злоумышленника к носителям этой информации, криптографическое преобразование действительно выходит на первое место. Шифрование данных делает бесполезными их хищение или несанкционированное копирование. Если данные и программы их обработки хранятся в памяти ПЭВМ в зашифрованном виде, то извлечь интересующую информацию из украденного накопителя или полученной физической копии жесткого диска злоумышленнику будет весьма затруднительно, а при стойком криптоалгоритме — практически невозможно. Ничего, кроме кажущейся случайной последовательности символов, он не увидит. Присутствующая в АИС система шифрования данных надежно защищает конфиденциальную информацию от утечки, вызванной несовершенством операционных систем, возможными недостатками реализации механизмов ограничения и разграничения доступа, борется с «технологическим мусором».

Криптография — наука точная, сложная и очень интересная. Тот, кто намерен познакомиться с ней ближе, может обратиться к изданиям, которые легко найти на полках книжных магазинов [24, 25, 26, 27]. Здесь мы приведем только основные сведения и понятия о криптографических методах защиты информации, применяемых в СЗИ.

Криптография существует уже несколько тысячелетий и в переводе с греческого языка означает «тайнопись». Ее основной задачей является обратимое преобразование открытого текста в некоторую, кажущуюся случайной, последовательность символов. Процесс преобразования множества открытых сообщений (O) в закрытый, или зашифрованный, текст ($З$) называется *зашифрованием* и символьно описывается с помощью следующей формулы:

$$З = E_k(O), \qquad (1)$$

где E_k — параметризированная функция зашифрования; k — ключ зашифрования (некоторый секретный параметр).

Обратный процесс преобразования закрытого сообщения в открытое называется *расшифрованием* и описывается формулой:

$$O = D_{k^*}(З), \qquad (2)$$

где D_k — функция расшифрования, обратная E_k; k^* — ключ расшифрования. Цикл «зашифрование — расшифрование» должен привести к получению открытого сообщения, тождественно равного (или адекватного в смысловом отношении) исходному. Это требование называется условием обратимости криптографического преобразования:

$$D_{k^*}(E_k(O)) \equiv O. \qquad (3)$$

Дешифрование — процесс нахождения открытого документа на основании анализа некоторого зашифрованного сообщения при неизвестной функции D_k или ключе криптографического преобразования. Именно дешифрованием занимаются злоумышленники, которые тем или иным способом получили в свое владение копии зашифрованных сообщений.

Выражения (1) и (2) показывают, что всякий алгоритм криптографического преобразования состоит из процедурной части (функций зашифрования E или расшифрования D, т. е. описания того, какие именно операции и в какой последовательности выполняются над данными) и некоторых параметров этих функций (ключей k и k^*, т. е. конкретных данных, используемых в преобразованиях). В криптографии существует правило Керкхоффа, которое гласит, что раскрытие процедурной части не должно приводить к увеличению вероятности успешного дешифрования сообщения. Из этого правила следует, что функции шифрования могут быть известны злоумышленнику. Незнание ключа (параметра этой функции) не позволит ему успешно атаковать (дешифровать) зашифрованное сообщение. Такое положение дел позволяет на практике применять стандартные разработанные высококвалифицированными специалистами алгоритмы шифрования. В каждом конкретном случае пользователь должен только синтезировать для себя криптографические ключи и обеспечить их надежное хранение. При общеизвестной процедуре шифрования ответственность за криптостойкость (устойчивость к дешифрованию) всего алгоритма полностью заключена в конфиденциальности ключа. Алгоритм является тем устойчивей, чем сложнее (длиннее) его ключ. Поэтому синтезу ключевой информации, способу ее ввода в ПЭВМ, осуществляющей шифрование информации, в криптографии уделяют большое внимание.

Криптографические алгоритмы можно классифицировать по нескольким признакам: по типу преобразования, по количеству раздельно обрабатываемых символов и по схеме преобразования.

Основными типами преобразования [26] являются замена и перестановка. В перестановочных шифрах символы открытого текста не преобразовываются, но изменяют свое местоположение. В шифрах замены символы открытого текста замещаются символами зашифрованного текста и не меняют своего местоположения. С целью повышения надежности шифрования открытый текст может зашифровываться последовательно несколько раз с применением различных типов преобразования. Такие шифры являются комбинацией шифров замены и перестановки и носят название композитных.

В поточных шифрах каждый символ открытого текста зашифровывается независимо от других и расшифровывается таким же образом. В блочных шифрах открытый текст разбивается на блоки определенной длины, далее каждый блок шифруется отдельно и преобразуется в зашифрованный блок равного исходному (или большего) размера.

Классическая схема шифрования информации использует такие алгоритмы, при которых ключи зашифрования и расшифрования совпадают ($k = k^*$), либо ключ расшифрования может быть легко вычислен из ключа зашифрования. Если процедура зашифрования сообщения E в качестве параметра использовала ключ k, то в процедуре расшифрования D необходимо опираться на этот же ключ. Такие криптоалгоритмы известны со времен Гая Юлия Цезаря, их принято называть *симметричными*. Известны простейшие симметричные алгоритмы, такие как шифры Цезаря, Виженера. Современные симметричные алгоритмы закрепляются государственными стандартами: в США, например, в течение нескольких десятилетий применялся широко распространенный во всем мире алгоритм DES (Data Encryption Standard), в настоящее время применяются шифры AES (Advanced Encryption Standard — Rijndael), RC5, RC6, Mars, Blowfish, Twofish; в Канаде — CAST; в Австралии — LOKI; в Швейцарии — ставший международным стандарт IDEA (Ascom). Одним из наиболее криптостойких симметричных алгоритмов криптопреобразования по праву считается шифрование по ГОСТ 28147–89 (Россия). ГОСТ «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» принят в качестве стандарта в 1989 году; длина ключа составляет 256 бит ($2^{256} \approx 1.2*10^{77}$ комбинаций); использует 32 раунда шифрования и имеет 4 режима работы: простая замена, гаммирование, гаммирование с обратной связью, выработка имитовставки. В нашей стране при обработке информации, составляющей государственную тайну, регламентировано использовать только отечественный стандарт шифрования.

За многовековую историю развития были разработаны мощные быстродействующие симметричные алгоритмы шифрования с относительно коротким ключом. Однако ученым и практикам не давала покоя так называемая проблема распространения симметричных ключей (проблема передачи секретного ключа по каналам связи). Действительно, организация шифрованного канала связи по открытым коммуникационным линиям предполагает наличие симметричного ключа у отправителя и получателя информации. Прежде, чем посылать друг другу зашифрованные сообщения, один из участников обмена должен синтезировать ключ и при личной встрече или посредством доверенного лица (например, с помощью фельдъегерской службы) передать его своему компаньону. При утрате или компрометации ключа действия по пересылке нового должны быть осуществлены заново.

В 1976 году вышла в свет работа Уитфрида Диффи и Мартина Хеллмана «Новые направления в криптографии», в которой описывались новые асимметричные криптоалгоритмы. Неклассическая схема (с открытым ключом) криптографического преобразования предполагала наличие двух различных ключей зашифрования и расшифрования: $k \neq k^*$. При этом, зная ключ k, невозможно

получить ключ k^*. Для полного цикла преобразования (зашифрования и расшифрования) необходимы оба ключа. Если информация была зашифрована на ключе k, то расшифровать ее можно только с помощью ключа k^*, и наоборот. Один из ключей (например, k) называется открытым (несекретным), другой (k^*) — закрытым (секретным).

Каждый участник информационного обмена (например, Соколов) может синтезировать для себя пару ключей и один из них (открытый) разослать по открытым каналам связи всем своим партнерам. Далее все, кто имеет открытый ключ Соколова k, могут зашифровать для него сообщение. Расшифровать криптотекст может только владелец закрытого ключа k^*, т. е. Соколов. Для того чтобы Соколову стать полноправным участником информационного обмена, ему необходимо получить по открытым каналам связи индивидуальные открытые ключи всех своих предполагаемых абонентов. Тем самым решается проблема распространения ключей шифрования.

Идея асимметричных алгоритмов тесно связана с теорией односторонних функций и с теорией сложности математических преобразований. Для обеспечения криптостойкости схем шифрования с открытым ключом требуются длинные ключевые последовательности. Кроме того, асимметричные алгоритмы включают в себя громоздкие операции возведения в степень и умножения больших чисел, поэтому они работают существенно медленней симметричных.

Наиболее распространенный асимметричный криптоалгоритм RSA (по фамилиям авторов, Rivest, Shamir, Adleman) был впервые опубликован в 1978 году и впоследствии принят в качестве стандарта в США. В стандарте RSA используется алгебраическое разложение больших целых чисел на множители, криптостойкость алгоритма базируется на сложности их факторизации. Кроме RSA известны алгоритм Эль-Гамаля, основанный на дискретном логарифмировании больших чисел, алгоритм на основе эллиптических кривых и др.

Асимметричная схема шифрования, безусловно, удобна при организации шифрованной связи. Однако в криптографических аппаратно-программных СЗИ сетевого действия часто применяется «гибридная» схема шифрования. Ярким примером такого СЗИ является американская система шифрования PGP, которая при инициализации встраивается в оболочку Windows, в Microsoft Outlook и Microsoft Outlook Express. Пользователи генерируют асимметричные ключевые последовательности и обмениваются открытыми ключами со своими партнерами. При отправлении каждого сообщения система PGP генерирует «сеансовый» симметричный ключ для шифрования данных и зашифровывает его на основе открытого ключа получателя. Передаваемое сообщение зашифровывается на основе симметричного ключа. Зашифрованные сообщение и сеансовый ключ в виде единого пакета направляются (например, посредством сервисов Internet) абоненту-получателю, где PGP на основе закрытого ключа расшифровывает симметричный ключ шифрования данных, а затем на его основе расшифровывает само сообщение.

СКЗИ предназначены для защиты конфиденциальной информации, хранящейся и обрабатываемой на персональных компьютерах, работающих, как

правило, под управлением ОС семейства Microsoft Windows в многопользовательском режиме, когда организация доверенной загрузки АС нецелесообразна.

Аппаратно-программные СЗИ, противодействующие НСД и предназначенные для обеспечения безопасности данных, хранящихся на локальном компьютере, используют классические симметричные алгоритмы шифрования. Это вполне разумно: охраняемые данные не предназначены для передачи по открытым каналам связи, и проблемы распространения ключей в этом случае просто не существует. Каждый пользователь формирует для себя личный симметричный ключ и сам несет ответственность за его сохранность. Применение классической схемы шифрования при этом целесообразно, т. к. обеспечивает б*о*льшую скорость при меньшей длине ключа.

СЗИ предлагают несколько вариантов шифрования информации. При шифровании *«по требованию»* — сообщения, документы, базы данных и т. д. редактируются в открытом виде. Готовый документ, каталог или подкаталог зашифровывается, например, для того, чтобы обеспечить его безопасное хранение на жестком диске ПЭВМ. Пользователь может поставить под таким зашифрованным документом свою цифровую подпись.

При шифровании *«на лету»* — в открытом виде информация существует только в оперативной памяти (в идеальном случае — в видеопамяти) ПЭВМ. Сохранение документа автоматически вызывает программу его шифрования. Такой метод называется *«прозрачным шифрованием»*, поскольку процессы криптографического преобразования протекают независимо от желания пользователя, скрытно (прозрачно) и удобно для него.

Удачным решением защиты информации является организация виртуального зашифрованного диска, который создается внутри дискового пространства ПЭВМ и «подключается» только при необходимости работы с конфиденциальными данными. О существовании такого диска, не говоря уже о процедуре его подключения, не знает никто кроме владельца. Виртуальный диск представляет собой специальным образом организованный файл и располагается в любом из каталогов файловой системы. После «подключения» виртуального диска операционная система может работать с ним как с любым другим логическим диском: создавать и удалять документы и каталоги, форматировать и т. д. Вся информация, размещаемая на виртуальном диске, автоматически зашифровывается. Такое шифрование принято называть «прозрачным с организацией виртуального диска». СЗИ, работающие с виртуальными дисками (например, «Secret Disk», «StrongDisk»), называют *менеджерами секретных файлов*.

Стандартный механизм шифрования шифрованных дисков приведен на рис. 2.1. Структура файла-образа виртуального диска содержит заголовок, непосредственно данные и ключ шифрования данных, который в свою очередь хранится в зашифрованном виде. При подключении диска пользователь должен ввести «ключевую информацию» в виде простого пароля и кодовых последовательностей, *раздельно* хранящихся в специальном файл-ключе и/или во внешней памяти. Введенная пользователем информация суммируется по схеме «И». Совокупная ключевая последовательность (комплексный пароль) подвергается операции ХЭШ-преобразования, в результате которой формируется «ключ ко-

дирования ключа». С помощью полученного «ключа кодирования ключа» и стойкого медленного алгоритма шифрования вычисляется ключ кодирования данных. Данные шифруются на основе быстрого симметричного алгоритма и ключа, который не хранится в компьютере в открытом виде, а формируется каждый раз при подключении логического диска.

Для формирования стойкого ключа СЗИ поддерживают программно и/или аппаратно достаточное количество различных вариантов внешних носителей ключевой информации. Среди них ключевые дискеты, пластиковые карты памяти различной технологии (электронные и с магнитной полосой), проксими-карты и ключи Touch Memory.

Кроме шифрования данных СЗИ могут шифровать и таблицы расположения данных. Конечно, существуют специальные программы, которые восстанавливают файловую систему на основании анализа дискового пространства. Однако, даже если злоумышленник «готов» к такой работе, восстановление таблиц расположения данных потребует от него определенного времени и обязательно оставит следы на атакуемом компьютере.

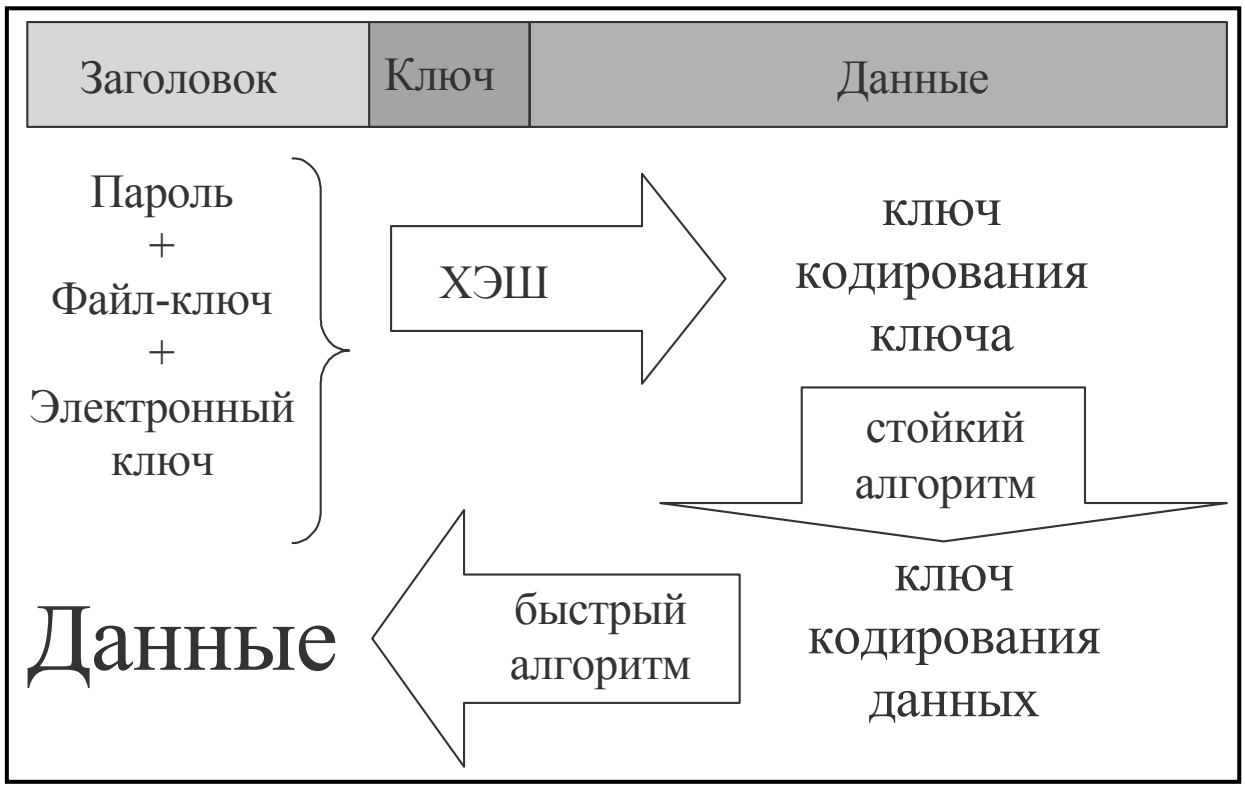


Рис. 2.1. Структура файла-образа виртуального шифрованного диска

СКЗИ кроме непосредственно шифрования данных гарантируют недоступность личных данных пользователей для остальных легальных субъектов, зарегистрированных в АС, и обеспечивают:

- защиту от несанкционированного доступа к зашифрованным данным (в том числе со стороны системного администратора);

- двухфакторную аутентификацию пользователя для доступа к защищенным данным (на основе ввода парольной информации и сканирования внешних устройств памяти);
- разграничение и контроль доступа к зашифрованной информации;
- многопользовательскую и коллективную работу с защищенными данными;
- безопасное надежное «уничтожение» документов, в которых может храниться остаточная информация, при их удалении;
- очистку критичных областей памяти (свободных областей диска и хвостов файлов, файлов виртуальной памяти);
- организацию безопасного хранения «временных файлов», создаваемых ОС, путем переадресации каталога «TEMP» на шифруемый налету диск;
- защитные действия при возникновении «экстренных» ситуаций.

При шифровании информации СКЗИ применяют встроенные в ОС симметричные алгоритмы криптопреобразования (например, RC4) или имеющиеся в составе самого средства стандартные алгоритмы шифрования (3DES; CAST-128; SAFER; Blowfish). СКЗИ предоставляют пользователю возможность подключать внешние программные модули, реализующие наиболее криптостойкие алгоритмы, в том числе по российскому ГОСТ 28147–89, например, эмулятор криптографической платы «Криптон» фирмы «Анкад».

Типичными представителями СКЗИ являются аппаратно-программные средства защиты информации «StrongDisk» (ООО «Физтех-Софт», г. Санкт-Петербург) и «Secret Disk» (компания ALADDIN Software Security R.D., г. Москва), предназначенные для создания на дисковом пространстве локальной рабочей станции (Strong Disk Pro, Secret Disk NG) и сервера (Strong Disk Server, Secret Disk Server) защищенных дисков с ограниченным (многопользовательским) доступом. СКЗИ «Strong Disk» предоставляет пользователю возможность шифровать данные на лету с организацией виртуального диска. В состав средства входят удобные встраиваемые в оболочку Windows утилиты очистки остаточной информации: безопасного удаления файлов, очистки неиспользуемых областей жестких дисков, очистки «хвостов» файлов и файла виртуальной памяти (win386.swp). «Strong Disk» предлагает расширенные возможности при возникновении «форс-мажорных» ситуаций. Одна из последних разработок ООО «Физтех-Софт» обеспечивает криптографическую защиту информации на «карманных» персональных компьютерах (КПК). Средство рассчитано на индивидуальное пользование зашифрованными логическими дисками но, к сожалению, не использует отечественный ГОСТ шифрования.

СКЗИ «Secret Disk» (рис. 2.2) ориентировано на многопользовательский режим обработки приватных данных, хранящихся на зашифрованных виртуальных дисках или разделах винчестеров. «Secret Disk» реализует ролевую модель разграничения доступа. Средство позволяет зашифровывать «по требованию» отдельные каталоги и документы. «Secret Disk» имеет свой собственный встроенный алгоритм шифрования на основе 128-битного ключа и позволяет подключать внешние криптомодули.

Ключи зашифрования и расшифрования данных СКЗИ формируются только при подключении виртуального диска на основании пароля, вводимого пользователем, ключевой информации, хранящейся в файле-ключе и во внешнем носителе (электронные ключи Touch memory — «Strong Disk», ключи eToken — «Secret Disk»). Ключ шифрования хранится только в оперативной памяти ПЭВМ и никогда не выгружается на устройства постоянной памяти.

СКЗИ зашифровывают разделы винчестера целиком или организовывают виртуальные логические диски в виде непрерывного файла-образа. Прочитать файловую структуру таких дисков, не вводя ключевой информации, невозможно. Поэтому средства криптографической защиты не скрывают своего присутствия в компьютерной системе, но обеспечивают сокрытие наличия в ней конфиденциальных данных.

Рис. 2.2. СЗИ «Secret Disk»

При выборе СЗИ, осуществляющего шифрование данных, необходимо учитывать стойкость применяемого криптографического преобразования. Современные ПЭВМ имеют высокую производительность и могут обеспечить шифрование на основе мощных алгоритмов, например по ГОСТ 28147–89, в реальном масштабе времени. Однако в большинстве СЗИ эти алгоритмы не применяются, что можно объяснить сложной и дорогостоящей процедурой сертификации СЗИ. Некоторые СЗИ («Панцирь», «Secret Disk») позволяют подключать внешние программные модули шифрования, в т. ч. по ГОСТ 28147–89.

2.2. Система защиты конфиденциальной информации PGP

2.2.1. Основные характеристики системы PGP

PGP объединяет в себе лучшие стороны симметричной криптографии и криптографии с открытым ключом. PGP – это гибридная криптосистема. Средство защиты встраивается в оболочку операционной системы, предоставляет пользователю возможность зашифровывать файлы по требованию через контекстное меню проводника или специальных клавиш, появляющихся в окнах почтовых программ после инициализации программы.

При шифровании файлов или почтовых сообщений PGP создаёт одноразовый симметричный ключ, применяемый для единственного сеанса связи. Сеансовый ключ представляет собой псевдослучайное число, сгенерированное от случайных движений мышки и нажатий клавиш. Сеансовый ключ используется надёжным и быстрым симметричным алгоритмом, которым PGP зашифровывает сообщение, превращая его в шифртекст. Для повышения криптостойкости, снижения нагрузки на каналы связи и экономии дискового пространства в системе применяется сжатие информации. Сеансовый ключ зашифровывается открытым ключом получателя. Зашифрованный открытым ключом получателя сеансовый ключ «прикрепляется» к шифртексту и передаётся вместе с ним получателю, образуя так называемый «цифровой конверт» (рис. 2.3).

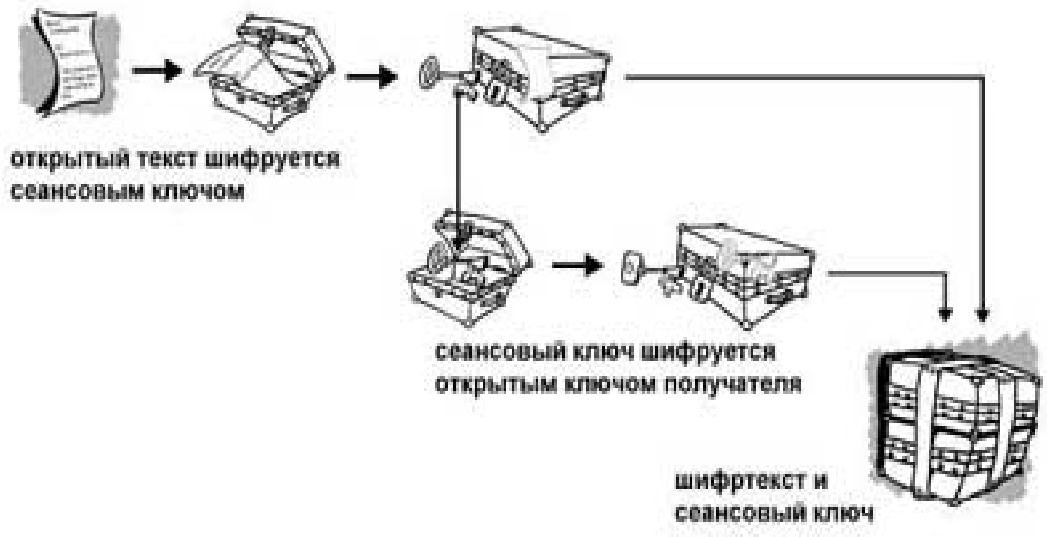


Рис. 2.3. Формирование цифрового конверта

Расшифрование цифрового конверта происходит в обратном порядке. На приемной стороне система PGP использует закрытый ключ получателя для извлечения из сообщения сеансового ключа. Полученный сеансовый ключ PGP, использует для преобразования исходного послания в открытый текст.

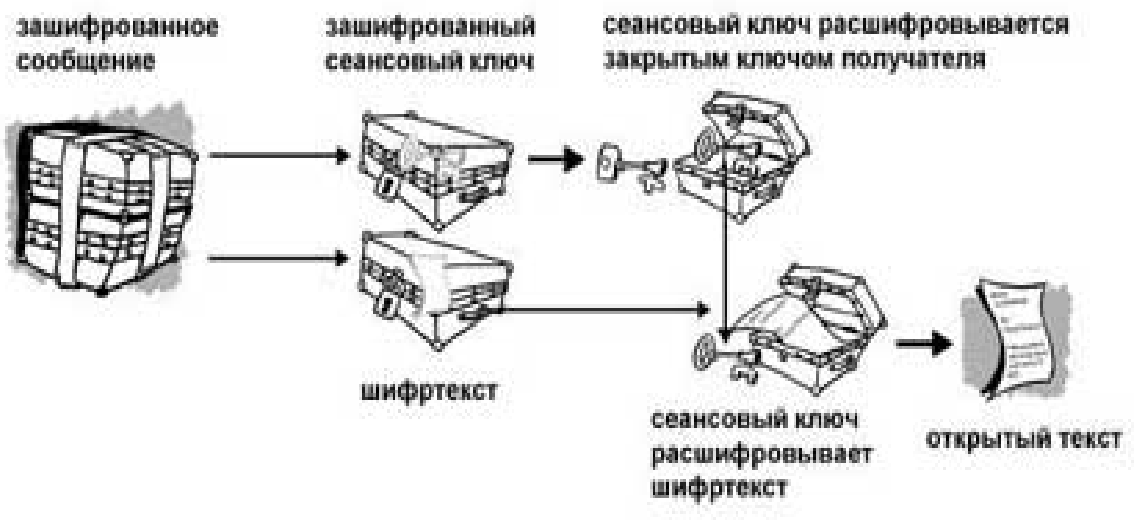


Рис. 2.4. Расшифровывание цифрового конверта

Используемые совместно системы шифрования взаимно дополняют друг друга без какого-либо ущерба безопасности. Симметричное шифрование, скорость и надежность которого в тысячи раз быстрее асимметричного, обеспечивает высокое быстродействие и криптостойкость системе. Возможность распределения ключей по открытым каналам связи, предоставляемая схемой шифрования открытым ключом, в свою очередь, предоставляет простое решение проблемы распределения ключей. Комбинация двух криптографических методов объединяет удобство шифрования открытым ключом со скоростью работы симметричного алгоритма.

2.2.2. Инициализация системы PGP на рабочей станции

Установка системы PGP на рабочую станцию чрезвычайно проста. Для инициализации системы PGP необходимо закрыть все работающие приложения Windows и запустить файл PGPDesktop.exe, который откроет окно диалоговой установки данной программы. Кроме стандартных лицензионных соглашений при ее инициализации следует соблюдать несколько правил.

В окне «User type» (Тип пользователя, рис. 2.5) необходимо выбрать опцию «No, I’m a New User», с тем, чтобы при установке системы пользователю была инициализирована пара (открытый и закрытый) ключей. Если выбрать пункт «Yes, I already have keyrings», то инициализировать ключи можно будет позже, пользуясь менеджером ключей.

Основные исполняемые программные блоки PGP устанавливается в директорию «C:\Program Files\Network Associates\PGP for Windows». Если нет каких-либо предписаний системного администратора (руководителя лабораторного практикума), то следует принять предложение программы-установщика системы. В окне выбора компонентов «Select Component» определяется набор

функций, устанавливаемый на рабочую станцию. На рис. 2.6 приведен набор компонентов, предлагаемый системой[1].

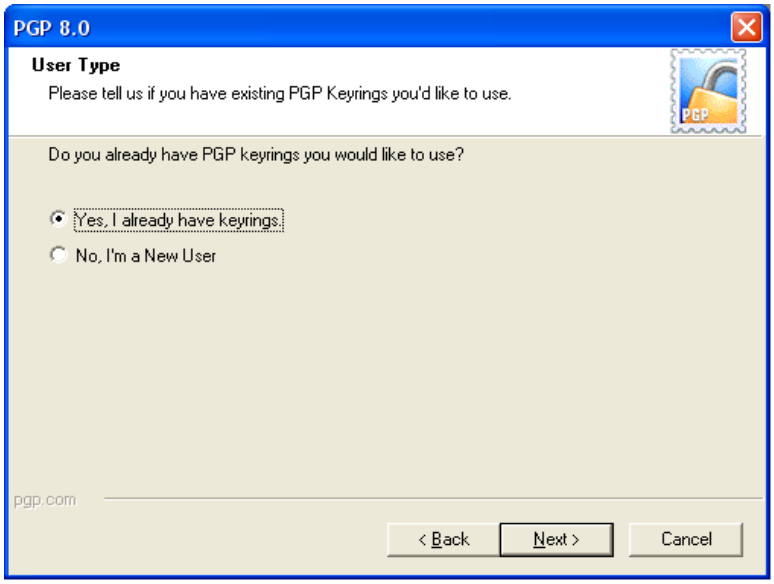


Рис. 2.5. Выбор «типа» пользователя

При инициализации системы в режиме «No, I'm a New User» осуществляется генерация пары симметричных ключей для нового пользователя. По умолчанию система PGP устанавливает размер персональных ключей пользователя, равный 2048 бит, алгоритм несимметричного шифрования – RSA и срок действия сигнатур (ключей) – один год. Индивидуальные параметры шифрования можно установить, если в окне «Key Generation Wizard» нажать кнопку «Expert» (рис. 2.7). При этом откроется окно выбора параметров шифрования «Expert Key Parameter Selection» (рис. 2.8), в котором нужно ввести полное имя пользователя, почтовый адрес и выбрать требуемые параметры ключей и алгоритм шифрования. Если информация о пользователе не будет введена в окне «Expert Key Parameter Selection», то система предложит ее ввести в специальном окне «Name and E-mail Assignment».

В следующем окне «Passphrase Assignment» задается (и подтверждается) пароль пользователя (рис. 2.9), на основе которого генерируются секретный и открытый ключи. PGP не ограничивает снизу количество символов в пароле, но рекомендует, чтобы их было не менее восьми. В окне «Passphrase Assignment» индуцируется качество «Passphrase Quality» вводимой ключевой фразы. После подтверждения ввода пароля осуществляется пошаговая генерация пары ключей (Key Generation и Generation Subkey), что сопровождается соответствующей индикацией в окне «Key Generation Progress». Для завершения инициализации PGP на рабочую станцию необходимо перегрузить компьютер, установив переключатель «Yes, I want to restart my computer now» во включенное состояние.

[1] Во избежание конфликтов с имеющимся сетевым программным обеспечением, следует отключить персональный сетевой фильтр «PGP net Personal Firewall», а так же менеджер защищенных дисков «PGP disk Volume Security».

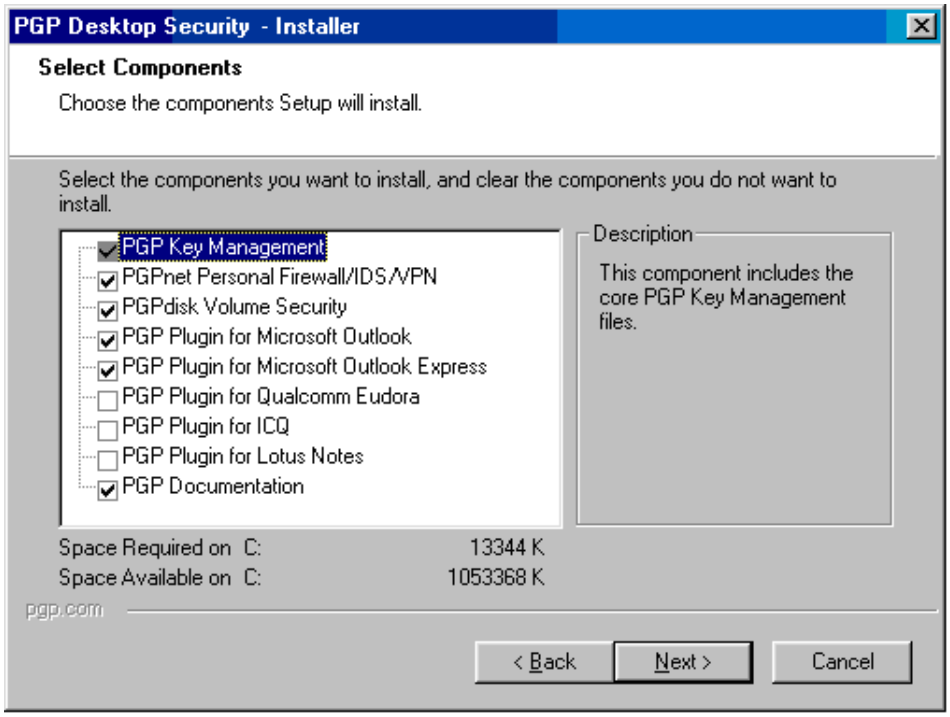


Рис. 2.6. Меню выбора устанавливаемых компонентов системы

Рис. 2.7. Окно мастера генерации ключей

При необходимости ввести в систему нового пользователя или изменить параметры шифрования существующего окно «Key Generation Wizard» может быть вызвано из меню установленной программы PGP ⇒ PGPkeys ⇒ Keys ⇒ New Key…

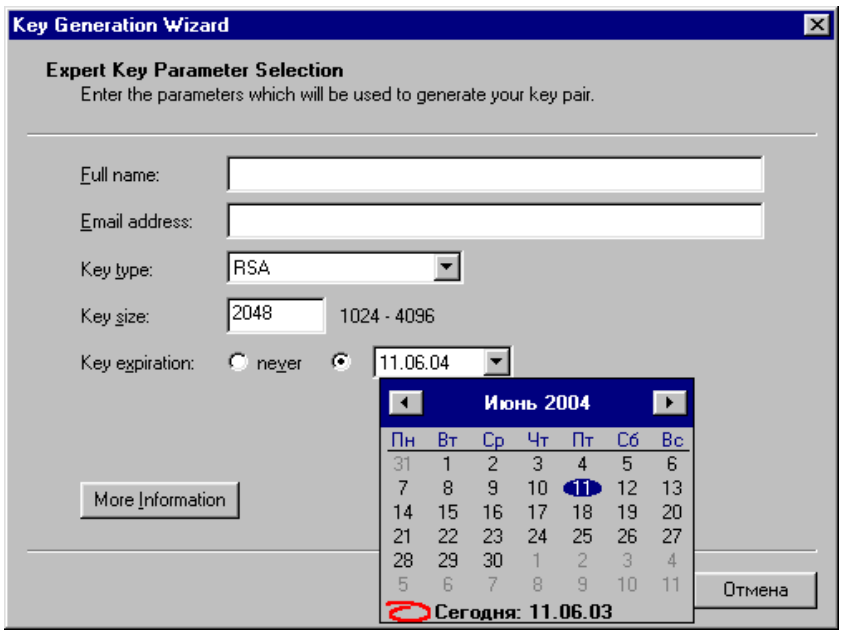


Рис. 2.8. Выбор параметров ключей и алгоритма шифрования

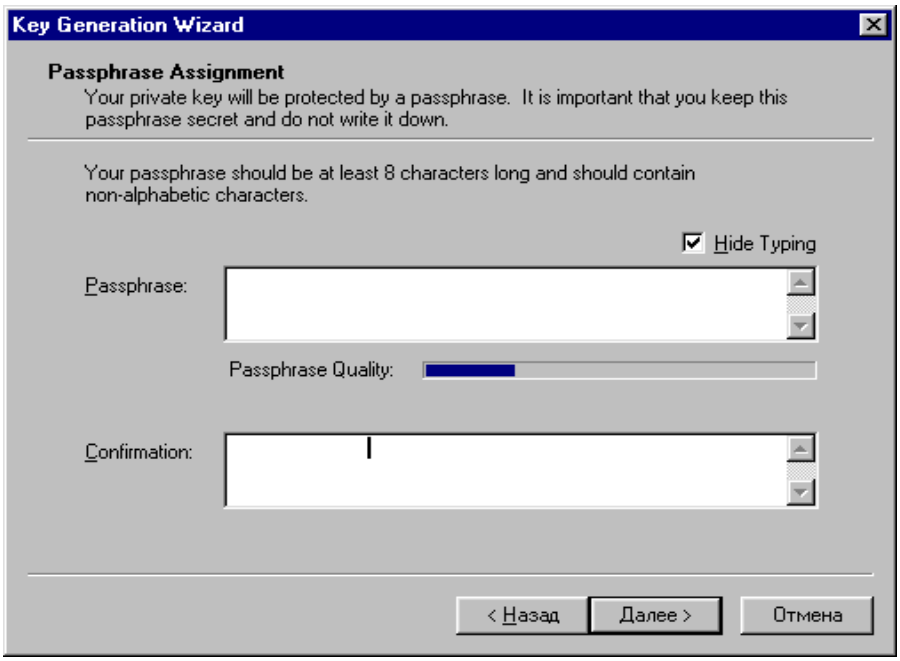


Рис. 2.9. Ввод ключевой фразы

Процесс инициализации PGP заканчивается перезапуском операционной системы. После установки в меню «пуск» ⇒ «все программы», создается новая группа PGP, в которой содержатся ярлыки программ входящих в состав системы : «PGPdisk», «PGPkeys» и «PGPmail». «PGPdisk» служит для создания и работы с защищенными логическими дисками; «PGPkeys» – для создания, редактирования, получения и управления ключами; «PGPmail» – для обработки шифрование и дешифрование файлов.

Успешная инициализация системы PGP сопровождается появлением на панели задач значка в виде навесного замка, строки PGP в меню Пуск ⇒ Про-

граммы ⇒ PGP и строки во всплывающем меню, появляющемся при нажатии правой клавиши мыши на ярлыке документа или каталога с документами (рис. 2.10).

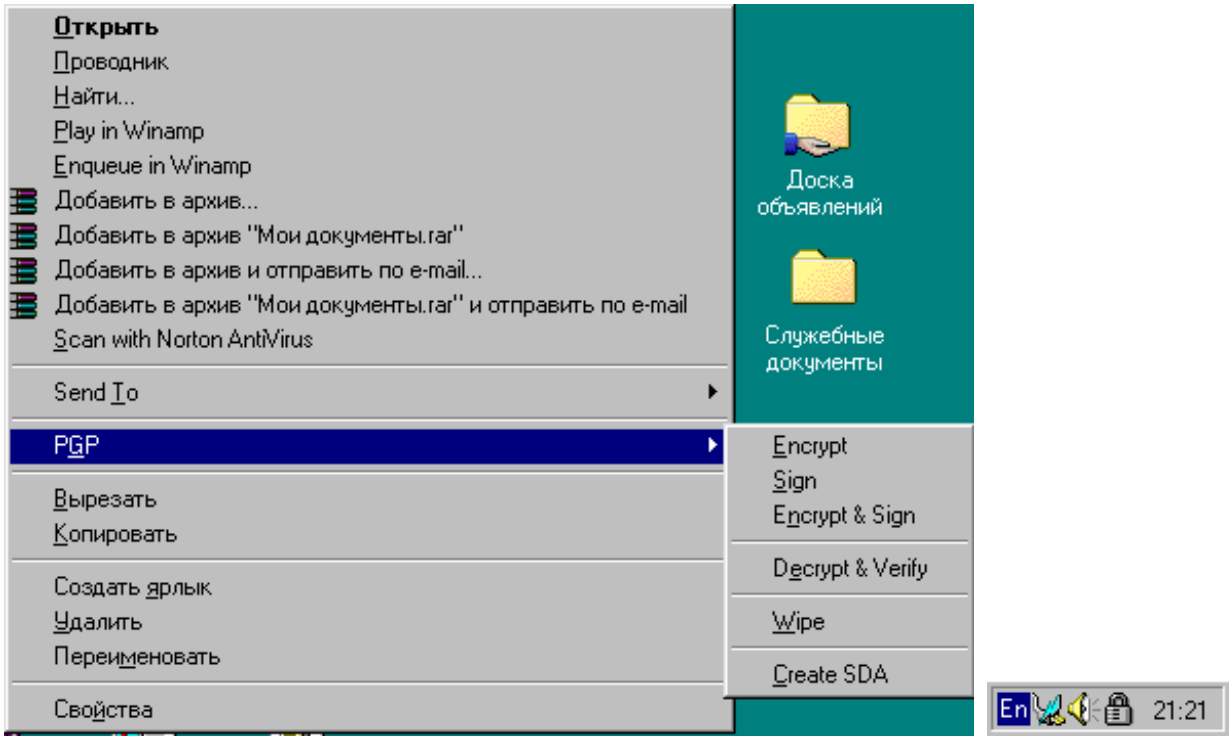


Рис. 2.10. Признаки успешной инициализации PGP на рабочей станции

ВЫПОЛНИТЬ!

1. Установить систему PGP на компьютер; в процессе инициализации генерировать ключи пользователя; для удобства последующей работы определить полное имя пользователя, содержащее номер компьютера в локальной сети (например, *Slushatel-i*).
2. На рабочем столе каждой ПЭВМ создать каталоги (см. рис. 2.10): для редактирования, хранения и зашифрования/расшифрования конфиденциальных документов – *Служебные документы-i.*
3. Для организации наглядного обмена зашифрованными документами и открытыми ключами один доступный для всех компьютеров каталог – *Доска объявлений*.

2.2.3. Генерация, импортирование и экспортирование ключей

Пользователь ПЭВМ может иметь несколько пар ключей для обмена приватными данными с различными категориями участников документооборота. На режимных предприятиях часто доступ в глобальные сети имеет один компьютер, с помощью которого сотрудники предприятия получают и отправляют почту. Поэтому на одном компьютере в системе PGP одновременно может быть зарегистрировано несколько пользователей с уникальными именами и ключа-

ми. Для генерации нового ключа (новому пользователю) необходимо вызвать главное меню PGP, нажав кнопку системы PGP на панели задач, и выбрать окно «PGPkeys», в котором осуществляются основные манипуляции с ключами (рис. 2.11). В меню окна «PGPkeys» вызвать подменю «Keys» и нажать кнопку «New Key»: PGP ⇒ PGPkeys ⇒ Keys ⇒ New Key. После чего появится диалоговое окно «Key Generation Wizard», которое появлялось при инициализации системы PGP на компьютер. Инициированные ключи вновь зарегистрированного пользователя отображаются в виде соответствующей строки в окне «PGPkeys» с именем пользователя.

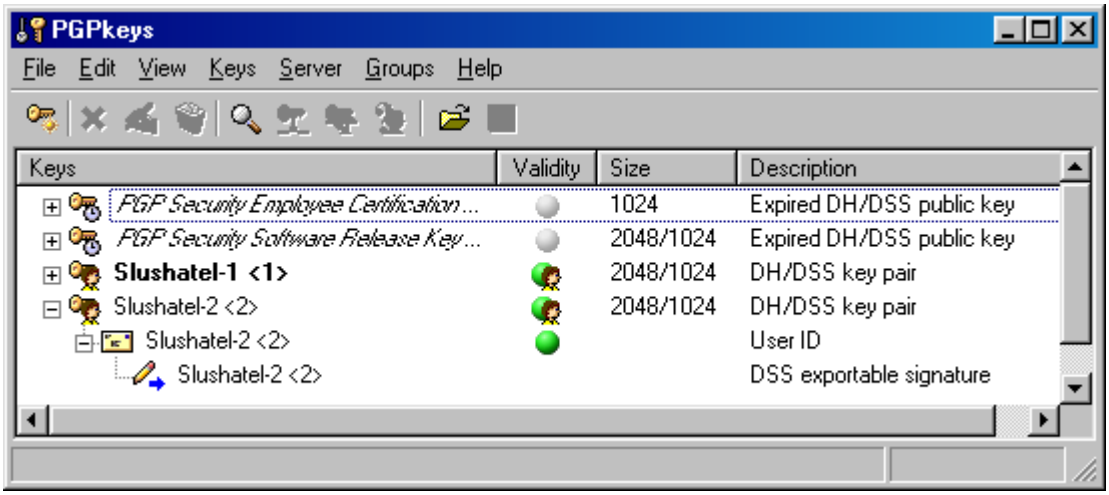


Рис. 2.11. Окно «PGPkeys»

Все ключи хранятся по умолчанию в папке «C:\Documents and Settings\Ivan Sedov\Мои документы\PGP». Но при желании её можно изменить, для чего достаточно нажать комбинацию клавиш «Ctrl-T» или выбрать меню «Edit-Options» и в закладке «files» вписать желаемый путь и имена файлов для хранения ключей. Если к этому моменту в системе уже были созданы ключи, то программа предложит скопировать содержание файла с ключами в новую директорию.

Для организации шифрованной связи участникам обмена, работающим на различных ПЭВМ локальной (глобальной) сети, необходимо обменяться открытыми ключами. Наиболее удобным способом обмена ключами является их пересылка через сервер-депозитари или посредством почтовых сервисов. Иногда может потребоваться отправить открытый ключ в виде отдельного файла (например, через FTP-сервер). В этом случае можно экспортировать или копировать ключи в файл. Чтобы сохранить ключ в виде отдельного файла необходимо в окне «PGPkeys» выделить ключ, подлежащий экспортированию, в строке меню нажать кнопку «Keys ⇒ Export» и указать имя файла и каталог назначения. При этом допускается экспортирование группы ключей, путем выделения нескольких нужных. Полученный файл с открытым ключом может быть передан партнеру по сети или на каком-либо машинном носителе КИ.

При выполнении практических заданий предлагается использовать вспомогательную папку «Доска объявлений» с разрешенным общим доступом. Для удобства и наглядности процесса обмена ключами в «оконном режиме» на ра-

бочих столах компьютеров должны быть открыты папки «PGPkeys» и «Доска объявлений». Чтобы подготовить свой открытый ключ к пересылке, следует «перетащить» его из окна «PGPkeys» в окно «Доска объявлений», взявшись мышью непосредственно за имя пользователя в строке ключа (рис. 2.12). В папке появится файл ключа с именем пользователя и расширением «acs». Поскольку к данной папке открыт общий доступ, заинтересованные участники обмена могут выложить на «Доску объявлений» свои открытые ключи и скопировать открытые ключи остальных пользователей к себе на компьютер.

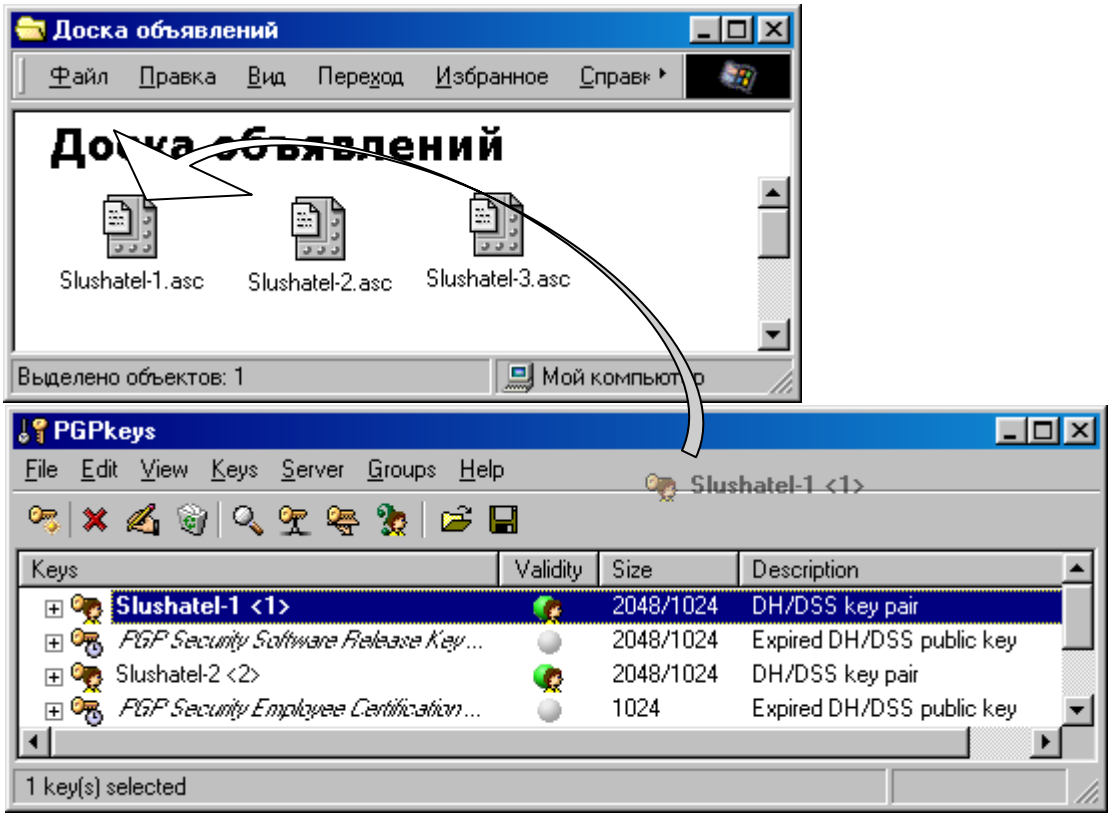


Рис. 2.12. Обмен открытыми ключами посредством «Доски объявлений»

Скопированный или полученный по сети ключ на стороне потенциального получателя необходимо импортировать в «набор ключей» системы PGP. Эту операцию также можно осуществить в оконном режиме: с помощью мыши следует «перетащить» файл, содержащий интересующий ключ, в окно «PGPkeys» своего компьютера. Для подтверждения импортирования ключа в систему в появившемся окне «Keys» необходимо выбрать команду «Import» (рис. 2.13).

Асимметричные криптосистемы решают проблему обмена ключами и зашифрованной информацией, однако они крайне уязвимы к атакам «человек в середине», когда злоумышленник пытается выдать свои поддельные открытые ключи за ключи корреспондентов, участвующих в двухстороннем обмене. Позднее это позволить ему полностью контролировать пересылаемые сообщения: перехватывать, читать и изменять. Взаимное заверение пользователями открытых ключей друг друга непосредственно после обмена – это основа распределённой модели доверия «Web of Trust» системы PGP, обеспечивающая про-

тиводействие таким атакам. Для того чтобы убедиться в легальности вновь импортированного ключа в системе имеется возможность сравнивать сигнатуры открытого ключа на компьютере-получателе и компьютере-источнике. Пользователь, переславший свой открытый ключ и пользователь, получивший его, должны одновременно открыть подменю «Keys» окон «PGPkeys» и просмотреть свойства «Properties» проверяемого ключа и сравнить их сигнатуры (рис. 2.14). Убедившись в истинности ключа, получатель может «подписать» его.

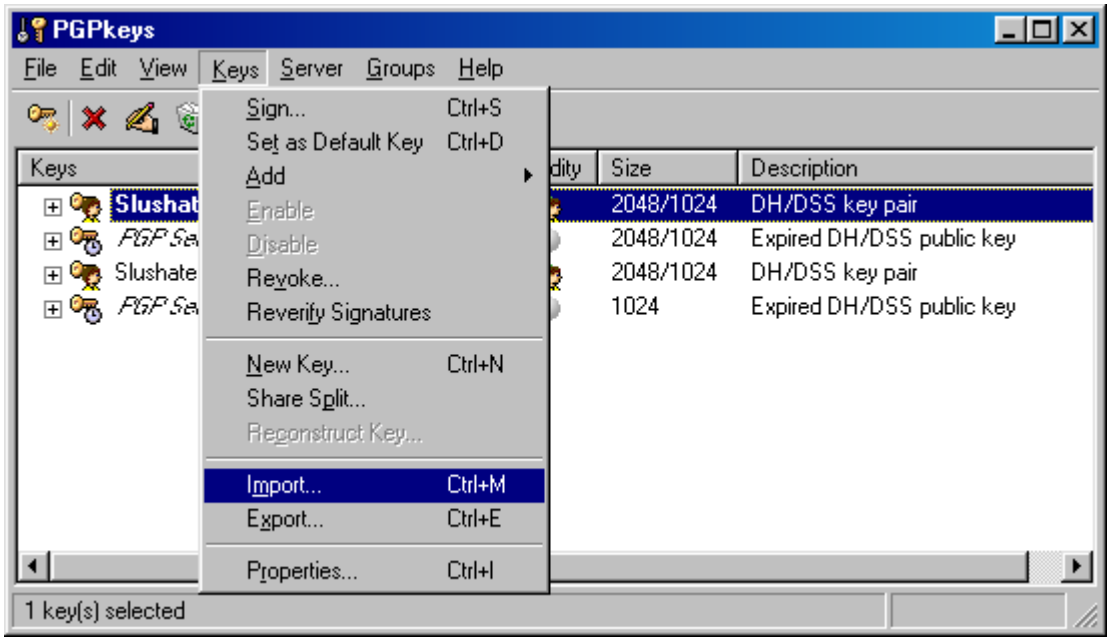


Рис. 2.13. Импортирование ключа посредством «Доски объявлений»

Чтобы подписать открытый ключ или любые из сведений его сертификата необходимо вокне «PGPkeys» выделить ключ или любые из сведений сертификата, подлежащие заверению подписью, в строке меню выбрать команду «Sign» в подменю «Keys» и ввести свой пароль. Легитимные ключи, которым теперь доверяет пользователь данной системы PGP, окрашиваются в окне «PGPkeys» в зеленый цвет.

В системе имеется возможность подписывать ключевую информацию партнеров особым образом. Для этого необходимо нажать кнопку «Sign the selected item в панели инструментов», в появившемся окне просмотреть список подписываемых ключей, сведений сертификата и их отпечатков и убедиться, что не выбрано ничего лишнего, нажать кнопку «More Choices» и в разделе «Signature Type» следует указать тип подписи, которым хотите заверить ключ, запись сертификата:

- Non-exportable – неэкспортируемая подпись – когда пользователь уверен в подлинности ключа или записи сертификата, но не хочет выступать его поручителем. Такая подпись не может быть экспортирована и служит только для информирования программы в том, что пользователь считает ключ не скомпрометированным, и позволяет наделить владельца определённым уровнем доверия в заверении других ключей.

- Exportable – экспортируемая подпись – когда пользователь уверен в подлинности ключа или записи сертификата и хочет выступать его поручителем. Такая подпись экспортируется наряду с ключом, чтобы другие пользователи могли на неё полагаться при определении достоверности данного ключа.

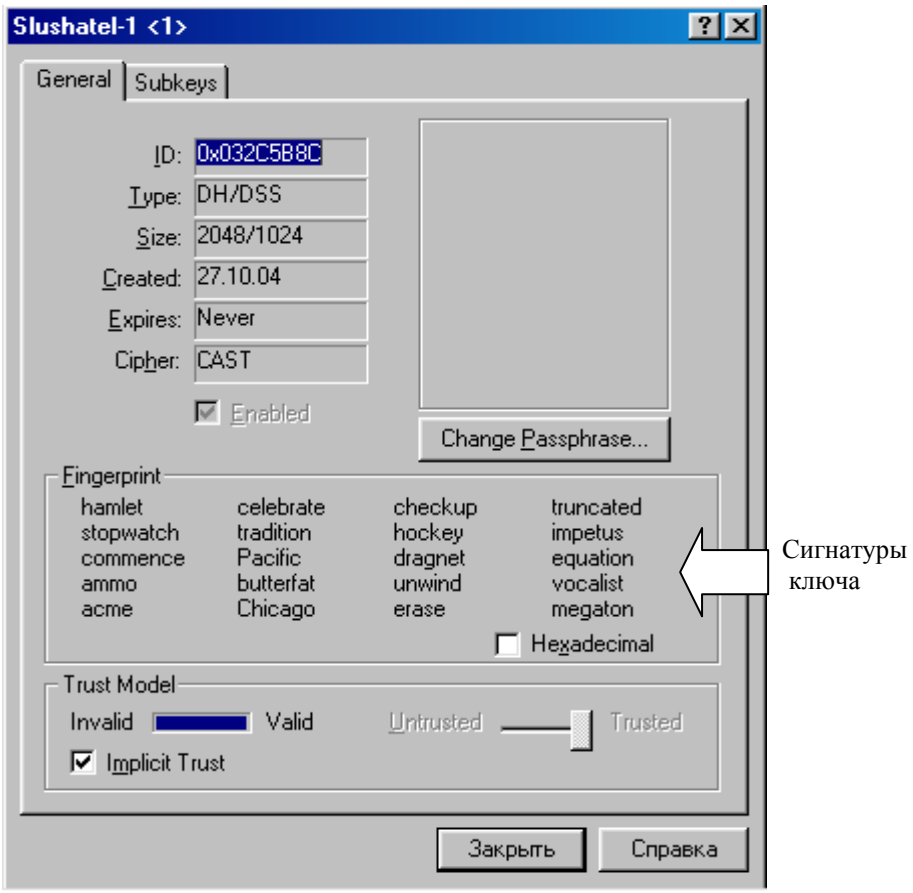


Рис. 2.14. Проверка легитимности полученного ключа

- Trusted Introducer Exportable – используется, когда пользователь уверен в подлинности ключа партнера и готов наделить его полномочиями доверенного поручительства: все заверенные доверенным партнером ключи становятся априорно достоверными как для самого пользователя, так и для всех, кто доверяет его подписи.
- Meta-Introducer Non-Exportable – заверение такой подписью какого-либо ключа сделает его владельца мета-поручителем пользователя компьютера: владельцы всех подписанных владельцем импортированного ключ становятся доверенными поручителями пользователя (то есть будут, как бы заверены подписями Trusted Introducer Exportable). Эта подпись неэкспортируема.

  При выборе одной из двух последних типов подписи, представляются дополнительные возможности:
- Maximum Trust Depth – на сколько уровней вниз вдоль цепи сертификации будет происходить заверение ключей доверенным поручителем или наделение полномочиями доверенного поручительства от мета-поручителя.

- Domain restriction – ограничение для доверенного поручителя на заверение ключей, принадлежащих только к указанному здесь домену. Например, если указать здесь pgpru.com, доверенный поручитель сможет заверять лишь те ключи, чьи email-адреса заканчиваются на pgpru.com.

Лучший способ установить подлинность полученной копии открытого ключа корреспондента – позвонить ему и попросить прочитать отпечаток с оригинала, хранящегося на его связке (прочитать отпечаток должен именно отправитель получателю, а не наоборот!). Маловероятно, что злоумышленник сможет перехватить такой произвольный звонок и провести активную атаку, попытавшись выдать себя за корреспондента. Если корреспонденту – получателю знаком голос корреспондента – отправителя, это сделать будет практически невозможно.

ВЫПОЛНИТЬ!

4. В оконном режиме с помощью мыши «перетащить» свой открытый ключ в доступную для остальных пользователей папку «Доска объявлений».
5. Импортировать открытый ключ партнера в окно «PGPkeys», проверить сигнатуры ключа и в случае их совпадения подписать импортированный ключ путем вода парольной информации.

2.2.4. Изменение настроек сервиса PGPkeys[1].

Система PGP предоставляет пользователю достаточно большое количество дополнительных сервисов, которые упрощают работу с подпрограммой «PGPkeys» и в частности процесс передачи ключей другим пользователям.

В первую очередь, если раньше до инициализации системы на конкретном компьютере были созданы PGP-ключи, то их можно добавить в файл ключей, путь к которому указывается в меню «File⇒Open». По желанию можно создать и новые файлы, которые будут хранить новые ключи. Также можно добавлять открытые ключи других пользователей: Keys⇒Import. И соответственно распространять свой ключ: Keys⇒Export. В системе предусмотрено глобальное распространение своих ключей в сети Интернет, для этого лишь надо указать сервер, на который необходимо отправить ключ. В программе по умолчанию имеется 2 сервера: keyserver.pgp.com и europe.keys.pgp.com. По желанию можно внести и свои адреса в меню «Edit⇒Options» на закладке «Servers».

Для разграничения пользователей реализована возможность распределять пользователей по группам. Для создания новой группы нужно выбрать контекстное меню «Groups⇒New Group» (Ctrl-R) и ввести название созданной группы: «Groups⇒Show Group» (Ctrl-U), которая будет показана в нижней части главного окна (рис. 2.15).

[1] Данный пункт является дополнительным, не обязательным для чтения.

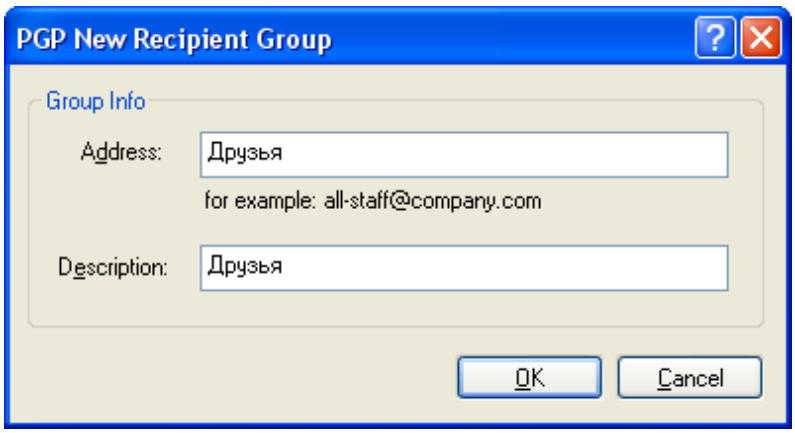


Рис. 2.15. Создание новой группы доверенных пользователей

Если требуется перенести пользователя в какую-либо группу, достаточно просто «нажать» на нем и удерживая левую кнопку мыши и перетащить запись в нужную группу в нижней части экрана. Данная функция значительно упрощает поиск пользователей и придает структурность в отображении всех записей.

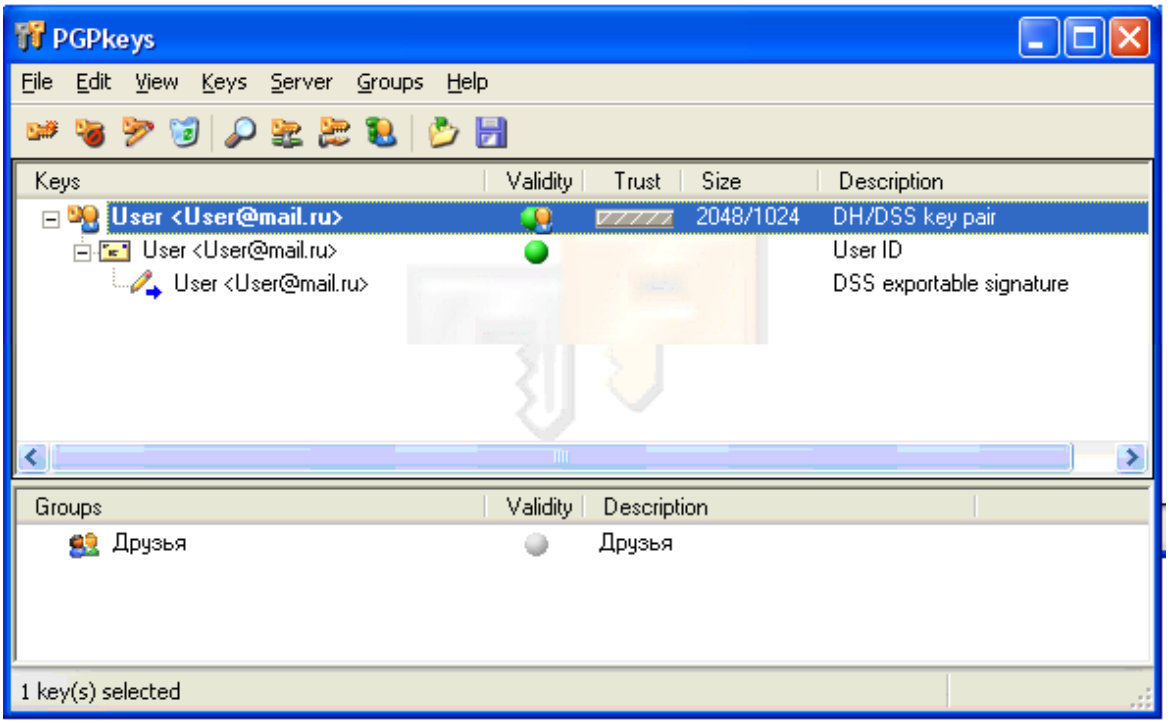


Рис. 2.16. Внесение пользователя в группу

Наряду с именами ключей окно «PGPkeys» отображает некоторые из их параметров и атрибутов. В меню «View» можно указать, какие атрибуты будут отображаться в окне менеджера, а в самом окне при желании можно изменить порядок расположения столбцов атрибутов (перетащив столбец за шапку) и сортировку списка ключей по любому из атрибутов (нажав левой кнопкой на шапку нужного столбца).

Окно «PGPkeys» может показывать следующие параметры ключей: имена (Keys), достоверность (Validity), размер (Size), идентификационный номер (Key ID), уровень доверия (Trust), дату создания (Creation Date), дату окончания действия (Expiration Date), наличие дополнительных ключей расшифрования (ADK), описание (Description). Также в меню View можно включить или выключить показ панели инструментов (Toolbar) и свойства подключенной смарт-карты (Smart Card Properties).

В окне «PGPkeys» версии системы 8.0 после создания или экспортирования ключей, появляется несколько видов «иконок» для пользователей:

- золотой ключ и человечек обозначают принадлежащую пользователю пару «открытый ключ - закрытый ключ» типа DH/DSS;
- серый ключ и человечек обозначают принадлежащую пользователю пару «открытый ключ - закрытый ключ» типа RSA;
- золотой ключ обозначает открытый ключ партнера типа DH/DSS;
- серый ключ обозначает открытый ключ партнера типа RSA;
- старомодный серый ключ обозначает открытый ключ обратной совместимости типа RSA Legacy;
- пара ключей обозначает разделённый ключ – такой ключ может использоваться для расшифрования / подписания только после объединения;
- тусклый ключ обозначает временно дезактивированный открытый ключ, такой не может использоваться для зашифрования, что удобно при большом количестве открытых ключей на связке, сильно захламляющих окно «Key Selection Dialog»;
- серый ключ на золотой карте обозначает сохранённый на смарт-карте ключ типа RSA;
- ключ с красным запрещающим знаком обозначает аннулированный открытый ключ, – это значит, что ключ либо был скомпрометирован, либо по иным причинам более не используется владельцем;
- ключ с часиками обозначает просроченный открытый ключ, чей период действия уже истёк;
- два человечка обозначают группу открытых ключей списка рассылки;

Следующие пиктограммы обозначают содержимое сертификата:

- конверт обозначает обычное имя в сертификате ключа; как правило, это просто имя и email-адрес владельца ключа, конверт может быть жёлтым или серым в зависимости от типа ключа (DH/DSS или RSA);
- конверт с красным запрещающим знаком обозначает аннулированную запись сертификата;
- картинка обозначает фотографическое удостоверение в сертификате;
- карандаш (или шариковая ручка) обозначает подпись, подтверждающую ту или иную запись сертификата ключа, иконка карандаша без дополнительных символов – это неэкспортируемая подпись, заверяющая ключ только на связке пользователя;

- карандаш с синей стрелкой обозначает экспортируемую со связки подпись, – используется как поручительство пользователя в подлинности ключа и данной записи сертификата.
- карандаш с красным запрещающим знаком обозначает отозванную подпись;
- тусклый карандаш обозначает неверную или повреждённую подпись;
- документ с печатью обозначает сертификат X.509;
- часики обозначают просроченный сертификат X.509;
- красный запрещающий знак обозначает аннулированный сертификат X.509.

ВЫПОЛНИТЬ!

6. В программе PGPkeys создать группу «друзья» и поместить туда один из импортированных ранее открытых ключей.

2.2.5. Шифрование и обмен шифрованной информацией

Незашифрованная личная информация (редактируемые текстовые файлы, рисунки, таблицы и т.д.), расшифрованные файлы, полученные от других участников обмена, не должны быть доступны пользователям по сети. Поэтому они должны обрабатываться (редактироваться, зашифровываться и расшифровываться) в каталоге, к которому нет сетевого доступа. При обмене конфиденциальной информацией в системе реализуется режим шифрования по требованию. Предназначенный для отправления по открытым каналам связи документ должен быть отредактирован в соответствующем формату документа стандартном приложении и закрыт. Этот документ не подвергался еще криптографическому преобразованию и содержит приватные сведения в открытом виде. Для шифрования документа с помощью системы PGP необходимо подвести курсор мыши к его ярлыку и нажать правую клавишу манипулятора. Во всплывающем меню следует выбрать один из трех вариантов шифрования файла (рис. 2.17):

- Encrypt – зашифровать файл (документ);
- Sign – сформировать под документом электронную цифровую подпись;
- Encrypt & sign – зашифровать и подписать документ.

В первом случае в текущей папке формируется файл, содержащий информацию в зашифрованном виде. Во втором случае, в текущей папке формируется файл, содержащий электронную цифровую подпись (ЭЦП) владельца исходного документа. В третьем случае, – единый файл, одновременно содержащий информацию в зашифрованном виде и ЭЦП.

При выборе пунктов «Encrypt» или «Encrypt & Sign» появляется окно выбора ключа (PGP Key Selection). В окне из верхней половины экрана следует выбирать реципиента (получателя), чьим ключом вы будете шифровать, щелкаете двойным нажатием мыши по нему и он автоматически переносится вниз.В левом нижнем углу этого окна имеется 4 опции для шифрования. Вы можете варьировать этими опциями в зависимости от данных, которые вы собираетесь шифровать:

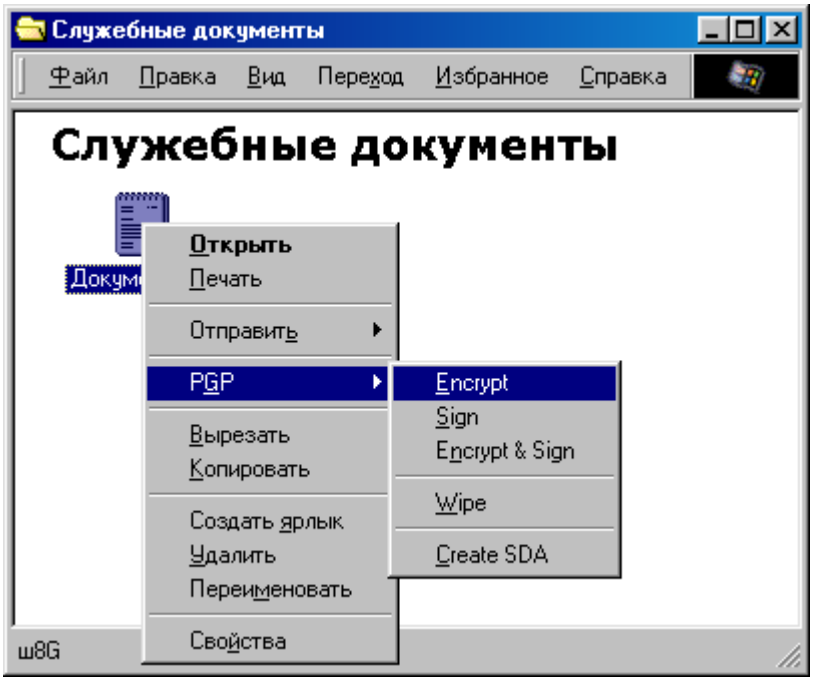


Рис. 2.17. Выбор режима зашифрования документа

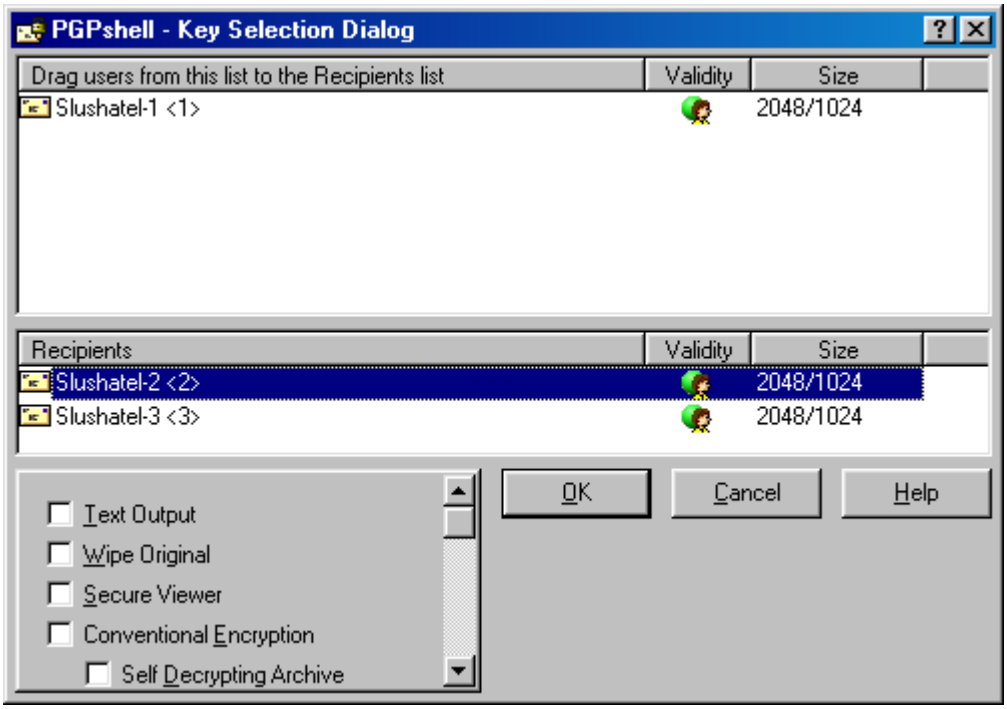


Рис. 2.18. Выбор отправителя и получателя зашифрованного документа

- Text Output («текст на выходе»). Когда вы отправляете файлы по почте, прикрепляя их к письму, вам можете воспользоваться этой функцией, для сохранения файла как ASCII текст. Это иногда необходимо, для того чтобы отправлять бинарные (двоичные) файлы, когда вы используете e-mail приложения более старых версий, которые не поддерживают эту функцию. При этом размер шифруемого файла увеличивается примерно на 30 процентов;

- Input Is Text («входящий это текст»)– инструктирует программу, что исходный файл содержит текстовую информацию, а не двоичный код. Используется только в целях совместимости зашифрованных текстовых документов с Unix-системами и их форматом возврата каретки (переносом строк). Не отмечайте опцию, если получатель файла не работает на Unix / Linux / Mac и исходный файл не содержит обычный текст;
- Wipe Original (Стирание оригинала). При выборе данной опции при шифровании будет затираться первоначальный документ, теперь никто, у кого есть доступ к жесткому диску компьютера, не сможет открыть данный файл;
- Conventional Encrypt (стандартное шифрование). При включении этой функцию пользователь полагается на общую кодовую фразу, а не на шифр открытого ключа. Файл шифруется с помощью сеансового ключа, который кодирует файл с использованием новой фразы.

Здесь же имеется дополнительная опция «Self Decrypting Archive - SDA» – саморасшифровывающийся архив. Название этой опции говорит само за себя. Здесь по аналогии с предыдущей функцией используется стандартное шифрование. При этом создается архив с расширением «.sda.exe». Данная функция очень похожа на создание «SFX» архивов при архивировании обычными архиваторами, такими как «RAR». В результате, выполняемый файл может быть расшифрован простым двойным нажатием мышки на данный файл и вводом кодовой фразы. Данная функция рассчитана на отправку пользователям, у которых нет программы PGP, что делает использование данного продукта более мобильными и широким в использовании. При использовании данного архива пользователь, отправляющий письмо, и тот который его получит, должны использовать одинаковую операционную систему.

Образованный в результате криптографического преобразования файл может быть отправлен по открытым каналам связи. При использовании различным опций создаются файл с различными иконками, что позволяет определить, какой из функций вы воспользовались (рис. 2.19).

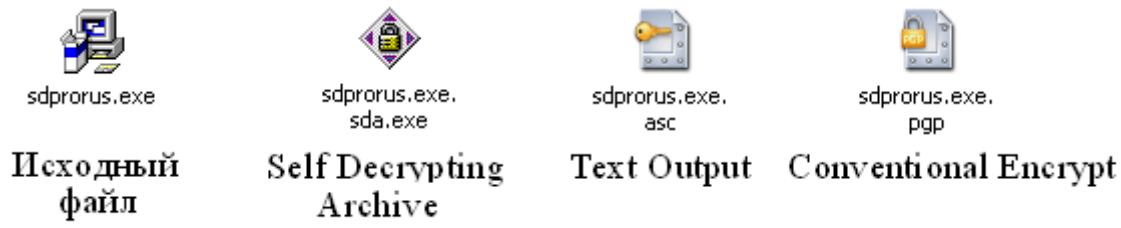


Рис. 2.19. Результаты криптографического преобразования

При шифровании папки, шифрование проходит над каждым файлом, находящимся в ней, по отдельности. Если имеются вложенные папки, программы PGP обрабатывает и их аналогичным способом.

Однако не всегда возникает необходимость полного шифрования данных. Часто отправитель и получатель не хотят скрывать информацию от других пользователей, но желают, чтобы никто эту информацию не мог модифициро-

вать. Для этого и используется функция генерации электронно-цифровой подписи «Sign», которая добавляет в исходный каталог цифровую подпись, полученную с помощью наложения хэш-функции на исходный файл и зашифрования полученного хэш-кода открытым ключом отправителя.

При выборе функции «Sign», в окне «Enter Passphrase» появится 3 опции: «Detached Signature», «Text Output» и «Input is Text». Последние две уже были описаны выше. А опция «Detached Signature» в переводе с английского обозначает изготовить «съёмную» цифровую подпись. Если опция включена (а она включена по умолчанию), цифровая подпись будет сохранена в виде отдельного крохотного файла, имеющего такое же имя, что и у подписанного файла, но с расширением «.sig» (рис. 2.20). Такой файл-подпись можно передавать и публиковать отдельно от подписанного, дабы не осложнять использование подписанного файла людям, не пользующимся PGP.

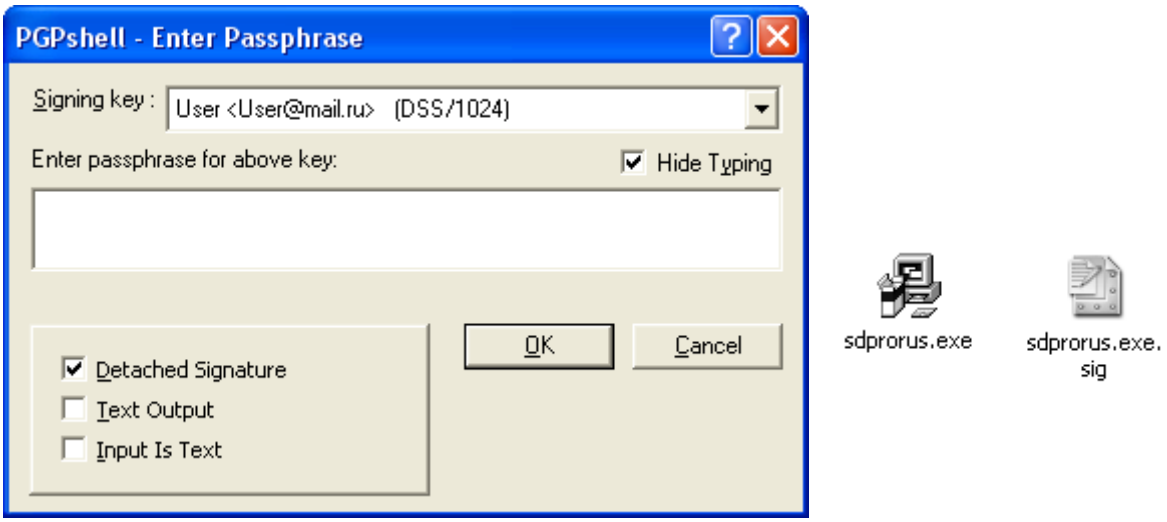


Рис. 2.20. Формирование электронной цифровой подписи

Если опцию «Detached Signature» выключить, файл будет сохранён, как при обычном шифровании, и использовать его без сверки ЭЦП будет невозможно. В том случае, если отправитель зашифровывает файл и подписывает его, то ЭЦП автоматически будет внесена в файл, а отдельный файл - подпись с расширением «*.sig» не имеется.

ВЫПОЛНИТЬ!

7. Создать в каталоге «*Служебные документы-i*» три текстовых документов с легко узнаваемыми именами. Помесить в документы произвольную различную текстовую информацию.
8. Зашифровать одни из файлов открытым ключом одного из потенциальных получателей.
9. Зашифровать и подписать второй файл.
10. Сформировать для третьего файла электронную цифровую подпись.

11. Поместить первый и второй зашифрованные файлы, незашифрованный третий файл и ЭЦП для него в доступный для всех каталог «*Доска объявлений*».

На стороне получателя зашифрованные файлы должны быть помещены в недоступный для остальных пользователей каталог, например, «*Служебные документы-j»*, в котором будут подвергаться операции расшифровывания. Чтобы расшифровать документ необходимо на его ярлыке щелкнуть правой клавишей мыши, при этом во всплывающем контекстном меню кроме строк, стандартных для ОС Windows появятся еще две строки: «Decrypt» – расшифровать и Decrypt/Verify – расшифровать и верифицировать (проверить подлинность) документа. Для расшифрования полученных по сети файлов достаточно просто дважды кликнуть мышкой по пиктограмме данного файла. Расшифровка данных при этом осуществляется буквально в одно действие. В случае если файл был зашифрован обычным способом, без использования функции «Conventional Encrypt», то программа выдаст окно, где определит, каким ключом был зашифрован файл и предложит ввести свою (получателя) ключевую фразу, что эквивалентно введению закрытого ключа получателя.

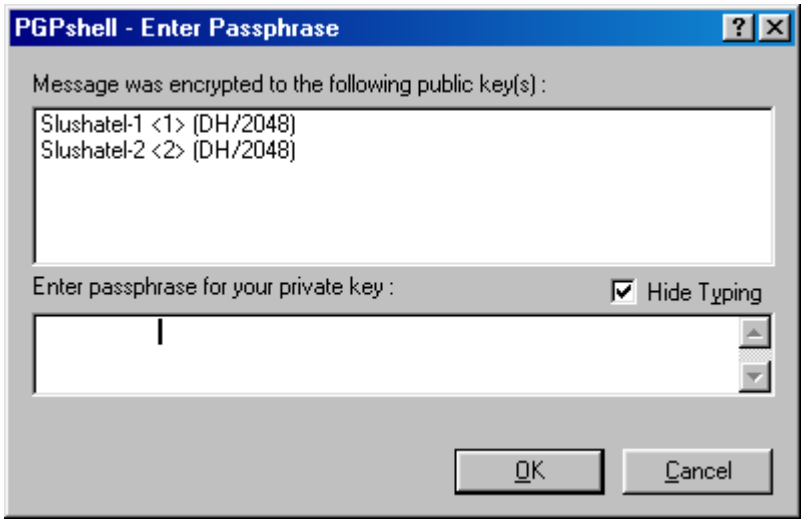


Рис. 2.21. Окно для ввода пароля при расшифровании и верификации файлов

В противном случае, если файл был зашифрован с использованием функции «Conventional Encrypt», будет выдано окно для ввода также секретной фразы, но без указания шифра, т.к. файл был зашифрован сеансовым (симметричным) ключом.

Для верификации незашифрованного файла, переданного по каналам связи совместно с ЭЦП, достаточно дважды щелкнуть мышкой по пиктограмме ЭЦП, система PGP при этом также потребует от получателя ввести свой секретный пароль. При успешной верификации (если информация в процессе передачи не была подвергнута изменениям) появится окно, информирующее получателя, от кого было получено истинное (немодифицированное) сообщение.

ВЫПОЛНИТЬ!

12. Штатным образом расшифровать файлы, помещенные партнером по защищенному обмену информацией в каталог «*Доска объявлений*». Убедиться в истинности подписанных документов.
13. Повторить верификацию подписанных файлов, при этом ввести неверный пароль. Что произошло?
14. Изменить один символ в незашифрованном файле, помещенном в каталог «*Доска объявлений*» совместно с ЭЦП. Произвести попытку верификации. Как отреагировала на модификацию информации система PGP?

В составе системы PGP имеется замечательная утилита PGPdisk – легкая в освоении и использовании программа для создания виртуальных логических защищенных дисков. Утилита создает защищенный файл - образ, который операционная система «видит» как новый виртуальный логический диск. Его можно подключать и отключать, форматировать и производить любые действия, возможные для логических дисков. Однако, авторы пособия предлагают познакомиться с технологией виртуальных логических дисков на примере популярного универсального отечественного СЗИ криптографического действия «StrongDisk».

2.3. Система защиты конфиденциальной информации «StrongDisk»

2.3.1. Основные характеристики системы «StrongDisk»

Аппаратно-программное средство защиты информации «StrongDisk» разработано ООО «Физтех-Софт» (г. Санкт-Петербург) и предназначено для создания на дисковом пространстве локальной рабочей станции («StrongDisk Pro») и сервера («StrongDisk Server») защищенных дисков с ограниченным (многопользовательским) доступом. Защищенный диск представляет собой специально созданный файл (образ диска), в котором хранятся зашифрованные данные. Драйвер, входящий в состав «StrongDisk», позволяет ОС Windows 9x/NT 5.0 (и пользователю) работать с этим файлом как с отдельным логическим диском, таким как CD-ROM, Zip-накопитель и т. д. При создании нового виртуального диска ему присваивается буквенное обозначение (*Z*, *Y*, *X*). Криптографическое преобразование данных при записи на диск осуществляется с помощью одного из встроенных стандартных симметричных алгоритмов шифрования: 3DES, CAST-128, SAFER, Blowfish.

При считывании данных осуществляется расшифрование «на лету». Симметричный ключ шифрования может инициализироваться путем логического сложения (по схеме «И») парольной информации, файл-ключа и электронного ключа (при наличии соответствующей аппаратной поддержки).

В состав системы «StrongDisk» входят также дополнительные утилиты, предотвращающие утечку конфиденциальной информации, связанную с несовершенством операционных систем. Утилиты позволяют:

- безопасно удалять «ненужные» файлы, в которых может храниться остаточная конфиденциальная информация;
- организовывать на защищенном диске каталог «TEMP» для хранения временных файлов;
- после окончания сеанса работы в ОС Windows затирать файл подкачки (win386.swp или pagefile.sys).

Версия, исследуемая в настоящем пособии, является бесплатной DEMO-версией «StrongDisk Pro» 2.8.5, работающей в ОС Windows 9x/2000 и имеющей единственное ограничение (по сравнению с рабочей) на максимальный размер (3 Мб) создаваемых виртуальных дисков.

2.3.2. Терминология СКЗИ «StrongDisk»

1. *Защищенный диск* — обыкновенный файл (файл-образ диска), который может быть размещен на любых логических дисках, доступных ОС Windows. В этом файле информация хранится в зашифрованном виде. «StrongDisk» позволяет на защищенном диске создавать каталоги и файлы, сканировать, проводить дефрагментацию, форматирование и т. д.
2. *Резиновый диск* — защищенный диск, размер которого увеличивается по мере пополнения его данными. На резиновом диске отсутствует свободное место.

3. *Внешний ключ* — объект, в котором хранится ключевая информация. Это может быть файл-ключ или электронный ключ (физический носитель ключевой информации).
4. *Код внешнего ключа* — код, который генерируется случайным образом при инициализации ключа и хранится непосредственно в этом ключе. Этот код вместе с паролем используется для криптографического преобразования информации.
5. *Электронный ключ* — внешнее устройство с записанным внутри кодом. В «StrongDisk» могут использоваться специальные USB-ключи (iKey) или миниатюрные ключи iButton Dallas. В случае использования ключей iButton к COM-порту компьютера подключается аппаратный считыватель кодов.
6. *Файл-ключ* — обыкновенный небольшой файл текстового формата, в котором, как в электронном ключе, хранится кодовая информация. Этот файл находится на сменном носителе и при работе с защищенным диском помещается в соответствующий накопитель.
7. *Пароль пользователя* — обычный пароль, который задается пользователем при создании защищенного диска.
8. *Полный пароль* — совокупность кодовой информации, хранимой во внешних ключах, и обычного пароля.
9. *Постоянный диск* — защищенный диск, который может автоматически подключаться при загрузке «StrongDisk».
10. *Главное окно* — основное окно меню «StrongDisk», используемое при работе с защищенными дисками.

2.3.3. Инициализация системы «StrongDisk»

Для инициализации системы «StrongDisk Pro» 2.8.5 необходимо закрыть все работающие приложения Windows и запустить на исполнение файл Sdprorus, который откроет окно диалоговой установки средства защиты.

На запрос установщика о лицензионном соглашении необходимо ответить «согласен». Далее следует выбрать каталог для установки системных файлов «StrongDisk». По умолчанию это — «C:\Program Files\StrongDisk». Драйверы внешних электронных ключей iButton и iKey (рис. 2.22) не требуют наличия самих устройств считывания ключей и занимают мало места на дисковом пространстве. Поэтому в процессе инициализации системы их целесообразно установить.

Далее следует подтвердить команду полной установки «StrongDisk» и по соответствующему запросу перезагрузить компьютер. Признаками успешной установки (наличия на ПЭВМ) системы «StrongDisk» являются возникновение на рабочем столе компьютера ярлыка «горящей корзины» для безопасного удаления файлов, строчки «Уничтожить» во всплывающем меню файлов и значка «StrongDisk» на панели задач (рис. 2.23). При выполнении задания следует убедиться в наличии всех указанных признаков. Нажатие на клавишу ζ приводит к появлению на рабочем столе ПЭВМ главного окна системы «StrongDisk» (рис. 2.24). При первом вызове программы появляется окно регистрации систе-

мы. Для нормальной работы бесплатной версии достаточно нажать на клавише «ОК» окна регистрации.

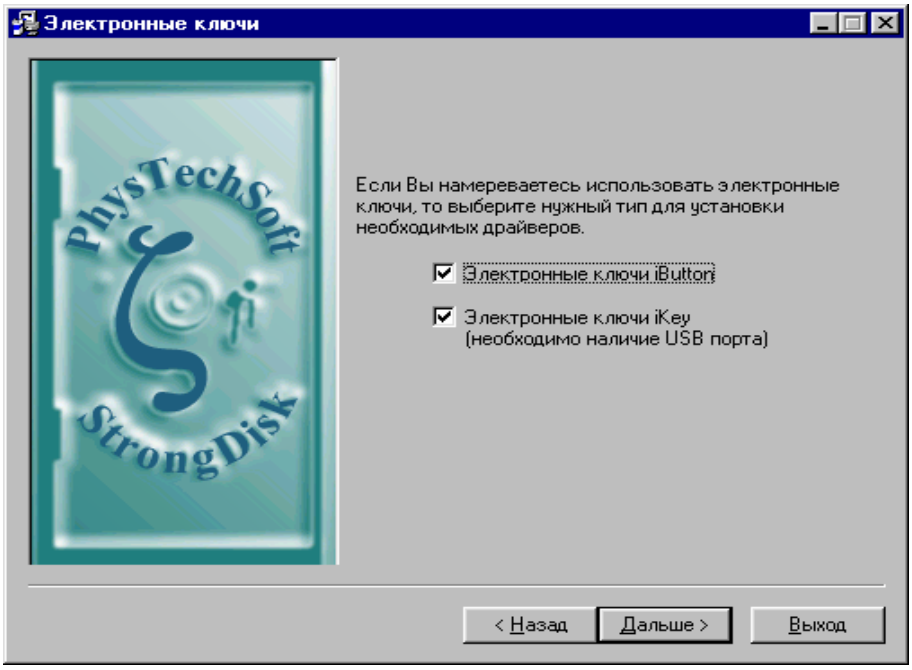


Рис. 2.22. Диалоговое окно установки «StrongDisk»

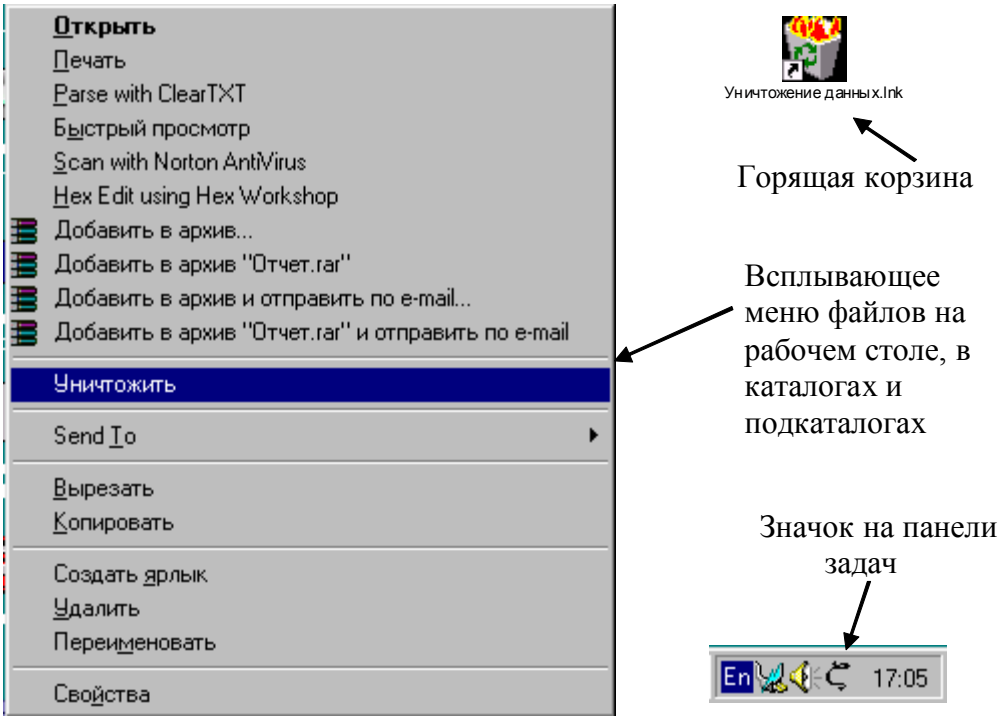


Рис. 2.23. Признаки наличия на ПЭВМ СЗИ «StrongDisk»

При необходимости ярлык «горящей корзины» и значок на панели задач могут быть удалены, тогда вызов системы можно осуществлять стандартными возможностями ОС Windows: ***Пуск*** ⇒ ***Программы*** ⇒ ***PhysTechSoft*** ⇒ ***StrongDisk***.

2.3.4. Создание защищенных логических дисков

Инициализация «StrongDisk» не предполагает автоматического создания защищенных логических дисков. Каждый пользователь рабочей станции может создать один или несколько защищенных дисков. При создании нового диска задается индивидуальная парольная информация, которая используется для генерации ключа шифрования.

Создание нового логического диска удобно производить из главного окна «StrongDisk» (рис. 2.24). Для этого необходимо выбрать пункт подменю «Создать», на рабочем столе появится диалоговое окно создания диска.

В первую очередь, необходимо назначить имя создаваемого файла-образа и определить ему каталог (подкаталог) размещения (рис. 2.25). Для сокрытия факта установки «StrongDisk» на ПЭВМ не следует использовать название файла и каталог назначения, предлагаемые системой по умолчанию (C:\Image4.grd). При создании образов дисков им можно назначить собственное имя, изменить по своему усмотрению каталог назначения и задать любое расширение (txt, doc, dll). При этом операционная система будет отображать файл-образ как текстовый документ, документ Word и т. д. В следующем окне необходимо определить размер и файловую систему защищенного диска (рис. 2.26).

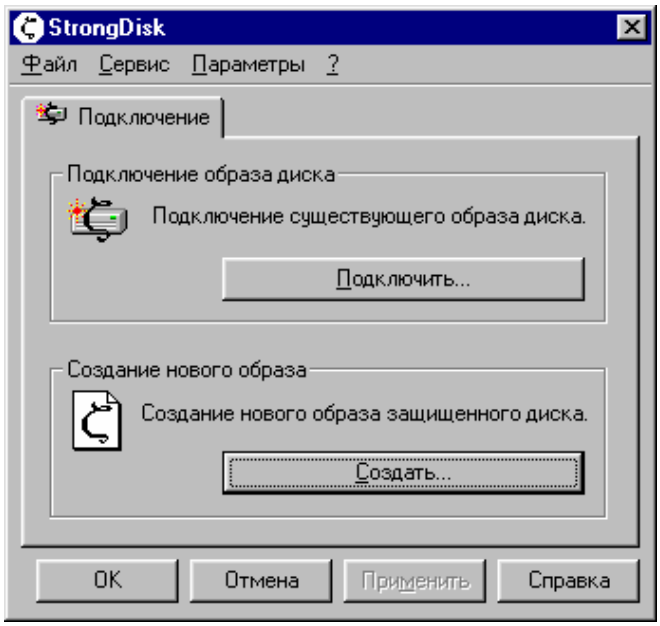


Рис. 2.24. Главное окно СЗИ «StrongDisk»

Для удобства пользователя в окне приводится размер свободной области в каталоге назначения. Создаваемый файл-образ может быть «резиновым», совпадающим по размеру с совокупным размером размещаемых на нем файлов. Свободное место диска постоянного размера может заполняться случайными данными. Для резинового диска эта опция не имеет смысла и не активна.

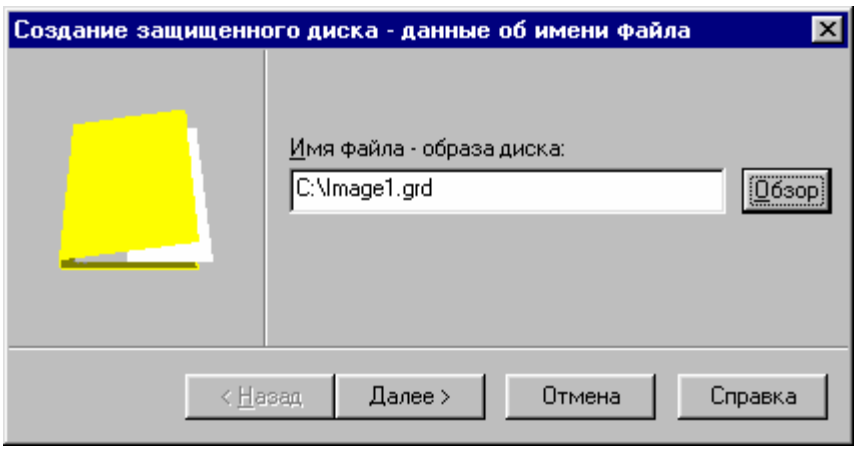


Рис. 2.25. Данные об имени создаваемого диска

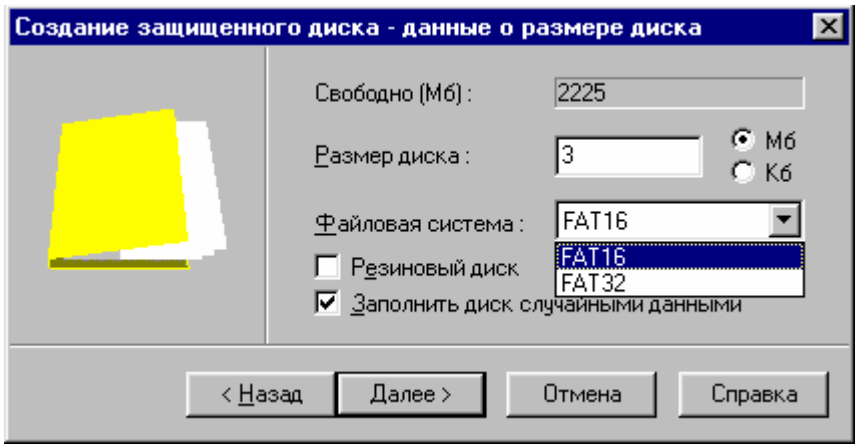


Рис. 2.26. Данные о размере создаваемого диска

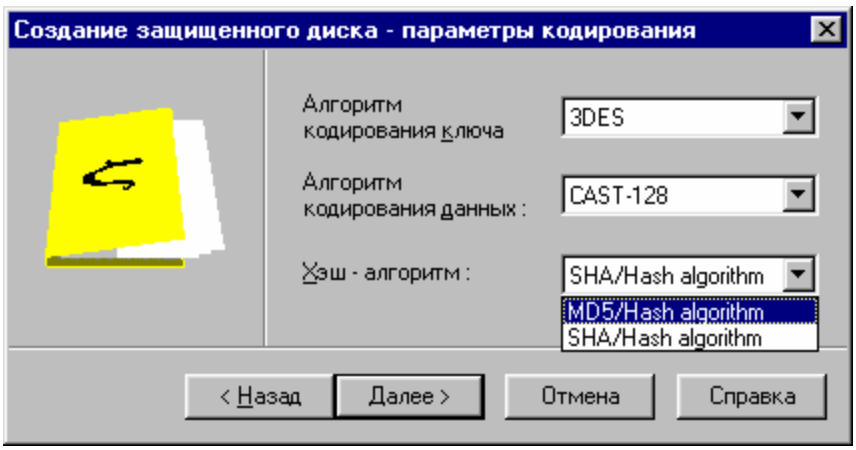


Рис. 2.27. Определение алгоритмов шифрования

Далее следует определить алгоритмы шифрования данных и ключа (рис. 2.27). Файл-образ диска состоит из двух частей: заголовка и непосредственно данных. В заголовке, помимо служебной информации, хранится специальная последовательность байт, которая используется системой в качестве ключа кодирования данных. Сама эта последовательность хранится в закодированном виде.

Шифрование данных в «StrongDisk» происходит по схеме, приведенной на рис. 2.1. Данные, размещаемые пользователем в виртуальном диске, шиф-

руются быстрым алгоритмом с использованием уникального ключа. Ключ кодирования данных генерируется «StrongDisk» при создании каждого нового виртуального диска и хранится в файле-образе в зашифрованном виде. Ключ кодирования ключа формируется каждый раз при подключении виртуального диска на основе вводимой пользователем информации с применением стойкого медленного алгоритма. Совокупность обычного пароля, информации, содержащейся в файле-ключе, и кода, записанного во внешнем электронном носителе, подвергается операции хеширования. Хэш-функция используется в качестве ключа для расшифровывания ключа кодирования данных. Разработчики «StrongDisk» рекомендуют выбирать криптографические алгоритмы, предлагаемые системой по умолчанию.

В диалоговом окне «данные о пароле» (рис. 2.28) следует установить переключатели «обычный пароль», «файл-ключ» и «электронный ключ» в соответствии с желаемой степенью защиты виртуального диска. Рекомендуется использовать все три составляющие парольной информации. Если по какой-либо причине применение внешнего электронного ключа недоступно, можно ограничиться защитой диска паролем и файлом-ключом. В крайнем случае, когда информация не имеет большой ценности или для защиты информации предусмотрены дополнительные меры (охранная сигнализация и т. д.), можно обойтись только обычным паролем. «StrongDisk» позволяет использовать для защиты файлов-образов только файлы-ключи или только внешние носители, однако применение обычного пароля целесообразно во всех случаях. В процессе работы с виртуальными дисками степень их защищенности можно менять. При создании файлов-образов дисков во время выполнения практического задания следует выбрать только обычный пароль, поскольку файлы-ключи еще не созданы, а внешних носителей в распоряжении слушателей не имеется.

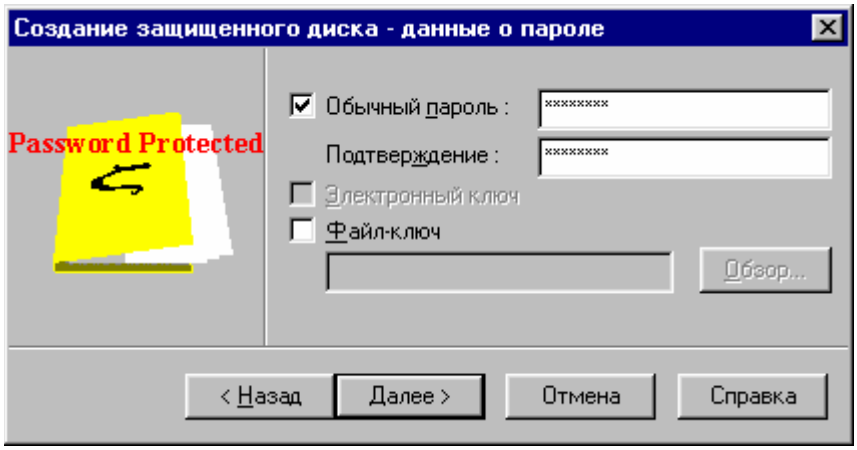


Рис. 2.28. Данные о способе защиты диска

Ответственность за надежность выбранного пароля в «StrongDisk» несет пользователь. Система накладывает ограничение только на длину парольной последовательности (не менее 8 символов). Если пароль не будет удовлетворять этому условию, система «не примет» его и выдаст соответствующее предупре-

ждение. Пароль в «StrongDisk» вводится дважды и без визуализации символов на экране дисплея.

На данном этапе все параметры создаваемого диска оказываются назначенными, и система предлагает подтвердить их в окне «свойства нового диска», рис. 2.29. Необходимо внимательно просмотреть это окно. Если все параметры введены правильно, следует нажать кнопку «Создать», и новый защищенный диск будет создан. Если какой-либо параметр не устраивает пользователя, можно вернуться в предыдущие окна с помощью кнопки «Назад».

Внимание! Пароль нигде не хранится. Если пользователь забудет пароль или потеряет внешний ключ, не сделав его копию, то доступ к данным будет невозможен.

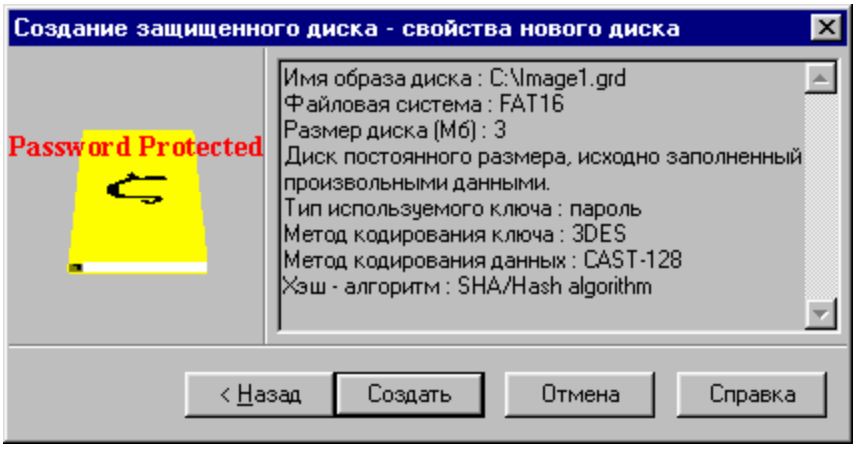


Рис. 2.29. Основные параметры создаваемого диска

После того, как очередной диск оказывается созданным, система «StrongDisk» предупреждает пользователя о необходимости делать резервную копию заголовка диска и резервную копию всего файла-образа после каждого важного дополнения или изменения его содержимого (рис. 2.30).

В заголовке диска хранится служебная информация о способе защиты, об используемых внешних ключах, закодированный ключ шифрования данных. Разрушение заголовка может произойти по независящим от пользователя причинам, в т. ч. когда «StrongDisk» не активен. Например, в результате ошибочных действий пользователя, сбоев операционной системы или системы электропитания может быть испорчена файловая система, произойти физическое повреждение диска. Если в небольшую часть логического диска, которая окажется испорченной, попадет заголовок файла-образа, то вся остальная неповрежденная часть информации будет недоступной. При восстановлении заголовка система считывает его из специального файла с резервной копией и записывает поверх имеющегося заголовка файла-образа.

Полное резервное копирование файла-образа не лишает смысла операцию сохранения заголовка. Данные на защищенном диске постоянно обновляются, и при возврате к резервной копии последние изменения безвозвратно теряются. Восстановление непосредственно заголовка, который меняется только при сме-

не способа защиты виртуального диска, дает шанс полностью или частично восстановить изменения, внесенные после последнего копирования файла-образа. Порядок создания резервных копий заголовка и файла-образа будет рассмотрен ниже.

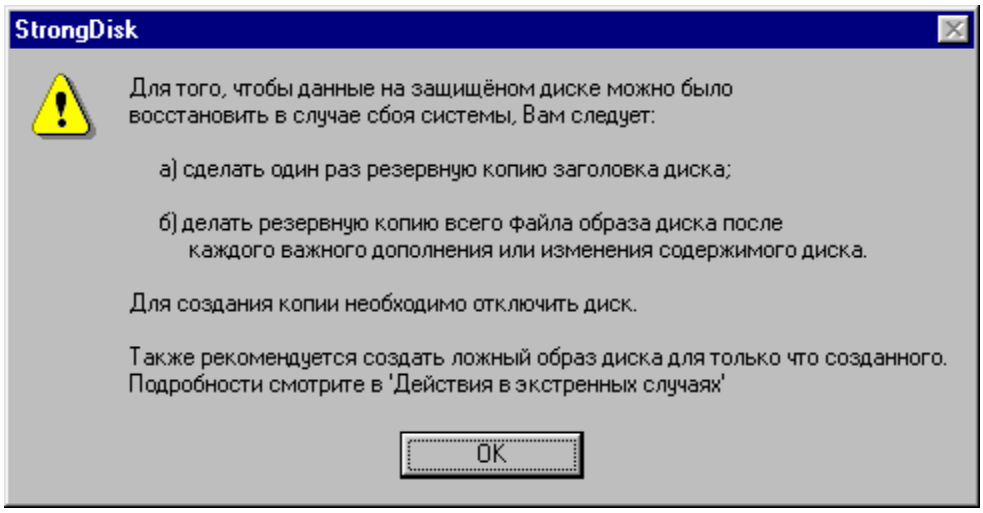


Рис. 2.30. Предупреждение «StrongDisk» о необходимости резервного копирования

При создании защищенного диска на нем автоматически создается каталог «Startup». В него могут помещаться ярлыки (а не сами исполняемые файлы) приложений и документов, которые будут автоматически загружаться при подключении диска.

ВЫПОЛНИТЬ!

15. Создать в корневом каталоге диска «C:\» три защищенных диска, вызывая диалоговое окно нажатием кнопки «Создать» в главном меню системы. Файлу-образу четвертого диска задать имя, отличающееся от предлагаемого системой по умолчанию, указать каталог назначения диск «A:\». Создать на диске простой текстовый документ и документ Word, отключить диск, просмотреть его содержимое всеми доступными средствами, включая утилиту «Disk Editor».

Вновь созданные виртуальные диски автоматически оказываются подключенными. Главное окно «StrongDisk» при последовательном создании трех виртуальных дисков будет выглядеть, как это показано на рис. 2.31. Изменение параметров любого созданного диска, их подключение/отключение осуществляется в главном окне системы. Для отключения файла-образа необходимо выбрать закладку с именем требуемого диска и нажать клавишу «Отключить» (рис. 2.32). При подключении (отключении) виртуальных дисков соответствующий ярлык появляется (исчезает) в системном окне «Мой компьютер» (рис. 2.33). В проводнике они становятся доступны (не доступны) всем приложениям.

Для подключения неактивизированного файла-образа необходимо нажать клавишу «Подключить», в окне «Обзор» выбрать требуемый образ, в окне «Подключение диска» (рис. 2.34) указать способы защиты диска (обычный пароль, электронный ключ или файл-ключ), указать параметры подключения, желаемое имя диска, нажать клавишу «Подключить». При подключении дисков важен порядок ввода ключевой информации. Первым должен загружаться файл-ключ (если таковой имеется), затем следует вводить пароль.

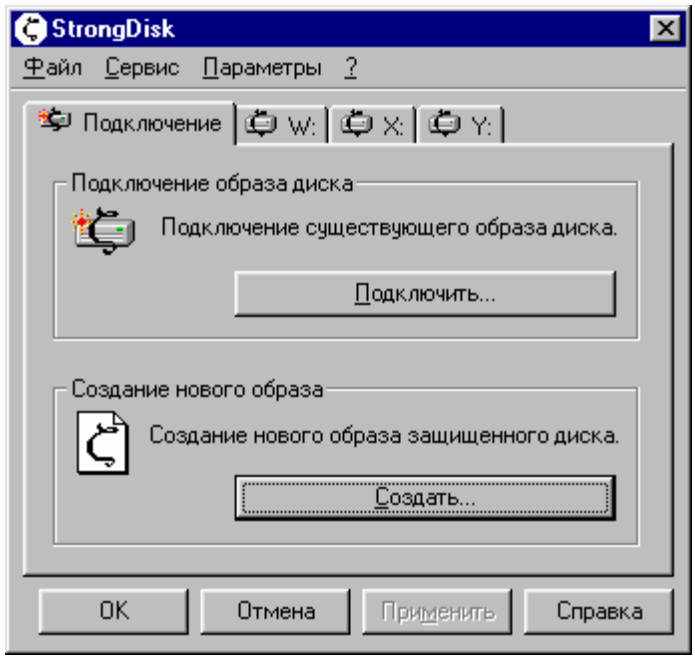


Рис. 2.31. Главное окно «StrongDisk» с подключенными защищенными дисками

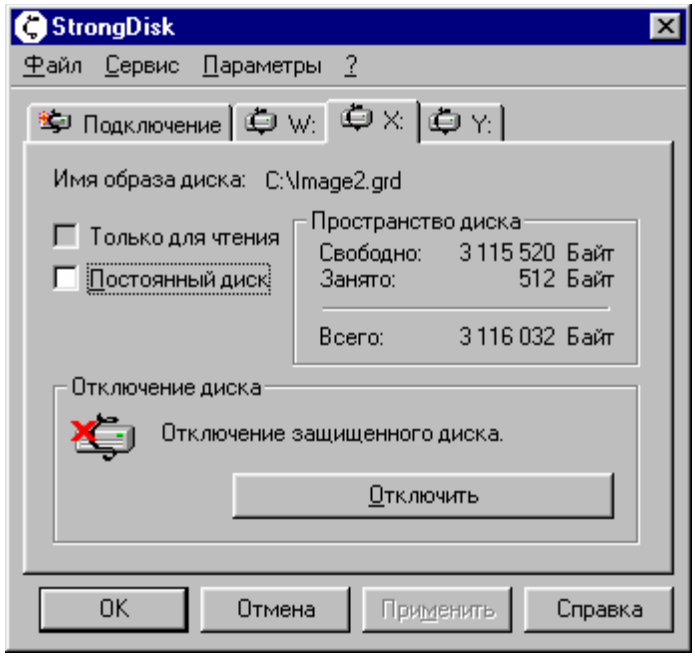


Рис. 2.32. Отключение виртуальных дисков

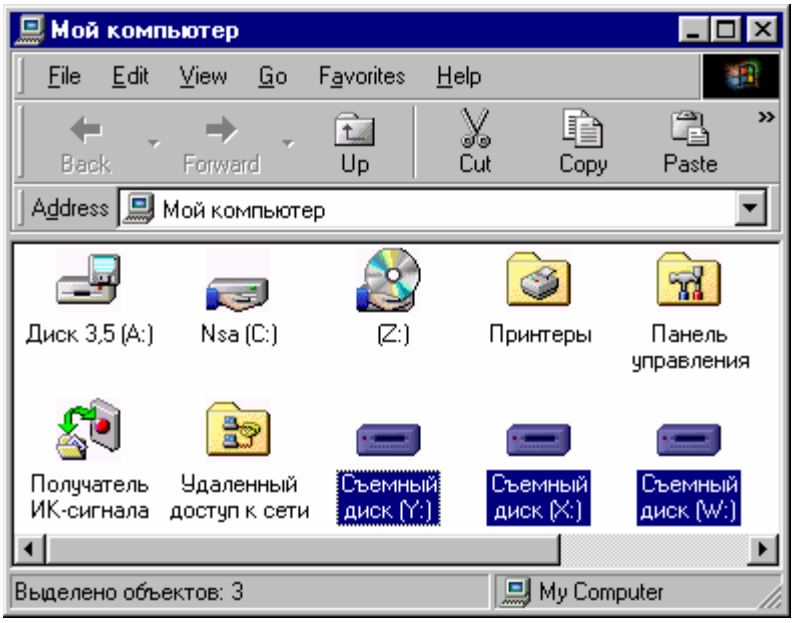


Рис. 2.33. Появление логических виртуальных дисков в системном окне «Мой компьютер»

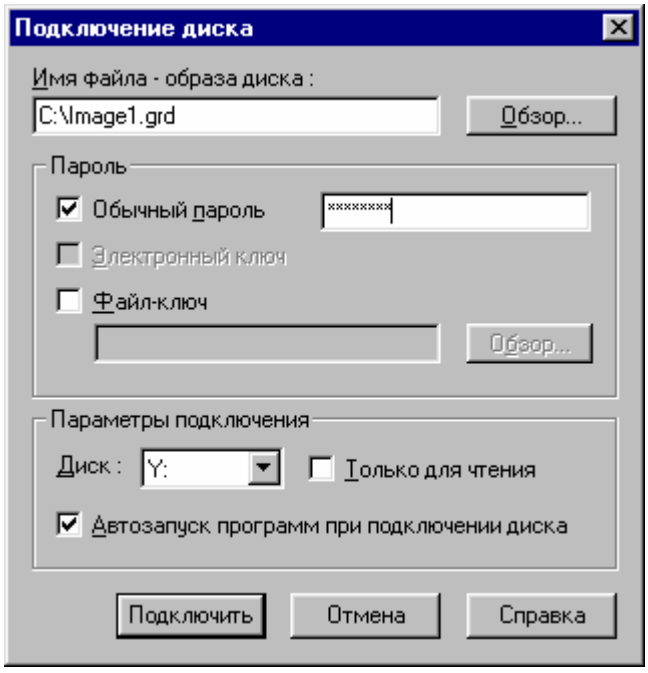


Рис. 2.34. Окно «Подключение диска»

ВЫПОЛНИТЬ!

16. Последовательно отключить (подключить) все созданные файлы и убедиться в отсутствии (наличии) ярлыков виртуальных дисков в окне «Мой компьютер». Для файла-образа «C:\Image2.grd» назначить новое имя виртуального диска «S», на закладке подключенного диска (рис. 2.32) присвоить ему статус постоянно подключаемого. В папки Startup файлов-образов «C:\Image1.grd» и «C:\Image3.grd» поместить ярлык Microsoft Word и создать на защищенных дисках документы в формате Microsoft Word. Убедиться в автоматической загрузке редактора при подключении дисков.

2.3.5. Настройка параметров системы «StrongDisk»

Для настройки параметров системы необходимо выбрать закладку «Параметры» в главном окне. Настройка «StrongDisk» осуществляется в пяти закладках (рис. 2.35): Общие, Внешние ключи, Безопасность, Экстренное отключение, Форс-мажор.

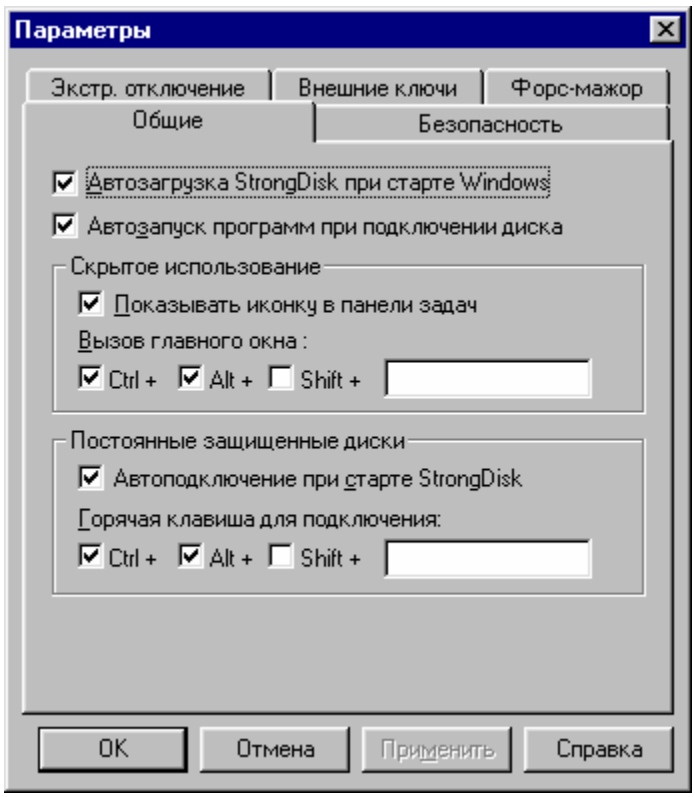


Рис. 2.35. Установка общих параметров

В закладке «Общие» указываются параметры автозагрузки, автоматического подключения дисков и назначаются «горячие» клавиши. При установке в этой закладке всех параметров «по умолчанию»:

- система «StrongDisk» загружается автоматически при старте операционной системы;
- при загрузке «StrongDisk» автоматически подключаются виртуальные диски, имеющие статус постоянных;
- при активизации подключенных дисков автоматически стартуют приложения и исполняемые файлы, ярлыки которых помещены в папку «Startup» соответствующего диска;
- иконка «StrongDisk» помещается на панели задач;
- «горячие» клавиши не назначаются.

При выполнении задания следует настроить «StrongDisk» для скрытного использования, для чего необходимо выключить переключатель «Показывать иконку на панели задач» и назначить «горячие» клавиши для вызова главного окна системы.

В закладке «Внешние ключи» необходимо выбрать тип ключа, который будет использоваться при подключении дисков. Если внешнего электронного ключа нет, то выбирается пункт «Ключ отсутствует». Состояния «Обычный пароль», «Электронный ключ» и «Файл-ключ», установленные по умолчанию, будут находиться изначально в диалогах «Подключение диска» и «Создание диска».

«StrongDisk» позволяет предотвратить утечку информации через временные файлы, создаваемые приложениями. Для этого необходимо на закладке «Безопасность» установить во включенное состояние переключатель «Защищенный TEMP на диске». Временный каталог может размещаться на любом подключаемом вручную виртуальном диске «Имеющийся диск» или на диске, который будет автоматически создаваться при каждом запуске системы. В последнем случае на соответствующих полях следует указать размер и параметры временного файла-образа.

На закладке «Безопасность» может быть активизирована дополнительная защитная функция «StrongDisk» — затирание файла подкачки. При этом конфиденциальная информация, которая может оказаться в файле подкачки Windows и быть восстановлена злоумышленником, например, содержимое редактируемого текстового документа, будет автоматически затираться при завершении работы системы.

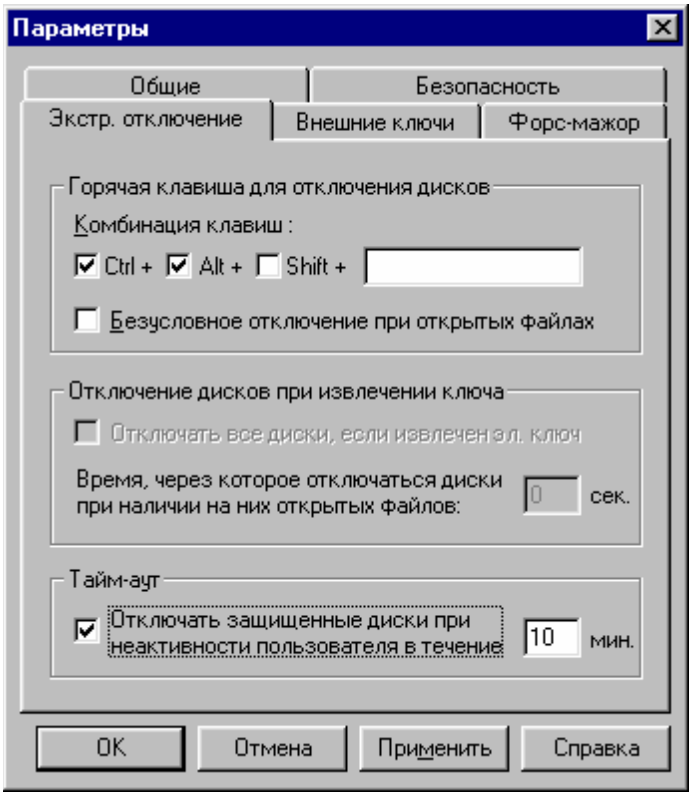


Рис. 2.36. Установка параметров экстренного отключения защищенных дисков

На закладке «Экстренное отключение» (рис. 2.36) можно назначить «горячие» клавиши, при нажатии которых происходит немедленное отключение всех подключенных дисков, если переключатель «Безусловное отключение при

открытых файлах» находится во включенном состоянии. В противном случае по команде экстренного отключения «StrongDisk» предложит сохранить документы и закрыть работающие на защищенных дисках приложения.

Внимание! Если диск, на котором располагается каталог TEMP, не будет подключен до запуска приложений, то приложения могут не запуститься или работать некорректно.

Установка переключателя «Отключать защищенные диски при неактивности пользователя» во включенное положение приведет к тому, что все подключенные диски будут отключены при отсутствии пользователя на рабочем месте по истечении указанного на закладке времени. «StrongDisk» позволяет отключать диски при извлечении электронного ключа из считывателя через определенное время. При отсутствии внешнего ключа эта опция не активна.

ВЫПОЛНИТЬ!

17. Назначить размещение каталога «TEMP» в файле-образе «C:\SDTemp.grd». На закладке «Безопасность» установить переключатель «Очищать файл подкачки при завершении работы» во включенное состояние. Для проверки затирания файла подкачки перезагрузить компьютер в режиме MS-DOS. При завершении работы Windows убедиться в появлении соответствующего сообщения. Переименовать файл win386.swp и просмотреть всеми доступными средствами. При повторном запуске Windows проконтролировать создание файла-образа для размещения каталога «TEMP» с указанными ранее параметрами.
18. Назначить «горячие клавиши» для безусловного экстренного выключения дисков. Подключить файл-образ с именем «C:\Image3.grd», открыть для редактирования имеющийся на нем текстовый документ, внести в документ изменения и произвести экстренное отключение дисков. Вновь подключить диск и просмотреть редактируемый документ. Повторить эти действия при отключенной опции «Безусловное отключение при открытых файлах».
19. Установить минимально допустимое время неактивности пользователя, подключить диск, открыть документ для редактирования и проконтролировать отключение защищенных дисков по истечении этого времени.

Особое место в «StrongDisk» занимают параметры закладки «Форс-мажор», с помощью которых можно противодействовать злоумышленникам при входе в систему по принуждению (рис. 2.37).

С помощью этой закладки активизируются специальные дополнительные функции — работа с ложными дисками. Ложные диски могут подключаться и имитировать настоящие в экстренных случаях, например, при работе под контролем злоумышленника, или при физическом принуждении легальных пользователей выдать пароль доступа к защищенным файлам-образам. Ложные диски создаются при включенном переключателе «Разрешить подключение ложных дисков» в любых указанных на закладке каталогах (подкаталогах в глубине

файловой структуры логического диска пользователя), в которых ложные образы непросто обнаружить. Они имеют совпадающие с истинными дисками имена и подключаются по своему индивидуальному паролю. При нажатии кнопки «Обзор» в закладке «Подключить» в окне обзора появится одно общее для истинного и ложного дисков имя файла-образа. В зависимости от того, какой пароль выберет пользователь, будет подключен тот или иной диск. Пароли ложного и истинного дисков могут отличаться на один символ и иметь одинаковые файлы-ключи и внешние идентификаторы. Естественно, что в реальных условиях на ложных дисках должна быть размещена правдоподобная информация.

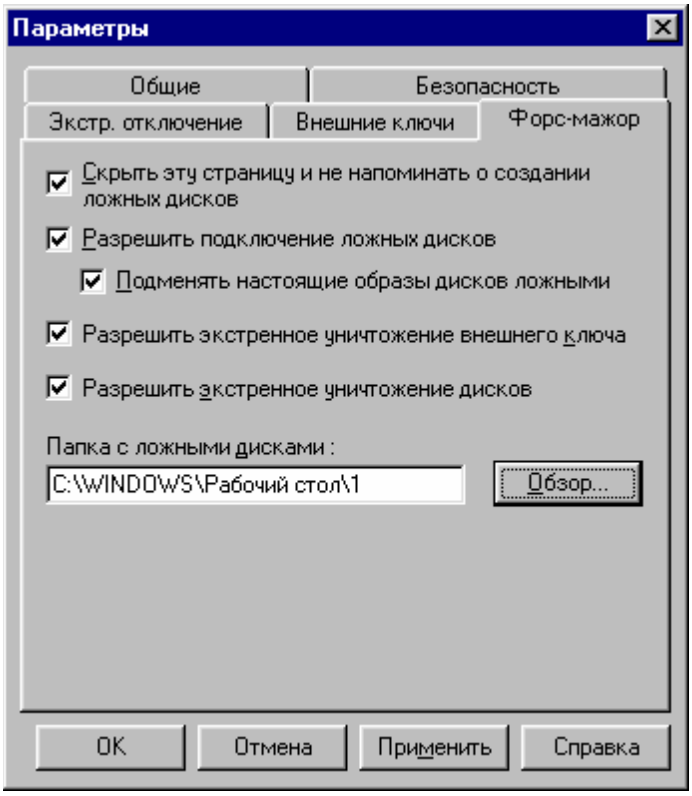


Рис. 2.37. Вкладка специальных форс-мажорных функций «StrongDisk»

«StrongDisk» позволяет подменять настоящие образы дисков ложными. Если соответствующий переключатель установлен, то по вводу ложного пароля (ключа) перед тем, как подключить ложный диск, система поменяет местами файлы-образы ложного и настоящего дисков. Недоброжелатель, решивший после подключения диска забрать файл-образ диска с собой для дальнейшего изучения, забирает уже не настоящий диск, а ложный. Причем он будет его успешно подключать с ложным паролем (ключом) и на любом другом компьютере с установленной системой «StrongDisk». В то же время файл-образ настоящего диска останется на легальном компьютере в папке с ложными дисками. После того как опасность миновала, следует подключить диск с истинным паролем, и файлы-образы установятся на свои места. Папка с ложными дисками может быть не одна. В каждой из них могут быть созданы ложные файлы-образы для всех истинных, но активна будет та папка, которая указана на закладке.

Если переключатель «Разрешить экстренное уничтожение внешнего ключа» установлен, то при возникновении форс-мажорных ситуаций модификации подвергается внешний ключ истинного диска, сам диск не уничтожается. При вводе специального пароля «на уничтожение» ложный диск будет перемещен на место настоящего и подключен. Настоящий диск будет перемещен в папку с ложными дисками. Внешний ключ будет переинициализирован случайным образом и совместно с введенным паролем «на уничтожение» будет назначен в качестве новых значений для подключения ложного диска. По внешним признакам злоумышленник не фиксирует уничтожение (подмену) внешнего ключа и факт подключения ложного диска. Все последующие подключения диска недоброжелатель будет осуществлять с помощью того же внешнего ключа и пароля, с которыми подключал диск в первый раз. При этом будет успешно подключаться ложный диск. Активизировать настоящий диск ему все равно не удастся, т. к. соответствующий ему внешний ключ был уничтожен.

Пароль «на уничтожение» — это пароль к ложному диску, дополненный любыми тремя символами. Это верно и в случае, когда совместно с паролем используется внешний ключ. Если ложный диск был создан только с помощью внешнего ключа без пароля, то ввод пароля на уничтожение будет невозможен.

При переинициализации внешнего ключа часть пароля, хранившаяся в нем, будет затерта. Подключение с помощью этого внешнего ключа дисков, для доступа к которым он использовался, будет невозможно. Если вышеописанная функция «StrongDisk» используется, то внешний ключ должен иметь резервную копию. Копия должна хранится в таком месте, где ее не смогут обнаружить. Лучше всего, если об этом месте и вообще о существовании копии не знает никто, включая близких людей.

Если установлен переключатель «Разрешить экстренное уничтожение дисков», то при вводе пароля «на уничтожение» ложный диск будет перемещен на место настоящего и подключен, а настоящий диск будет уничтожен. При отсутствии копии образа-файла истинного диска все данные будут утрачены безвозвратно.

После установки желаемых форс-мажорных функций рекомендуется установить переключатель «Скрыть эту страницу и не напоминать о создании ложных дисков». Закладка «Форс-мажор» больше не будет появляться в диалоговом окне «Параметры», из меню будет удален пункт «Форс-мажор», и при создании новых дисков не будут появляться напоминания о создании ложных дисков. Для того чтобы вновь попасть на закладку «Форс-мажор», следует сразу после открытия закладки «Общие» диалогового окна «Параметры» нажать клавишу <F8>. Если клавиша <F8> задействована в каком-либо другом приложении в качестве горячей клавиши, то можно нажать <F8> в любом сочетании с клавишами <Shift>, <Alt> или <Ctrl>.

ВЫПОЛНИТЬ!

20. Создать в структуре каталогов диска «C:\» папку для размещения ложных дисков. На закладке «Форс-мажор» разрешить создание ложных дисков и подмену дисков. В папке создать ложные образы для первого и третьего дисков, на дисках создать подложные текстовые файлы. Проконтролировать подключение ложных дисков и подмену настоящих и ложных дисков при наборе ложного пароля.
21. Разрешить уничтожение дисков. При подключении первого диска ввести пароль «на уничтожение». Проконтролировать подключение ложного и полное уничтожение настоящего дисков.

2.3.6. Сервисные операции

Выполнение функций копирования и восстановления заголовков, смены парольной информации и инициализации внешних ключей для подключения дисков осуществляется из пункта меню «Сервис» главного окна «StrongDisk». Для сохранения заголовка вновь созданного защищенного диска следует выбрать закладку «Сохранение», выбрать в окне «Имя файла-образа диска» требуемый образ (рис. 2.38). Файл копии заголовка может иметь любое имя и расширение. Хранить копию заголовков защищенных дисков следует на съемных носителях в недоступных для злоумышленника местах.

Для восстановления заголовка диска следует выбрать пункт меню «Восстановление».

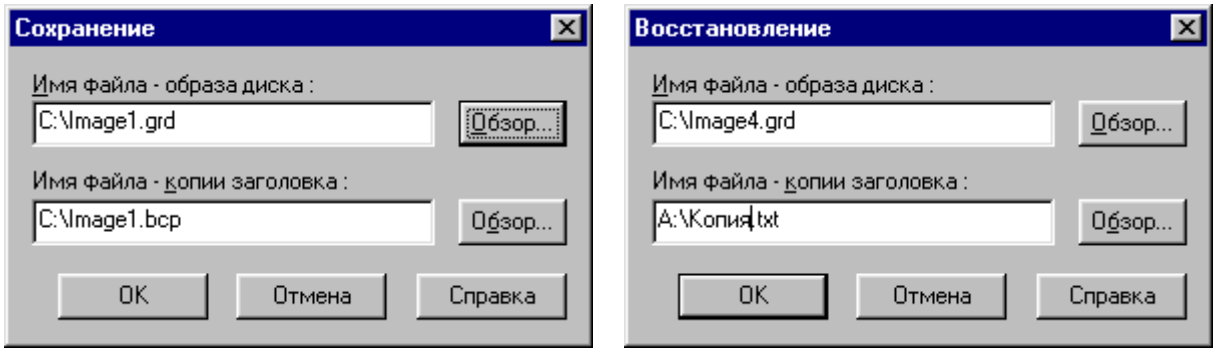


Рис. 2.38. Сохранение и восстановление заголовков дисков

Для надежной защиты виртуальных дисков целесообразно использовать при подключении файлов-образов пароль, файл-ключ и внешний идентификатор. Прежде чем назначить защищенному диску дополнительные ключи, их необходимо инициализировать. Инициализацию файлов-ключей и кода для внешних ключей осуществляет сама система «StrongDisk» на основе генерации случайной последовательности. При отсутствии считывателей для электронных ключей в окне «Инициализация ключа» соответствующая опция будет недоступной (рис. 2.39).

Система «StrongDisk» для файлов-ключей и электронных носителей генерирует случайную последовательность одинаковой длины. Электронный и файл-ключ оказываются взаимозаменяемыми. Файлу-ключу можно назначить любое имя с любым расширением, закамуфлировать его под текстовый или другой документ и хранить глубоко в структуре каталогов одного из логических дисков компьютера. Однако более надежная защита дисков обеспечивается при хранении ключевых файлов на съемных носителях.

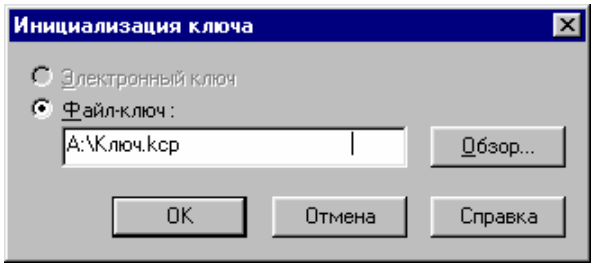


Рис. 2.39. Окно инициализации ключей

После того как ключи инициализированы их можно назначить защищенным дискам. Операция смены и назначения новых ключей и пароля осуществляется в окне «Смена пароля/ключа», которое вызывается из пункта меню «Сервис». Любому файлу-образу может быть назначен полный комплект, даже если ранее он подключался только по обычному паролю. Для смены ключевой информации необходимо ввести текущие установки и указать новые. При этом следует соблюдать порядок ввода ключевой информации: первым указывается файл-ключ, затем вводится обычный пароль (рис. 2.40).

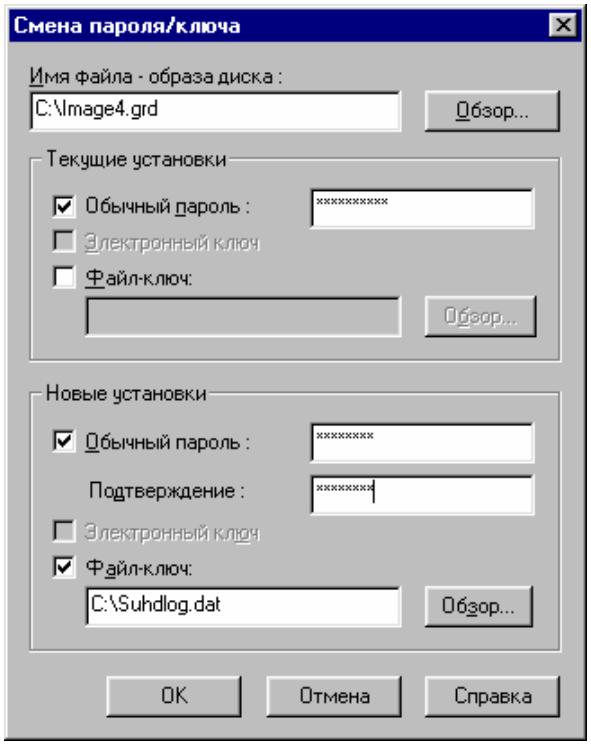


Рис. 2.40. Установка нового пароля и файла-ключа образу диска C:\Image4.grd, подключаемому ранее только по обычному паролю

ВЫПОЛНИТЬ!

22. Отключить все диски. Инициализировать два файла-ключа с различными именами, уточнить размер файлов и просмотреть их содержимое доступными средствами. Один из них скопировать на дискету, а оригинал удалить. Для двух созданных дисков сменить пароль и назначить файлы-ключи. Подключить диски с новой ключевой информацией. Попытаться осуществить операцию смены ключа и пароля на подключенном диске и подключить файл-образ с «чужим» ключом. Сделать выводы.

2.3.7. Гарантированное удаление данных

В состав системы «StrongDisk» входит утилита «Burner», предназначенная для безопасного удаления файлов с полным затиранием содержащихся в них данных без возможности восстановления. Для уничтожения файла (или целой папки) его необходимо с помощью манипулятора «мышь» «перетащить» на ярлык «горящей корзины» — «Уничтожение данных» (рис. 2.23). Если «Рабочий стол» скрыт под активными окнами, уничтожение файла можно осуществить в любом из приложений, для чего в «Проводнике» щелкнуть на нем правой клавишей мыши и во всплывающем меню выбрать пункт «Уничтожить». Под уничтожением (затиранием) данных в «StrongDisk» понимается заполнение соответствующей области данных на логическом диске случайными символами. При уничтожении объекта утилита «Burner» уточнит у пользователя его намерение удалить данные с полным затиранием. Последние версии системы «StrongDisk» при первом запуске утилиты «Burner» запрашивают у пользователя настройку параметров затирания уничтожаемых данных. В появляющемся окне (**рис. 2.41**) можно установить количество проходов при затирании файлов и хвостов файлов.

Внимание! Файлы, находящиеся на защищенных дисках, можно удалять с помощью обычных средств. Для их восстановления потребуется минимум подключить защищенный диск, т. е. иметь пароль и внешний ключ к нему.

В состав системы входят средства для затирания свободного места на дисках. В процессе затирания происходит заполнение всего свободного места на указанном логическом диске, включая остатки удаленных файлов, случайными данными. После затирания свободного места восстановление информации, содержавшейся в удаленных файлах, становится невозможным.

Для затирания свободного места на диске, включая хвосты файлов, следует:

- закрыть все работающие приложения;
- в «проводнике» щелкнуть правой кнопкой мыши на иконке диска, на котором требуется затереть свободное место;
- во всплывающем меню выбрать пункт «Затереть свободное место».

- в открывшемся окне (рис. 2.42) установить переключатели «Затереть свободное место» и «Затереть хвосты файлов» во включенное состояние.

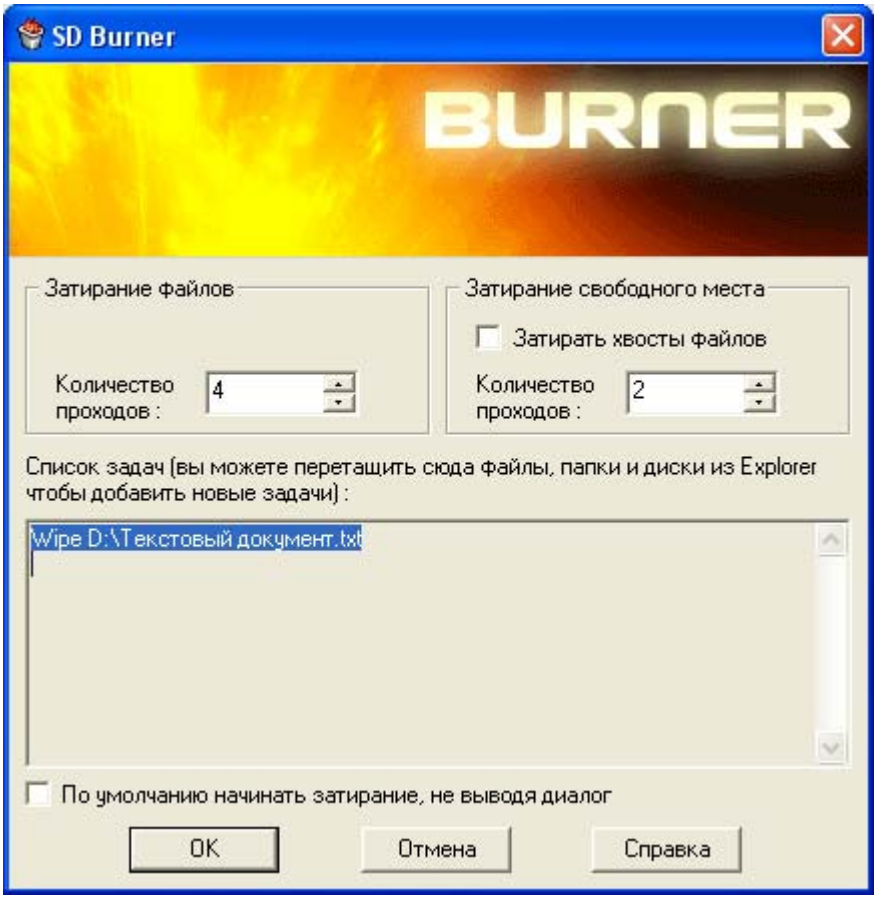


Рис. 2.41. Установка параметров затирания файлов в утилите «Burner»

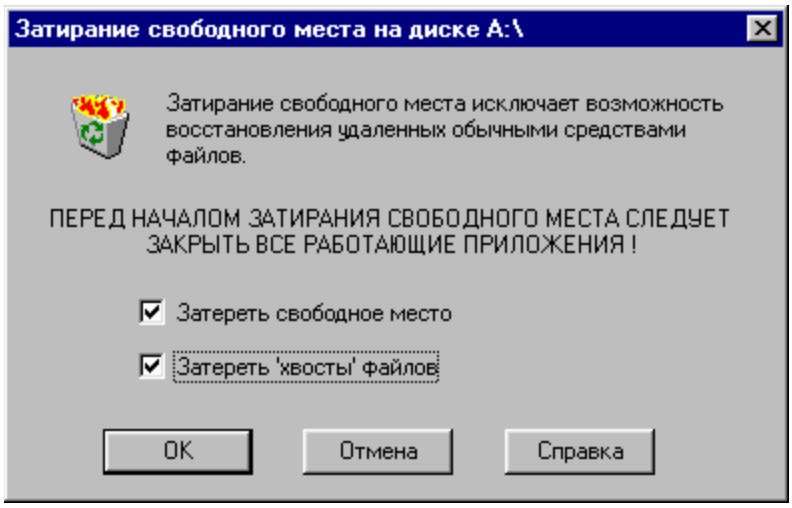


Рис. 2.42. Всплывающее окно «Затирание свободного места на диске»

ВЫПОЛНИТЬ!

23. Отформатировать дискету. Скопировать на нее (создать) три коротких текстовых файла. С помощью утилиты «Disk Editor» просмотреть содержимое файлов и свободное место на диске. Просмотреть хвосты файлов, убедится в том, что они пусты. Удалить один из файлов стандартными средствами

Windows. Убедиться, что область данных файла на дискете осталась неизменной. Средствами «StrongDisk» произвести затирание свободного места на диске «A:\» и просмотреть область данных, занимаемую ранее удаленным файлом. Просмотреть хвосты файлов, убедиться в том, что они заполнены случайными символами. Средствами «StrongDisk» безопасно удалить (уничтожить) следующий файл. С помощью утилиты «Disk Editor» убедиться в невозможности восстановления удаленного файла. Эту же операцию можно выполнить с любым файлом на любом незашифрованном разделе жесткого диска. При этом следует пользоваться более современными дисковыми редакторами, работающими с NTFS-разделами.

2.4. Система защиты корпоративной информации «Secret Disk»

2.4.1. Основные характеристики системы «Secret Disk»

Линейка аппаратно-программных средств криптографической защиты информации «Secret Disk», разработанная компанией ALADDIN Software Security R.D. (г. Москва), является менеджером секретных дисков и предназначена для шифрования разделов жесткого диска и создания на дисковом пространстве компьютера защищенных виртуальных дисков с многопользовательским доступом. Для работы с дисками в состав системы входит VXD-драйвер. Система «Secret Disk» работает только в режиме двухфакторной аутентификации пользователей, когда наряду с вводом пароля пользователь обязан подключить к ПЭВМ внешний носитель ключевой последовательности (eToken в виде USB-ключа или смарт-карты или электронный ключ PCCard (PCMCIA) для портативных компьютеров).

В «Secret Disk 2.0» для шифрования данных могут использоваться следующие алгоритмы:

- собственный алгоритм преобразования данных системы «Secret Disk»;
- криптографический алгоритм ГОСТ 28147–89 (программный эмулятор криптографической платы Криптон фирмы «Анкад»);
- алгоритм RC4, встроенный в ОС Windows (Microsoft CryptoAPI).

2.4.2. Инициализация системы «Secret Disk»

В процессе установки системы «Secret Disk 2.0» необходимо указать имеющийся в наличии носитель ключевой информации, выбрав соответствующий пункт в окне «Выбор компонентов» (рис. 2.43). После установки и перезагрузки компьютера будет запущен «Мастер первого запуска», который предложит создать на жестком диске защищенный виртуальный диск.

При этом необходимо активизировать электронный ключ, на котором будет храниться ключевая информация для доступа к создаваемому диску. Эта ключевая информация в СКЗИ «Secret Disk» называется «личным ключом». Для активизации следует подключить по запросу СКЗИ носитель eToken к USB-порту, а затем сгенерировать случайную последовательность путем нажатия произвольных клавиш или перемещением «мыши» (рис. 2.44). Сгенерированный личный ключ будет записан в перепрограммируемую составляющую носителя eToken. Обратим внимание, что в результате будет уничтожен ранее записанный на eToken личный ключ, который, возможно, уже применялся при шифровании пользовательских данных. В связи с возможным ошибочным уничтожением личных ключей в СКЗИ предусмотрена возможность сохранения личного ключа в виде файла на ином носителе (например, на дискете) для последующего восстановления. После активации ключа соответствующее предупреждение выводится на экран.

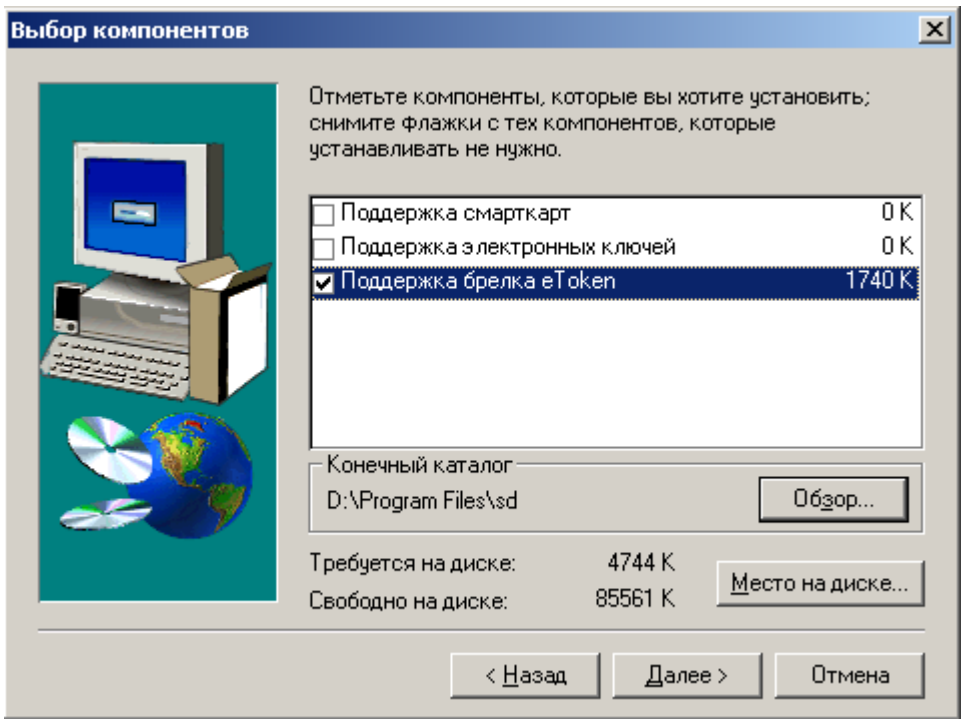


Рис. 2.43. Выбор электронного ключа

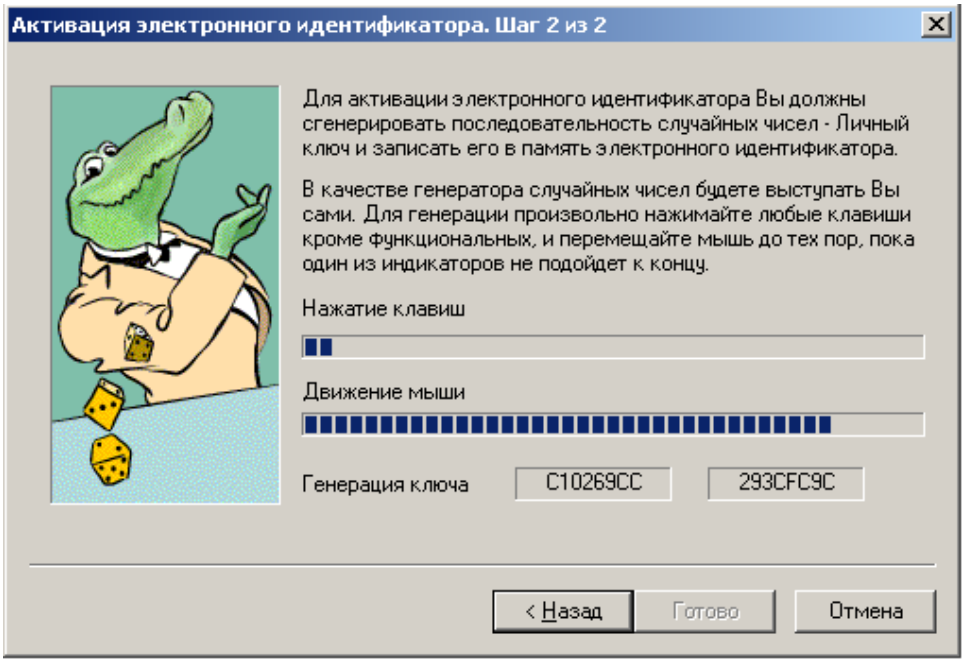


Рис. 2.44. Генерация личного ключа

2.4.3. Создание защищенных логических дисков

«Мастер первого запуска» предлагает создать защищенный виртуальный диск. В качестве параметров виртуального диска необходимо указать имя файла и каталога, где он будет создан, объем создаваемого диска, пароль доступа к информации на диске, тип используемого электронного ключа, алгоритм шифрования данных (рис. 2.45), а также пароль для входа под принуждением.

Отдельно задаваемым параметром является ключ шифрования данных (называемый в СКЗИ «рабочим ключом»), который будет храниться в заголовке файла-образа диска в зашифрованном виде. Рабочий ключ создается как генерируемая случайным образом последовательность символов (рис. 2.46).

СКЗИ «Secret Disk» рекомендует сделать резервную копию сгенерированного рабочего ключа на внешнем носителе (дискете), хранить который необходимо в защищенном месте (в сейфе). Эта резервная копия будет содержать рабочий ключ в виде незашифрованного файла, с помощью которого при необходимости (потере электронного ключа или пароля) можно будет получить доступ ко всей информации на зашифрованном диске.

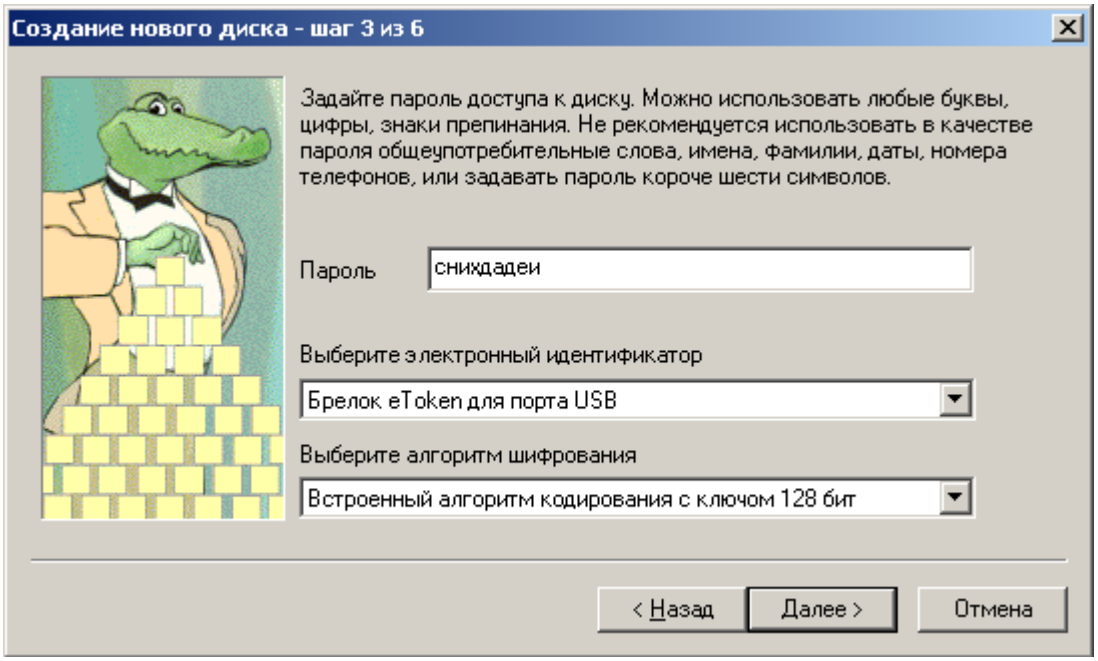


Рис. 2.45. Параметры виртуального диска

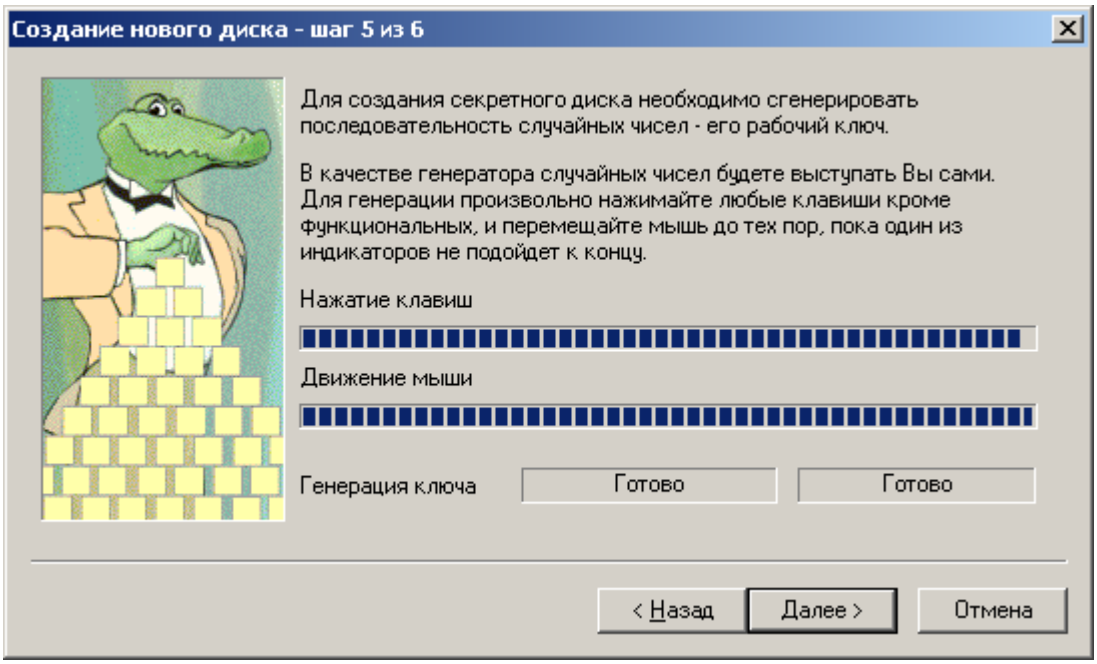


Рис. 2.46. Генерация ключа шифрования данных

Основная копия рабочего ключа будет храниться в заголовке файла-образа диска в зашифрованном виде, а ключом для ее расшифрования будет являться совокупность пароля и личного ключа (который хранится на eToken).

Таким образом, безопасному хранению внешних носителей, содержащих резервные копии рабочих ключей, должно уделяться особое внимание. Ни в коем случае не должно быть допущено резервное сохранение рабочих ключей на основном носителе.

2.4.4. Работа с защищенными дисками

После создания файл-образ диска может быть подключен. Для этого необходимо подключить электронный ключ и ввести пароль (рис. 2.47). При их совпадении в системе появится дополнительный логический диск (рис. 2.48), работа с которым осуществляется как с обычным съемным носителем.

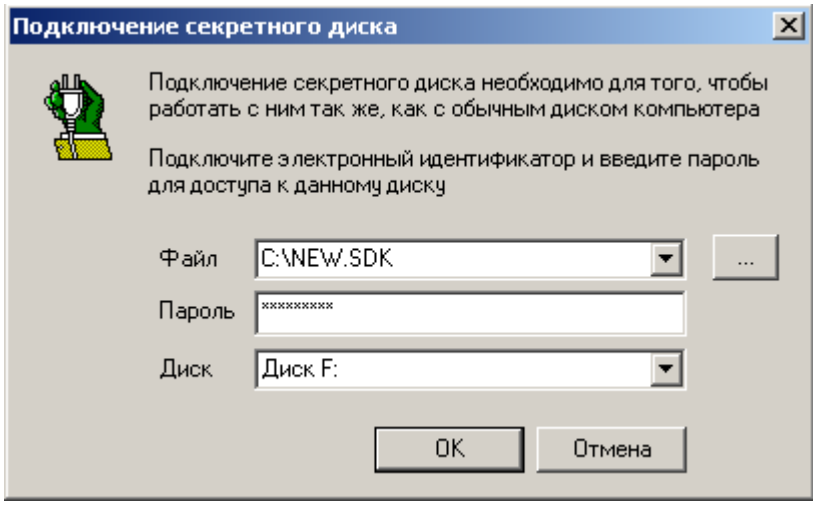


Рис. 2.47. Подключение секретного диска

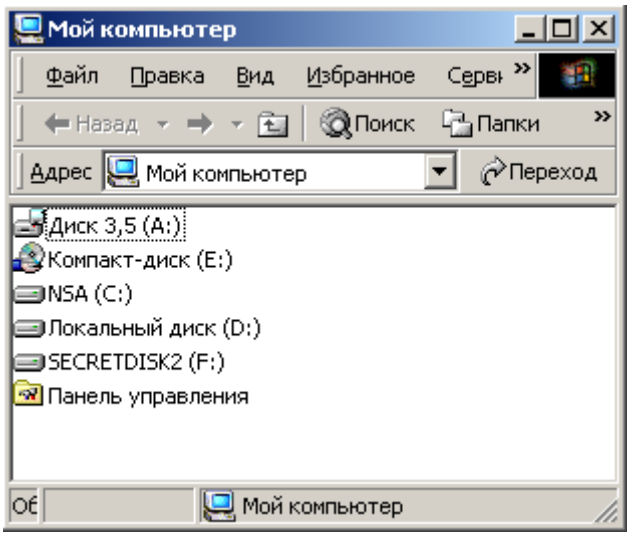


Рис. 2.48. Виртуальный диск F:

СКЗИ «Secret Disk» позволяет организовать многопользовательский доступ к зашифрованной информации (рис. 2.49). Пользователь, создавший диск,

может разрешить доступ к своему диску любому иному пользователю, имеющему электронный ключ. Для этого необходимо подключить электронный ключ добавляемого пользователя (рис. 2.50), в результате чего будет сделана еще одна копия рабочего ключа в заголовке файла-образа, но уже зашифрованная с использованием личного ключа добавляемого пользователя.

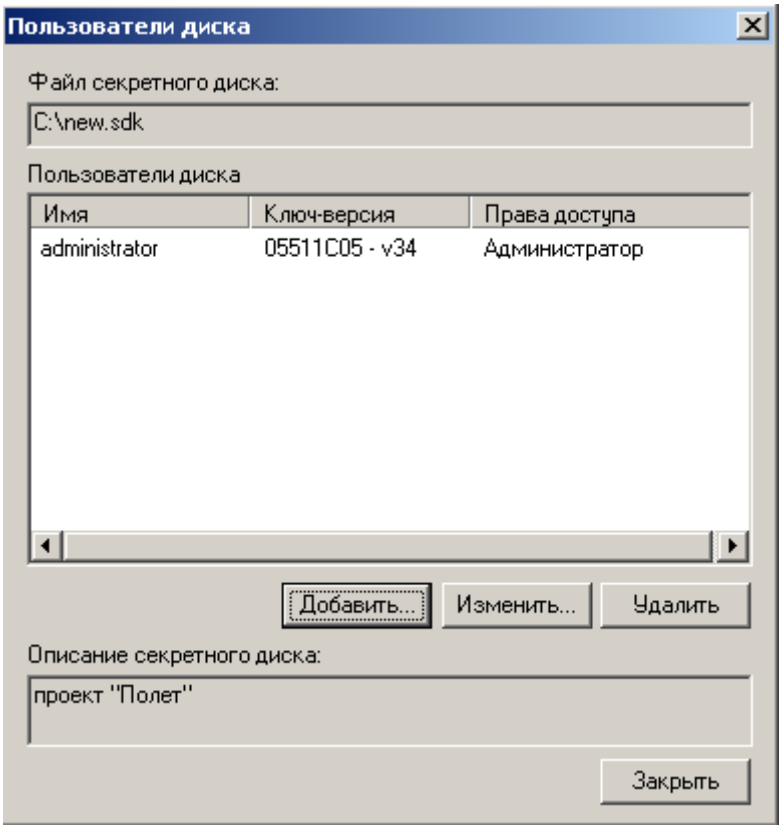


Рис. 2.49. Многопользовательский режим доступа

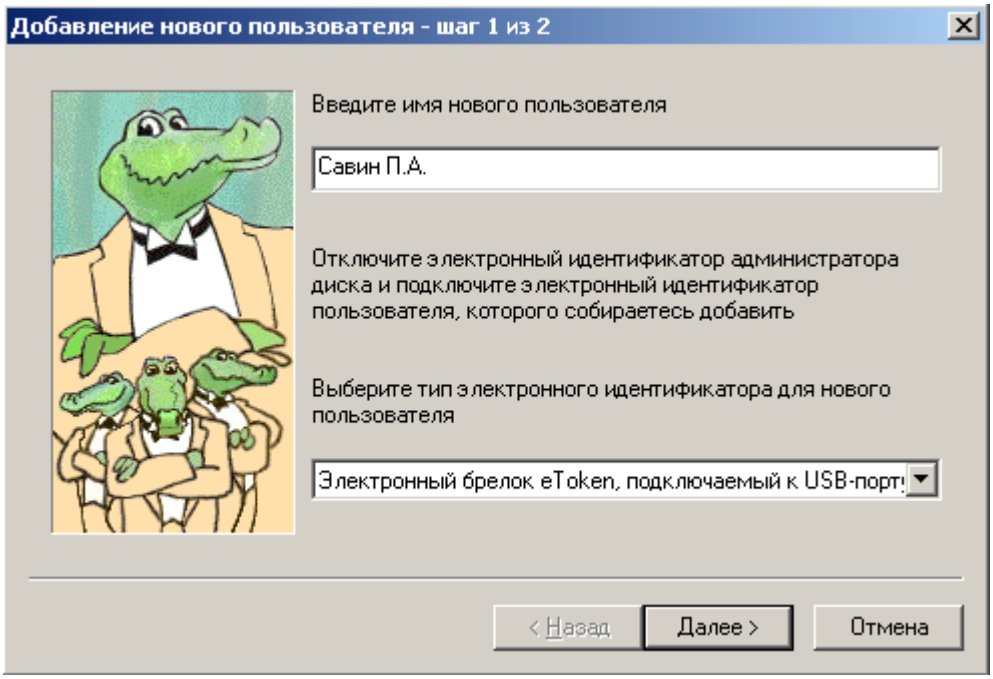


Рис. 2.50. Добавление нового пользователя

ВЫПОЛНИТЬ!

24. Установить и активировать СКЗИ «Secret Disk», используя электронный ключ eToken. Сделать резервную копию электронного ключа на внешний носитель.
25. Создать в корневом каталоге диска «C:\» файл-образ защищенного диска. Сделать резервную копию рабочего ключа на внешний носитель.
26. Подключить защищенный диск. Создать на диске простой текстовый документ и документ Word, отключить диск. Просмотреть содержимое файла-образа диска всеми доступными средствами, включая дисковый редактор.

2.4.5. Настройка СКЗИ «Secret Disk»

Настройка СКЗИ «Secret Disk» производится в окне «Параметры системы» и заключается в установке ряда параметров для обеспечения безопасности данных при наступлении «форс-мажорных» обстоятельств. Если пользователь отлучился на продолжительное время либо извлек электронный ключ, не отключив секретный диск, система самостоятельно через определенное время (рис. 2.51) может включить блокировку экрана программой-заставкой. Для абсолютного блокирования доступа к секретным данным применяется режим «Красной кнопки», когда при нажатии специально задаваемой комбинации клавиш не только отключаются все секретные диски, но и стирается информация из подключенных электронных ключей.

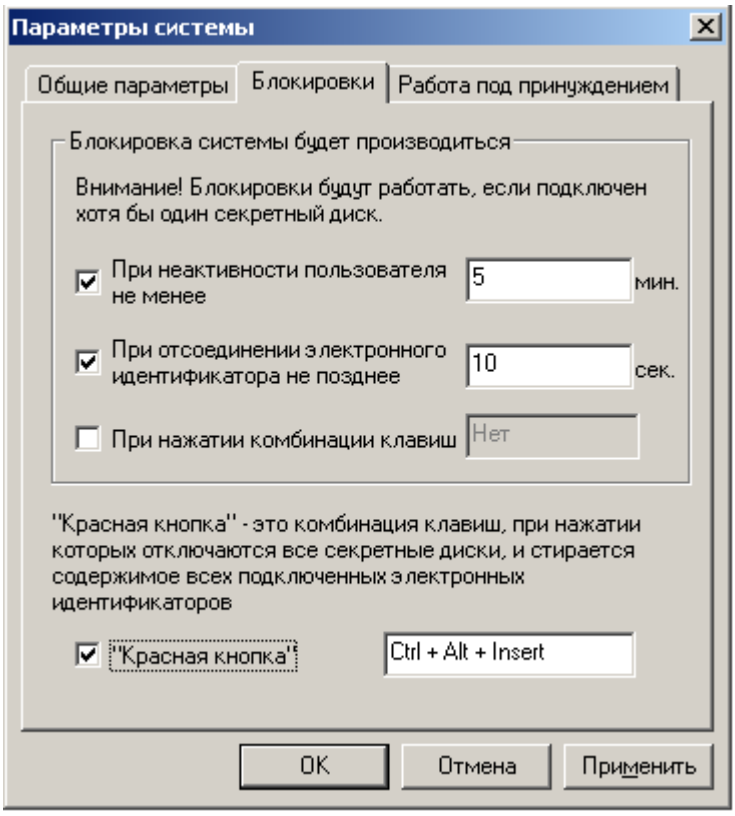


Рис. 2.51. Настройка режима блокировок

Стирание ключевой информации может произойти и в режиме работы под принуждением. Данный режим включается, когда в процессе подключения секретного диска будет введен специально заданный пароль. Кроме стирания информации из электронного ключа может имитироваться «зависание» компьютера (рис. 2.52).

ВЫПОЛНИТЬ!

27. Установить минимально допустимое время неактивности пользователя, подключить диск, открыть документ для редактирования и проконтролировать блокировку экрана по истечении этого времени.
28. Назначить «горячие клавиши» для включения режима «Красная кнопка». Подключить секретный диск, открыть для редактирования имеющийся на нем текстовый документ, внести в документ изменения и включить режим «Красная кнопка». Попытаться вновь подключить секретный диск, возможно ли это?

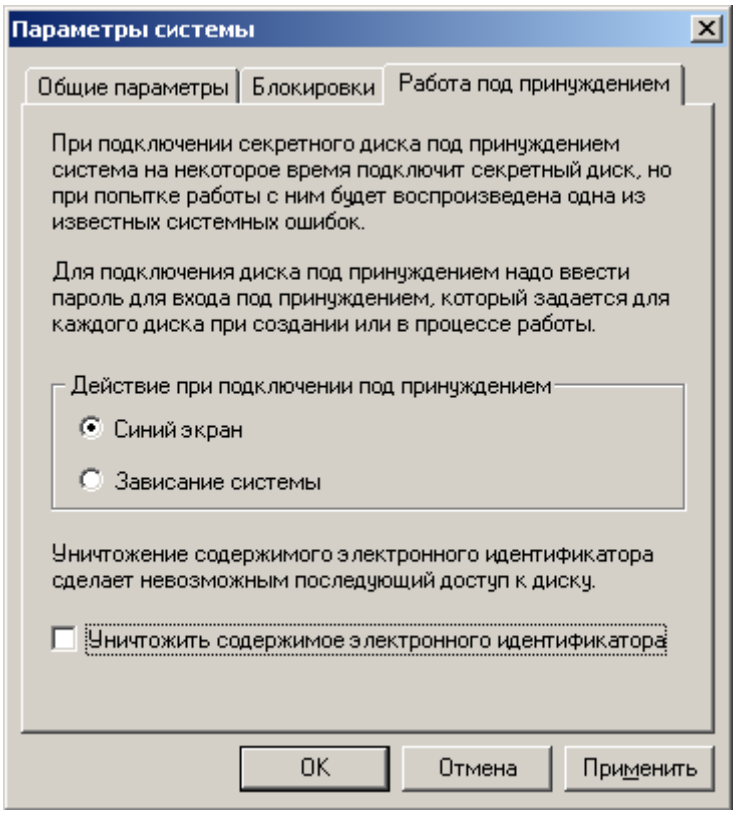


Рис. 2.52. Настройка режима работы под принуждением

2.4.6. Управление секретными дисками

Для управления секретными дисками предназначена программа «Администратор секретного диска» (рис. 2.53), которая позволяет настроить ряд параметров подключенного диска. В частности, может быть изменен пароль и/или электронный идентификатор, пароль входа под принуждением, а также сделана резервная копия рабочего ключа секретного диска (рис. 2.54). Кроме того, мо-

жет быть осуществлен просмотр журнала обращений к секретному диску. Программа «Администратор секретного диска» позволяет создать резервную копию личного ключа, хранящегося в электронном идентификаторе, а также выполнить обратную операцию — восстановление ключа.

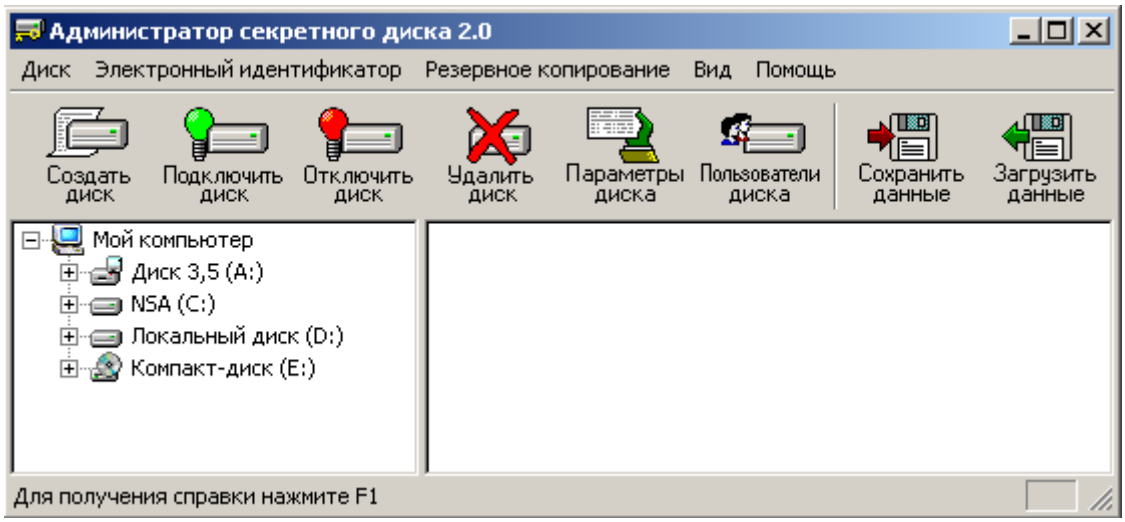


Рис. 2.53. Управление секретными дисками

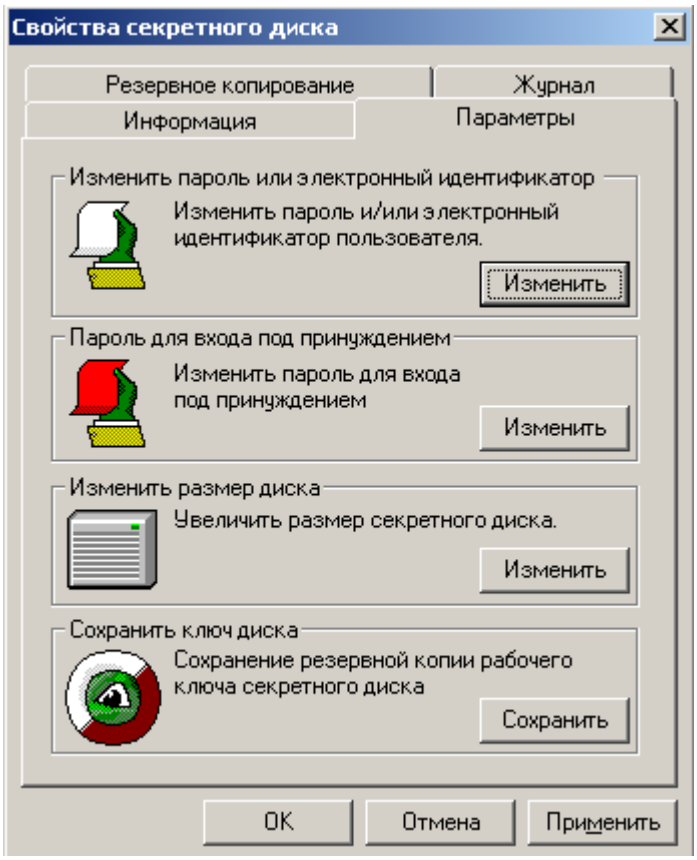


Рис. 2.54. Изменение параметров секретного диска

ВЫПОЛНИТЬ!

29. Восстановить личный ключ из ранее сохраненной резервной копии. Вновь подключить секретный диск, отключенный в режиме «Красная кнопка».

2.4.7. Хранение секретной информации на съемных носителях

В СЗКИ «Secret Disk» предусмотрен режим работы в качестве архиватора, который не только сжимает, но и шифрует данные. Данный режим полезен, если необходимо перенести секретную информацию на сменном носителе на другой компьютер, где также установлена СКЗИ «Secret Disk». Программа архивации позволяет выбрать ключ шифрования (рис. 2.55) и перечень шифруемых файлов. В результате будет создан файл архива, содержащий указанные файлы в зашифрованном и (при необходимости) сжатом видах и готовый для переноса на другой компьютер.

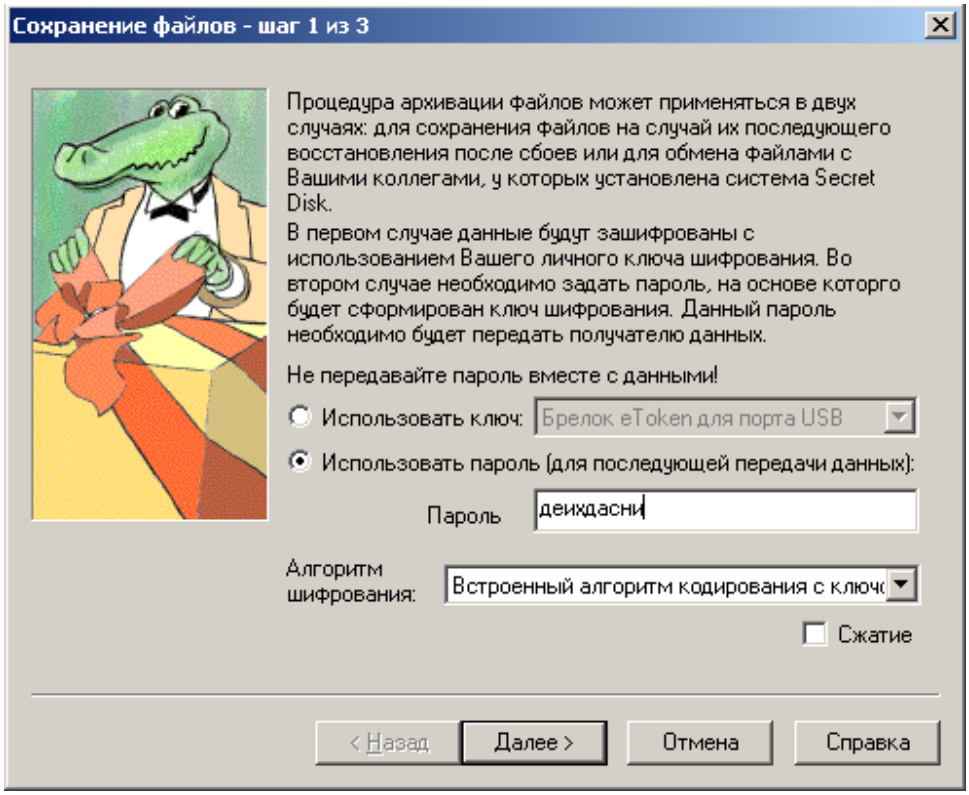


Рис. 2.55. Архивация данных в СЗКИ «Secret Disk»

В качестве ключа шифрования «Secret Disk» позволяет использовать либо личный ключ, хранящийся в электронном идентификаторе, либо пароль. Если файл не предназначен для отправки иному лицу, а должен храниться на съемном носителе, то в качестве ключа рекомендуется использовать личный ключ. Если предполагается передача файла иному лицу, то ключом шифрования должен быть пароль. Вместе с тем возникает проблема передачи этого секретного пароля, так как при шифровании применяется симметричная схема.

Следует отметить, что режим архивации нельзя использовать для обработки (чтения, модификации) документов, так как в процессе редактирования на носителе будет создан «технологический мусор», содержащий секретные данные в открытом виде.

3. ПРИМЕНЕНИЕ СЗИ ОТ НСД ДЛЯ ОРГАНИЗАЦИИ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

3.1. Меры противодействия несанкционированному доступу

В пункте 1.2 пособия были перечислены основные меры по защите информации в компьютерной системе. Большинство из них направлено на обеспечение безопасности КИ от несанкционированного доступа. Эти меры можно назвать каноническими, они в той или иной мере реализованы в распространенных универсальных и специализированных операционных системах. Для неискушенных читателей, прежде чем перейти к изучению аппаратно-программных средств защиты от НСД, дополняющих классические компьютерные системы, целесообразно познакомиться с некоторыми теоретическими и практическими правилами предотвращения несанкционированного доступа.

3.1.1. Идентификация и аутентификация пользователей

Для гарантии того, чтобы только зарегистрированные в АС пользователи могли включить компьютер (загрузить операционную систему) и получить доступ к его ресурсам, каждый доступ к данным в защищенной АС осуществляется в три этапа: идентификация — аутентификация — авторизация.

Идентификация — присвоение субъектам и объектам доступа зарегистрированного имени, персонального идентификационного номера (PIN-кода), или идентификатора, а также сравнение (отождествление) предъявляемого идентификатора с перечнем присвоенных (имеющихся в АС) идентификаторов. Основываясь на идентификаторах, система защиты «понимает», кто из пользователей в данный момент работает на ПЭВМ или пытается включить компьютер (осуществить вход в систему). *Аутентификация* определяется как проверка принадлежности субъекту доступа предъявленного им идентификатора, либо как подтверждение подлинности субъекта. Во время выполнения этой процедуры АС убеждается, что пользователь, представившийся каким-либо легальным сотрудником, таковым и является. *Авторизация* — предоставление пользователю полномочий в соответствии с политикой безопасности, установленной в компьютерной системе.

Процедуры идентификации и аутентификации в защищенной системе осуществляются посредством специальных программных (программно-аппаратных) средств, встроенных в ОС или СЗИ. Процедура идентификации производится при включении компьютера и заключается в том, что сотрудник «представляется» компьютерной системе. При этом АС может предложить сотруднику выбрать свое имя из списка зарегистрированных пользователей или правильно ввести свой идентификатор. Далее пользователь должен убедить АС в том, что он действительно тот, кем представился. Аутентификация в защищенных АС может осуществляться несколькими методами:

- парольная аутентификация (ввод специальной индивидуальной для каждого пользователя последовательности символов на клавиатуре);

- на основе биометрических измерений (наиболее распространенными методами биометрической аутентификации пользователей в СЗИ являются чтение папиллярного рисунка и аутентификация на основе измерений геометрии ладони, реже встречаются голосовая верификация и считывание радужной оболочки или сетчатки глаз);
- с использованием физических носителей аутентифицирующей информации.

Наиболее простым и дешевым способом аутентификации личности в АИС является ввод пароля (трудно представить себе компьютер без клавиатуры). Однако существование большого количества различных по механизму действия атак на систему парольной защиты делает ее уязвимой перед подготовленным злоумышленником. Биометрические методы в СЗИ пока не нашли широкого применения. Непрерывное снижение стоимости и миниатюризация, например, дактилоскопических считывателей, появление «мышек», клавиатур и внешних флеш-носителей со встроенными считывателями неминуемо приведет к разработке средств защиты с биометрической аутентификацией.

В настоящее время для повышения надежности аутентификации пользователей в СЗИ применяют внешние носители ключевой информации. В технической литературе производители этих устройств и разработчики систем безопасности на их основе пользуются различной терминологией. Можно встретить подходящие по контексту термины: *электронный идентификатор*, *электронный ключ*, *внешний носитель ключевой или кодовой (аутентифицирующей) последовательности*. Следует понимать, что это устройства внешней энергонезависимой памяти с различным аппаратным интерфейсом, работающие в режимах чтение или чтение/запись и предназначенные для хранения ключевой (для шифрования данных) либо аутентифицирующей информации. Наиболее распространенными устройствами являются электронные ключи «Touch Memory» на базе микросхем серии DS199X фирмы Dallas Semiconductors. Другое их название — «iButton» или «Далласские таблетки» (устройства выпускаются в цилиндрическом корпусе диаметром 16 мм и толщиной 3 или 5 мм, рис. 3.1).

Рис. 3.1. Внешний вид электронного ключа iButton и считывателя информации

В СЗИ активно используются пластиковые карточки различных технологий (чаще всего с магнитной полосой или проксими-карты, рис. 3.2). Пластиковые карточки имеют стандартный размер 54х85,7х0,9 — 1,8 мм.

Рис. 3.2. Пластиковая карта с магнитной полосой

Удобными для применения в СЗИ являются электронные ключи eToken (рис. 3.3), выполненные на процессорной микросхеме семейства SLE66C Infineon, обеспечивающей высокий уровень безопасности. Они предназначены для безопасного хранения секретных данных, например, криптографических ключей. eToken выпускается в двух вариантах конструктивного оформления: в виде USB-ключа и в виде смарт-карты стандартного формата.

В большинстве программно-аппаратных средств защиты информации предусмотрена возможность осуществлять аутентификацию личности пользователя комбинированным способом, т. е. по нескольким методам одновременно. Комбинирование способов аутентификации снижает риск ошибок, в результате которых злоумышленник может войти в систему под именем легального пользователя.

Рис. 3.3. Электронные ключи eToken

3.1.2. Ограничение доступа на вход в систему

Прежде всего, еще раз напомним, что ограничение доступа к ресурсам АС начинается с ограничения *физического* доступа сотрудников и «гостей» предприятия в помещение, в котором размещаются и функционируют элементы компьютерной системы. Этот рубеж защиты организуется путем установки средств инженерной укрепленности помещений, автономных устройств охранной сигнализации, телевизионных систем наблюдения, устройств защиты рабочего места и непосредственно ПЭВМ и к функционированию программных и аппаратных СЗИ отношения не имеет.

В практике защиты объектов информатизации под методом «ограничение доступа на вход в систему» имеют в виду целый комплекс мер, выполняемых в процессе загрузки операционной системы. Поэтому для описания процесса правильного и легального включения компьютера специалисты часто используют термин «доверенная загрузка ОС». Правильно организованная доверенная загрузка обеспечивает выполнение 1, 2 и отчасти третьего пунктов требований к системе защиты информации, сформулированных в п. 1.1. пособия.

Благодаря процедурам идентификации и аутентификации АС разрешает дальнейшую работу только зарегистрированным пользователям в именованном режиме. Однако для всецело доверенной загрузки этого не достаточно. Безопасный вход в компьютерную систему включает в себя также процедуру ограничения доступа по дате и времени, процедуру проверки целостности системного программного обеспечения и аппаратуры, а также защиту от загрузки ОС со съемных носителей и входа в АС в незащищенном режиме. Первая из этих мер помимо поддержания дисциплины (что необходимо на предприятии, где обрабатывается информация ограниченного доступа) обеспечивает дополнительную защиту от злоумышленников, пытающихся атаковать АС во внерабочее время.

Одной из встроенных в программно-аппаратную среду самого компьютера процедур ограничения *логического* доступа является операция ввода пароля BIOS при включении ПЭВМ. Чтобы понять, какое место в комплексе защитных мер занимает парольная защита, рассмотрим процесс загрузки персонального компьютера без использования СЗИ (рис. 3.4).

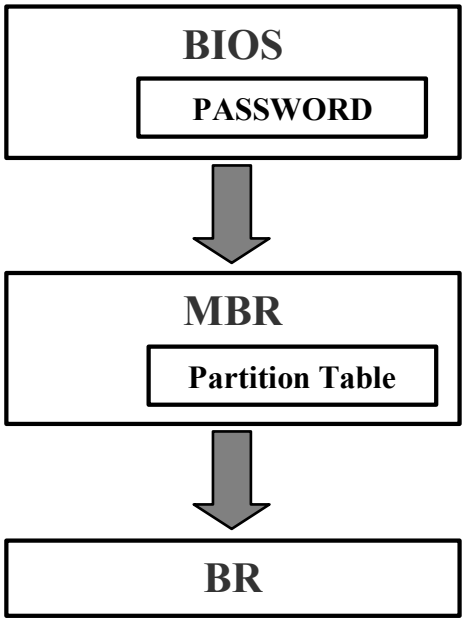


Рис. 3.4. Процесс стандартной загрузки персонального компьютера

При включении питания управление ПЭВМ берет на себя программа, записанная в ПЗУ BIOS, которая проводит процедуру самотестирования компьютера (Power-On Self-Test, POST). После тестирования из ПЗУ BIOS в оперативную память ПЭВМ загружается содержимое первого сектора нулевого цилиндра нулевой стороны накопителя на жестком магнитном диске (НЖМД). В данном секторе НЖМД находится главная загрузочная запись (Master Boot Record — MBR), на которую передается управление компьютером. Программа первоначальной загрузки (Non-System Bootstrap — NSB — несистемный загрузчик) является первой частью MBR. NSB анализирует таблицу разделов жесткого диска (Partition Table), являющуюся второй частью MBR, и определяет по ней расположение (номера сектора, цилиндра и стороны) активного раздела, содержащего рабочую версию ОС. Определив активный (загрузочный) раздел НЖМД, программа NSB считывает его нулевой сектор (Boot Record — BR — загрузочную запись) и передает ей управление ПЭВМ. Алгоритм работы загрузочной записи зависит от операционной системы, но обычно состоит в запуске непосредственно операционной системы или программы — загрузчика ОС.

Парольная система BIOS имеет только два варианта паролей с категориями «пользователь» и «суперпользователь». Ввод парольной информации выполняется (если функция активирована в соответствующих настройках BIOS) до обращения к жесткому диску компьютера, т. е. до загрузки операционной системы. Это только один из эшелонов защиты АС, который способен разде-

лить потенциальных пользователей на легальных (своих, знающих пароль пользователя) и нелегальных. Парольная система BIOS не обеспечивает идентификации конкретного пользователя.

Защита от входа в АС в незащищенном режиме является весьма серьезной мерой, обеспечивающей безопасность информации и противодействующей попыткам подготовленных нарушителей запустить компьютер в обход системы защиты. Целостность механизмов защиты может быть нарушена, если злоумышленник имеет возможность загрузить на компьютере какую-либо операционную систему с внешнего носителя либо установленную ОС в режиме защиты от сбоев. Опасность загрузки ОС в режиме защиты от сбоев заключается в том, что загружается лишь ограниченный перечень системных драйверов и приложений, в составе которых могут отсутствовать модули СЗИ. Конфиденциальные данные при неактивном СЗИ могут оказаться совершенно незащищенными, и злоумышленник может получить к ним неограниченный доступ.

Для противодействия подобной угрозе необходимо, во-первых, сделать недоступным для просмотра содержимое дисков при загрузке ОС с внешнего носителя. Данная задача может быть решена путем криптографического преобразования информации на жестком диске. Зашифрованным должно быть не только содержимое конфиденциальных файлов, но и содержимое исполняемых и иных файлов, а также служебные области машинных носителей.

Во-вторых, следует внести изменения в стандартный процесс загрузки компьютера, внедрив в него процедуры инициализации механизмов защиты еще до загрузки ОС. Запуск защитных механизмов СЗИ обычно выполняется по одному из следующих способов: с использованием собственного контроллера СЗИ либо путем модификации главной загрузочной записи.

При реализации первого способа СЗИ должно быть программно-*аппаратным* комплексом и содержать собственный контроллер, который обычно устанавливается в слот ISA или PCI. В процессе выполнения процедуры POST после проверки основного оборудования BIOS компьютера начинает поиск внешних ПЗУ в диапазоне адресов от C800:0000 до E000:0000 с шагом в 2Kb. Аппаратная часть СЗИ должна быть организована так, чтобы ее ПЗУ, содержащее процедуры идентификации и аутентификации пользователей, обнаруживалось компьютерной системой по одному из проверяемых системой адресов. При обнаружении внешнего ПЗУ POST BIOS передает управление программе, расположенной в найденном ПЗУ. Таким образом, защитные механизмы (процедуры идентификации и аутентификации, контроля целостности и т. п., записанные в ПЗУ контроллера СЗИ) начинают работать еще до загрузки ОС. И только после удачной отработки механизмов защиты средство защиты возвращает управление процедуре POST, либо непосредственно передает управление на MBR жесткого диска. Кроме ПЗУ, хранящего программы защитных механизмов, в составе СЗИ должны быть перепрограммируемые ПЗУ, в которые заносятся список зарегистрированных пользователей с образами аутентифицирующей их информации и временными рамками разрешения входа в АС. Одним из примеров подобной реализации доверенной загрузки является СЗИ НСД «Аккорд-АМДЗ» (рис. 3.5).

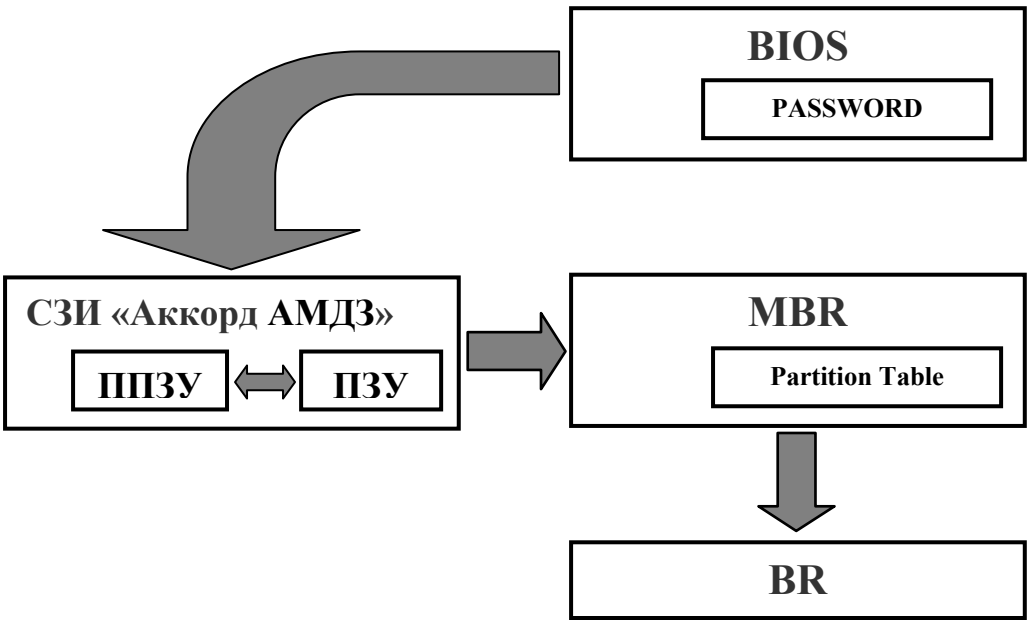


Рис. 3.5. Процесс загрузки персонального компьютера с использованием контроллера СЗИ

Второй способ запуска защитных механизмов применяется в программных СЗИ, примерами которых являются «Страж NT» и «Dallas Lock», которые не имеют собственных аппаратных контроллеров. Задача надежного запуска защитных механизмов (до загрузки ОС) решается здесь путем модификации главной загрузочной записи в *процессе установки* системы защиты. Обычно модификации подвергается только первая часть MBR — программа первоначальной загрузки. В процессе инициализации СЗИ программа первоначальной загрузки меняется на собственную программу средства защиты, задачей которой является передача управления на программный код, реализующий запуск и отработку защитных механизмов доверенной загрузки. После удачного выполнения всех предусмотренных СЗИ процедур управление ПЭВМ передается либо на штатную программу первоначальной загрузки ОС, которая при установке средства защиты копируется в некоторый сектор нулевой дорожки НЖМД, либо напрямую на загрузочную запись активного раздела жесткого диска (рис. 3.6).

В теории и практике обеспечения безопасности АС хорошо известен такой способ преодоления злоумышленником системы защиты, как подбор пароля. Он заключается в переборе всех возможных вариантов паролей («лобовая атака») или наиболее вероятных комбинаций (оптимизированный перебор). Для того чтобы исключить возможность осуществления штурма парольной системы защиты в СЗИ предусматривается режим блокировки компьютера после нескольких (обычно трех — пяти) неудачных попыток ввода пароля. Выход АС из этого режима возможен только после выключения питания (полной перезагрузки системы). Режим блокировки может быть запущен при обнаружении системой защиты любых нештатных действий пользователя как во время доверенной загрузки (например, если код, записанный в предъявляемую карту памяти, не соответствует введенным идентификатору и/или паролю), так и во

время последующей работы (например, при попытке обратиться к запрещенным для доступа портам, устройствам ввода-вывода). Естественно, все попытки неудачного входа в систему, приведшие к блокированию компьютера, должны быть зафиксированы в специальном журнале.

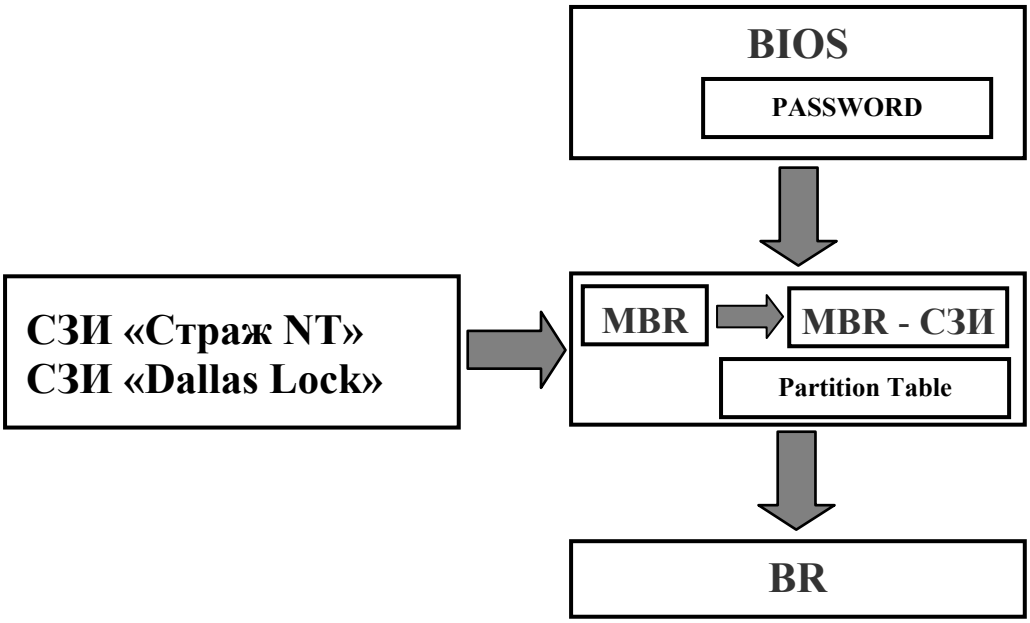


Рис. 3.6. Процесс загрузки персонального компьютера с использованием модификации MBR

Следует отметить, что при отсутствии в функциональном наборе СЗИ процедуры шифрования защищаемых данных, необходимо обеспечить надежную защиту самого компьютера от непосредственного физического доступа. Действительно, если злоумышленнику удастся извлечь контроллер СЗИ из слота ПЭВМ, процесс загрузки ОС перестанет носить защищенный характер, и будет осуществляться стандартно. При наличии физического доступа к элементам АС подготовленный злоумышленник может просто украсть жесткий диск и попытаться добыть интересующую его информацию путем анализа НЖМД с помощью различных низкоуровневых редакторов. Запрет входа в систему в обход механизмов защиты является необходимой составляющей частью процесса доверенной загрузки и обеспечивает выполнение 1, 2 и 3 пунктов требований к системе защиты информации.

3.1.3. Разграничение доступа

Одним из ключевых методов защиты информации от НСД является разграничение полномочий и прав доступа пользователей к ресурсам АС. Напомним, что под доступом к информации понимают [5] ознакомление с информацией, ее обработку, в частности, копирование модификация или уничтожение информации. Разграничение доступа — организация и осуществление доступа субъектов к объектам доступа в строгом соответствии с порядком, установленным политикой безопасности предприятия. Доступ к информации, не нару-

шающий правила разграничения доступа называется санкционированным. Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами, — несанкционированным.

Данное направление деятельности включает разработку организационной схемы функционирования АС, анализ потоков данных, уточнение задач и полномочий пользователей, создание функциональных групп работников на основе круга решаемых задач, построение схемы категорирования объектов АС по критерию доступа различных пользователей.

В своде *правил разграничения доступа* (ПРД) из множества элементов произвольной автоматизированной системы выделяют два подмножества: множество *объектов* и множество *субъектов* доступа. Объект доступа (диск, каталог, файл, системная служба) — любой элемент системы, доступ к которому может быть произвольно ограничен. Субъект доступа (пользователь) — любая сущность, способная инициировать выполнение операций над объектами. Для различных типов объектов вводятся различные операции или методы доступа. Некоторые методы доступа для удобства использования объединяются в группы, называемые правами доступа. Так, например, право доступа к файлу «изменение» подразумевает возможность доступа к нему по методам «чтение» и «запись». А право «полного» доступа — по всем существующим методам, включая «изменение прав доступа».

В качестве дополнительного множества иногда вводятся процессы, порождаемые (инициируемые) субъектами над объектами. Одной из важнейших задач разграничения доступа в АС является обязательная проверка полномочий любых процессов по отношению к обрабатываемым данным.

На этапах проектирования и эксплуатации защищенных АС возникает задача синтеза системы разграничения доступа пользователей информационной системы к ее ресурсам. Предельная открытость системы, когда максимальному числу пользователей предоставляются максимальные права на доступ ко всем ресурсам, приводит к максимальной эффективности ее функционирования, однако увеличивает риск возможных нарушений информационной безопасности. В то же время любые меры безопасности и ограничения объективно снижают отдельные характеристики эффективности функционирования системы. Наличие или отсутствие прав доступа определяется принятой в организации политикой безопасности, при разработке которой следует учитывать следующие принципы:

- доступ любого субъекта к любому объекту доступа может осуществляться только на основе явного или косвенного санкционирования администратором системы или владельцем объекта доступа;
- правила разграничения доступа не должны допускать изменения и удаления жизненно важных системных объектов;
- каждый объект должен иметь владельца;
- должна быть исключена возможность случайной (непреднамеренной) утечки конфиденциальной информации, включая так называемые скрытые каналы утечки информации [15].

Теория и практическая реализация механизмов разграничения доступа обсуждается во многих литературных источниках [10, 11, 15, 16, 17]. Механизмы разграничения доступа оперируют с множествами операций, которые субъекты могут инициировать над объектами. Для каждой пары «субъект — объект» вводится множество *разрешенных* операций, являющееся подмножеством всего множества *допустимых* операций [11]. Оставшиеся операции будут составлять подмножество запрещенных данному пользователю методов доступа к конкретному объекту.

Существуют две основных модели разграничения доступа: дискреционная (одноуровневая) и мандатная (многоуровневая). Большинство ОС, применяющихся в настоящее время на практике (ОС семейства MS Windows NT[1], Novell NetWare, UNIX), реализуют дискреционную модель разграничения доступа. Система правил дискреционной модели разграничения доступа формулируется следующим образом [13]:

1. У каждого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать (или разрешать) доступ других субъектов к данному объекту.
3. Для каждой тройки субъект-объект-метод возможность доступа определена однозначно (рис. 3.7).
4. Существует хотя бы один привилегированный пользователь, имеющий возможность обратиться к любому объекту по любому методу доступа.

Формально дискреционная модель разграничения доступа может быть представлена в виде матрицы доступа, строки которой соответствуют субъектам системы, а столбцы — объектам. Элементы матрицы характеризуют права доступа конкретного субъекта к конкретному объекту. Матрица доступа может формироваться на основе двух различных принципов: централизованного и децентрализованного. При реализации централизованного (принудительного) принципа возможность доступа субъектов к объектам определяется администратором. При реализации децентрализованного (добровольного) принципа доступом управляет владелец объекта. Первый принцип жесткого администрирования обеспечивает более четкий контроль над соблюдением ПРД. Второй принцип более гибкий, однако, труднее поддается контролю со стороны лиц, несущих ответственность за безопасность данных. На практике часто применяют принудительный принцип управления доступа с элементами добровольного подхода.

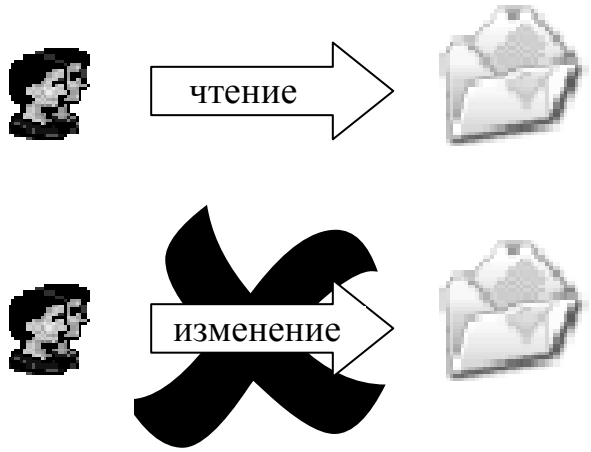
В большинстве случаев матрица доступа имеет весьма существенные размеры (в компьютерной системе присутствует множество различных субъектов и объектов) и является разреженной (субъектам необходим доступ только к небольшим подмножествам объектов). В целях экономии памяти матрица доступа может задаваться в виде списков прав субъектов (для каждого субъекта

[1] Под семейством ОС MS Windows NT авторы понимают известные на момент написания пособия системы Windows NT 4.0 Workstation, Windows NT 4.0 Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows Server 2003.

создается список доступных объектов) или в виде списков прав доступа (для каждого объекта создается список субъектов, имеющих права доступа к нему).

В практических реализациях используется хранение матрицы доступа в виде списков прав доступа, ассоциированных с каждым объектом. Известны два способа кодирования строки матрицы доступа: механизм битов защиты, применяемый в ОС семейства UNIX, и механизм списков прав доступа, применяемый, например, в ОС семейства MS Windows NT.

При реализации дискреционной модели в рамках определенной ОС применяются различные алгоритмы проверки прав доступа субъекта к объекту.



Субъект	Объект	Метод	Возможность
Ювченко	C:\ Приказы и распоряжения	Чтение	Разрешено
Ювченко	C:\ Приказы и распоряжения	Изменение	Запрещено

Рис. 3.7. Тройки субъект-объект-метод

Формализованный алгоритм проверки прав доступа при использовании механизма битов защиты, реализованный в ОС семейства Unix, приведен в [10]. С объектом (файлом) связываются биты защиты, указывающие права доступа для трех категорий субъектов: все пользователи, члены группы владельца и владелец объекта (рис. 3.8). Множество допустимых операций составляют три метода: чтение, запись и выполнение. При попытке доступа производится:

- проверка того, является ли субъект владельцем объекта;
- проверка вхождения субъекта в группу владельца;
- сравнение полномочий, предоставляемых всем пользователям системы, с запрашиваемым типом доступа.

При этом отсутствие разрешений для конкретного субъекта в приоритетной категории пользователей, к которой он принадлежит, приводит к отказу в доступе. Если, например, у владельца нет соответствующих прав, ему будет отказано в доступе к его объекту, и его права как члена своей группы и пользователя проверяться не будут. Пример реализации механизма битов защиты в ОС семейства Unix приведен на рис. 3.9.

Владелец			Группа владельца			Все зарегистрированные пользователи		
Чтение	Запись	Выполнение	Чтение	Запись	Выполнение	Чтение	Запись	Выполнение
*	*	*	*					

Рис. 3.8. Пример механизма битов защиты

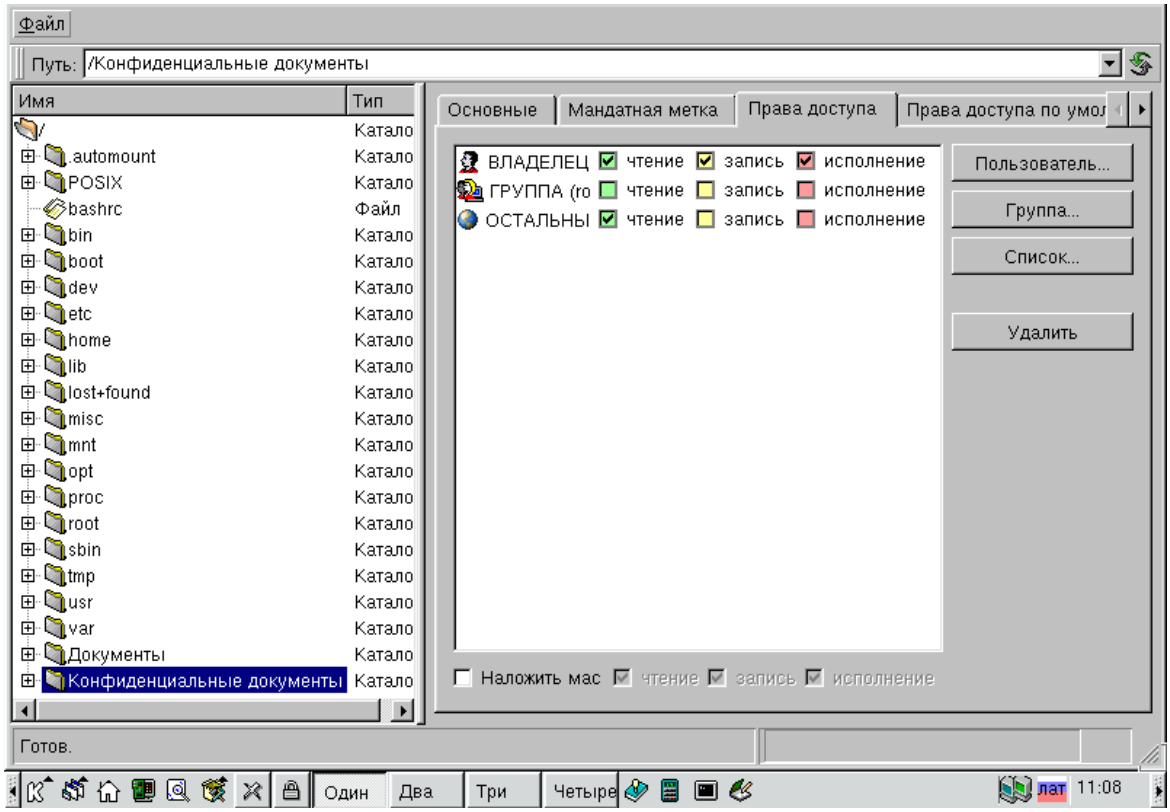


Рис. 3.9. Пример реализации механизма битов защиты в ОС семейства Linux

При использовании механизма списков прав доступа (Access Control List — ACL) не выделяют категорий пользователей (рис. 3.10). В то же время для удобства администрирования доступа пользователи могут объединяться в группы, например, по их функциональному признаку. Конкретный список субъектов (групп) доступа ассоциируется с каждым объектом с указанием прав доступа к нему для каждого пользователя (группы). Каждый список ACL состоит из так называемых записей управления доступом (Access Control Entries — ACE). Всего существует три типа записей. Два из них относятся к управлению доступом: первый разрешает указанный доступ и определяет метод доступа (ACE Allowed), а второй запрещает доступ (ACE Denied). Третий тип записей определяет настройки аудита доступа к объекту (ACE Audit).

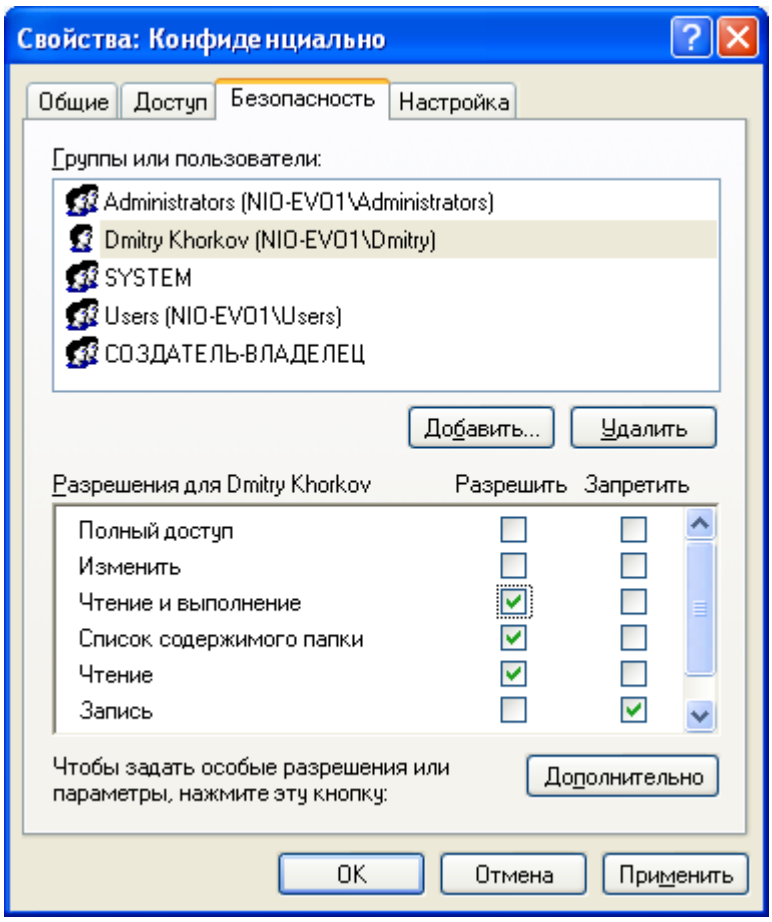


Рис. 3.10. Пример реализации механизма списки прав доступа в ОС MS Windows XP

Каждая запись управления доступом (ACE) состоит из идентификатора пользователя или группы пользователей и совокупности разрешенных методов доступа. При принятии решения о предоставлении доступа к объекту в ОС семейства MS Windows NT записи управления доступом обрабатываются с учетом иерархической структуры каталогов следующим образом ([12, 13]):

- система сравнивает идентификатор пользователя, запросившего доступ к объекту, а также идентификаторы всех групп, к которым он принадлежит, с идентификаторами, присутствующими в ACL объекта. Если в ACL отсутствует упоминание идентификаторов пользователя и его групп, то доступ запрещается;
- если идентификаторы присутствуют в ACL, то сначала обрабатываются ACE типа Denied (по запрещенным методам доступа). Для всех записей ACE типа Denied, идентификатор которых совпадает с идентификатором пользователя или его групп, запрашиваемый метод доступа сравнивается с указанным в ACE. Если метод (чтение, запись и т.д.) присутствует в ACE данного типа, то доступ запрещается, и дальнейшая обработка по данному методу не производится, и ACE типа Allowed не анализируются;

- если система не обнаруживает запрета на доступ по запрашиваемому методу в ACE типа Denied, она осуществляет анализ ACE типа Allowed (по разрешенным методам доступа). Для всех записей, имеющих тип Allowed, запрашиваемый метод доступа также сравнивается с указанным в ACE. По результатам сравнения отмечается, какие методы запрашиваемого доступа разрешены;
- если все методы доступа, которые указаны в запросе, встретились в ACE типа Allowed и не были обнаружены в ACE типа Denied, то запрашиваемый пользователем доступ будет удовлетворен системой полностью. В противном случае доступ разрешается только по тем методам, которые не запрещены в ACE типа Denied и разрешены в ACE типа Allowed [10].

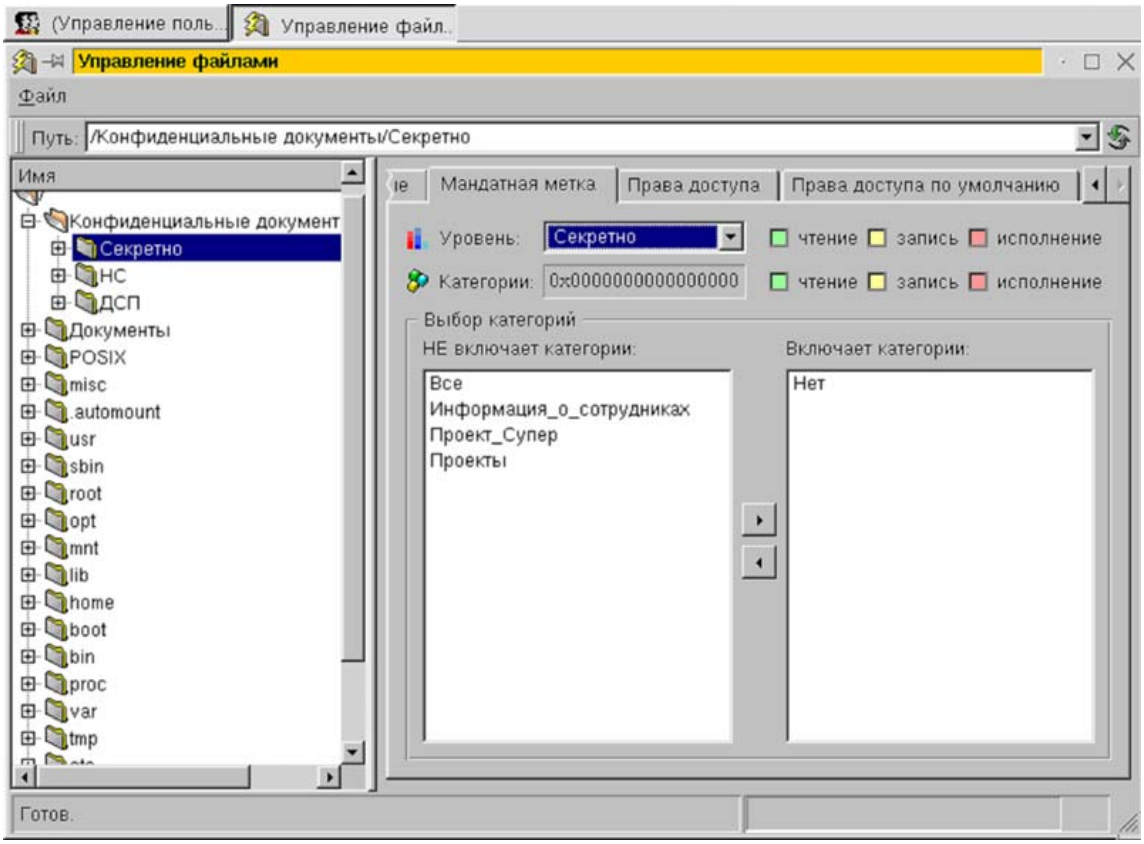


Рис. 3.11. Пример категорирования каталогов по уровню конфиденциальности в ОС семейства Linux

Многоуровневая (мандатная, полномочная) модель разграничения доступа подробно описана в [11, 13–17]. Мандатная модель предполагает категорирование объектов доступа по уровню конфиденциальности (рис. 3.11), а субъектов — по степени (уровням) допуска (рис. 3.12).

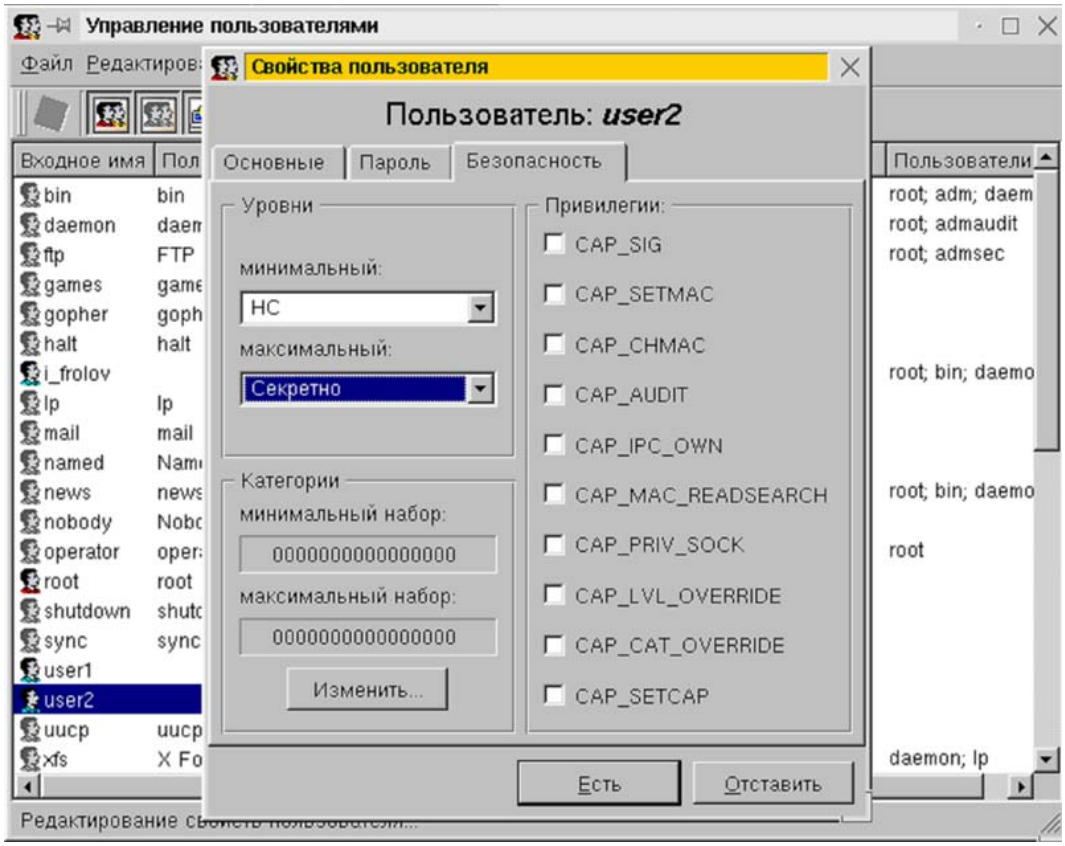


Рис. 3.12. Пример категорирования пользователей ОС семейства Linux по уровням допуска

Мандатная модель разграничения доступа обычно применяется в совокупности с дискреционной. Различают два способа реализации мандатной модели: с контролем информационных потоков и, более простой, без контроля потоков, который на практике встречается крайне редко. Правила мандатной модели разграничения доступа с контролем информационных потоков формулируются следующим образом [13].

1. У любого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать (или разрешать) доступ других субъектов к данному объекту.
3. Для каждой четверки субъект-объект-метод-процесс возможность доступа определена *однозначно в каждый момент времени.*
4. Существует хотя бы один привилегированный пользователь, имеющий возможность удалить любой объект.
5. Во множестве объектов выделяются множества объектов полномочного разграничения доступа. Каждый объект имеет свой уровень конфиденциальности.
6. Каждый субъект имеет уровень допуска.
7. Запрет чтения вверх (Not Read Up — NRU): запрет доступа по методу «чтение», если уровень конфиденциальности объекта выше уровня допуска субъекта, осуществляющего запрос.
8. Каждый процесс имеет уровень конфиденциальности, равный максимуму из уровней конфиденциальности объектов, открытых процессом.

9. Запрет записи вниз (Not Write Down — NWD): запрет доступа по методу «запись», если уровень конфиденциальности объекта ниже уровня конфиденциальности процесса, осуществляющего запрос.
10. Понизить гриф секретности объекта может субъект, который имеет доступ к объекту (по правилу 7) и обладает специальной привилегией.

Основная цель, которая достигается применением мандатной модели разграничения доступа с контролем информационных потоков, — это предотвращение *утечки информации* определенного уровня конфиденциальности к субъектам, чей уровень допуска ниже. Как известно, распространенные операционные системы не обеспечивают безопасности обрабатываемых данных на уровне приложений. Виной тому особенности механизма распределения памяти, использование буфера обмена данных, применение «свопирования» памяти, файлов подкачки и специфика самих приложений. Все это неизбежно приводит к тому, что при одновременной обработке файлов, имеющих различный уровень конфиденциальности, оберегаемая конфиденциальная информация или ее фрагменты могут попадать в документы с меньшим уровнем конфиденциальности. Неконтролируемое проникновение информации из одного документа в другой (с меньшим уровнем конфиденциальности) и принято называть ее утечкой. Выполнение 7, 8 и 9-го правил многоуровневой модели разграничения доступа гарантирует отсутствие утечки конфиденциальной информации.

Мандатная модель разграничения доступа *должна быть использована*, согласно руководящим документам Гостехкомиссии России [5, 6], в автоматизированных системах, начиная с класса 1В, предполагающего возможность обработки информации, составляющей государственную тайну. Таким образом, для обработки информации, составляющей государственную тайну в автоматизированных системах, в которых одновременно обрабатывается и (или) хранится информация различных уровней конфиденциальности, необходимо использовать компьютерные системы, в которых в обязательном порядке реализована мандатная модель разграничения доступа.

В широко распространенных ОС семейства MS Windows NT и Unix-подобных ОС реализована только дискреционная модель. Следовательно, для распространенных ОС, при условии обработки информации, составляющей государственную тайну, необходимо применение дополнительных средств, реализующих мандатную модель разграничения доступа. Программно-аппаратные средства защиты информации «Страж NT», «Dallas Lock», «Secret Net 2000» и «Аккорд-АМДЗ», обсуждаемые в данном пособии, являются надстройкой над существующей программной средой АС и предназначены, в частности, для внедрения мандатной модели в системы, работающие под управлением ОС семейства MS Windows NT.

Совокупность дискреционной и мандатной моделей разграничения доступа позволяет организовать выполнение сформулированного в п.1.1 требования 4: пользователи должны получать доступ только к той информации и с теми возможностями по ее обработке, которые соответствуют их функциональным обязанностям.

В дополнение к дискреционной и мандатной моделям в защищенных многопользовательских АС должен применяться режим изолированной или замкнутой программной среды. Данный режим целесообразно задействовать в тех случаях, когда для обработки информации применяется определенный перечень программных продуктов, и политикой безопасности запрещается использование других программ в целях, не имеющих отношение к выполнению функциональных обязанностей пользователями (см. требование 5). Также этот метод обеспечивает защиту компьютера от создания и запуска на нем вредоносного программного кода.

Суть метода заключается в том, что для каждого пользователя формируется перечень исполняемых файлов, которые могут быть им запущены. Реализация метода часто осуществляется формированием для каждого пользователя списка имен исполняемых файлов, иногда без указания полного пути. В более качественных системах для каждого исполняемого файла указывается признак возможности его запуска тем или иным пользователем. В том и в другом случаях целесообразно осуществлять проверку целостности исполняемых файлов при каждом их запуске.

Разграничение доступа пользователей к данным, программам и устройствам АИС является одним из важнейших методов обеспечения защиты информации и обеспечивает выполнение 2, 4–8 требований, приведенных в п. 1.1. пособия. Совместно с контролем целостности программного обеспечения (см. ниже) режим замкнутой программной среды обеспечивает «чистоту» компьютерной системы и затрудняет запуск в АИС вредоносных программ.

3.1.4. Регистрация событий (аудит)

Регистрация событий или аудит событий безопасности — фиксация в файле-журнале событий, которые могут представлять опасность для АС.

Регистрация событий как механизм защиты предназначена для решения двух основных задач: расследование инцидентов, произошедших с применением АС, и предупреждение компьютерных преступлений. При этом вторая задача может по степени важности выйти на первое место — если недобросовестный сотрудник организации знает о том, что все его действия в АС протоколируются, он воздержится от совершения действий, которые не входят в круг его функциональных обязанностей.

В связи с тем, что журналы аудита событий используются при расследовании происшествий, должна обеспечиваться полная объективность информации, фиксируемой в журналах. Для обеспечения объективности необходимо выполнение следующих требований к системе регистрации событий:

- только сама система защиты может добавлять записи в журнал;
- ни один субъект доступа, в том числе сама система защиты, не имеет возможности редактировать отдельные записи;
- в АС кроме администраторов, регистрирующих пользователей и устанавливающих права доступа, выделяется дополнительная категория — аудиторы;

- только аудиторы могут просматривать журнал;
- только аудиторы могут очищать журнал;
- полномочия администратора и аудитора в рамках одного сеанса несовместимы;
- при переполнении журнала система защиты аварийно завершает работу.

Средствами ОС семейства MS Windows NT могут регистрироваться следующие категории событий (рис. 3.13):

- вход/выход пользователей из системы;
- изменение списка пользователей;
- изменения в политике безопасности;
- доступ субъектов к объектам;
- использование опасных привилегий;
- системные события;
- запуск и завершение процессов.

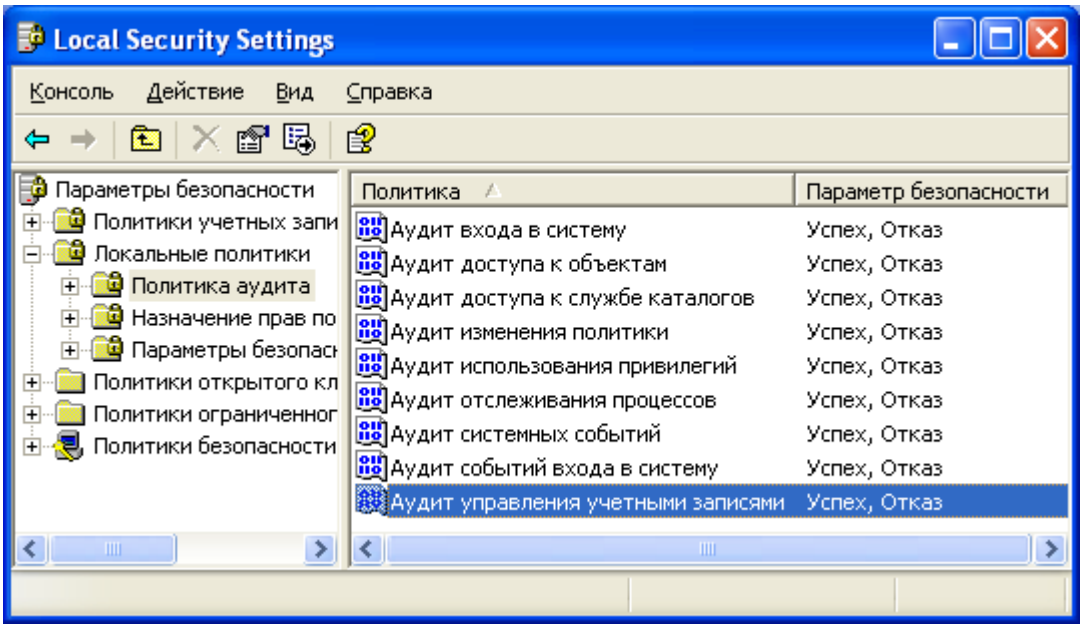


Рис. 3.13. Пример настройки политики аудита в ОС MS Windows XP

Вместе с тем при определении количества регистрируемых событий, следует вести речь об адекватной политике аудита, т. е. такой политике, при которой регистрируются не все возможные категории событий, а только действительно значимые и необходимые.

Так, на примере операционных систем семейства MS Windows NT, можно сформулировать следующую адекватную политику аудита [13, 16] (рис. 3.14):

- вход и выход пользователей регистрировать всегда;
- доступ субъектов к объектам регистрировать только в случае обоснованных подозрений злоупотребления полномочиями;
- регистрировать применение опасных привилегий;

- регистрировать только успешные попытки внесения изменений в список пользователей;
- регистрировать изменения в политике безопасности;
- не регистрировать системные события;
- не регистрировать запуск и завершение процессов, кроме случая обоснованных подозрений, например, вирусных атак.

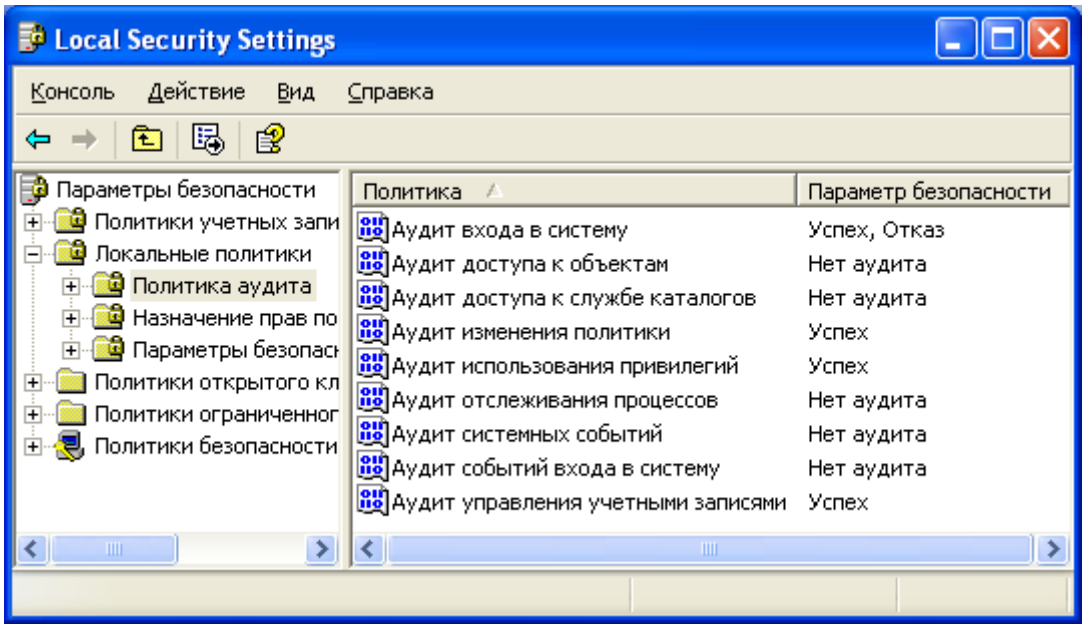


Рис. 3.14. Пример настройки адекватной политики аудита в ОС MS Windows XP

Механизм защиты *регистрация событий* позволяет организовать выполнение сформулированного в п.1.1 требования 8: в целях профилактики и расследования возможных инцидентов автоматически должна вестись регистрация в специальных электронных журналах наиболее важных событий, связанных с доступом пользователей к защищаемой информации и компьютерной системе в целом. Специальным образом организованная регистрация бумажных документов, распечатываемых в АИС, гарантирует выполнение требования 9.

3.2. Модель защищенной компьютерной системы

Для построения модели защищенной компьютерной системы, отвечающей перечисленным в главе 1 требованиям, рассмотрим некое предприятие НПО «Сигма», ведущее разработку проектно-конструкторской документации по различным инженерным направлениям. Несколько не связанных между собой групп специалистов ведут разработку самостоятельных инженерных проектов «Луна-1», «Юпитер-9», «Полет» и т. д. Сами проекты являются конфиденциальными программами (конфиденциальная информация — информация, требующая защиты [5]), а их документация — охраняемыми данными.

Рис. 3.15. Структура каталогов компьютерной системы предприятия

Документация проектов представляет собой ряд текстовых и графических электронных документов, обрабатываемых в единой компьютерной системе и имеющих различный уровень конфиденциальности: «открытые данные», «конфиденциально» и «строго конфиденциально». Уровней конфиденциальности может быть и больше: «ограниченного доступа», «особо конфиденциально» и т. д. Система уровней конфиденциальности определяется градацией информационных ресурсов в зависимости от величины и характера (качества) ущерба при неограниченном распространении соответствующей информации. В СЗИ различных производителей уровни конфиденциальности имеют различное наименование. Так, «открытые данные» иногда именуют «несекретными» или «общедоступными»; «конфиденциальные» называют «ДСП», «служебная тайна» или «конфиденциальные документы»; «строго конфиденциальные документы» — «секретными». В дальнейшем в пособии для обозначения уровней конфиденциальности будем пользоваться терминами «Несекретно», «ДСП», «Секретно» (рис. 3.15).

К документации каждого из инженерных проектов имеют доступ конкретные сотрудники предприятия, которые в рамках соответствующих проектов имеют различные уровни допуска к информации.

Руководит предприятием «Сигма» Клинов А.В., он имеет максимальный уровень допуска к информации и возможность работы с документацией любого проекта. Экономист Ювченко А.Н. работает над проектом «Продажи». Администратор компьютерной системы (администратор безопасности) Чистяков А.В. имеет полный доступ к любым документам, имеет возможность

управлять настройками компьютерной системы и реализует на практике политику безопасности предприятия, в части, касающейся информационных технологий. Для удобства работы всех пользователей АС в ее состав включена база данных, содержащая нормативно-правовые документы, требования ЕСПД, технические справочники. Администратор следит за состоянием базы данных, своевременно обновляет ее. Руководитель предприятия издает приказы и указания и размещает их в электронном виде в соответствующем каталоге. Сотрудники предприятия могут беспрепятственно знакомиться с содержимым базы данных и распоряжениями руководителя предприятия, копировать необходимую им информацию, но вносить изменения в эти каталоги они не имеют право.

Пусть к документации проекта «Полет» имеют доступ инженеры Свалов А.В., Савин П.А. и Соколов С.Ю., имеющие уровни допуска к секретной, ДСП, и несекретной информации соответственно (табл. 2.1).

Таблица 2.1

Уровни допуска сотрудников

Уровень допуска	Сотрудники
Несекретно	С.Ю. Соколов
ДСП	П.А. Савин, А.Н. Ювченко
Секретно	А.В. Свалов, А.В. Клинов, А.В. Чистяков

В зависимости от своих функциональных обязанностей сотрудники могут осуществлять различные действия с документами проекта (защищаемыми данными): редактировать, просматривать, удалять, копировать, распечатывать. В общем случае специалисты организации одновременно могут работать над несколькими проектами, но в нашем примере инженеры Свалов, Савин и Соколов заняты только проектом «Полет» и только к нему имеют доступ. В то же время они выполняют весь необходимый объем работы по данному проекту, поэтому доступ остальных инженеров предприятия к его документации запрещен. Для предварительной проработки проектной документации инженеры могут создавать черновики документов. Черновики создаются в специальном каталоге для индивидуального пользования, они доступны только авторам, администратору и руководителю предприятия.

Права доступа сотрудников к документации предприятия разрешенного уровня конфиденциальности находят свое отражение в матрице доступа, которая вместе с установленной системой допусков и уровней конфиденциальности информационных ресурсов формализует политику разграничения доступа. Возможный вариант матрицы, приведен в табл. 2.2, где буквой «П» обозначен тип доступа *полный доступ*, буквой «Ч» — *только чтение*, пробелом — *запрет доступа*.

Предполагается, что администратор системы Чистяков и руководитель предприятия Клинов имеют допуск в систему в любой день недели с 7.00 до 23.00. Остальные сотрудники могут регистрироваться в системе только в рабочие дни с 8.30 до 17.30.

Далее в пособии приводятся рекомендации по применению различных СЗИ для построения и эксплуатации защищенной компьютерной системы, базирующейся на предложенной политике безопасности, выполняющей перечисленные в главе 1 требования и использующей описанные методы защиты информации.

По каждому из СЗИ от НСД читателю предлагается реализовать предложенную политику безопасности на примере НПО «Сигма» и последовательно применить методы защиты:

- идентификацию и аутентификацию пользователей, создавая требуемые учетные записи и назначая им пароли;
- разграничение доступа, реализовывая мандатную и дискреционную модели, а также принцип замкнутой программной среды;
- контроль целостности, включая подсистемы контроля целостности для защиты конфиденциальных данных от несанкционированной модификации;
- регистрацию событий, настраивая политику аудита для выявления наиболее опасных действий нарушителя;
- уничтожение остаточной информации, выполняя гарантированное удаление конфиденциальных данных.

При изучении СКЗИ читателю предлагается применить метод криптографической защиты конфиденциальных данных путем создания защищенных виртуальных логических дисков.

Таблица 2.2

Матрица доступа предприятия

Каталог	Соколов (инженер)	Савин (инженер)	Свалов (инженер)	Чистяков (администра-тор)	Ювченко (экономист)	Клинов (начальник)
С:\Экономика\Канцелярские товары (НС)				П	П	П
С:\ Экономика\Продажи (ДСП)				П	П	П
С:\ Приказы и распоряжения	Ч	Ч	Ч	П	Ч	П
С:\ База данных (Консультант Плюс)	Ч	Ч	Ч	П	Ч	Ч
С:\Проекты\Полет\ Графические докумен-ты\Несекретно	П	П	П	П		П
С:\Проекты\Полет\ Графические документы\ДСП		П	П	П		П
С:\Проекты\Полет\ Графические докумен-ты\Секретно			П	П		П
С:\Проекты\Полет\ Текстовые докумен-ты\Несекретно	П	П	П	П		П
С:\Проекты\Полет\ Текстовые документы\ДСП		П	П	П		П
С:\Проекты\Полет\ Текстовые докумен-ты\Секретно			П	П		П
С:\Проекты\Полет\ Черновики\Соколов	П			П		П
С:\Проекты\Полет\ Черновики\Савин		П		П		П
С:\Проекты\Полет\ Черновики\Свалов			П	П		П

3.3. Система защиты информации от несанкционированного доступа «Страж NT»

3.3.1. Общие сведения

СЗИ «Страж NT» версии 2.5 (разработчик ЗАО НПЦ «Модуль») представляет собой программно-аппаратный комплекс, способный работать в среде операционных систем фирмы Microsoft Windows NT 4.0, Windows 2000, Windows XP и Windows 2003 и добавляющий к системе безопасности ОС следующие функциональные возможности:

1. Организация доверенной загрузки с возможностью идентификации и аутентификации пользователей при помощи дискет, устройств iButton, USB-ключей eToken R2, eToken Pro, Guardant;
2. Реализация мандатной модели разграничения доступа на основе меток конфиденциальности пользователей, защищаемых ресурсов и прикладных программ;
3. Создание замкнутой программной среды для пользователей путем разрешения запуска ограниченного количества прикладных программ и динамических библиотек;
4. Контроль потоков защищаемой информации;
5. Очистка освобождаемой памяти и дискового пространства;
6. Контроль целостности указанных администратором файлов;
7. Аудит доступа к защищаемым ресурсам;
8. Управление вводом-выводом на отчуждаемые носители.

3.3.2. Запуск и регистрация в системе защиты

Установка системы защиты должна производиться пользователем из группы администраторов. Политикой безопасности предприятия должен быть предусмотрен один привилегированный пользователь (Чистяков А.В.), выполняющий обязанности системного администратора и администратора безопасности. В соответствии с разработанной политикой безопасности установку СЗИ «Страж NT» должен производить именно этот пользователь. Целесообразно использовать в качестве учетной записи Чистякова встроенную учетную запись Администратора. Таким образом, после инсталляции системы защиты, администратор получит неограниченные права по настройке и управлению как СЗИ, так и операционной системой. Перед инсталляцией необходимо убедиться, что пароль Администратора не содержит символов кириллицы и специальных знаков, а его длина не превышает 14 символов.

Установка системы производится стандартным образом. В ходе установки необходимо ввести лицензионный номер. После завершения копирования файлов на жесткий диск будет предложено выбрать тип используемого персонального идентификатора и ввести пароль администратора безопасности, после чего будет создан его персональный идентификатор, для чего потребуется «чистый» идентификатор, например, отформатированная дискета.

Практическое освоение средства защиты информации «Страж NT» (и всех последующих, см. Приложение) осуществляется с предварительно установленном экземпляром СЗИ в виде образа системы VMware, в котором по умолчанию имеется только один пользователь – «Администратор». Поскольку у многих современных компьютеров дисковод для флоппи-дисков просто отсутствует, в качестве ключевой дискеты при работе с СЗИ «Страж NT» следует использовать ее электронный образ, хранящийся в одном каталоге вместе с образом самой системы в виде файла с именем «дискета».

Для реализации функций защиты в СЗИ «Страж NT» необходимо настроить BIOS ПЭВМ на загрузку с жесткого диска, а также установить пароль на изменение параметров BIOS, чтобы эти настройки не могли быть модифицированы пользователями, в противном случае становится возможна загрузка ПК со съемного носителя. Если требуемые установки BIOS не выполнены, СЗИ при запуске системы выведет соответствующее сообщение и приостановит ее дальнейшую работу.

В СЗИ «Страж NT» идентификация и аутентификация пользователя производится до загрузки операционной системы. Это позволяет исключить возможность получения доступа к информации, содержащейся на жестком диске компьютера, не пройдя успешно процедуру аутентификации. Процедура идентификации предполагает сравнение информации, содержащейся на энергонезависимом носителе ключевой информации (дискете), с информацией, записанной на жестком диске компьютера.

Программа идентификации и аутентификации записана в главной загрузочной записи (MBR) жесткого диска и вызывается автоматически после прохождения процедуры POST BIOS: пользователю предлагается предъявить персональный идентификатор и ввести пароль.

Модификация главной загрузочной записи, выполняемая СЗИ при его инициализации, предотвращает попытки НСД при загрузке компьютера с внешнего носителя, так как любая операционная система «повиснет» при попытке монтирования раздела, на котором установлена СЗИ «Страж NT». Таким образом, для злоумышленника исключается несанкционированный доступ к содержимому жесткого диска, несмотря на гипотетическую возможность загрузки ПЭВМ с внешнего носителя или подключения НЖМД к другому ПК.

ВЫПОЛНИТЬ!

1. Зарегистрироваться в системе пользователем Администратор, предъявив при включении компьютера (перезагрузке) ключевую дискету[1] и введя пароль «12345».
2. Попытаться загрузить компьютер без ключевой дискеты, затем вставить дискету и три раза подряд неправильно ввести пароль. Какова реакция СЗИ «Страж NT»?

[1] В VMware чтение дискеты будет осуществляться автоматически при загрузке операционной системы, если в свойствах образа ОС заранее указан образ дискеты.

3.3.3. Создание пользователей

В «Страж NT» возможны две стратегии создания учетных записей пользователей. Первая предполагает создание всех требуемых пользователей до установки СЗИ, а вторая – создание пользователей после установки средства защиты. После установки СЗИ все операции по созданию и удалению пользователей, а также по назначению им прав доступа производятся Администратором безопасности с использованием «Менеджера пользователей» программы «Управление СЗИ», которая вызывается командой ***Пуск ⇒ Программы ⇒ Страж NT ⇒ Управление СЗИ***. Менеджер пользователей (рис. 3.16) открывается командой меню ***Администрирование ⇒ Менеджер пользователей***. В случае создания пользователей до установки СЗИ (штатными средствами ОС Windows) после установки необходимо установить уровни допуска для каждого из пользователей, задать пароли и создать персональные идентификаторы (сформировать носители ключевой информации).

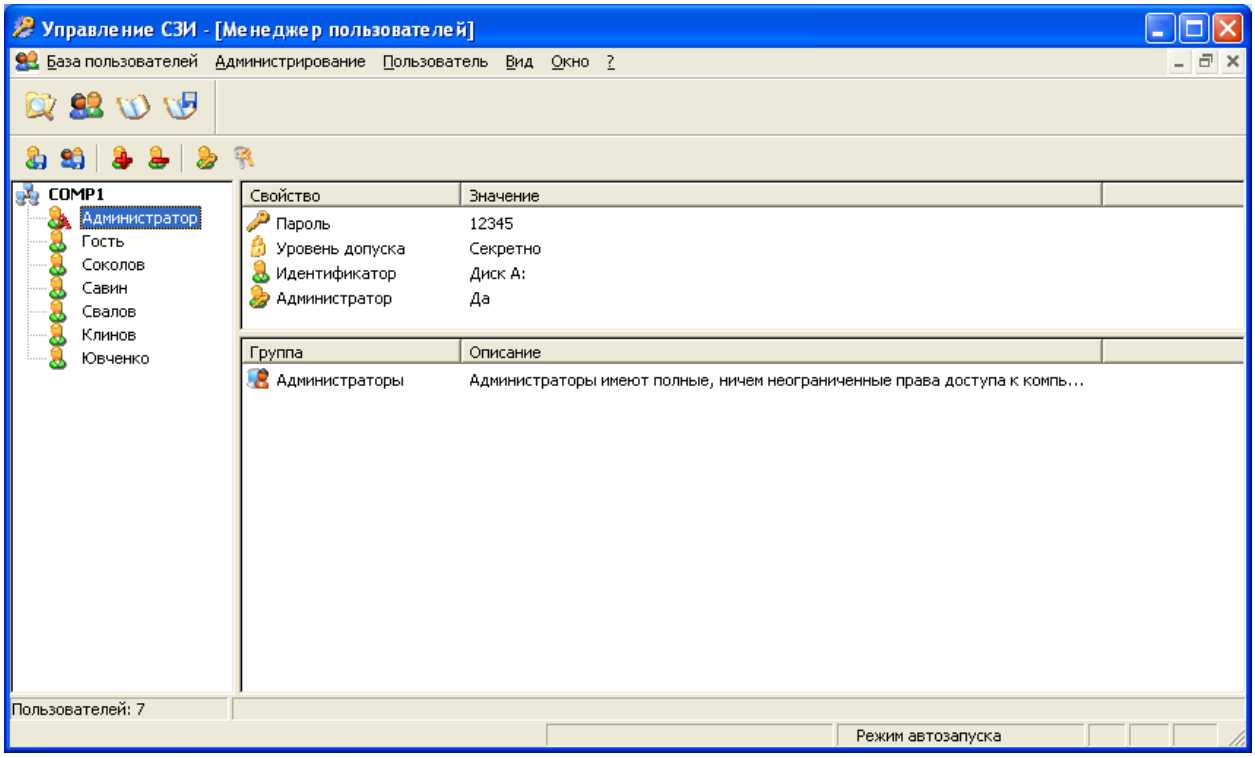


Рис. 3.16. Менеджер пользователей

В рассматриваемом примере построения защищенной системы учетные записи пользователей будут создаваться после установки СЗИ. Чтобы создать учетную запись с использованием «Менеджера пользователей», необходимо выполнить команду меню ***Пользователь ⇒ Добавить пользователя***, после чего ввести имя вновь создаваемого пользователя. В правой верхней части окна отображается информация о выделенной учетной записи. Чтобы задать для нее пароль, необходимо щелкнуть на поле «Значение» строки «Пароль», а затем ввести новый пароль и подтвердить его.

Внимание! При вводе пароля его значение отображается на мониторе в открытом виде (в том числе у Администратора), поэтому существует повышенная опасность его подсматривания, в том числе преднамеренного.

Любые изменения в параметрах учетной записи пользователя необходимо сохранять. Пиктограмма учетной записи пользователя, параметры которой изменились, становится красной и сдвигается вправо (рис. 3.17). Для сохранения параметров нужно выполнить команду меню ***База пользователей ⇒ Сохранить*** или выбрать «Сохранить» из контекстного меню, появляющегося при щелчке правой клавишей мыши на имени пользователя.

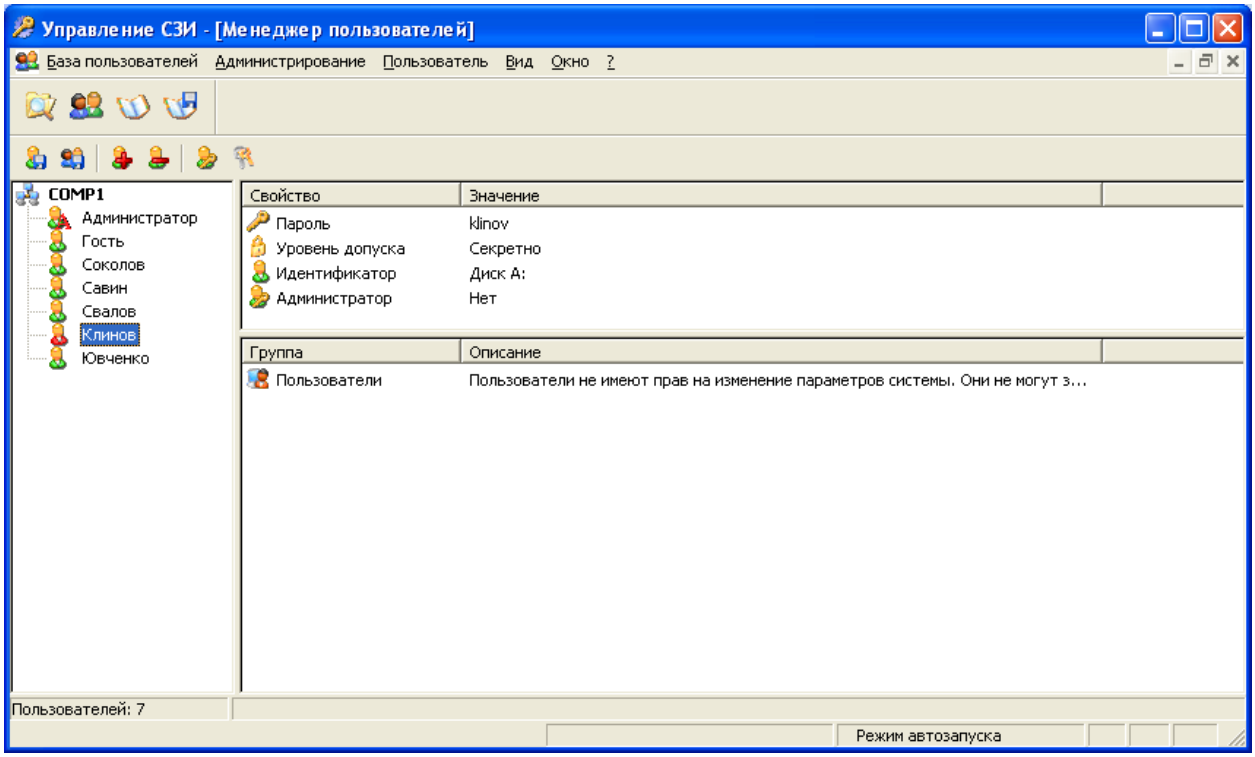


Рис. 3.17. Настройки учетной записи изменены

К сожалению, зарегистрироваться вновь созданным пользователем не удастся, так как личные каталоги пользователей создаются в Windows *после* первой регистрации пользователя в системе, а «Страж NT» бдительно охраняет каталог Documents and Settings от записи. Чтобы обеспечить возможность создания этих каталогов, необходимо временно приостановить работу механизмов защиты СЗИ «Страж NT», а затем зарегистрироваться новым пользователем в системе, не перезагружая компьютер. Остановка механизмов защиты делается выбором пункта меню «Останов» при нажатии правой кнопкой мыши на иконке СЗИ «Страж NT» в системном трее и действует до следующей перезагрузки компьютера либо до выбора пункта меню «Запуск» там же. Рекомендуется сначала создать всех пользователей, приостановить механизмы защиты, а после этого последовательно зарегистрироваться в системе от имени всех вновь созданных пользователей. Все эти действия может и должен выполнить Администратор системы.

После того как учетные записи всех пользователей созданы, необходимо сформировать персональные идентификаторы для каждого из них. Это действие выполняется также с использованием «Менеджера пользователей». Программа «Управление СЗИ» должна находиться в режиме администрирования (команда меню ***Администрирование ⇒ Режим администрирования***). Чтобы создать персональный идентификатор, необходимо выбрать пользователя, а затем выполнить команду меню ***Пользователь ⇒ Сформировать идентификатор***… Система защиты попросит вставить персональный идентификатор Администратора, затем создать список доступных пользователю компьютеров, и после поместить «чистый» носитель, на который будет записана уникальная ключевая информация, и идентификатор пользователя будет создан.

Внимание! Изменение уровня допуска пользователя или его пароля требуют повторного создания персональных идентификаторов.

ВЫПОЛНИТЬ!

3. Создать учетные записи пользователей и назначить им уровни допуска в соответствии с табл. 2.1. Пароли выбрать произвольно. Приостановить функционирование механизмов защиты выбором пункта меню «Останов» при нажатии правой кнопкой мыши на иконке СЗИ «Страж NT» в системном трее. Последовательно зарегистрироваться в системе всеми пользователями.

3.3.4. Реализация мандатной модели разграничения доступа

Мандатная модель разграничения доступа в СЗИ «Страж NT» реализована посредством назначения защищаемым ресурсам, каждому пользователю системы и прикладным программам меток конфиденциальности и сопоставления их при запросах на доступ. В качестве меток конфиденциальности выступают:

- для защищаемых ресурсов — гриф;
- для пользователей — уровень допуска;
- для прикладных программ — допуск и текущий допуск.

В СЗИ «Страж NT» по умолчанию используются следующие наименования меток конфиденциальности в порядке повышения: несекретно, секретно, совершенно секретно. Чтобы изменить наименования меток (если это не было сделано на этапе установки СЗИ), необходимо, зарегистрировавшись Администратором безопасности, запустить программу настройки СЗИ (***Пуск ⇒ Программы ⇒ Страж NT ⇒ Настройка системы защиты***) и отметить пункт «Изменить наименования меток конфиденциальности информации» (рис. 3.18). После нажатия кнопки «Далее» будет предложено ввести наименования меток конфиденциальности.

Настройка системы защиты в части реализации мандатной модели разграничения доступа заключается в выполнении следующих действий:

- в соответствии с политикой безопасности назначить каждому пользователю уровень допуска при помощи окна «Менеджер пользователей» программы «Управление СЗИ» (это должно быть сделано на этапе создания пользователей до создания их персональных идентификаторов);
- для прикладных программ, предназначенных для обработки защищаемых ресурсов, разрешить режим запуска (см. ниже) и установить значение допуска при помощи окна «Администратор ресурсов» программы «Управление СЗИ» в (рис. 3.19);
- в соответствии с политикой безопасности определить защищаемые ресурсы и присвоить им гриф секретности также при помощи окна «Администратора ресурсов».

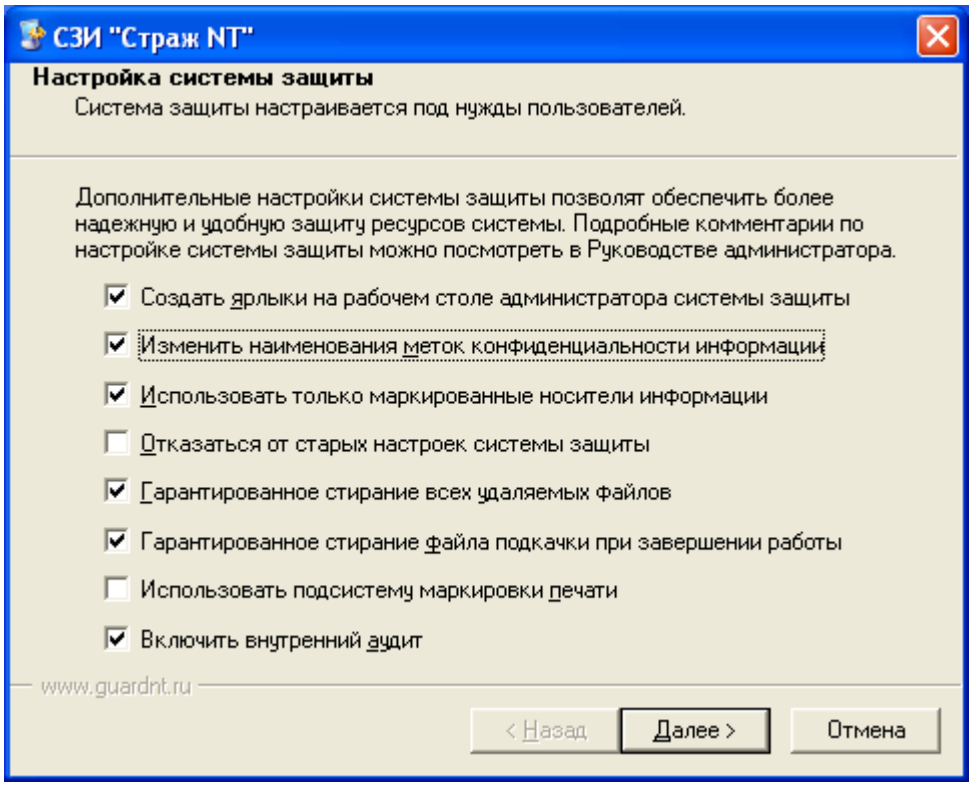


Рис. 3.18. Диалоговое окно «Настройка системы защиты»

«Администратор ресурсов» открывается из программы «Управление СЗИ» командой меню ***Администрирование ⇒ Администратор ресурсов***. Операции, связанные с изменением прав доступа, могут производиться только в режиме администрирования. Чтобы включить его, необходимо выполнить команду меню ***Администрирование ⇒ Режим администрирования***.

Исходно все объекты, участвующие в процессе мандатного управления доступом, имеют метки конфиденциальности «Несекретно». Метки конфиденциальности можно присваивать как отдельным файлам, так и каталогам. Для установки метки конфиденциальности ресурса необходимо в окне «Администратора ресурсов» щелкнуть правой клавишей мыши на файле или каталоге и в раскрывшемся контекстном меню выбрать пункт «Гриф и режим запуска». Будет открыто диалоговое окно, вид которого показан на рис. 3.20.

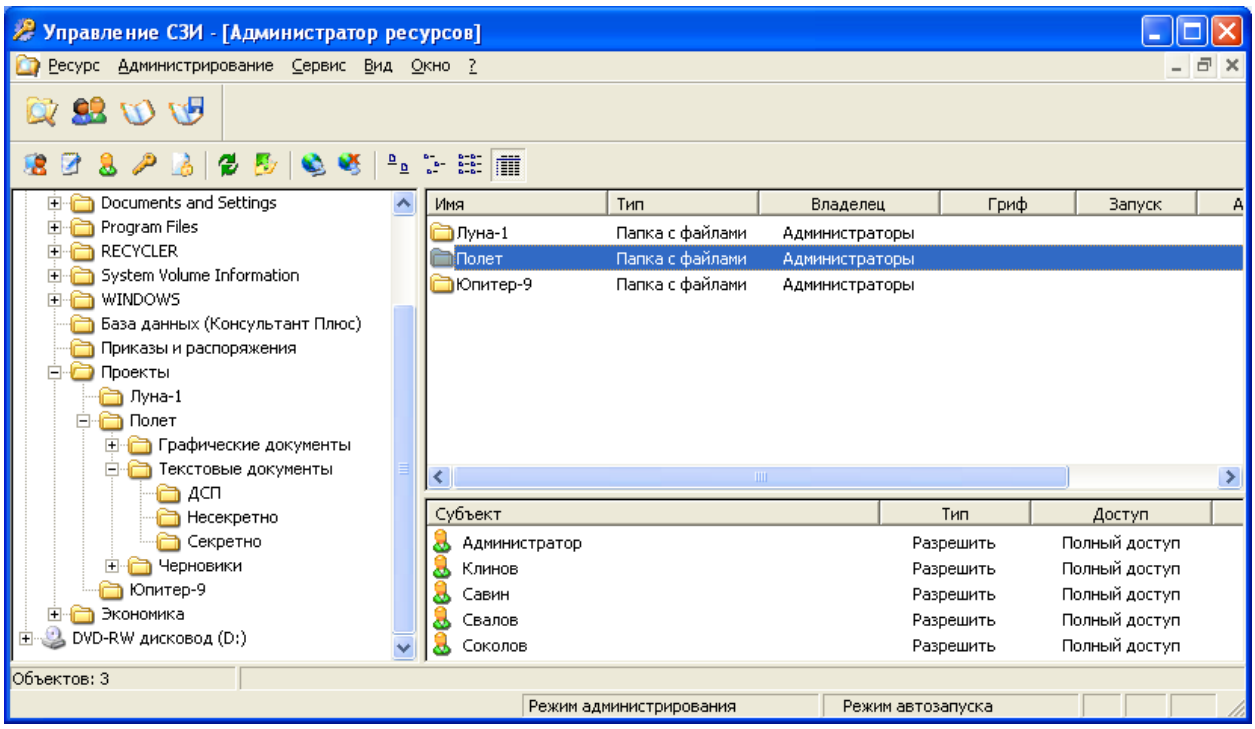


Рис. 3.19. Администратор ресурсов

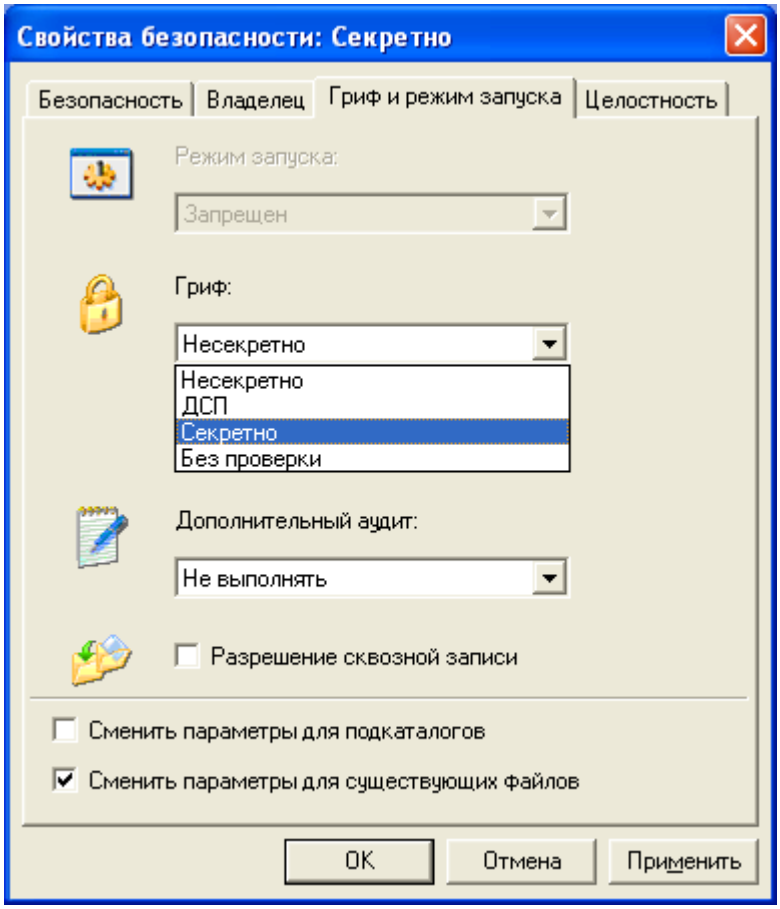


Рис. 3.20. Диалоговое окно «Гриф и режим запуска»

3.3.5. Реализация дискреционной модели разграничения доступа

Дискреционная модель разграничения доступа реализуется посредством списков доступа, которые представляют собой наборы записей, содержащих код субъекта и маску доступа. Маски доступа определяют права доступа субъекта доступа к защищаемым ресурсам. В целом процедура назначения прав доступа посредством списков доступа в СЗИ «Страж NT» совпадает с соответствующей процедурой, осуществляемой штатными средствами Windows NT для файловой системы NTFS. Устанавливать разрешения на доступ можно только в программе «Управление СЗИ» в окне «Администратора ресурсов». Программа должна быть переведена в режим администрирования (***Администрирование ⇒ Режим администрирования***). Диалоговое окно, в котором производится настройка разрешений, можно открыть, щелкнув правой клавишей мыши на пиктограмме соответствующего ресурса и выбрав пункт «Разрешения и аудит» в контекстном меню. Следует отметить отличия в реализации дискреционного принципа контроля доступа по сравнению с ОС Windows NT. Во-первых, если пользователь не имеет разрешений на чтение ресурса, данный ресурс (кроме устройств и портов) становится для него невидимым. Это справедливо и для администраторов системы защиты. Чтобы администратор увидел такие ресурсы, необходимо запустить «Администратор ресурсов» и включить режим администрирования. Во-вторых, эксклюзивными правами на назначение прав доступа к файлам и каталогам обладает только Администратор безопасности (а не создатель-владелец, как в ОС Windows NT).

ВЫПОЛНИТЬ!

4. С помощью «Администратора ресурсов» в режиме администрирования разграничить права доступа пользователей к созданным каталогам в соответствии с табл. 2.2. Зарегистрироваться пользователем Ювченко и просмотреть содержимое каталога «C:\Экономика». Убедиться, что каталог «C:\Проекты» для этого пользователя не отображается.
5. Зарегистрироваться пользователем Свалов и просмотреть содержимое каталога «C:\Проекты\Полет\Текстовые документы\Секретно». Убедиться, что каталог «C:\Экономика» не для него отображается.
6. Создать в каталоге «C:\Приказы и распоряжения» пользователем Клинов короткий текстовый файл «Приказ1.txt» с приказом об увольнении Соколова. Зарегистрироваться Администратором и просмотреть разрешения, которые установлены для вновь созданного файла. Привести эти разрешения в соответствие с разрешениями, установленными для каталога, если они различаются.
7. Убедиться, что Соколов сможет прочитать приказ о своем увольнении, но не сможет изменить его.

3.3.6. Создание замкнутой программной среды

Замкнутость программной среды в СЗИ «Страж NT» обеспечивается путем установки соответствующих разрешений на запуск для исполняемых файлов (прикладных программ). Существует несколько режимов запуска исполняемых файлов, из которых для рядовых пользователей системы наиболее важными являются:

- запрещен – запуск на выполнение запрещен, кроме администратора системы защиты;
- приложение – запуск исполняемого файла разрешен для всех пользователей системы.

Файлы, не имеющие разрешения на запуск, ни при каких условиях не могут быть запущены на выполнение. Разрешение на запуск прикладных программ может производить только Администратор системы защиты. При создании новых исполняемых файлов режим запуска для них устанавливается в значение «запрещен». Файлы, разрешенные на запуск, автоматически становятся доступны только на чтение и выполнение, обеспечивая целостность программной среды.

Кроме того, каждой запущенной программе соответствует текущий допуск, который выбирается пользователем при запуске программы и определяет степень секретности сведений, обрабатывающихся в данный момент. Все документы, сохраняемые программой, имеют гриф, равный текущему уровню допуска в момент сохранения. Увидеть, какой текущий уровень допуска имеет программа, можно в строке заголовка — он отображается в квадратных скобках. Текущий уровень допуска можно изменить, щелкнув на главном меню программы (пиктограмма в левой части строки заголовка), а затем выбрав пункт «Текущий допуск». В открывшемся диалоговом окне необходимо выбрать требуемый уровень допуска, не превышающий уровень допуска текущего пользователя.

Для всех используемых пользователями компьютерной системы программ Администратором должен быть установлен режим запуска «Приложение», а также уровень допуска, соответствующий максимальной степени секретности документов, с которыми разрешено работать данной программе. Это делается в диалоговом окне «Гриф и режим запуска».

Рядовым пользователям запрещен запуск программ, для которых не был установлен соответствующий режим запуска. На пользователей из группы Администраторы данное ограничение не действует, и они вправе запускать любые исполняемые файлы. Изменение файлов, у которых установлен режим запуска «Приложение», запрещено, в том числе Администратору.

ВЫПОЛНИТЬ!

8. С помощью «Администратора ресурсов» создать иерархическую структуру каталогов, как показано на рис. 3.15. Назначить созданным каталогам грифы секретности в соответствии с их названиями.

9. Установить для файла «%SystemRoot%\explorer.exe» режим запуска «Приложение», максимальный уровень допуска и режим запроса текущего уровня допуска «При старте».
10. Установить для файла «%SystemRoot%\system32\notepad.exe» режим запуска «Приложение», максимальный уровень допуска и режим запроса текущего уровня допуска «По умолчанию».
11. Перезагрузить компьютер, зарегистрироваться пользователем Клинов. Далее при загрузке будет выведено диалоговое окно, в котором предлагается выбрать текущий уровень допуска для программы «Проводник». Необходимо выбрать уровень допуска «Секретно». Запустив «Проводник», просмотреть содержимое созданных каталогов. Все ли каталоги отображаются? Можно ли открыть эти каталоги?
12. Выйти из системы и зарегистрироваться пользователем Соколов. В диалоговом окне выбора текущего уровня допуска для программы «Проводник» попытаться выбрать уровень допуска «Секретно». Возможно ли это при условии, что Соколов имеет допуск лишь к несекретным документам? При помощи «Проводника» просмотреть содержимое созданных каталогов. Какие каталоги отображаются?
13. Запустить редактор «Блокнот». Какой текущий уровень допуска имеет программа? Попытаться изменить текущий уровень допуска так, чтобы можно было работать с документами грифа «ДСП». Получилось ли это?
14. Создать короткий текстовый документ «Соколов.txt» и сохранить его в каталоге «C:\Проекты\Полет\Текстовые документы\Несекретно».
15. Зарегистрироваться в системе пользователем Свалов, запустить «Блокнот», установить максимальный текущий допуск («Секретно»), создать короткий текстовый документ «Свалов.txt» и попытаться сохранить его в каталог «C:\Проекты\Полет\Текстовые документы\Несекретно». Получилось ли это? Сохранить документ в каталоге «C:\Проекты\Полет\Текстовые документы\Секретно».
16. Попытаться открыть несекретный документ программой «Блокнот» при установленном уровне допуска «Секретно». Существует ли возможность сделать это?
17. Запустить еще один экземпляр редактора «Блокнот» с текущим уровнем допуска «Несекретно», и попытаться скопировать содержимое из секретного документа в несекретный с использованием команд ***Правка ⇒ Копировать*** и ***Правка ⇒ Вставить***. Получилось ли это? Работает ли обратная операция вставки несекретных сведений в секретный документ?
18. Проверить, может ли пользователь Свалов запустить «Калькулятор» («%SystemRoot%\system32\calc.exe»). Может ли запустить эту программу Администратор? Сделать так, чтобы все пользователи могли запускать «Калькулятор» и использовать его для работы с несекретными данными (установить режим запуска «Приложение» и уровень допуска «Несекретно»).

3.3.7. Контроль целостности

В СЗИ «Страж NT» реализована возможность контроля со стороны Администратора и ограниченно со стороны пользователей фактов изменения наиболее критичных с точки зрения безопасности файлов (как санкционированного, так и нет), для чего предусмотрена функция контроля целостности файлов. Включение контроля осуществляется администратором безопасности с использованием «Администратора ресурсов» программы «Управление СЗИ». Программа должна быть переведена в режим администрирования.

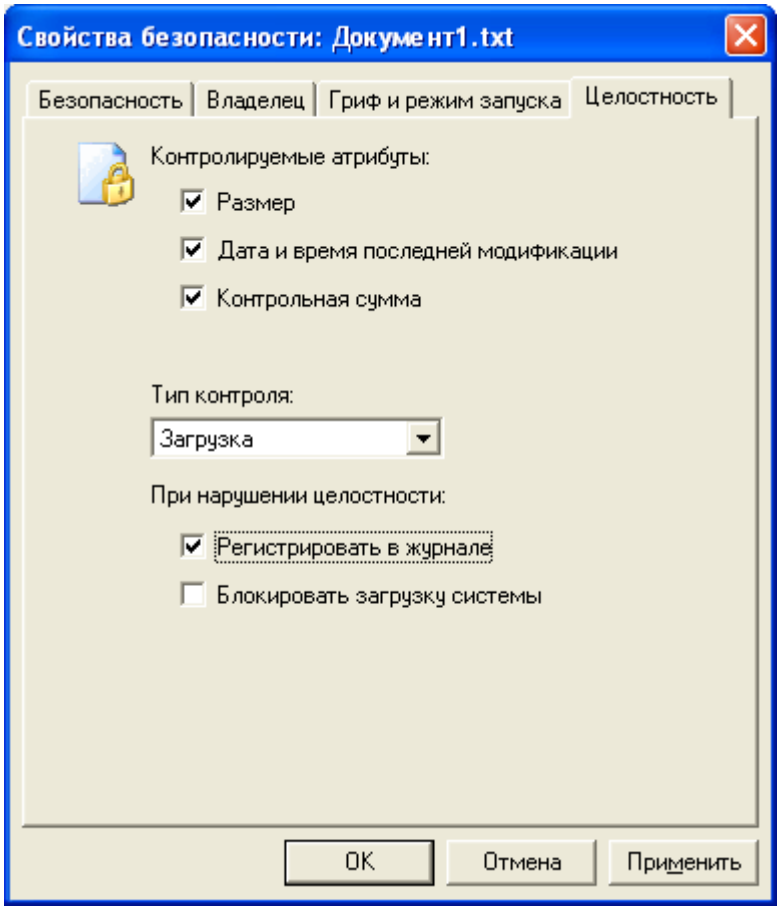


Рис. 3.21. Настройка контроля целостности ресурса

Чтобы вызвать диалоговое окно, в котором производятся настройки контроля целостности файла, нужно выполнить команду меню ***Ресурс ⇒ Целостность*** или воспользоваться контекстным меню. Общий вид диалогового окна, в котором производится настройка, показан на рис. 3.21.

В качестве контролируемых атрибутов могут выступать: размер, дата и время последней модификации, а также контрольная сумма файла. Проверка контролируемых параметров может производиться в нескольких режимах, который можно установит в раскрывающемся списке «Тип контроля»:

- «Загрузка» — при загрузке операционной системы (только для файлов, находящихся на системном диске);
- «Автомат» — при загрузке операционной системы (для любых файлов);

- «Открытие» — при открытии на чтение файла, целостность которого нарушена, выдается ошибка, и файл не открывается.

В режиме «Загрузка» при обнаружении нарушения целостности можно произвести блокировку дальнейшей загрузки ОС для всех пользователей, исключая администратора безопасности. Кроме того, в режимах «Загрузка» и «Автомат» есть возможность регистрации факта нарушения целостности файла в «Журнале регистрации событий» (см. ниже).

ВЫПОЛНИТЬ!

19. Зарегистрироваться в системе пользователем Администратор и настроить контроль целостности всех параметров файла «C:\Проекты\Полет\Текстовые документы\Несекретно\Соколов.txt» в режиме «Автомат» с записью в журнал. Для файла «C:\Проекты\Полет\Текстовые документы\Секретно\Свалов.txt» настроить контроль целостности всех параметров в режиме «Открытие».
20. Выйти из системы и зарегистрироваться пользователем Свалов. Изменить файлы «Соколов.txt» и «Свалов.txt». Перезагрузить компьютер, зарегистрироваться пользователем Клинов. Что происходит при загрузке ОС? Сможет ли пользователь открыть файл «Свалов.txt»?
21. Зарегистрироваться Администратором, открыть «Журнал регистрации событий» в программе «Управление СЗИ» (***Администрирование ⇒ Журнал регистрации событий***) и найти записи журнала, в которых отражено изменение контрольной суммы файла «Соколов.txt». Есть ли возможность установить, какой пользователь изменил файл?
22. Отключить контроль целостности файлов.

3.3.8. Организация учета съемных носителей информации

СЗИ «Страж NT» позволяет ограничивать доступ к съемным носителям информации путем создания списка носителей, разрешенных к использованию. Данный список содержится в «Журнале учета носителей информации», который можно открыть, выбрав пункт меню ***Администрирование ⇒ Журнал учета носителей*** в программе «Управление СЗИ». Учету могут подвергаться гибкие магнитные диски, CD-ROM/RW, DVD-ROM/RW, магнитооптические диски, ленточные носители информации, USB flash-диски, а также съемные жесткие магнитные диски (кроме установленных в Mobile Rack). Общий вид «Журнала учета съемных носителей информации» показан на рис. 3.22.

Чтобы поставить на учет носитель информации, необходимо войти в режим администрирования (***Администрирование ⇒ Режим администрирования***), а затем выбрать пункт меню ***Журнал ⇒ Поставить на учет…*** В открывшемся диалоговом окне (рис. 3.23) необходимо ввести учетный номер носителя, выбрать его тип, метку конфиденциальности и ввести имя ответственного лица.

Чтобы снять носитель с учета, необходимо выбрать его в списке, а затем выбрать пункт меню ***Журнал ⇒ Снять с учета*** либо воспользоваться контекстным меню. Изменения, сделанные в списке учтенных носителей, необходимо сохранять. Это делается командой ***Журнал ⇒ Экспортировать***. Сохранение производится в файле %SystemRoot%\Guard\Guard.car, который, при необходимости, может быть скопирован на другой компьютер, что позволяет организовать единый список учтенных носителей информации в подразделении или на предприятии.

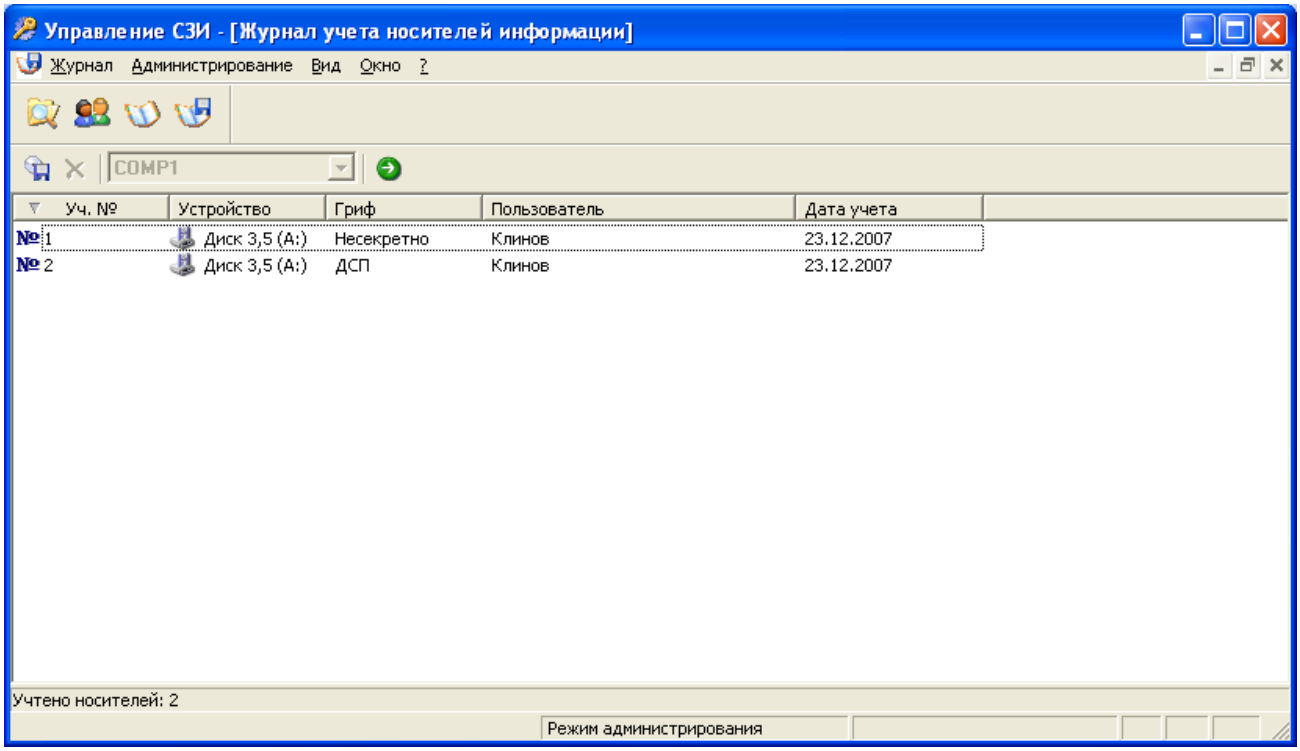


Рис. 3.22. Журнал учета съемных носителей информации

3.3.9. Регистрация событий

СЗИ «Страж NT» позволяет использовать стандартные средства регистрации событий, присутствующие в ОС Windows NT. Кроме того, средствами СЗИ дополнительно реализована автоматическая регистрация следующих событий:

- вход в систему (включение компьютера, аутентификация с использованием носителя ключевой информации);
- попытка запуска неразрешенных на выполнение исполняемых файлов;
- факт нарушения целостности ресурса (при условии, что осуществляется контроль целостности этого ресурса).

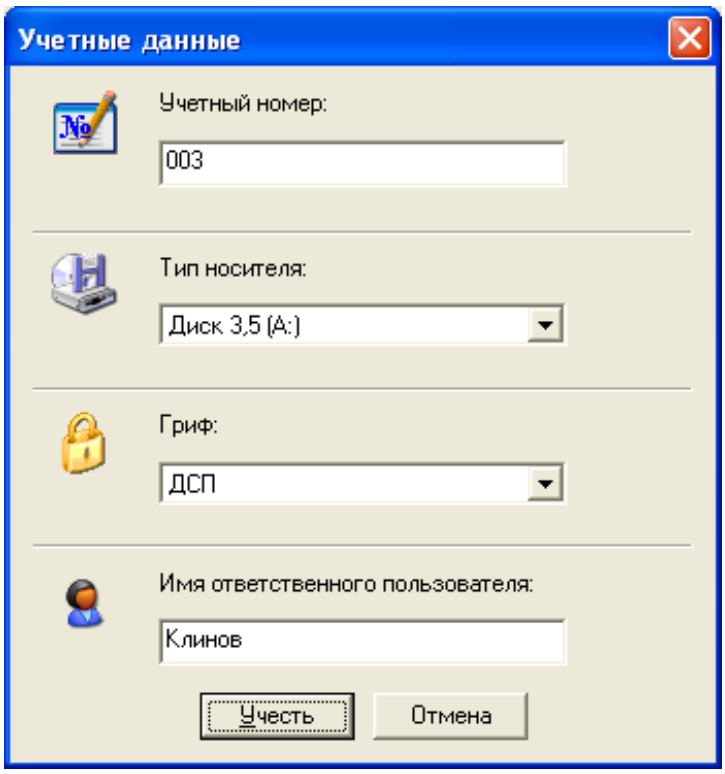


Рис. 3.23. Постановка на учет носителя информации

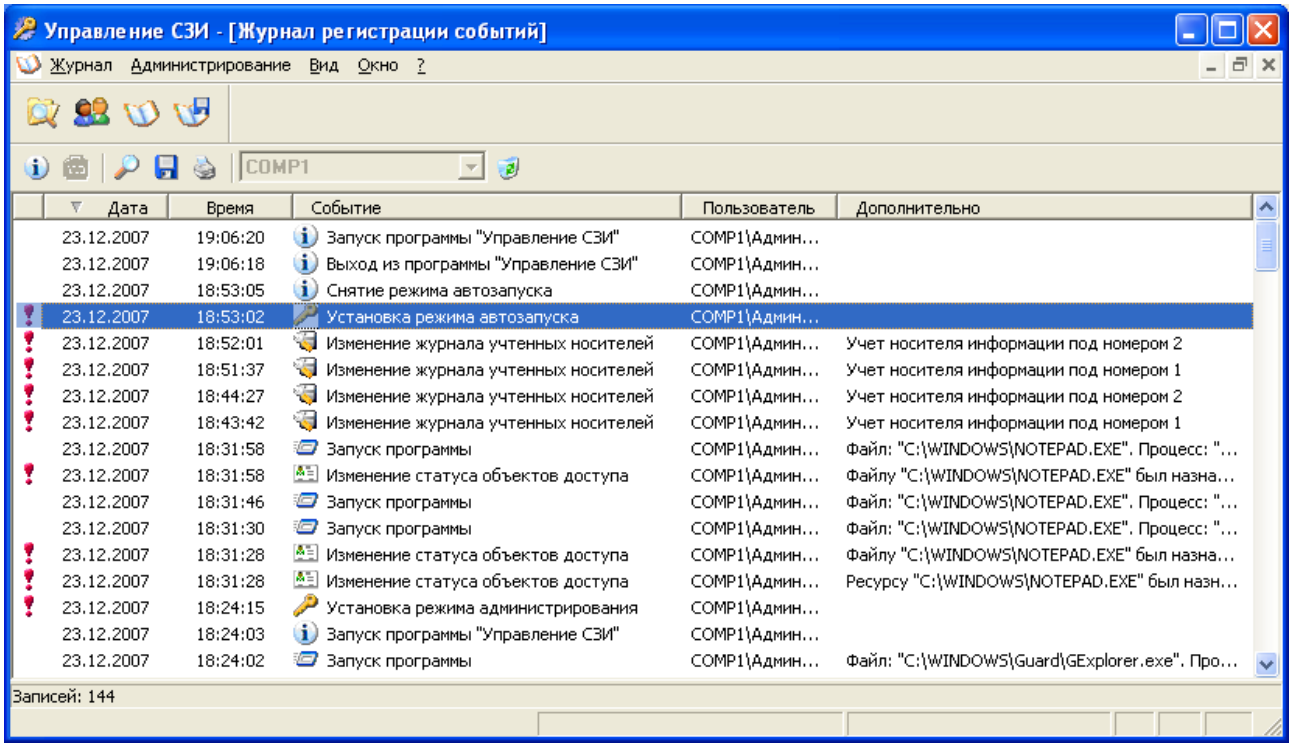


Рис. 3.24. Журнал регистрации событий

Регистрируются также важные с точки зрения безопасности системы действия, выполняемые только пользователем с правами администратора, например такие, как:

- включение режима администрирования;
- изменение грифа ресурсов;
- назначение допуска пользователей;
- изменение паролей пользователей;
- очистка журнала регистрации событий.

Сведения об этих событиях записываются не в системный журнал операционной системы, а в специальный «Журнал регистрации событий» (рис. 3.24), который открывается командой меню ***Администрирование ⇒ Журнал регистрации событий*** из программы «Управление СЗИ».

При формировании политик аудита в компьютерной системе кроме событий, фиксируемых СЗИ автоматически (см. выше), рекомендуется настроить регистрацию следующих категорий событий:

- регистрация пользователей в ОС Windows NT;
- изменения в политике безопасности Windows NT.

Аудит указанных событий, а также событий, связанных с доступом к защищаемым ресурсам (при наличии достаточных для этого оснований), необходимо производить с использованием стандартных средств регистрации Windows NT. Разработчики СЗИ «Страж NT» не рекомендуют регистрировать события, связанные с применениями привилегий пользователей, так как это будет приводить к быстрому переполнению журнала. По умолчанию в ОС Windows NT регистрация всех категорий событий отключена. Чтобы включить ее, необходимо сделать соответствующие изменения в настройках локальной политики безопасности в разделе «Политика аудита» (рис. 3.25) (***Панель управления ⇒ Администрирование ⇒ Локальная политика безопасности ⇒ Локальные политики ⇒ Политика аудита***).

Как уже было сказано, аудит событий доступа к защищаемым ресурсам должен производиться только при наличии обоснованных подозрений в злоупотреблении полномочиями. Кроме того, в связи с особенностями реализации защитных механизмов в СЗИ «Страж NT», регистрация событий отказа в доступе к ресурсам будет приводить к появлению в журнале большого количества посторонних записей. Поэтому можно рекомендовать устанавливать аудит лишь для событий успешного доступа к ресурсам. Настройка регистрации производится при помощи окна «Администратор ресурсов». Для того чтобы включить регистрацию событий, необходимо щелкнуть правой клавишей мыши на ресурсе (файле, каталоге, диске и т. д.), выбрать пункт контекстного меню «Разрешения и аудит», а затем в открывшемся диалоговом окне нажать кнопку «Дополнительно…». Откроется окно «Параметры управления доступом», вкладка «Аудит» которого отвечает за регистрацию событий, связанных с доступом к выбранному ресурсу (рис. 3.26).

ВЫПОЛНИТЬ!

23. Изменить настройки локальной политики безопасности так, чтобы производилась регистрация следующих категорий событий: вход в систему (успех, отказ), доступ к объектам (успех).
24. С использованием «Администратора ресурсов» в режиме администрирования назначить аудит всех типов событий доступа каталогу «C:\Проекты\Полет\Текстовые документы\Секретно».
25. Перезагрузиться, зарегистрироваться пользователем Свалов и прочитать содержимое указанного выше каталога. После этого выйти из системы и зарегистрироваться пользователем Клинов. Также попытаться прочитать содержимое каталога.
26. Перезагрузиться, зарегистрироваться пользователем Администратор, просмотреть содержимое «Журнала регистрации событий» СЗИ «Страж NT». Какие категории событий отражены в журнале?
27. Открыть «Журнал безопасности» и найти записи, связанные с получением доступа к каталогу «C:\Проекты\Полет\Текстовые документы\Секретно» пользователями Свалов и Клинов.

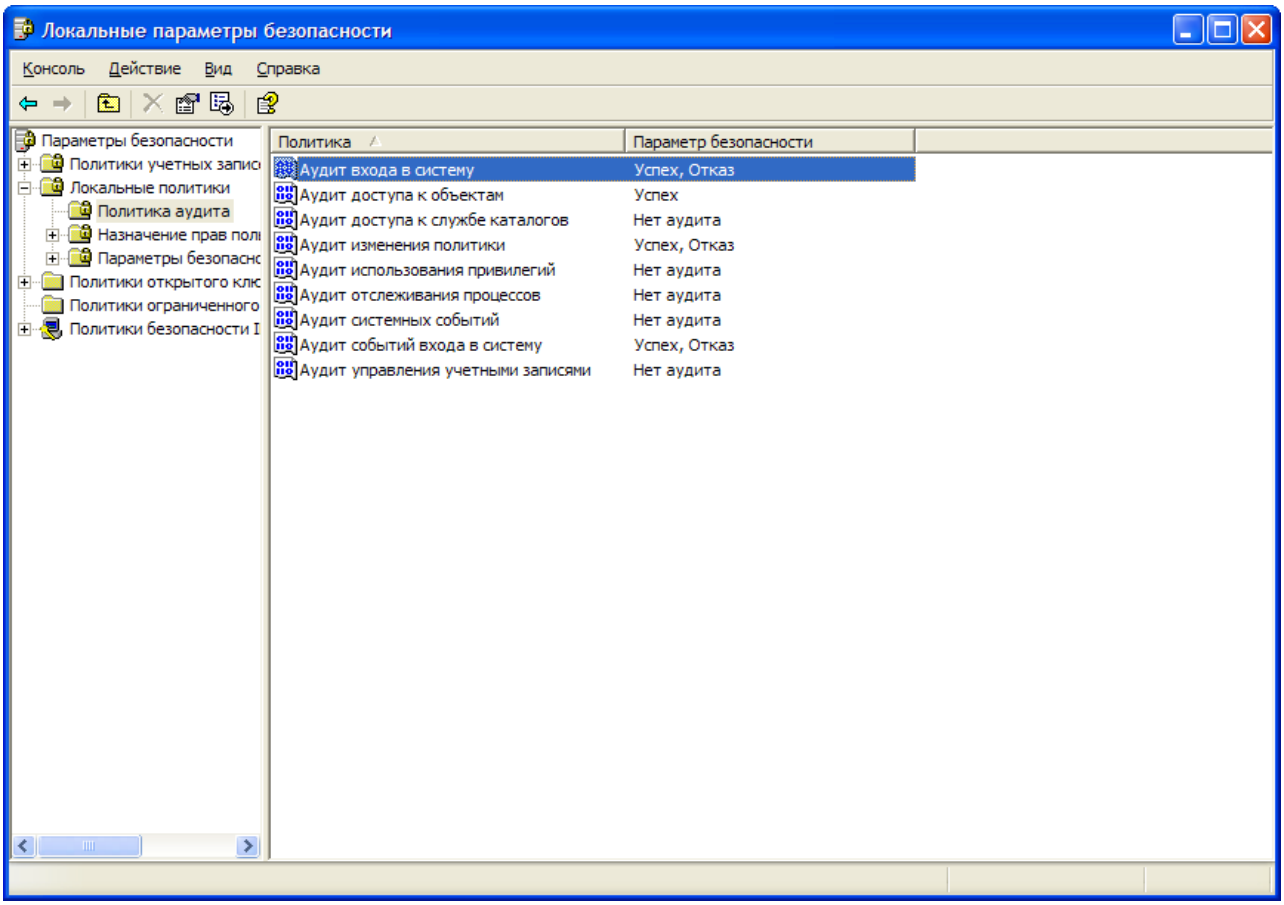


Рис. 3.25. Настройка политики аудита

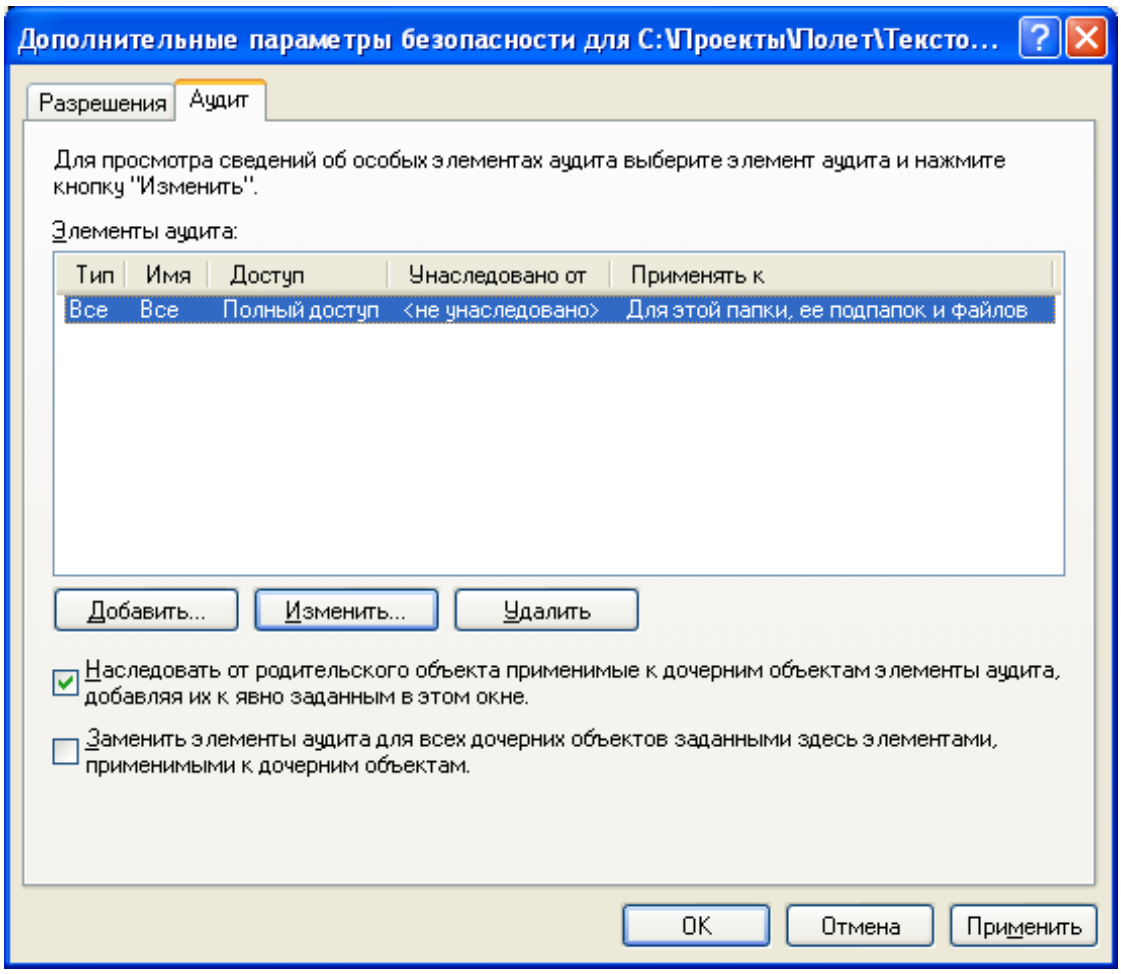


Рис. 3.26. Настройка регистрации событий доступа к ресурсу

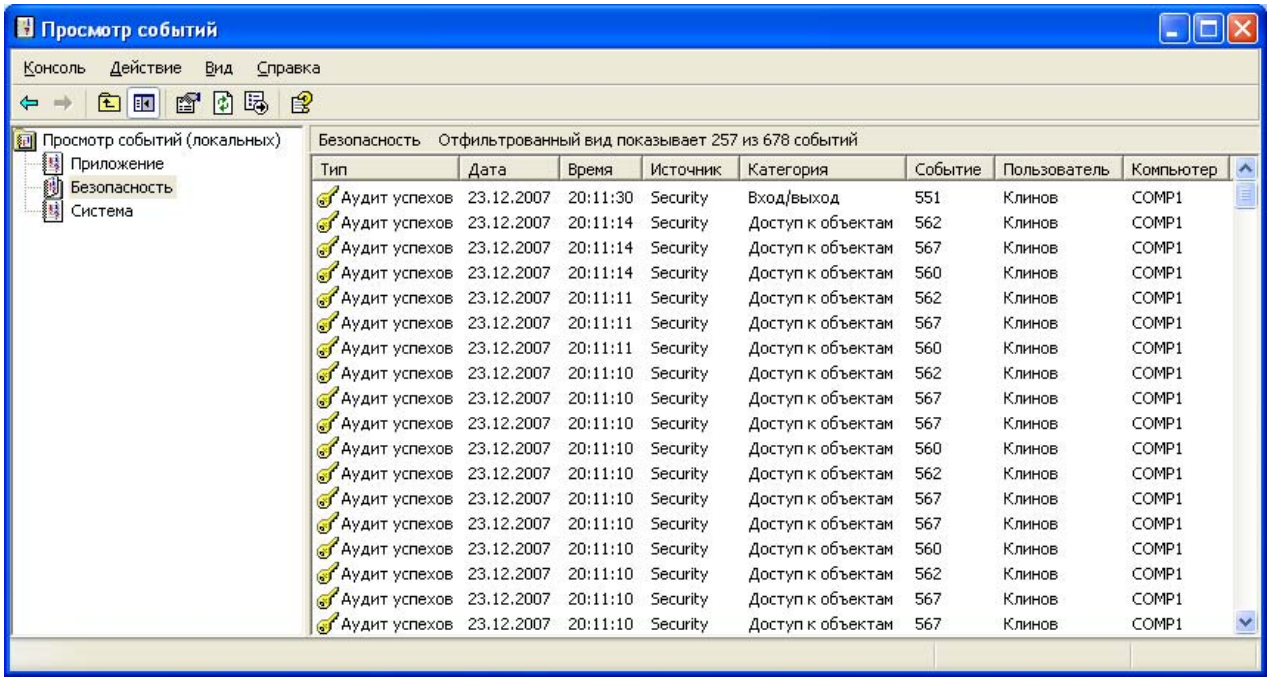


Рис. 3.27. Журнал безопасности

3.3.10. Гарантированное удаление данных

СЗИ «Страж NT» соответствует требованиям класса защищенности 3 «РД Гостехкомиссии России. СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» и кроме всего прочего включает в себя механизм гарантированного стирания всех удаляемых файлов, файла подкачки и критичных областей оперативной памяти. При удалении «грифованных» файлов механизм их гарантированного стирания в СЗИ действует по умолчанию.

ВЫПОЛНИТЬ!

28. Работая пользователем Соколов, создать в каталоге «C:\Проекты\Полет\Текстовые документы\Несекретно» короткий текстовый файл «Соколов2.txt», содержащий произвольную строку символов (запомнить или переписать строку).
29. Зарегистрироваться пользователем Свалов. Создать в каталоге «C:\Проекты\ Полет\Текстовые документы\Секретно» текстовый файл «Свалов2.txt», содержащий произвольную строку символов (запомнить или переписать строку).
30. С использованием редактора WinHEX (или любого другого двоичного редактора), запущенного из основной операционной системы, открыть файл образа диска с установленной СЗИ «Страж NT». Найти и записать смещение, по которому расположены два созданных файла (поиск файловых записей можно вести как по имени файла, так и по содержимому).
31. Удалить файлы «Соколов2.txt» и «Свалов2.txt», воспользовавшись комбинацией <Shift+Delete> в «Страж NT» (пользователем Свалов или Администратор). Попытаться найти содержимое удаленных файлов с использованием редактора WinHEX. Удалось ли это?

3.4. Система защиты информации от несанкционированного доступа «Dallas Lock»

3.4.1. Общие сведения

СЗИ «Dallas Lock» (разработчик ООО «Конфидент») представляет собой программно-аппаратный комплекс, добавляющий к системе безопасности Windows следующие функциональные возможности:

1. Организация доверенной загрузки с возможностью идентификации и аутентификации при помощи электронных идентификаторов Touch Memory;
2. Создание замкнутой программной среды для пользователей путем разрешения запуска ограниченного количества прикладных программ и динамических библиотек;
3. Реализация мандатной модели разграничения доступа на основе меток конфиденциальности пользователей и защищаемых ресурсов;
4. Контроль потоков защищаемой информации;
5. Очистка секторов, занимаемых защищаемыми файлами при их удалении, а также очистка памяти, выделяемой прикладным программам;
6. Контроль целостности указанных администратором файлов и системных областей диска;
7. Аудит доступа к защищаемым ресурсам;
8. Защита данных путем криптографического преобразования информации на диске.

3.4.2. Запуск и регистрация в системе защиты

Установка системы защиты «Dallas Lock» производится стандартным образом с вводом кода активации, получаемого в сервисном центре фирмы «Конфидент».

Для работы с системой на практических занятиях используется предварительно установленный экземпляр СЗИ в виде образа системы VMware, в котором имеется пользователь Администратор.

После запуска образа системы и отработки процедуры POST BIOS происходит инициализация системы защиты «Dallas Lock» из MBR активного раздела. При этом запрашиваются идентификатор и пароль пользователя (рис. 3.28). После предъявления правильного пароля и идентификатора выполняется процедура контроля целостности (рис. 3.29), при удачном завершении которой стандартным образом загружается ОС Windows 2000.

ВЫПОЛНИТЬ!

1. Загрузить образ СЗИ «Dallas Lock» и зарегистрироваться в системе пользователем Администратор, введя пароль «12345».

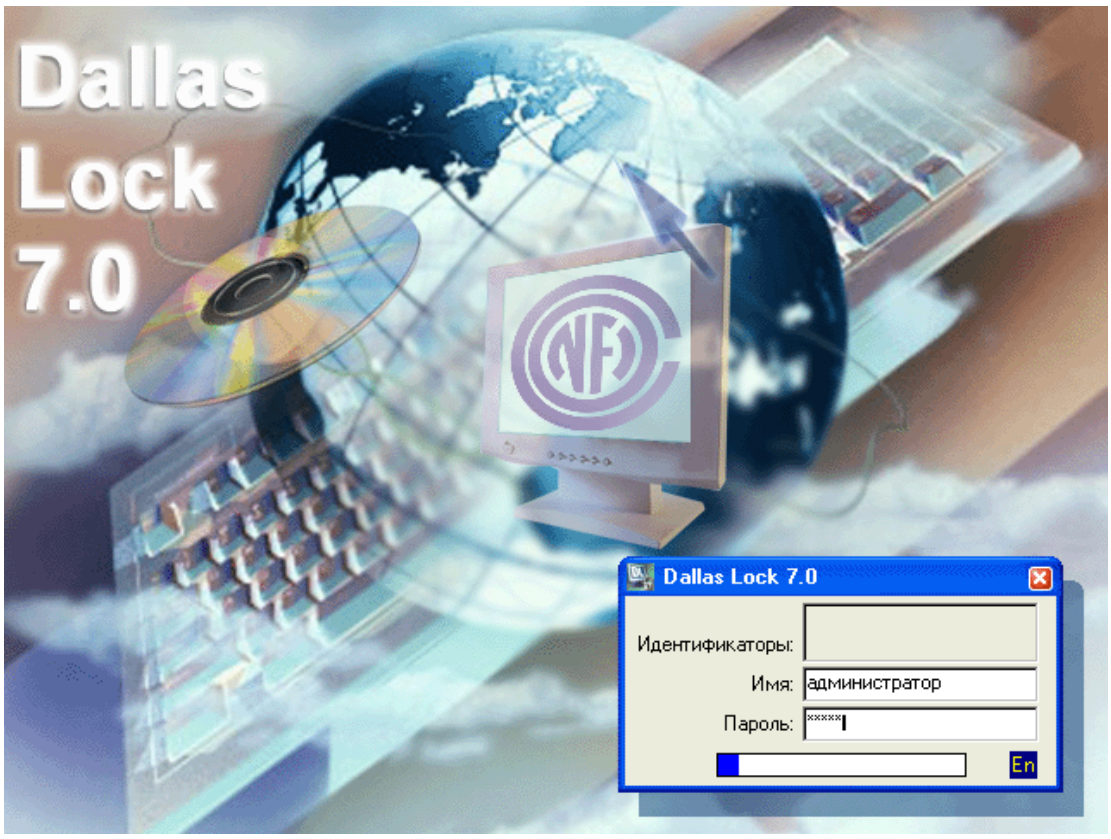


Рис. 3.28. Регистрация в СЗИ «Dallas Lock»

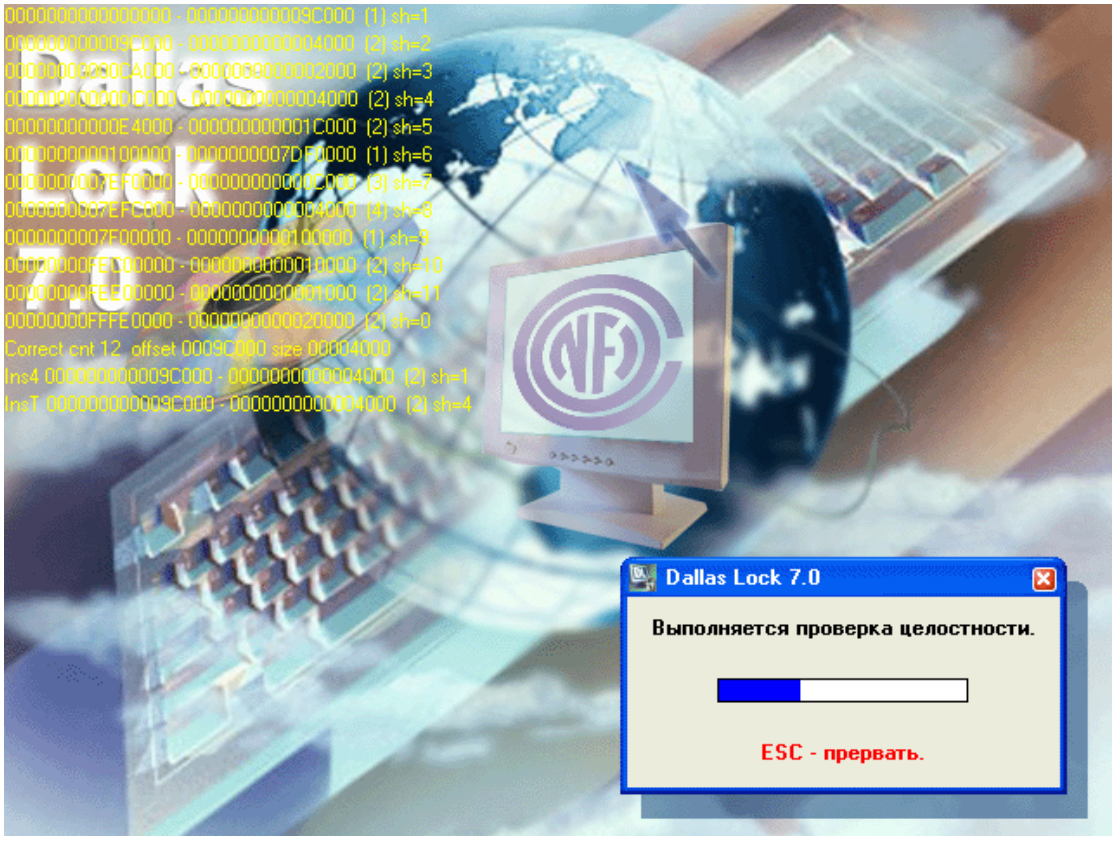


Рис. 3.29. Окно проверки целостности в СЗИ «Dallas Lock»

3.4.3. Создание пользователей

Создание пользователей в СЗИ осуществляется с использованием программы «Администратор DL 7.0», которая вызывается командой ***Пуск ⇒ Программы ⇒ Dallas Lock 7.0 ⇒ Администратор DL 7.0***. Для создания учетных записей необходимо выполнить команду меню ***Пользователи ⇒ Создать***. Открывающееся окно «Новый пользователь» имеет четыре вкладки: «Общие», «Идентификация», «Расписание», «Группы» (рис. 3.30).

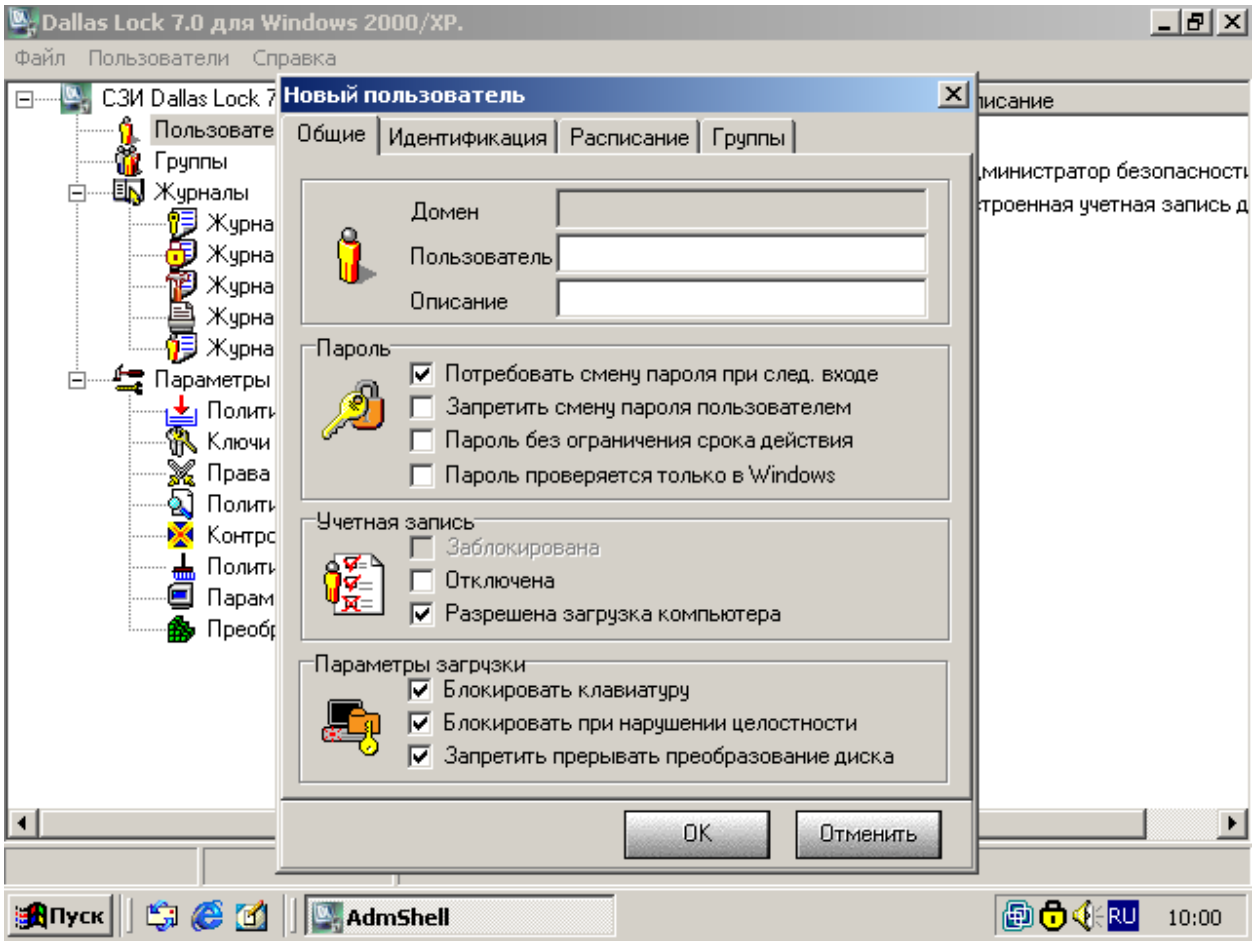


Рис. 3.30. Окно «Новый пользователь» программы «Администратор DL 7.0»

Вкладка «Общие» позволяет установить для каждого из создаваемых пользователей следующие рекомендуемые параметры: «Потребовать смену пароля при следующем входе» (после первой регистрации каждый из пользователей должен будет изменить свой пароль), «Разрешена загрузка компьютера» (все пользователи могут включать защищаемый компьютер), «Блокировать клавиатуру», «Блокировать при нарушении целостности», «Запретить прерывать преобразование диска».

Вкладка «Идентификация» позволяет установить для каждого из пользователей электронный идентификатор Touch Memory.

С помощью Вкладки «Расписание» указываются разрешенные дни недели и время работы пользователей, а вкладка «Группы» предназначена для включения учетной записи в одну или несколько рабочих групп.

После задания необходимых параметров для каждой учетной записи вводится пароль.

ВЫПОЛНИТЬ!

2. Создать учетные записи пользователей: Клинов, Соколов, Савин, Свалов, Ювченко. Пароли выбрать произвольно. По очереди зарегистрироваться в системе каждым из пользователей.

3.4.4. Реализация мандатной модели разграничения доступа

Мандатная модель разграничения доступа в СЗИ «Dallas Lock» реализована посредством назначения защищаемым ресурсам и каждому пользователю системы меток конфиденциальности и сравнения их при запросах на доступ. В качестве меток конфиденциальности выступают:

- для защищаемых ресурсов — классификационная метка мандатного доступа;
- для пользователей — уровень допуска.

В СЗИ «Dallas Lock» используются следующие наименования меток конфиденциальности в порядке повышения: «Открытые данные», «Конфиденциально» (соответствует ДСП) и «Строго конфиденциально» (соответствует Секретно).

Наличие уровня допуска определяется значениями параметров «Уровень доступа: Конфиденциально» и «Уровень доступа: Строго конфиденциально», входящих в группу параметров безопасности «Права пользователей» программы «Администратор DL 7.0». Значением этих параметров является список учетных записей пользователей и групп, которым назначается соответствующий допуск. По умолчанию значением параметра «Уровень доступа: Конфиденциально» является группа «Конфиденциально» (рис. 3.32), а значением параметра «Уровень доступа: Строго конфиденциально» — группа «Строго конфиденциально».

Применение такого подхода к назначению уровней допуска позволяет воспользоваться идеологией рабочих групп: для назначения пользователю допуска следует включить его учетную запись в состав одной из групп — «Конфиденциально» или «Строго конфиденциально». Если пользователь не включен в одну из этих групп, он допускается только к открытым данным. По умолчанию для каждого создаваемого пользователя устанавливается доступ к открытым данным.

Для защищаемых ресурсов (диски, каталоги, файлы) должны быть установлены классификационные метки мандатного доступа. По умолчанию все объекты относятся к категории «Открытые данные», доступ к которым могут получать пользователи с любым уровнем допуска.

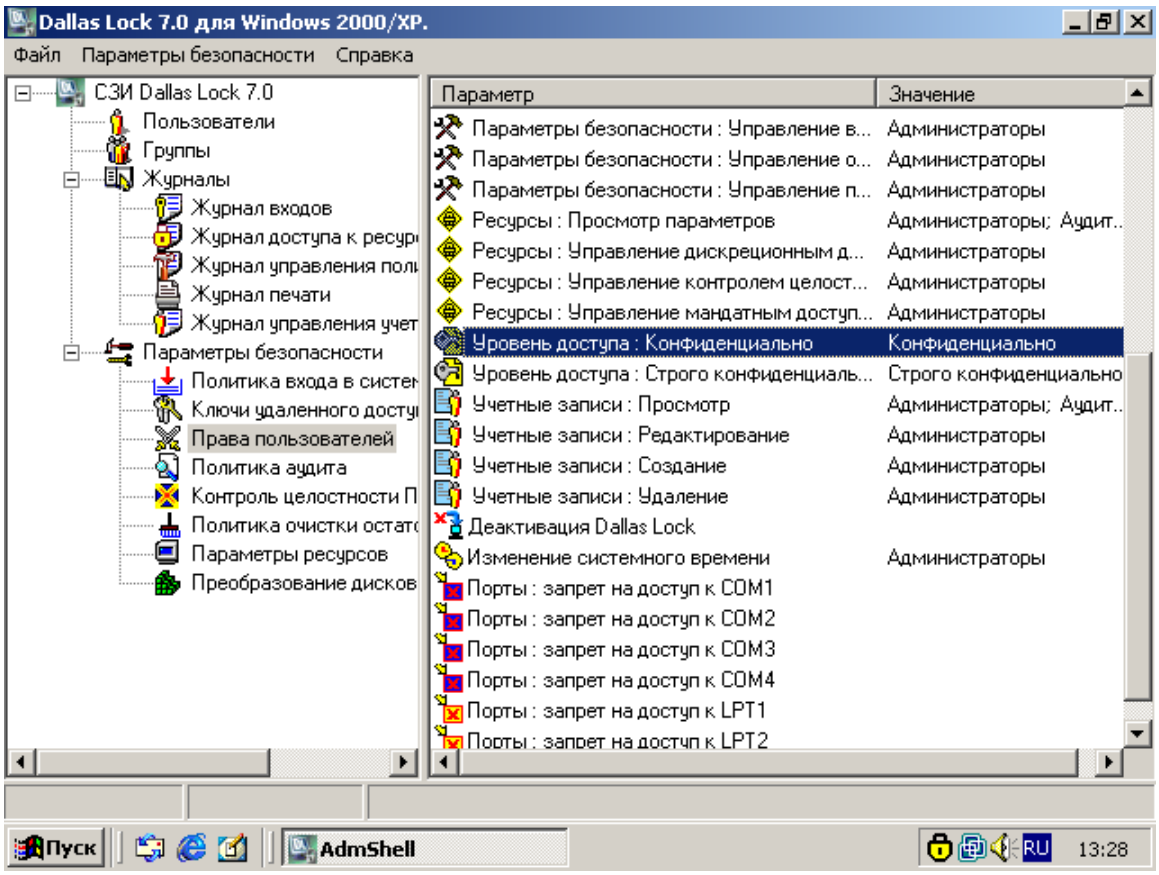


Рис. 3.31. Группа параметров безопасности «Права пользователей»

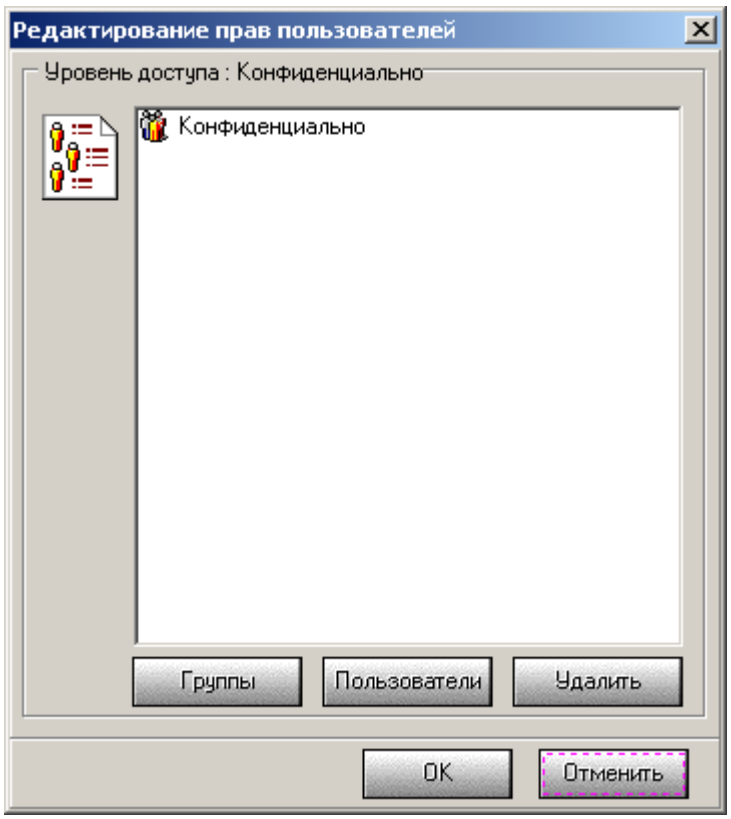


Рис. 3.32. Значение параметра «Уровень доступа: Конфиденциально» по умолчанию

Для изменения уровня конфиденциальности следует вызвать в контекстном меню объекта пункт «Dallas Lock 7.0», перейти к вкладке «Мандатный доступ» и, отключив параметр «По умолчанию», установить требуемый уровень (рис. 3.33).

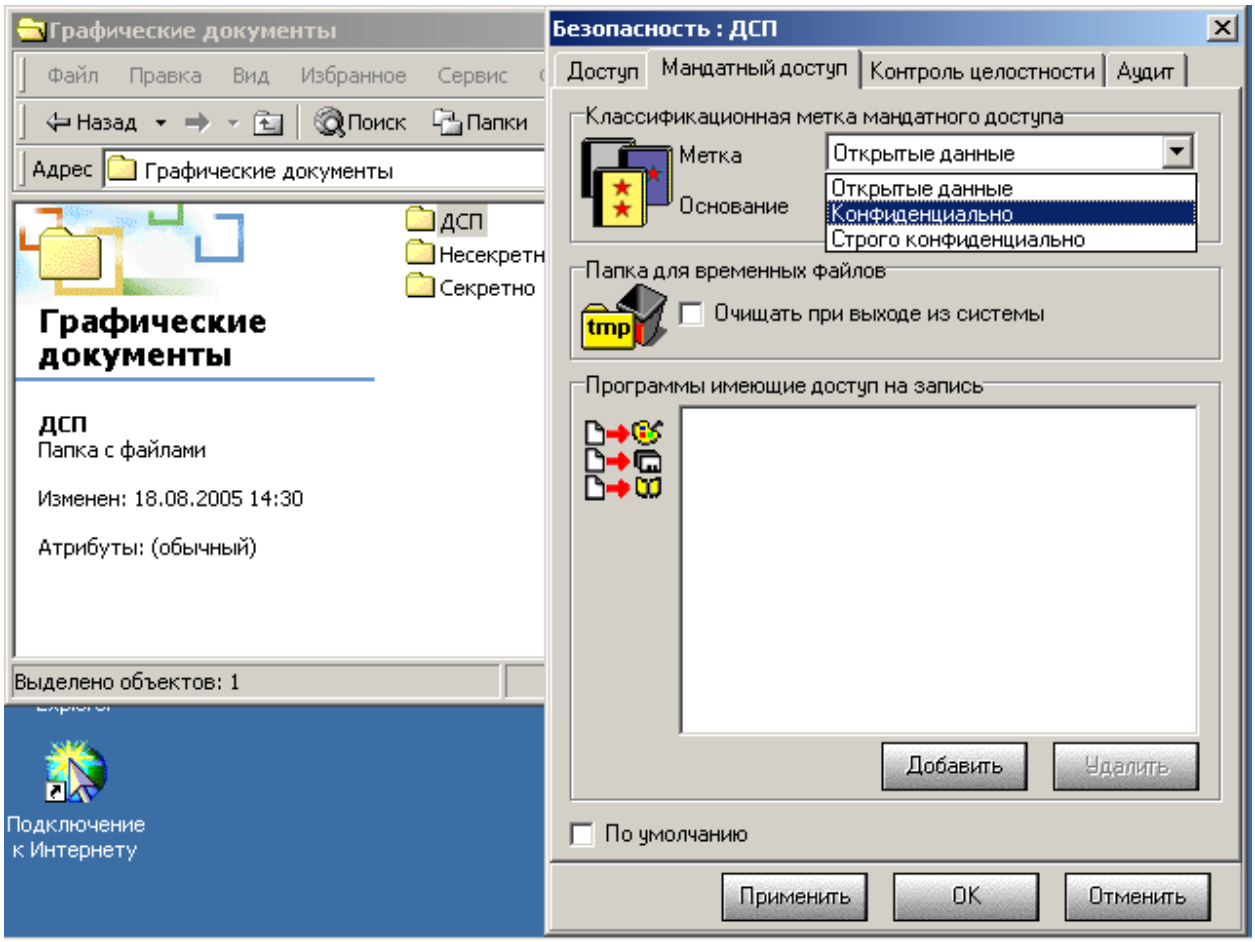


Рис. 3.33. Изменение уровня конфиденциальности каталога

ВЫПОЛНИТЬ!

3. Назначить созданным учетным записям пользователей уровни допуска в соответствии с табл. 2.1 путем включения их в соответствующие группы.
4. Создать иерархическую структуру каталогов, как показано на рис. 3.15. Назначить созданным каталогам грифы секретности в соответствии с их названиями.

По умолчанию пользователи регистрируются с уровнем допуска «Открытые данные». Однако каждый пользователь *при регистрации* в системе может выбрать текущий уровень допуска, не превышающий максимально установленный для него уровень (рис. 3.34).

Внимание! Первая регистрация пользователя в системе связана с созданием профиля пользователя, т. е. набора каталогов и файлов в каталоге «Documents and Settings», имеющем гриф секретности «Открытые данные». Создание каталогов и файлов с грифом «Открытые данные» возможно только в том случае, когда текущий уровень допуска не превышает «Открытые данные». Таким образом, первая регистрация пользователя в системе должна быть осуществлена с текущим уровнем допуска «Открытые данные».

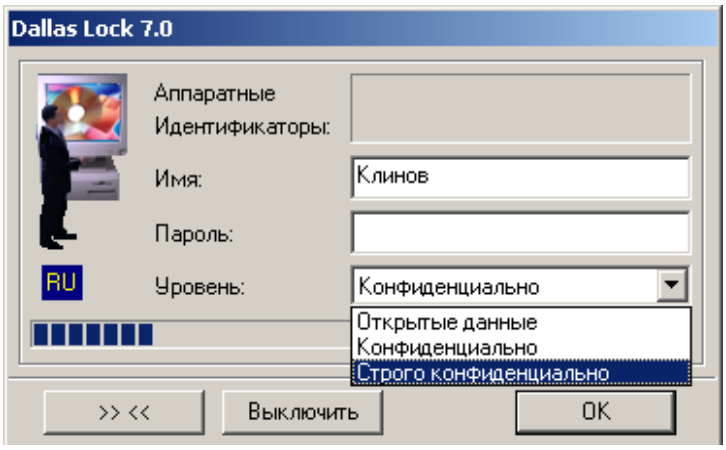


Рис. 3.34. Выбор уровня текущего допуска при регистрации

ВЫПОЛНИТЬ!

5. Зарегистрироваться в системе пользователем Клинов, выбрав уровень допуска «Строго конфиденциально». Запустить «Проводник», просмотреть содержимое созданных каталогов. Все ли каталоги отображаются? Можно ли открыть эти каталоги?
6. Выйти из системы и зарегистрироваться пользователем Соколов, выбрав уровень допуска «Конфиденциально». Возможно ли это при условии, что Соколов имеет допуск лишь к несекретным документам? При помощи «Проводника» просмотреть содержимое созданных каталогов. Какие каталоги отображаются? Содержимое каких каталогов доступно данному пользователю?
7. Работая пользователем Соколов, создать короткий текстовый документ «Соколов.txt» и сохранить его в каталоге «C:\Проекты\ Полет\Текстовые документы\Несекретно».
8. Зарегистрироваться в системе пользователем Свалов с максимальным текущим допуском («Строго конфиденциально»), создать короткий текстовый документ «Свалов.txt» и попытаться сохранить его в каталог «C:\Проекты\Полет\Текстовые документы\Несекретно». Получилось ли это? Сохранить документ в каталоге «C:\Проекты\ Полет\Текстовые документы\Секретно».
9. Попытаться скопировать содержимое из секретного документа в несекретный с использованием команд ***Правка ⇒ Копировать*** и ***Правка ⇒ Вставить***. Получилось ли это? Работает ли обратная операция вставки несекретных сведений в секретный документ?

3.4.5. Реализация дискреционной модели разграничения доступа

Дискреционная модель разграничения доступа реализуется в СЗИ «Dallas Lock» посредством стандартных списков доступа. Для просмотра или редактирования списков доступа необходимо из контекстного меню объекта выбрать пункт «Dallas Lock 7.0», в появившемся окне — вкладку «Доступ» (рис. 3.35).

Основным отличием данного СЗИ является то, что списки доступа выполнены не средствами ОС Windows NT (не средствами файловой системы NTFS), а собственным механизмом. Следствием этого является, во-первых, то, что списки доступа можно реализовать на разделах с файловой системой FAT (а не только NTFS). Во-вторых, вводится собственный, отличный от принятого в ОС Windows NT (см. п. 3.1.3), алгоритм определения права доступа пользователя к ресурсу [18].

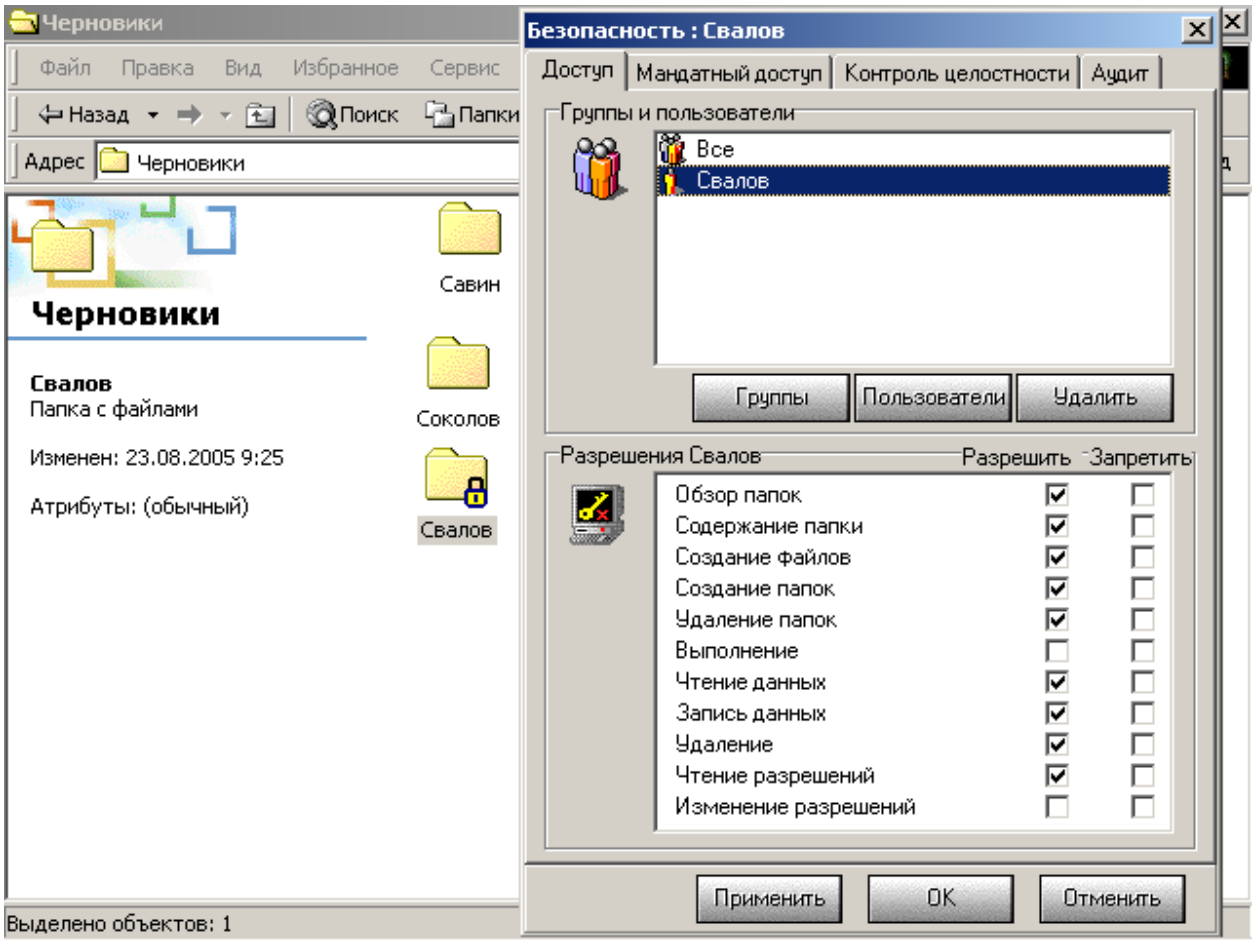


Рис. 3.35. Редактирование списков доступа

При попытке текущего пользователя совершить с объектом любую операцию система защиты анализирует в первую очередь локальные параметры данного объекта. Для этого она проверяет:

1. К какому разряду по отношению к объекту защиты принадлежит пользователь. Если это индивидуальный пользователь и ему назначены локальные параметры по отношению к данному объекту, то право на совершение запрошенной операции устанавливается исходя из этих параметров. Если параметру, контро-

лирующему данную операцию, присвоено значение «Разрешить», то операция выполняется. Если параметру присвоено значение «Запретить», она блокируется и выдается сообщение об ошибке.

2. Если текущий пользователь не относится к разряду индивидуальных пользователей или значение контролирующего данную операцию параметра явно не указано, то система защиты проверяет, входит ли текущий пользователь в какую-либо из групп пользователей, для которой назначены локальные параметры по отношению к данному ресурсу. Если это так, то право пользователя на совершение запрошенной операции устанавливается исходя из параметров этой группы. Если группе пользователей предоставлено право на совершение операции (контролирующему параметру присвоено значение «Разрешить»), то операция выполняется. Если параметру присвоено значение «Запретить», она блокируется и выдается сообщение об ошибке.

3. Если текущий пользователь не принадлежит ни к одному из указанных выше разрядов или значение контролирующего параметра явно не указано, то анализируются локальные параметры, установленные для разряда «Все» по отношению к этому ресурсу. Если разряду «Все» предоставлено право на совершение операции (контролирующему параметру присвоено значение «Разрешить»), то операция выполняется. Если параметру присвоено значение «Запретить», она блокируется и выдается сообщение об ошибке.

4. Если значение контролирующего параметра для разряда «Все» явно не указано или для данного разряда не установлены локальные параметры, то система защиты проверяет, входит ли данный объект в состав другого объекта. При положительном результате повторяются действия пунктов 1-3, при отрицательном система защиты переходит к проверке глобальных параметров.

Анализ глобальных параметров осуществляется по той же самой схеме, что и локальных.

ВЫПОЛНИТЬ!

10. Разграничить права доступа пользователей к каталогам в соответствии с табл. 2.2.
11. Зарегистрироваться пользователем Ювченко и просмотреть содержимое каталога «C:\Экономика». Убедиться, что каталог «C:\Проекты» для этого пользователя недоступен.
12. Зарегистрироваться пользователем Свалов и просмотреть содержимое каталога «C:\Проекты\Полет\Текстовые документы\Секретно». Убедиться, что каталог «C:\Экономика» недоступен.
13. Создать в каталоге «C:\Приказы» и распоряжения пользователем Клинов короткий текстовый файл «Приказ1.txt» с приказом об увольнении Савина.
14. Убедиться, что Савин сможет прочитать приказ о своем увольнении, но не сможет изменить его.

3.4.6. Обеспечение замкнутости программной среды

Механизм замкнутой программной среды реализуется в СЗИ «Dallas Lock» путем установки для пользователей глобального запрета на запуск программ и разрешения запуска лишь определенных исполняемых файлов. Стратегия может быть следующей:

1. Определить, какие исполняемые файлы должны запускаться для нормальной работы операционной системы;
2. Решить, какие файлы разрешается запускать пользователям для работы;
3. Запретить запуск всех исполняемых файлов для сменных дисков;
4. Запретить запуск всех исполняемых файлов для каждого из фиксированных логических дисков, доступных операционной системе;
5. Установить разрешение на исполнение выбранных файлов для конкретных пользователей или групп пользователей.

Очевидно, что пользователю должно быть запрещено изменение файлов, которые он имеет право запускать на выполнение.

Для установки глобального запрета на запуск программ на сменных носителях необходимо в программе «Администратор DL 7.0» в группе параметров безопасности «Параметры ресурсов» выбрать «Параметры сменных дисков по умолчанию» (рис. 3.36). Диалоговое окно с настройками разрешений аналогично показанному на рис. 3.35. В этом окне необходимо установить запрет на выполнение для группы пользователей «Все», а также разрешить выполнение для группы «Администраторы». В результате все пользователи, за исключением администраторов, не смогут запускать исполняемые файлы, находящиеся на сменных носителях (CD-ROM, дискеты).

Установка запрета на запуск файлов, находящихся на фиксированных носителях, производится через контекстное меню объекта (пункт меню Dallas Lock 7.0»). Запрет запуска при помощи «Администратора DL 7.0» (как в случае со сменными носителями) недопустим, так как он не вступает в силу.

Чтобы обеспечить возможность нормальной загрузки и работы операционной системы, необходимо разрешить выполнение файлов, находящихся в каталоге «*%SystemRoot%\system32*», а также файла «*%SystemRoot%\explorer.exe*».

ВЫПОЛНИТЬ!

15. Зарегистрироваться в системе Администратором, запретить запуск программ со съемных и фиксированных носителей для всех пользователей. Для группы Администраторов разрешить полный доступ ко всем указанным носителям. Разрешить выполнение программ, находящихся в каталоге «%SystemRoot%\system32», а также программы «%SystemRoot%\ explorer.exe», запретив любые действия по их изменению (группе Администраторов разрешить полный доступ). Разрешить всем пользователям выполнение программы «C:\DlLock70\BlockIcon.exe» (Администраторам — полный доступ).
16. Проверить, может ли пользователь Свалов запустить «Калькулятор» («%SystemRoot%\system32\calc.exe»). Может ли он запустить Internet Ex-

plorer («C:\Program Files\Internet Explorer\iexplore.exe»)? Может ли запустить Internet Explorer Администратор?

17. Проверить, имеет ли пользователь Клинов возможность изменить содержимое каталога «%SystemRoot%\system32».

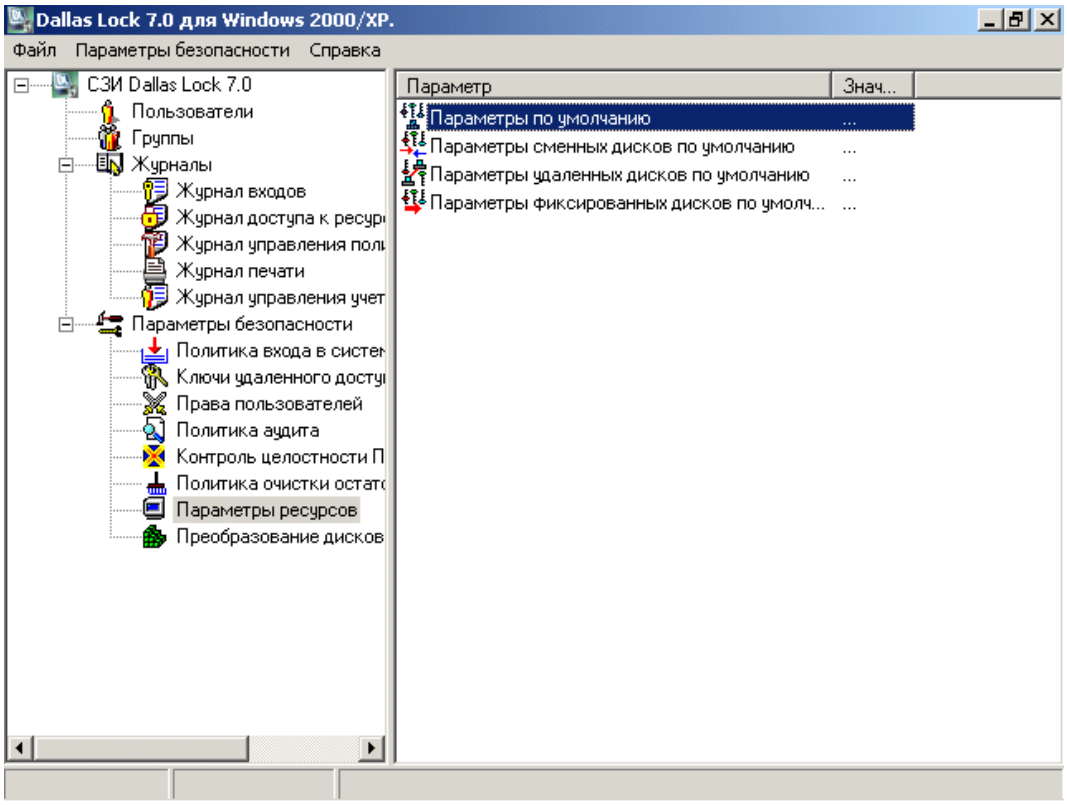


Рис. 3.36. Настройка параметров ресурсов по умолчанию

3.4.7. Контроль целостности

СЗИ «Dallas Lock 7.0» включает в свой состав подсистему проверки целостности. Она запускается до загрузки ОС и обеспечивает проверку целостности BIOS, CMOS и MBR жесткого диска, а также проверку дисков, каталогов и файлов в случае установки соответствующих параметров.

Включение контроля целостности BIOS, CMOS, MBR и загрузочного сектора производится с использованием программы «Администратор DL 7.0» (группа настроек ***Параметры безопасности ⇒ Контроль целостности ПЭВМ***). Чтобы включить контроль целостности для файла или каталога, необходимо в контекстном меню выбрать пункт «Dallas Lock 7.0», и в открывшемся диалоговом окне открыть вкладку «Контроль целостности» (рис. 3.37).

Для расчета контрольной суммы могут использоваться следующие алгоритмы: CRC32, хэш по ГОСТ Р 34.11–94 или хэш MD5.

Если для объекта файловой системы задан контроль целостности, то система не позволит изменить этот объект, и он будет доступен только для чтения и выполнения.

Проверка целостности осуществляется при загрузке компьютера до начала загрузки операционной системы. При нарушении целостности хотя бы одного файла, загрузка компьютера блокируется для всех пользователей, кроме администратора безопасности (пользователя Администратор).

Возможно возникновение ситуации, когда файл, для которого был установлен контроль целостности, удаляется администратором безопасности (остальные пользователи изменить этот файл не смогут). При попытке сверить контрольную сумму этого файла с эталонной будет принято решение о нарушении целостности, так как файла вообще не будет найдено. В результате загрузка всех пользователей, кроме администратора безопасности, будет заблокирована. Ситуация является ошибочной, так как администратор не сможет отключить контроль целостности несуществующего файла. Чтобы обойти подобную ситуацию в СЗИ «Dallas Lock» предусмотрена функция пересчета списка дескрипторов. Активизация этой функции производится в программе «Администратор DL 7.0» командой меню ***Файл ⇒ Перестроить список дескрипторов***.

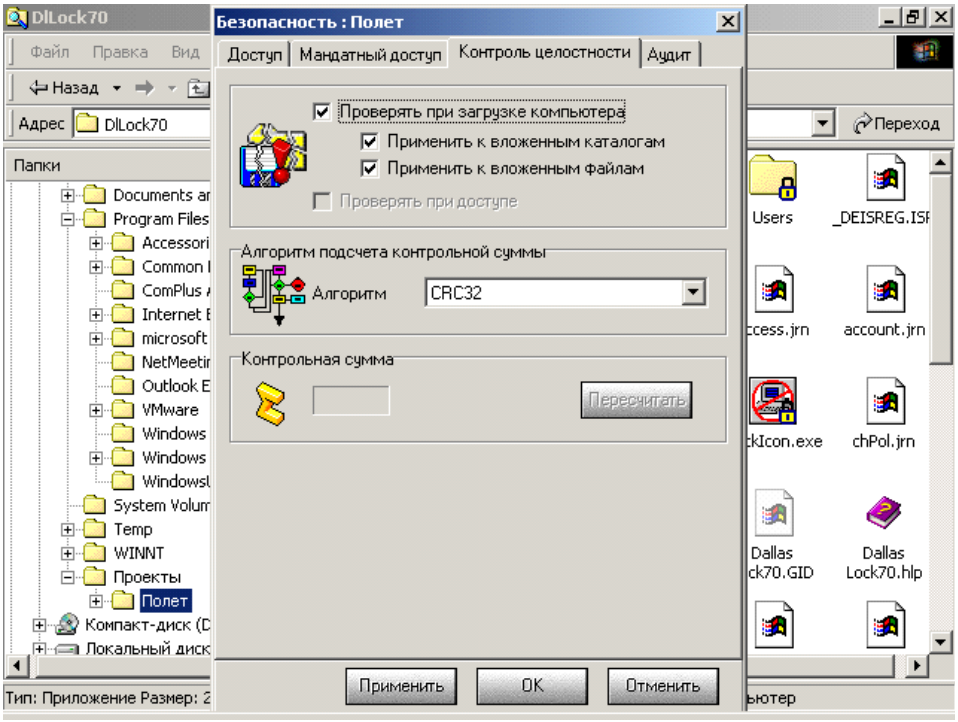


Рис. 3.37. Настройка контроля целостности ресурса

ВЫПОЛНИТЬ!

18. Зарегистрироваться Администратором, создать в каталоге «C:\База данных» короткий текстовый файл «DB.txt». Настроить контроль целостности этого файла с использованием алгоритма CRC32.
19. Перезагрузить компьютер, зарегистрироваться Администратором и изменить содержимое файла «DB.txt». Снова перезагрузить компьютер и попытаться зарегистрироваться пользователем Свалов. Возможно ли это? Перезагрузить компьютер, после чего зарегистрироваться Администратором и отключить контроль целостности файла «DB.txt».

3.4.8. Регистрация событий

СЗИ Dallas Lock 7.0 включает средства аудита, автоматически ведущие запись в пять системных журналов: «журнал входов», «журнал доступа к ресурсам», «журнал управления политиками безопасности», «журнал печати» и «журнал управления учетными записями». В «журнале входов» фиксируются события, связанные с загрузкой компьютера и регистрацией пользователя в операционной системе. «Журнал доступа к ресурсам» предназначен для отслеживания обращений пользователя к защищаемым ресурсам. «Журнал управления политиками безопасности» содержит информацию о действиях пользователя по настройке параметров системы защиты. В «журнале печати» отображаются все попытки печати. «Журнал управления учетными записями» предназначен для учета действий по изменению прав пользователей.

Включение регистрации указанных категорий событий производится в программе «Администратор DL 7.0» в разделе «Политика аудита» (рис. 3.38).

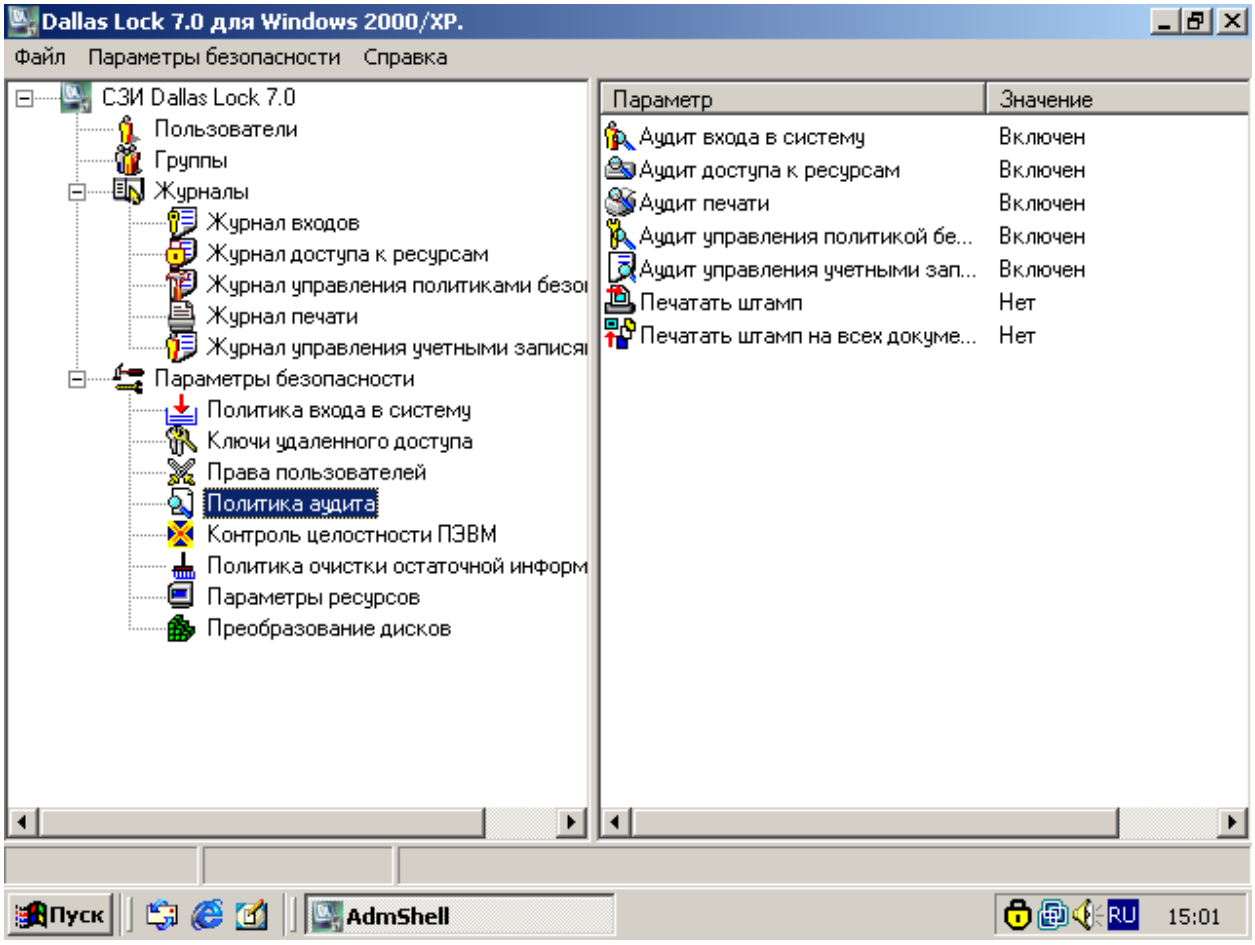


Рис. 3.38. Настройка политики аудита

Назначение аудита доступа к ресурсам производится отдельно для каждого ресурса. Чтобы включить регистрацию событий, связанных с конкретным ресурсом, необходимо в контекстном меню ресурса выбрать пункт «Dallas Lock 7.0», затем выбрать вкладку «Аудит» в открывшемся диалоговом окне и снять отметку «По умолчанию». Существует возможность фиксировать все ти-

пы событий доступа, которые могут контролироваться средствами СЗИ (обзор папки, создание файлов, выполнение и т. д.).

При просмотре содержимого журналов можно использовать средства фильтрации записей. Для включения фильтра необходимо зайти в любой из журналов, и в контекстном меню записи выбрать пункт «Настроить фильтр». Правила фильтрации действуют на все журналы одновременно. Включение и выключение фильтра делается командой «Фильтрация» упомянутого контекстного меню.

ВЫПОЛНИТЬ!

33. Работая пользователем Администратор, включить регистрацию следующих категорий событий средствами СЗИ «Dallas Lock»: вход в систему, доступ к объектам, доступ к ресурсам, управление политикой безопасности и управление учетными записями.
34. Назначить аудит всех типов событий доступа каталогу «C:\Проекты\Полет\Текстовые документы\Секретно».
35. Перезагрузиться, зарегистрироваться пользователем Свалов и прочитать содержимое указанного выше каталога. После этого выйти из системы и зарегистрироваться пользователем Клинов. Прочитать содержимое каталога, изменить файл «Свалов.txt».
36. Зарегистрироваться пользователем Администратор, просмотреть журналы регистрации событий в программе «Администратор DL». Какие категории событий отражены в журнале?

3.4.9. Печать штампа

СЗИ «Dallas Lock» позволяет создавать штамп на документах, отправляемых на печать. Настройка печати штампа производится с использованием программы «Администратор DL 7.0» в разделе ***Параметры безопасности ⇒ Политика аудита***. Включение печати штампа для конфиденциальных и строго конфиденциальных документов, а также настройка информации, выводимой на штампе, производится в диалоговом окне «Штамп», которое открывается двойным щелчком на пункте «Печатать штамп». В этом диалоговом окне можно настроить положение штампа на странице (он печатается в верхней ее части), шрифт, которым он будет напечатан, а также содержимое штампа. Сам штамп представляет собой текстовый блок, который может содержать как неизменяемый текст, так и служебные метаданные. Чтобы вставить в штамп служебную информацию, необходимо в контекстном меню поля ввода текста выбрать, какая именно информация должна быть добавлена.

Как уже было сказано, по умолчанию штамп печатается только на конфиденциальных и строго конфиденциальных документах. Чтобы печатать штамп на всех документах, нужно в «Администраторе DL» активизировать параметр «Печатать штамп на всех документах».

В силу особенностей программной реализации расположение штампа может незначительно меняться в зависимости от программы, из которой осуществляется печать. Так, при печати из программы WordPad требуется добавлять в штамп несколько пустых строк перед текстом, иначе верхняя строка надписи не будет видна. Поэтому рекомендуется проверять корректность вывода штампа из каждого используемого приложения, делая, при необходимости, соответствующие изменения в настройках внешнего вида штампа.

ВЫПОЛНИТЬ!

20. Настроить печать штампа следующего содержания на всех документах:

<УРОВЕНЬ ДОСТУПА>
Отп. <ПОЛЬЗОВАТЕЛЬ>
С <КОМПЬЮТЕР>,
файл <ДОКУМЕНТ>
<ДАТА И ВРЕМЯ>

21. Если имеется возможность напечатать документ, проверить, будет ли напечатан штамп. Какие недостатки можно отметить в содержании выводимой информации?
22. Модифицировать штамп для исправления выявленных недостатков.

3.4.10. Гарантированное удаление данных

СЗИ «Dallas Lock 7.0» включает подсистему очистки остаточной информации, которая позволяет:

1. Заполнять очищаемое в результате удаления и изменения размеров файлов пространство жесткого диска маскирующей последовательностью;
2. Очищать (таким же образом) файл подкачки Windows при завершении работы;
3. Обнулять оперативную память при ее выделении;
4. Очищать все каталоги, помеченные как временные, при старте системы, завершении работы и завершении сеанса работы пользователя.

Включение указанных функций производится в программе «Администратор DL» в разделе «Очистка остаточной информации». Существует возможность задать от одного до пяти циклов затирания.

ВЫПОЛНИТЬ!

23. Включить опцию очистки освобождаемого дискового пространства, установив количество циклов затирания равным 1 (для учебных целей этого вполне достаточно).
24. Работая пользователем Соколов, создать в каталоге «C:\Проекты\ Полет\ Текстовые документы\Несекретно» короткий текстовый документ «Соколов2.txt», содержащий сочетание символов «123454321».

25. Зарегистрироваться пользователем Савин с максимальным возможным уровнем допуска. Создать в каталоге «C:\Проекты\Полет\Текстовые документы\ДСП» короткий текстовый документ «Савин.txt», содержащий сочетание символов «567898765».
26. С использованием дискового редактора, запущенного из основной операционной системы, открыть файл образа диска с установленной СЗИ «Dallas Lock». Найти и записать смещение, по которому расположены два созданных файла (поиск файловых записей можно вести как по имени файла, так и по содержимому).
27. Удалить файлы Соколов2.txt и Савин.txt (пользователем, который имеет на это полномочия). Попытаться найти содержимое удаленных файлов с использованием дискового редактора. Удалось ли это?

3.4.11. Реализация запрета загрузки ПЭВМ в обход СЗИ

Запрет загрузки компьютера в обход защитных механизмов реализуется в СЗИ «Dallas Lock» путем внедрения процедур аутентификации пользователей и контроля целостности данных в программу, загрузка которой производится через MBR жесткого диска. Таким образом, загрузить операционную систему, например, в режиме защиты от сбоев становится невозможно.

Запрет загрузки со съемных носителей, а также противодействие анализу защищаемых данных при подключении жесткого диска к иному компьютеру осуществляется в СЗИ «Dallas Lock» путем включения режима прозрачного преобразования дисков. Алгоритм преобразования жесткого диска выбирается при установке СЗИ. Преобразованию может быть подвергнут весь диск либо его часть. Преобразование выполняется с использованием программы «Администратор DL 7.0», для чего необходимо в параметрах безопасности выбрать «Преобразование дисков» и указать область преобразования (рис. 3.39). Основным достигаемым результатом является невозможность обращения к диску в обход системы защиты.

Внимание! Преобразование жесткого диска, реализованное в обсуждаемой версии 7.0 СЗИ «Dallas Lock», не является криптографической защитой данных — это лишь некое «кодирование» с использованием алгоритма, известного только разработчикам СЗИ. Вместе с тем даже такое кодирование является существенной преградой для злоумышленников.

При очередной загрузке компьютера начнется процесс преобразования указанной области. После преобразования получение доступа к данным, обрабатываемым на диске, в обход СЗИ становится невозможным. Таким образом, преобразование диска является важнейшим элементом для предотвращения несанкционированного доступа к данным и выполнения пункта 2 требований к защите компьютерной системы от НСД. Для гарантированного блокирования возможности НСД при загрузке с внешних носителей необходимо осуществлять преобразование всего диска. Дополнительной мерой защиты является ус-

тановка запрета загрузки с внешних носителей в настройках BIOS Setup, подкрепляемая паролем.

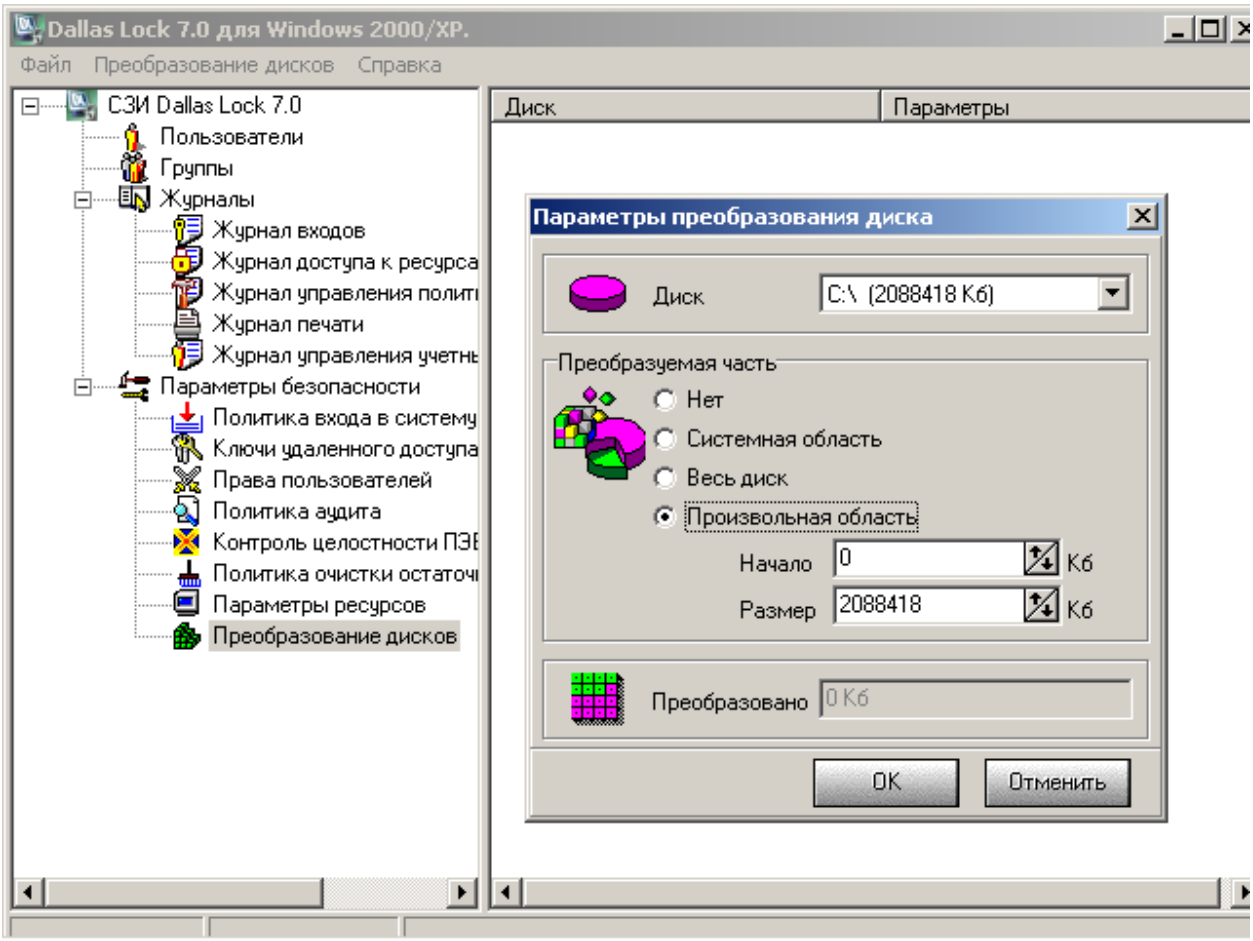


Рис. 3.39. Окно преобразования дисков

ВЫПОЛНИТЬ!

28. Подготовьте загрузочный носитель (дискету или CD-ROM), позволяющую осуществлять монтирование разделов с файловой системой NTFS. Перезагрузите компьютер, убедитесь, что в настройках BIOS Setup разрешена загрузка с внешнего носителя (рис. 3.40).
29. Загрузите компьютер с внешнего носителя, убедитесь, что в обход механизмов защиты СЗИ при отсутствии преобразования дисков возможно получение доступа к защищаемой информации любой степени конфиденциальности.
30. Загрузите СЗИ «Dallas Lock 7.0» с правами администратора. Выполните преобразование начальной области диска C: размером 100 кб (выберите вариант «Произвольная область», начало — 0 кб, размер 100 кб).

Внимание! Преобразование всего диска объемом 2 Гб занимает более 30 минут, что неприемлемо на практических занятиях, ограниченных по времени проведения. Преобразование только 100 кб начальной области, которое осуществляется в течение нескольких секунд, рекомендуется производить только в

процессе обучения. Для полноценной защиты от НСД в соответствии с требованиями четвертого класса защищенности [6] необходимо выполнить преобразование всего диска.

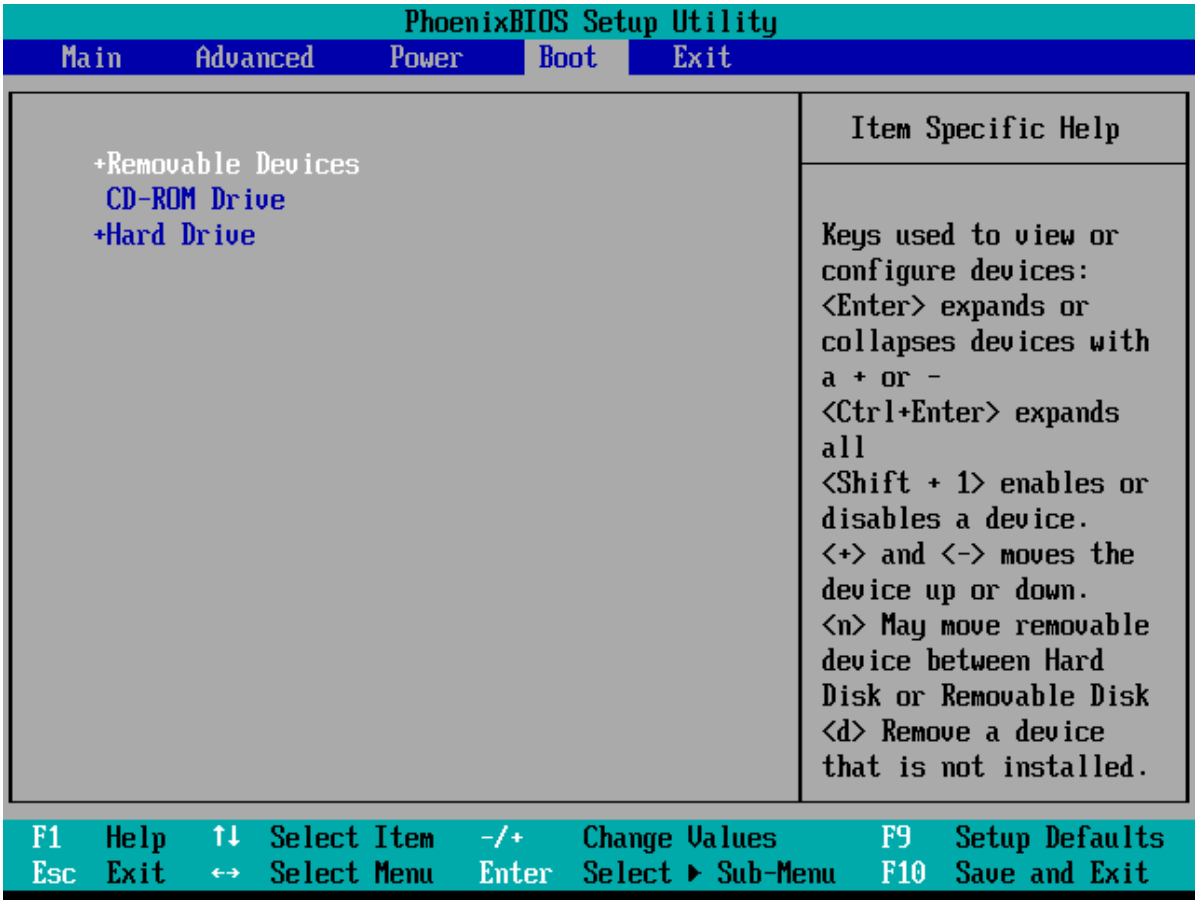


Рис. 3.40. Окно настройки BIOS Setup

31. Еще раз загрузите компьютер с внешнего носителя, убедитесь, что при включенном режиме преобразования дисков невозможно получение доступа к защищаемой информации в обход механизмов защиты СЗИ.
32. Установите в настройках BIOS Setup запрет загрузки с внешних носителей и задайте пароль на изменение настроек. Убедитесь, что загрузка компьютера с внешнего носителя теперь невозможна.

3.4. Система защиты информации «Secret NET 5.0-C»

3.4.1. Общие сведения

СЗИ «Secret Net 5.0-C» (разработчик ЗАО НИП «ИНФОРМЗАЩИТА») является программно-аппаратным комплексом, аппаратная часть которого предназначена для выполнения процедуры идентификации пользователей с применением электронных идентификаторов. Система «Secret Net 5.0-C» предназначена для защиты от несанкционированного доступа к информационным ресурсам компьютеров, функционирующих на платформах операционных систем MS Windows 2000/XP/2003. Компьютер с установленной системой может работать автономно (без подключения к сети), в одноранговой сети или в сети с доменной организацией. Система «Secret Net 5.0-C» не подменяет стандартные защитные механизмы, предоставляемые ОС Windows, и не ограничивает возможность их использования, а расширяет их за счет дополнительных программных и аппаратных средств.

Для более тесного взаимодействия «Secret Net 5.0-C» с программно-аппаратным комплексом ПАК «Соболь» предусмотрен режим интеграции, позволяющий средствами администрирования «Secret Net 5.0-C» управлять важнейшими функциями «электронного замка».

С помощью программных и аппаратных средств «Secret Net 5.0-C» реализуются следующие защитные механизмы:

1. Механизм контроля входа в систему с использованием аппаратных средств.
2. Механизмы разграничения доступа и защиты ресурсов:
   - механизм полномочного разграничения доступа к объектам файловой системы;
   - механизм замкнутой программной среды;
   - механизм шифрования файлов;
   - механизм разграничения доступа к устройствам компьютера;
   - механизм затирания информации, удаляемой с дисков компьютера.
3. Механизмы контроля и регистрации событий:
   - механизм функционального контроля;
   - механизм регистрации событий безопасности;
   - механизм контроля целостности;
   - механизм контроля аппаратной конфигурации компьютера.

Наличие механизма шифрования файлов выгодно отличает СЗИ «Secret Net 5.0-C» от рассмотренных выше аналогов и делает универсальным и комплексным средством защиты компьютерной информации. СЗИ «Secret Net 5.0-C» является программно-аппаратным комплексом, однако практическое знакомство с ним и обучение основам работы возможны и при отсутствии аппаратной составляющей. При этом в качестве идентификаторов можно использовать имена пользователей, а для их аутентификации – только обычные пароли ОС Windows.

3.4.2. Запуск и регистрация в системе защиты

Установку системы защиты «Secret Net 5.0-C» необходимо производить в ОС MS Windows 2000/XP/2003 *с предустановленным офисным пакетом*. Для работы с системой на практических занятиях используется предварительно установленный экземпляр системы в виде образа виртуальной машины VMware, в котором имеется пользователь Администратор с паролем **12345**.

В процессе загрузки ОС появляется окно запроса идентификатора пользователя, являющееся модификацией стандартного окна загрузки ОС Windows, в оболочку которой встраивается средство защиты (рис. 3.41). Дальнейшие действия по конфигурированию СЗИ осуществляются с помощью инструментов из меню ОС Windows ***«Пуск» ⇒ «Программы» ⇒ «Secret Net 5».***

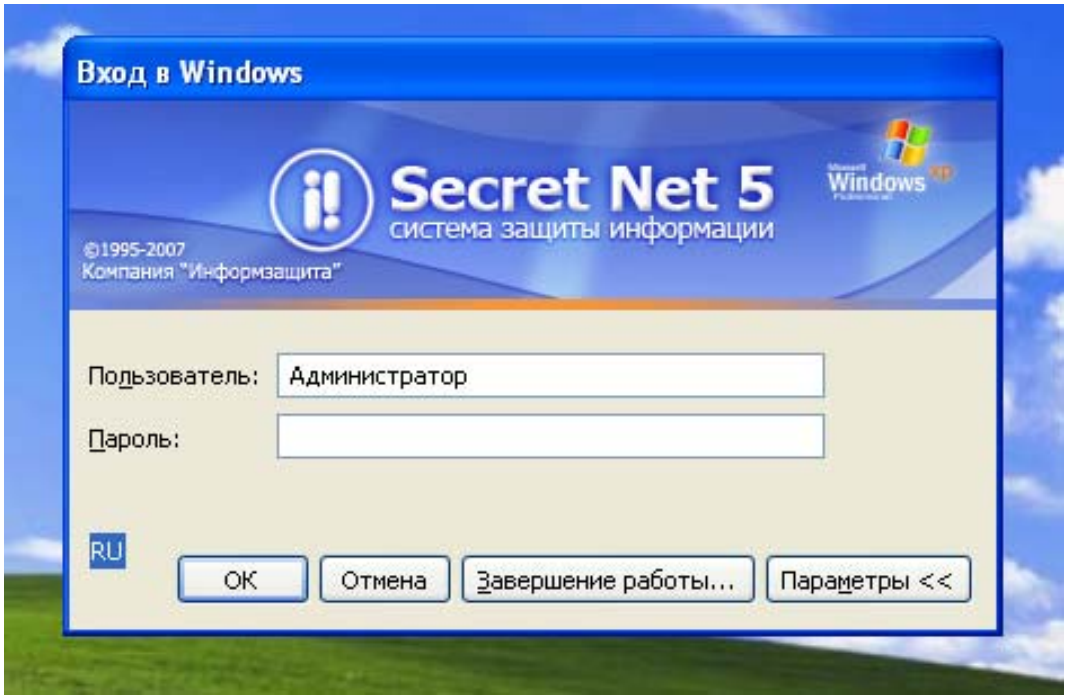


Рис. 3.41. Регистрация в СЗИ «Secret Net 5.0-C»

ВЫПОЛНИТЬ!

1. Загрузить образ СЗИ «Secret Net 5.0-C» и зарегистрироваться в системе пользователем Администратор, введя пароль «12345».

3.4.3. Создание учетных записей пользователей

В отличие от предыдущих версий СЗИ, создание учетных записей пользователей в «Secret Net 5.0-C» осуществляется с использованием стандартной оснастки ОС Microsoft Windows «***Управление компьютером***», что делает эту работу вполне привычной для администратора. Для создания учетных записей необходимо из этого окна выполнить команду ***«Пользователи» ⇒ «Новый пользователь…»***. В стандартном окне следует ввести имя пользователя и за-

дать для него пароль (рис. 3.42). На вкладке «Общие» рекомендуется установить параметр «Потребовать смену пароля при следующем входе в систему». Затем следует настроить свойства нового пользователя, вызвав элемент «Свойства» его контекстного меню и выбрав вкладку «Secret Net 5.0-C» (рис. 3.43). Открывающееся окно имеет ряд принадлежащих СЗИ элементов:

a. «Идентификатор» – подготовка и присвоение пользователю электронных идентификаторов;
b. «Криптоключ» – генерация и «выдача» пользователю криптографического ключа;
c. «Доступ» – назначение пользователю уровня допуска для организации полномочного управления доступом;
d. «Сервис» – копирование ключей для управления электронным замком «Соболь».

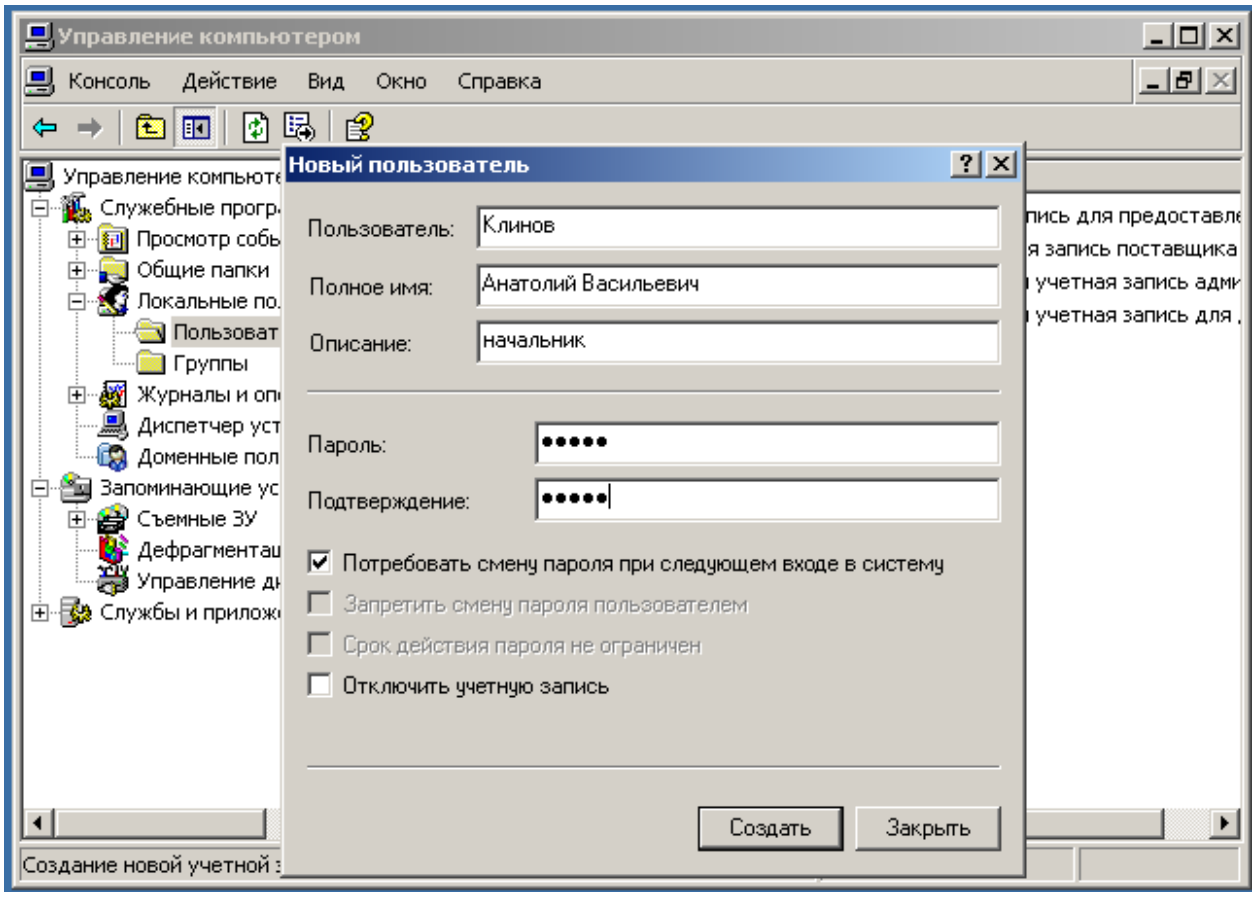


Рис. 3.42. Добавление учетных записей новых пользователей

ВЫПОЛНИТЬ!

2. Создать учетные записи пользователей: Клинов, Соколов, Савин, Свалов, Ювченко. Пароли выбрать произвольно.

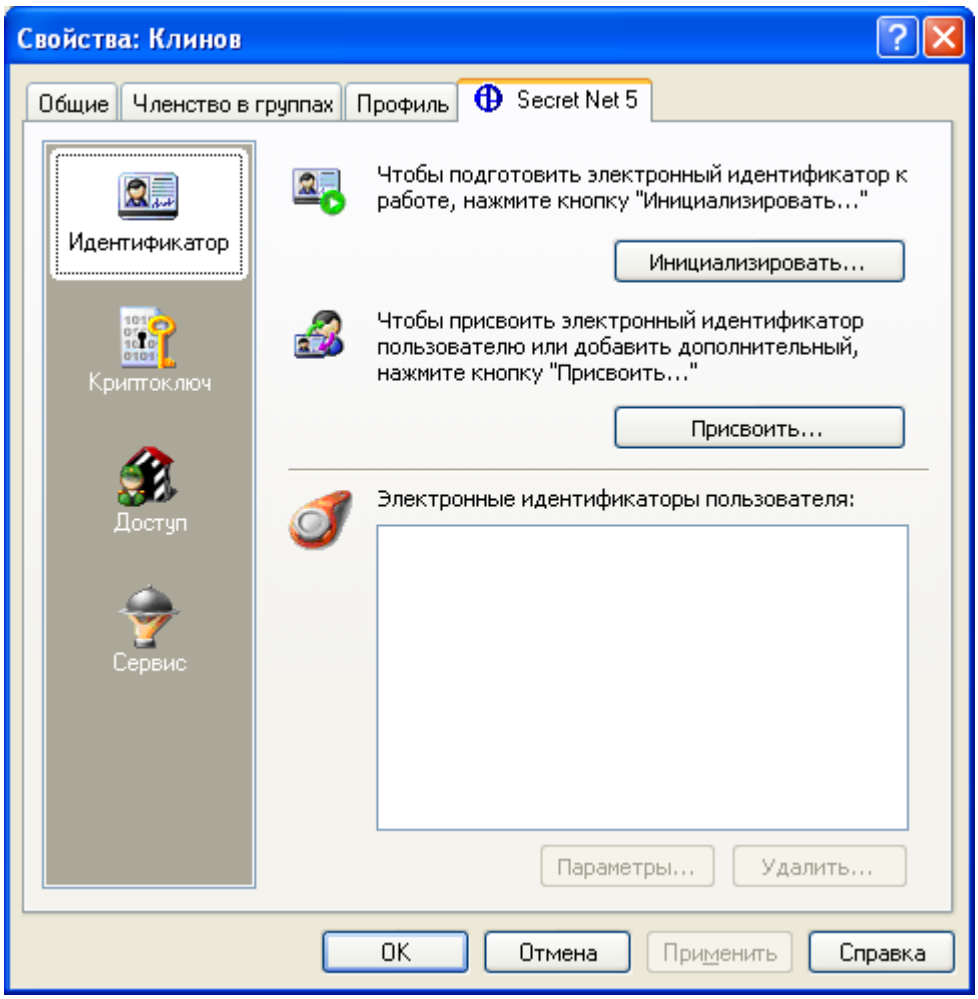


Рис. 3.43. Вкладка «Secret Net 5»

3.4.4. Реализация дискреционной модели разграничения доступа

Дискреционная модель разграничения доступа к файлам и каталогам реализуется в СЗИ «Secret Net 5.0-C» стандартным способом посредством списков доступа ОС Windows 2000/XP/2003 (рис. 3.44).

В тоже время списки NTFS-разрешений дополнены средствами разграничения доступа к дискам и портам. СЗИ позволяет управлять доступом к сменным накопителям (дисковод, привод CD-ROM), логическим дискам и портам ввода/вывода (COM-, LPT-, USB-портам). Режим управления доступа к дискам и портам по умолчанию работает в *мягком* режиме (режиме накопления информации в журнале). Чтобы перевести его в *жесткий* режим, необходимо установить параметр «Разграничение доступа к устройствам: Режим работы» (в оснастке «Локальные политики безопасности» $\Rightarrow$ «Настройки подсистем») в значение «жесткий» (рис. 3.45).

После включения указанного режима необходимо указать возможность доступа к дискам и портам, изменяя свойства этих устройств в оснастке «Локальные политики безопасности» $\Rightarrow$ «Устройства» (рис. 3.46).

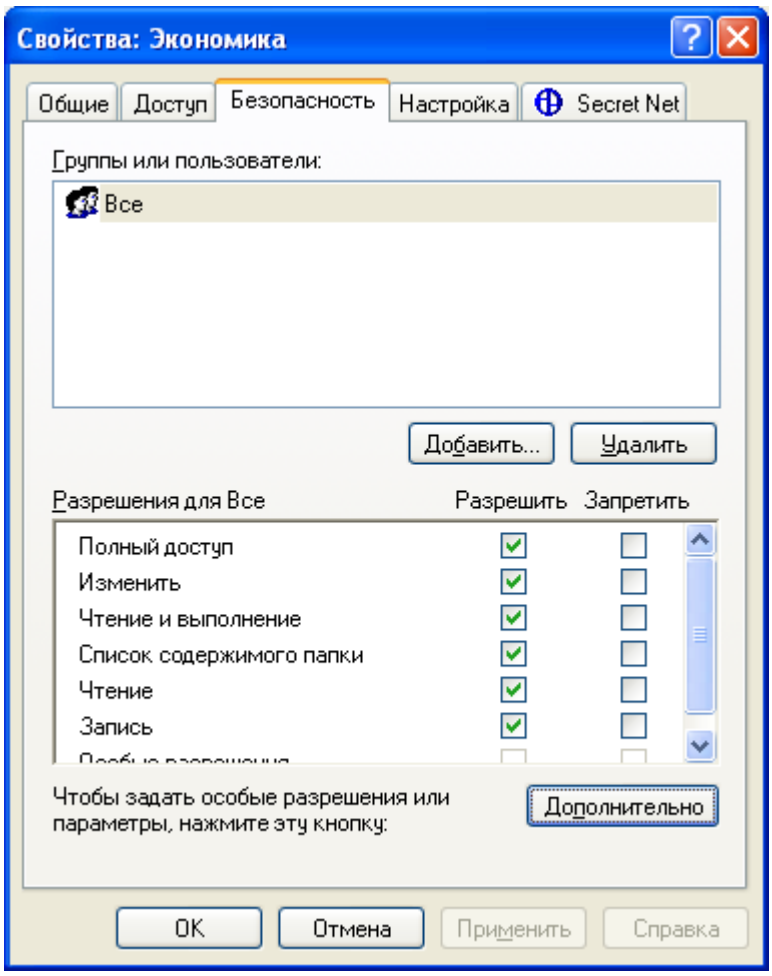


Рис. 3.44. Редактирование NTFS-разрешений

ВЫПОЛНИТЬ!

3. В соответствии с рис. 3.15 создать иерархическую структуру каталогов. Разграничить права доступа пользователей к созданным каталогам в соответствии с табл. 2.2.
4. Группе «Пользователи» разрешить доступ к каталогу «C:\Проекты\Полет\Текстовые документы» и его подкаталогам с правом «Изменения».
5. Зарегистрироваться пользователем Свалов, убедиться, что каталог «C:\Экономика» для него недоступен, но доступен для пользователя Ювченко.
6. Создать в каталоге «C:\Приказы и распоряжения» пользователем Клинов короткий текстовый файл «Приказ1.txt» с приказом об увольнении Соколова. Убедиться, что Соколов сможет прочитать приказ о своем увольнении, но не сможет изменить его.

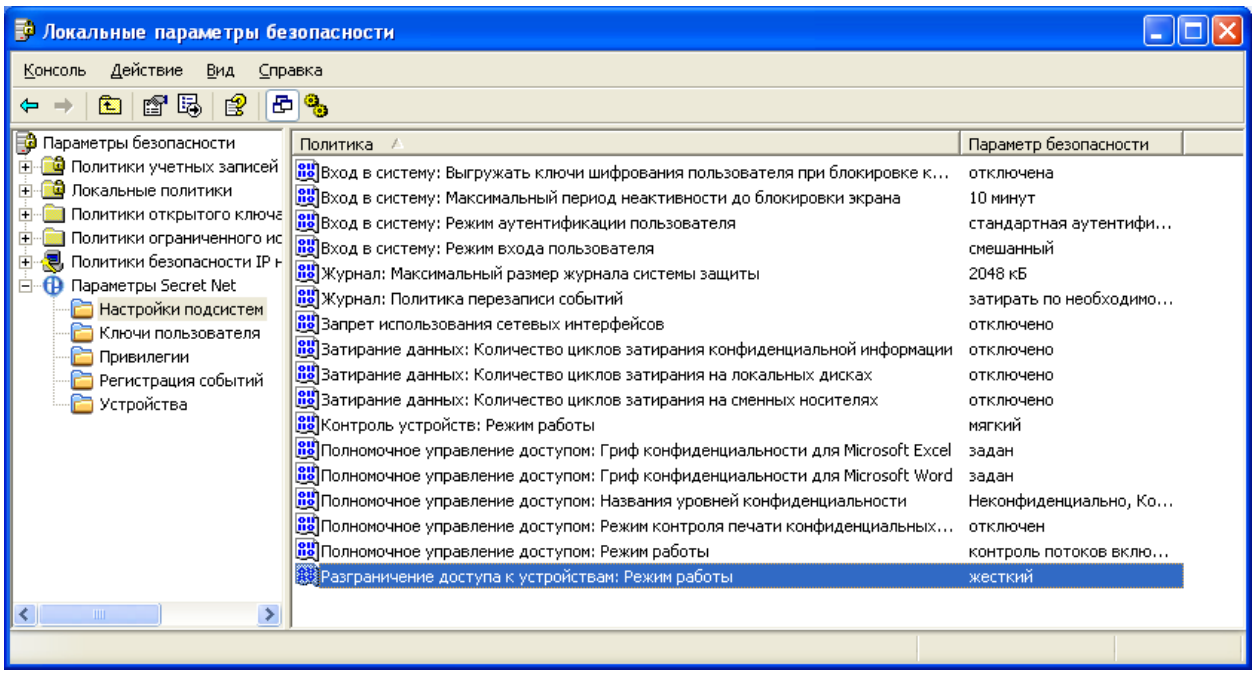


Рис. 3.45. Включение жесткого режима управления доступом к дискам и портам

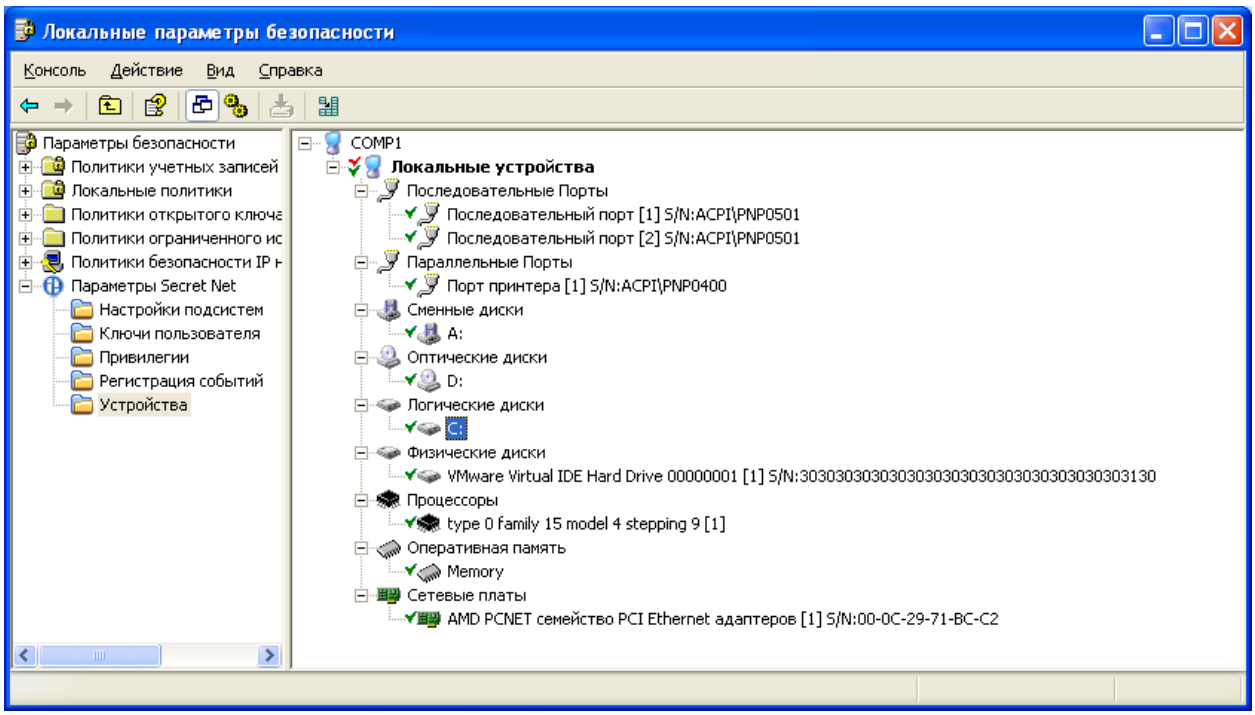


Рис. 3.46. Предоставление прав доступа к дискам

3.4.5. Реализация мандатной модели разграничения доступа

Мандатная модель разграничения доступа в СЗИ «Secret Net 5.0-C» реализована посредством назначения защищаемым ресурсам и каждому пользователю автоматизированной системы специальных меток конфиденциальности и сравнения их при запросах на доступ. В СЗИ «Secret Net 5.0-C» мандатная модель разграничения доступа именуется «Полномочное управление доступом».

Мандатное управление доступом по умолчанию включено. Однако для предотвращения утечки информации из конфиденциальных документов (см. требование 7 к защите компьютерной системы, приведенное в п. 1.1), необходимо установить параметр «Полномочное управление доступом: Режим работы» в активное состояние: «Контроль потоков включен». Данная настройка находится в стандартной оснастке ОС Windows «Локальные политики безопасности» (***«Пуск» ⇒ «Программы» ⇒ «Secret Net 5»***), в ней выбрать ***«Параметры безопасности» ⇒ «Параметры Secret Net» ⇒ «Настройки подсистем»*** (рис. 3.47).

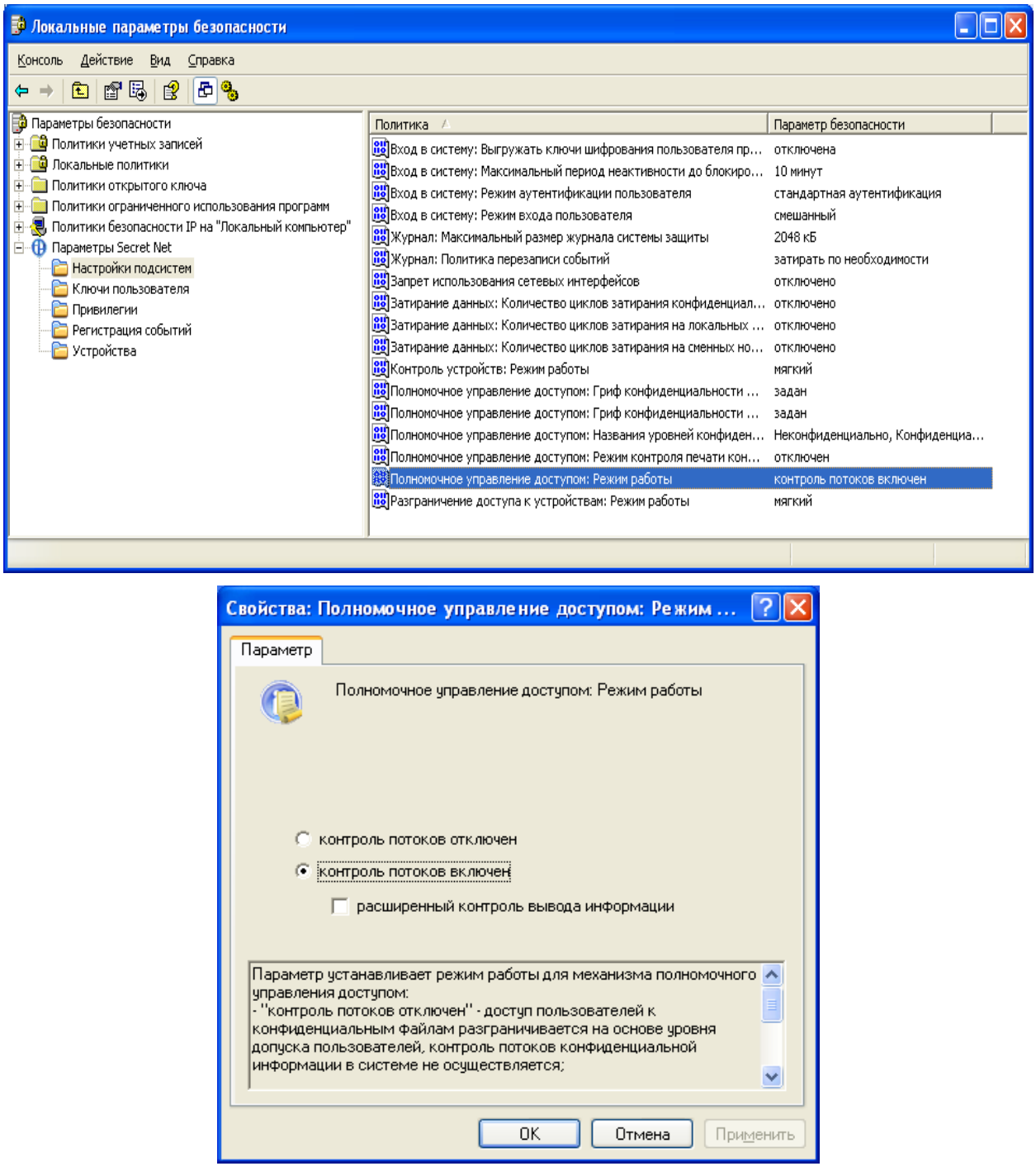


Рис. 3.47 Установка режима мандатного принципа управления доступом

ВЫПОЛНИТЬ!

7. Включить режим контроля потоков конфиденциальной информации.

Метки конфиденциальности могут быть установлены для логических дисков, каталогов и файлов, находящихся только на разделах с файловой системой NTFS. В СЗИ «Secret Net 5.0-C» используются следующие наименования меток конфиденциальности в порядке их повышения: «Неконфиденциально», «Конфиденциально» (соответствует грифу «Секретно») и «Строго конфиденциально» (соответствует грифу «Совершенно секретно»). Все ресурсы, созданные до включения режима мандатного принципа управления доступом, имеют метку «Неконфиденциально». Для включения наследования меток конфиденциальности при добавлении объектов доступа необходимо в свойствах каталога установить пункт «Автоматически присваивать новым файлам» (рис. 3.48).

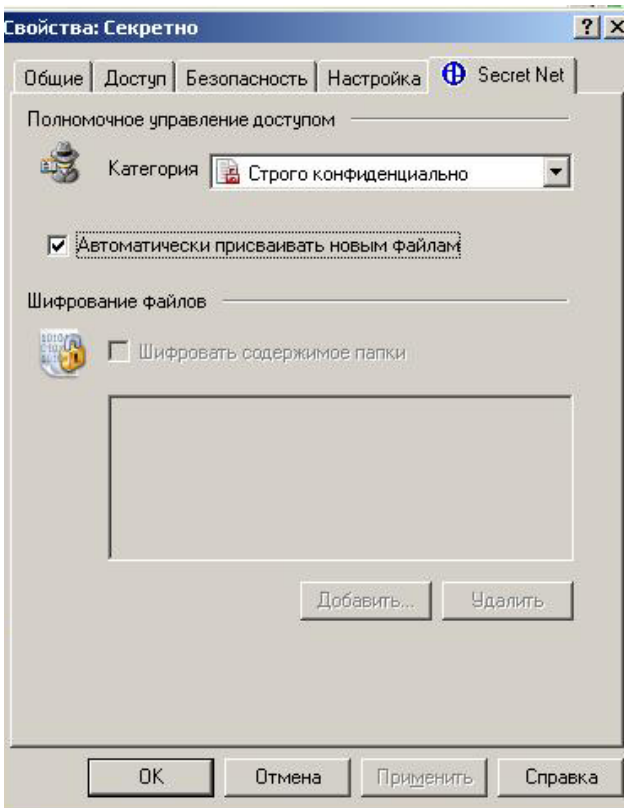


Рис. 3.48. Установка метки конфиденциальности

При назначении пользователем метки конфиденциальности уже существующему каталогу по желанию пользователя в окне, которое автоматически генерируется системой, можно присвоить такой же уровень доступа ко всем вложенным каталогам и файлам (рис. 3.49).

Привилегией засекречивания (повышения метки конфиденциальности) ресурсов обладает любой пользователь в пределах уровня конфиденциальности сессии. Для понижения уровня конфиденциальности ресурсов требуется наличие привилегии «Управление категориями конфиденциальности», которой целесообразно наделять только для администратора системы.

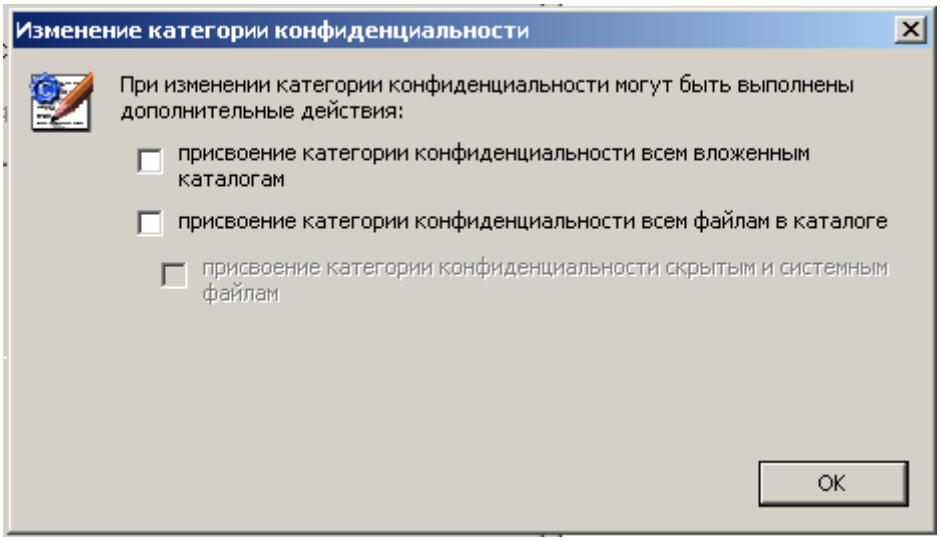


Рис. 3.49. Назначение меток конфиденциальности вложенным каталогам и файлам.

Возможность доступа пользователя к конфиденциальному документу определяется установкой уровня допуска для каждого из пользователей на странице «Доступ» вкладки «Secret Net 5.0-C» окна свойств пользователя (рис. 3.50). По умолчанию для всех пользователей системы установлен уровень допуска «Неконфиденциально». Правами установки уровня допуска обладает только администратор СЗИ, который в свою очередь может разрешить пользователям управление категориями конфиденциальности создаваемых ими объектов (рис. 3.50).

ВЫПОЛНИТЬ!

8. Назначить созданным учетным записям пользователей уровни допуска в соответствии с табл. 2.1. Администратору назначить уровень допуска «Строго конфиденциально».
9. Перезагрузить систему. Зарегистрироваться администратором с максимальным уровнем допуска.
10. Назначить созданным каталогам метки конфиденциальности в соответствии с их названиями. Установить наследование меток конфиденциальности. В каталоге «C:\Проекты\Полет\Текстовые документы\Секретно» создать текстовый файл. Убедиться в наличии у файла соответствующей метки конфиденциальности.

После назначения меток конфиденциальности работа с конфиденциальными файлами организуется в соответствии с рядом правил [**Ошибка! Источник ссылки не найден.**], предназначенных для защиты информации от утечки (при включенном контроле потоков):

1. Доступ пользователя к файлу разрешается, если уровень конфиденциальности текущего сеанса пользователя не ниже категории конфиденциальности файла.

2. Пользователь, не имеющий доступ к файлу, может просмотреть содержимое конфиденциального каталога, в котором находится файл, но не может открыть файл.
3. Конфиденциальные файлы размещаются в каталогах, имеющих категорию конфиденциальности не ниже категории конфиденциальности файла.
4. Приложению присваивается уровень конфиденциальности соответствующий уровню конфиденциальности текущего сеанса пользователя. Открывать разрешается только файлы, имеющие уровень конфиденциальности не выше уровня конфиденциальности текущего сеанса. При сохранении отредактированного содержимого файла с более низким уровнем конфиденциальности его «метка» повышается до уровня конфиденциальности сеанса.
5. Пользователь, не обладающий привилегией «Управление категориями конфиденциальности», может повысить категорию конфиденциальности файлов не выше уровня конфиденциальности текущего сеанса.

Управление полномочным доступом возможно только при наличии соответствующих разрешений доступа на уровне дискреционной модели, которые могут быть назначены администратором системы, например, с помощью стандартных механизмов ОС MS Windows 2000/XP/2003.

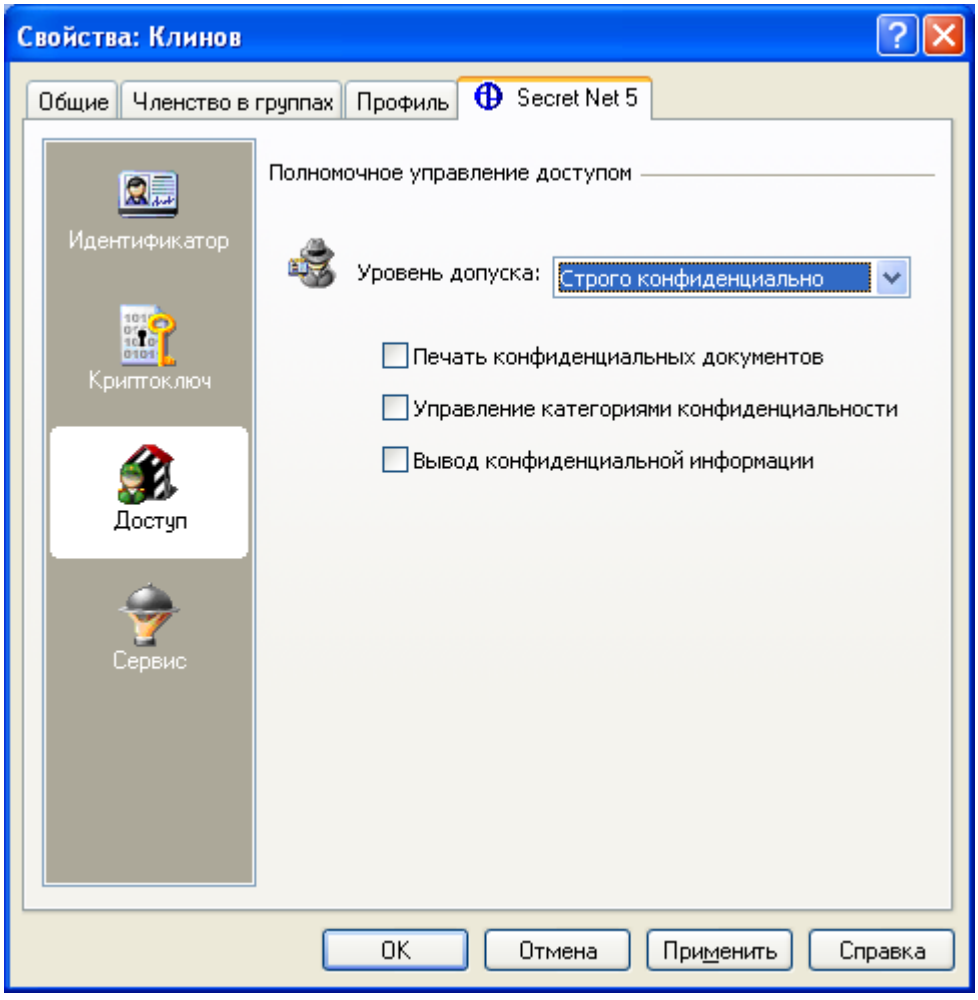


Рис. 3.50. Установка уровня допуска

ВЫПОЛНИТЬ!

11. Зарегистрироваться в системе пользователем Клинов с низшим уровнем конфиденциальности, просмотреть содержимое созданных каталогов. Все ли каталоги отображаются? Можно ли открыть эти каталоги? Войти в систему с высшим уровнем конфиденциальности, просмотреть содержимое созданных каталогов еще раз. Содержимое каких каталогов доступно данному пользователю?
12. От имени пользователя Клинов с высшим уровнем конфиденциальности, создать короткий текстовый документ «Клинов.txt» и попытаться сохранить его в каталог «С:\Проекты\Полет\Текстовые документы\Несекретно». Получилось ли это? Сохранить документ в каталоге «С:\Проекты\ Полет\Текстовые документы\ Секретно». Получилось ли это?
13. Попытаться скопировать содержимое из секретного документа в несекретный с использованием команд ***Правка ⇒ Копировать*** и ***Правка ⇒ Вставить***. Получилось ли это? Работает ли обратная операция вставки несекретных сведений в секретный документ?
14. Убедиться в невозможности копирования секретных файлов в несекретный каталог.
15. Зарегистрироваться пользователем Соколов, создать короткий текстовый документ «Соколов.txt» и сохранить его в каталоге «С:\Проекты\ Полет\Текстовые документы\Несекретно». Получилось ли это? Создать еще один текстовый документ «Соколов.txt» и сохранить его в каталоге «С:\Проекты\ Полет\Текстовые документы\Секретно». Получилось ли это? Почему? Может ли пользователь Соколов получить доступ к содержимому файлов из каталога «Секретно».

Следует отметить, что в СЗИ съемным носителям нельзя присвоить метку конфиденциальности, поэтому наличие даже полного доступа к накопителям не предоставляет пользователю возможности копирования на них конфиденциальных файлов или их фрагментов. Если принятая в организации технология обработки конфиденциальных документов допускает хранение их на съемных носителях, то пользователю дополнительно должно быть установлена привилегия «Вывод конфиденциальной информации» (рис. 3.50). Хотя такое действие сопровождается выводом окна предупреждения (рис. 3.51) и регистрацией данного действия в журнале, оно приводит к неконтролируемым возможностям по копированию конфиденциальных файлов и, следовательно, может быть применено лишь в исключительных случаях.

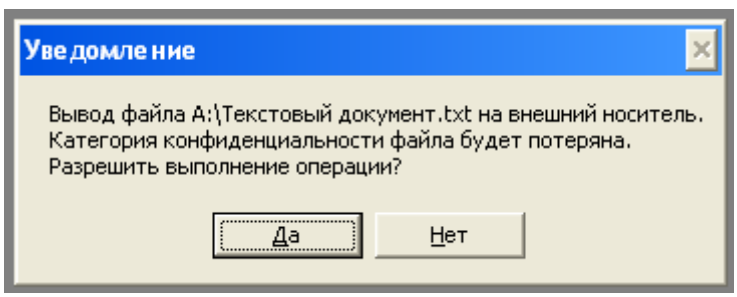


Рис. 3.51. Предупреждение о снижении метки конфиденциальности

3.4.6. Режим замкнутой программной среды

Механизм замкнутой программной среды (ЗПС) активизируется в СЗИ «Secret Net» путем выбора программы «Контроль программ и данных» из меню ***«Пуск» ⇒ «Программы» ⇒ «Secret Net»***. При первом запуске окна система предложит автоматически настроить контролируемые ресурсы, на что потребуется несколько минут.

ВЫПОЛНИТЬ!

16. Зарегистрироваться администратором с несекретным уровнем допуска. Запустить программу «Контроль программ и данных».
17. Для включения режима «Замкнутая программная среда» установить галочку «Режим ЗПС включен» на закладке ***«Субъекты управления» ⇒ «Имя компьютера» ⇒ «Свойства» ⇒ «Режимы»*** (рис. 3.52, рис. 3.53).
18. Здесь же целесообразно активировать режимы «Проверить целостность модулей перед запуском» и «Проверять заголовки модулей перед запуском». Однако для повышения быстродействия при выполнении работы указанные режимы включать не рекомендуется.
19. Отключить «Мягкий режим».
20. Зарегистрироваться Клиновым, убедиться, что он может пользоваться программами Блокнот и Калькулятор, но не может запустить программы офисного пакета.

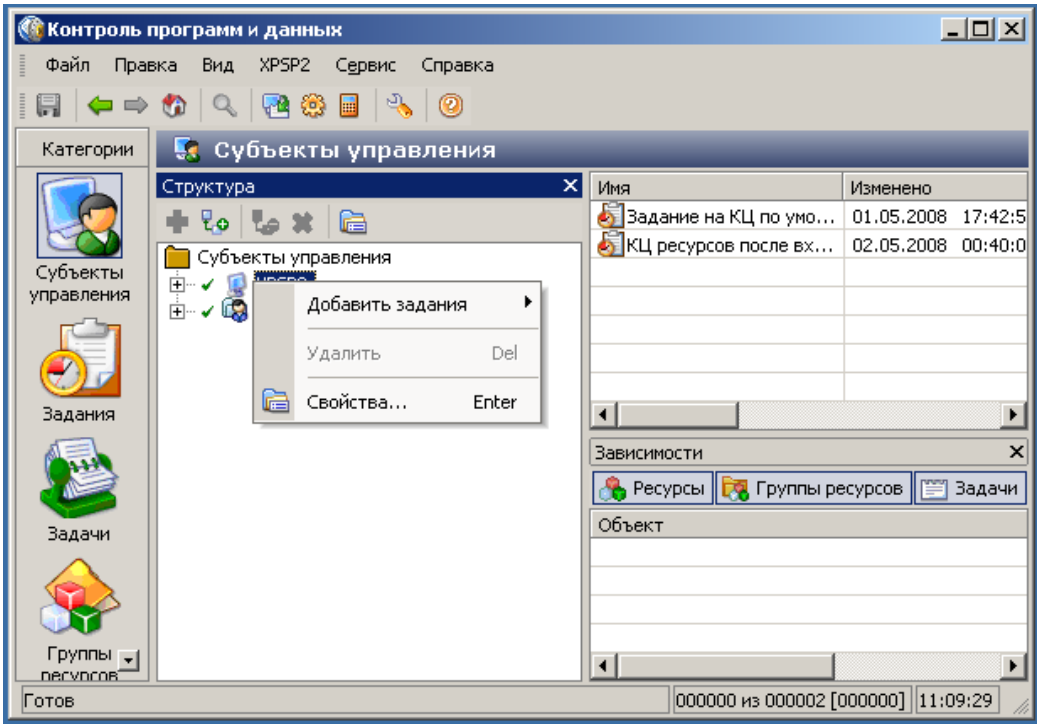


Рис. 3.52. Программа «Контроль программ и данных»

Теперь всем пользователям может быть назначен индивидуальный список разрешенных к запуску программ. В связи со сложностью перечисления всех исполняемых модулей приложений, которые должны запускаться пользовате-

лем в сеансе работы, разработчиками СЗИ предлагается включение «мягкого» режима работы (рис. 3.53).

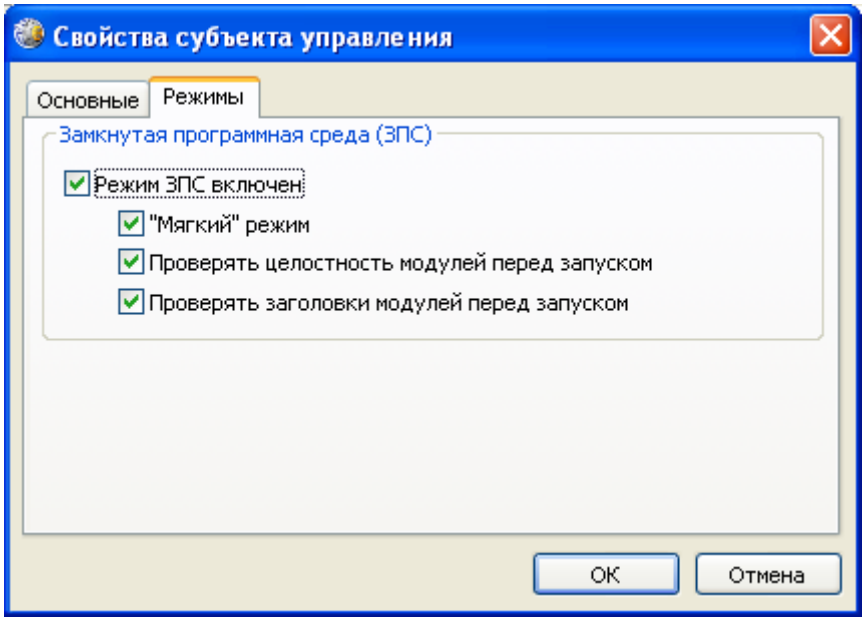


Рис. 3.53. Включение механизма замкнутой программной среды

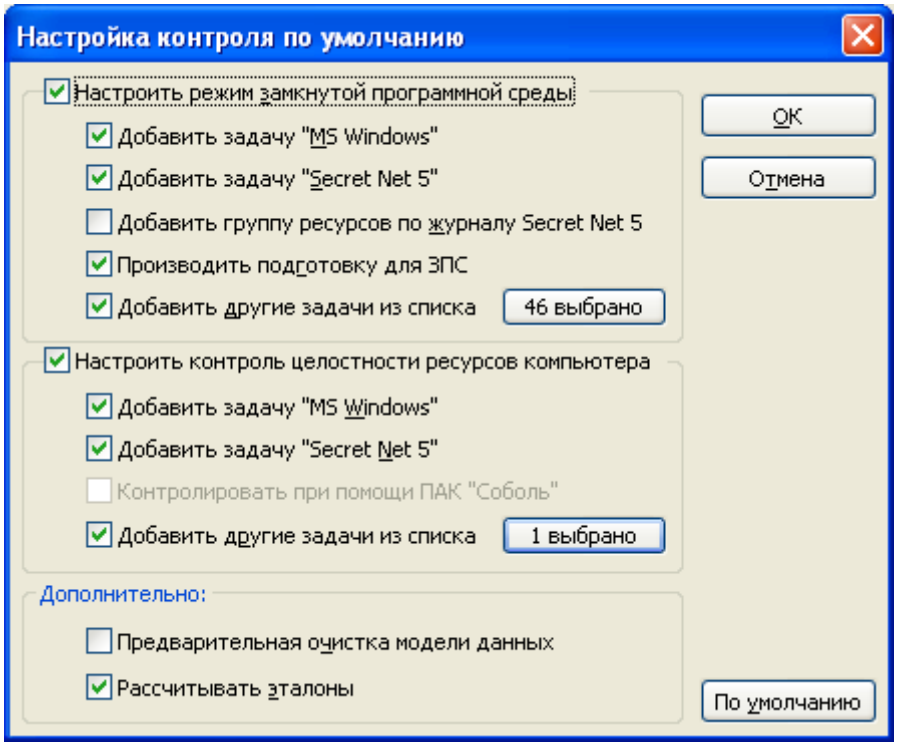


Рис. 3.54. Автоматический способ создания списка исполняемых модулей приложений

Этот режим особенно необходим в период отладочной эксплуатации системы, при его включении пользователю разрешается запускать любые приложения, а в журнале будут фиксироваться все программные модули, которые были запущены. После анализа журнала администратором будет получен список необходимых пользователю приложений, который и будет являться осно-

вой для формирования списка разрешенных к запуску исполняемых модулей приложений. Список может быть создан вручную или автоматически. При автоматическом способе необходимо первый раз запустить «Контроль программ и данных» (рис. 3.54), поставить галочку «Добавить другие задачи из списка», нажать кнопку «0 выбрано» и выбрать необходимые задачи для добавления в ЗПС. Данное действие приведет к формированию списка разрешенных для пользователя исполняемых модулей программ, который теперь может быть модифицирован вручную. Одновременно можно создать и список файлов для контроля целостности (КЦ). Пример списка разрешенных программ приведен на рис. 3.55.

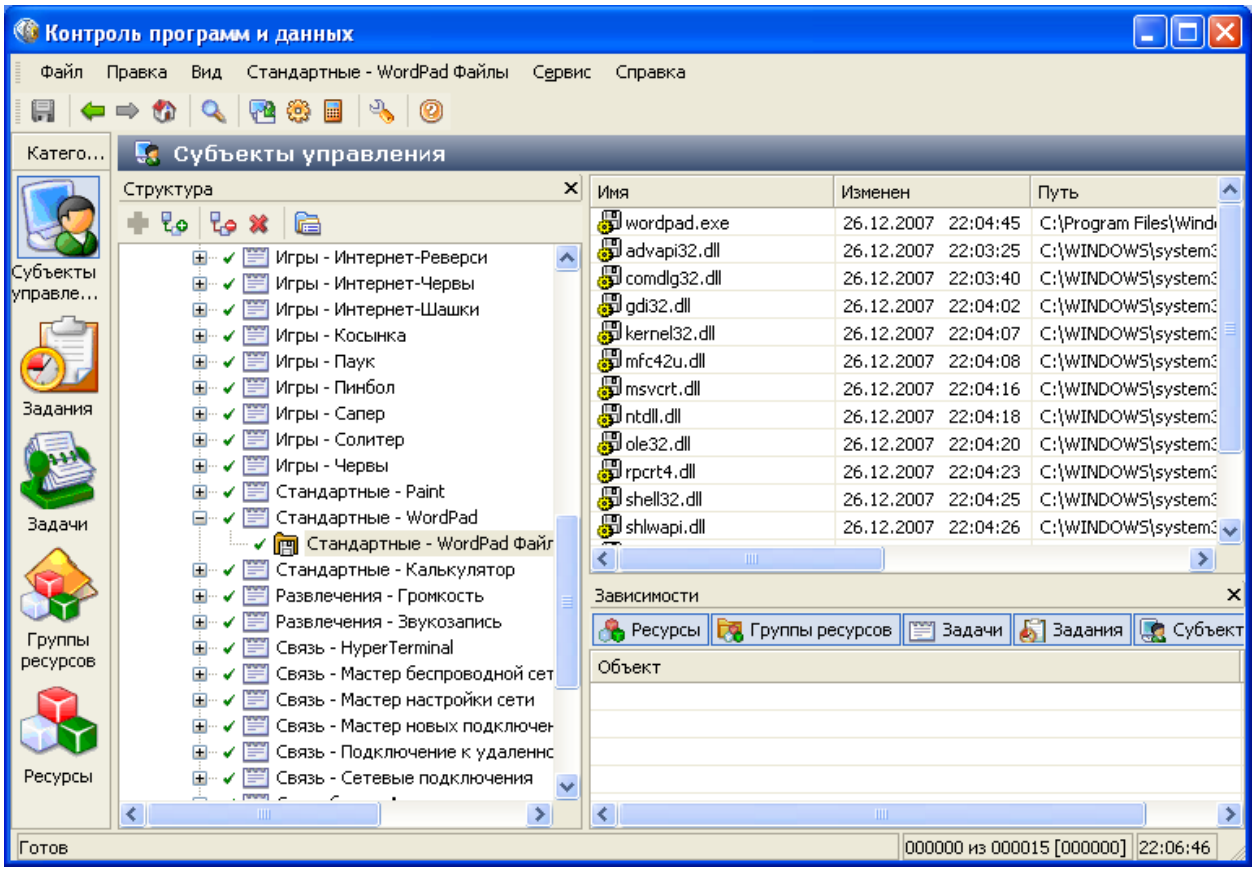


Рис. 3.55. Список разрешенных программ

Следует иметь в виду, что режим автоматического добавления исполняемых модулей в список ЗПС часто добавляет не все возможные приложения. Поэтому администраторам безопасности можно рекомендовать список разрешенных к запуску программ создавать вручную. Делается это, например, для ресурсов Documents and Settings, Program Files, WINDOWS и ряда специальных программ.

ВЫПОЛНИТЬ!

21. Зарегистрироваться администратором с несекретным уровнем допуска. Запустить программу «Контроль программ и данных». Выбрать пункт ***«Задания» ⇒ «ЗПС для группы Users»*** (рис. 3.57).

22. Выбрать пункт ***«Добавить задачи/группы» ⇒ «Новую группу по каталогу…»***. Указать каталог «C:\Program Files».
23. Зарегистрироваться пользователем Клинов, убедиться, что теперь он может запускать программы офисного пакета.

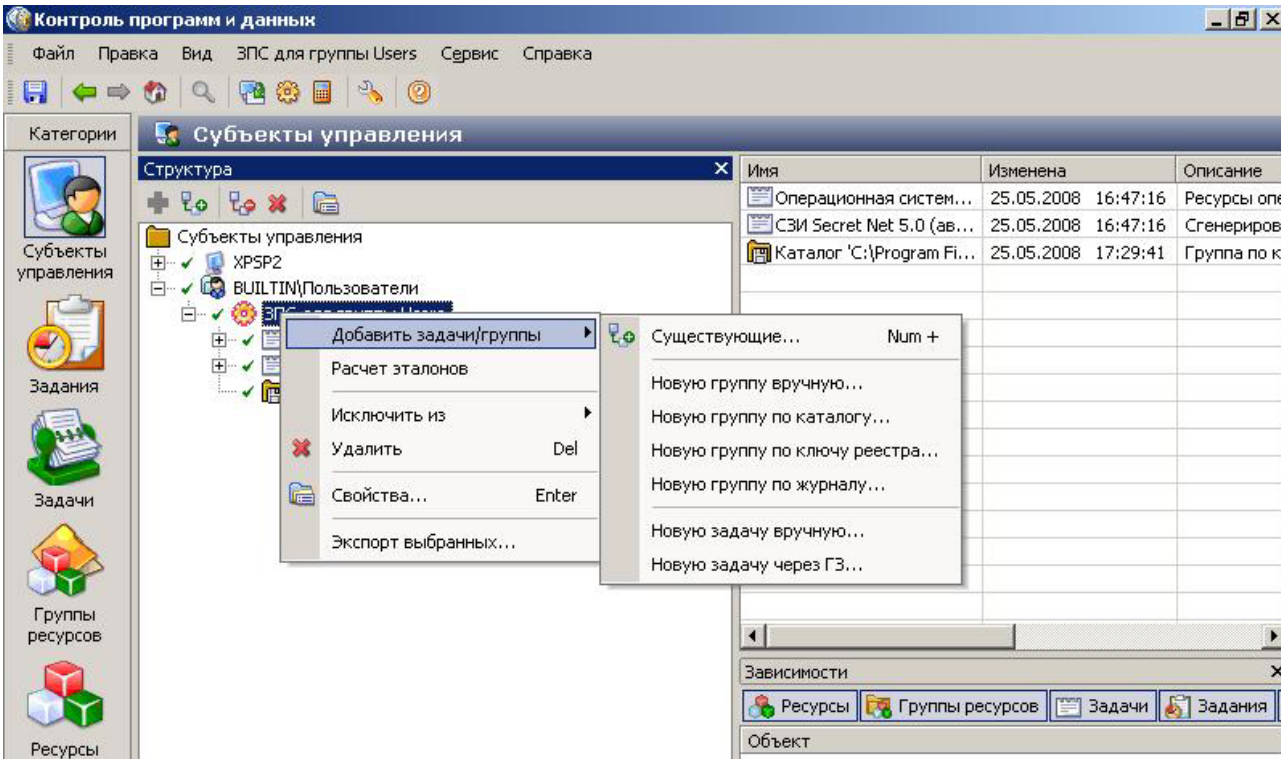


Рис. 3.56. Добавление разрешенных программ для групп пользователей

Механизм замкнутой программной среды (ЗПС) надежно защищает систему от запуска пользователем несанкционированных приложений. Так, в случае несанкционированного создания пользователем исполняемого файла в разрешенном каталоге, например, в папке «C:\WINDOWS», он не будет входить в список ЗПС. Подменить исполняемый файл, разрешенный к запуску, также невозможно, так как для каждого исполняемого модуля из списка ЗПС вычисляется контрольный эталон по одному из пяти алгоритмов (CRC7, ЭЦП, ХЭШ, имитовставка, полное совпадение).

3.4.7. Контроль целостности

СЗИ «Secret Net 5.0-C» включает в свой состав подсистему проверки целостности. СЗИ позволяет осуществлять контроль целостности файлов, каталогов, ключей реестра и их значений. По каждому из объектов может быть задан один из четырех типов контроля: сравнение содержимого объекта, атрибутов объекта, прав доступа, существование объекта. Алгоритмами проверки содержимого могут быть: сравнение содержимого, алгоритм CRC-7, имитовставка по ГОСТ 28147–89, электронно-цифровая подпись по ГОСТ Р 34.10–94, хэш-функция.

При нарушении целостности в СЗИ предусмотрена реакция в виде регистрации события в журнале, блокировки компьютера, восстановления исходного контролируемого параметра из эталона, либо пересчета контрольного значения. Контроль целостности может выполняться при загрузке ОС, при регистрации пользователя, при выходе пользователя либо по специально заданному расписанию. Добавление задания на контроль целостности производится в программе «Контроль программ и данных» автоматически или вручную, аналогично созданию списка ЗПС: ***«Контроль программ и данных» ⇒ «Задания» ⇒ «задания на КЦ по умолчанию» ⇒ «Свойства задания на КЦ»***. В окне «расписание» (рис. 3.57) можно настроить расписание периодического автоматического выполнения КЦ. Контроль целостности выбранных объектов может выполняться также при загрузке операционной системы, при логическом входе пользователя в систему или при выходе пользователя из нее.

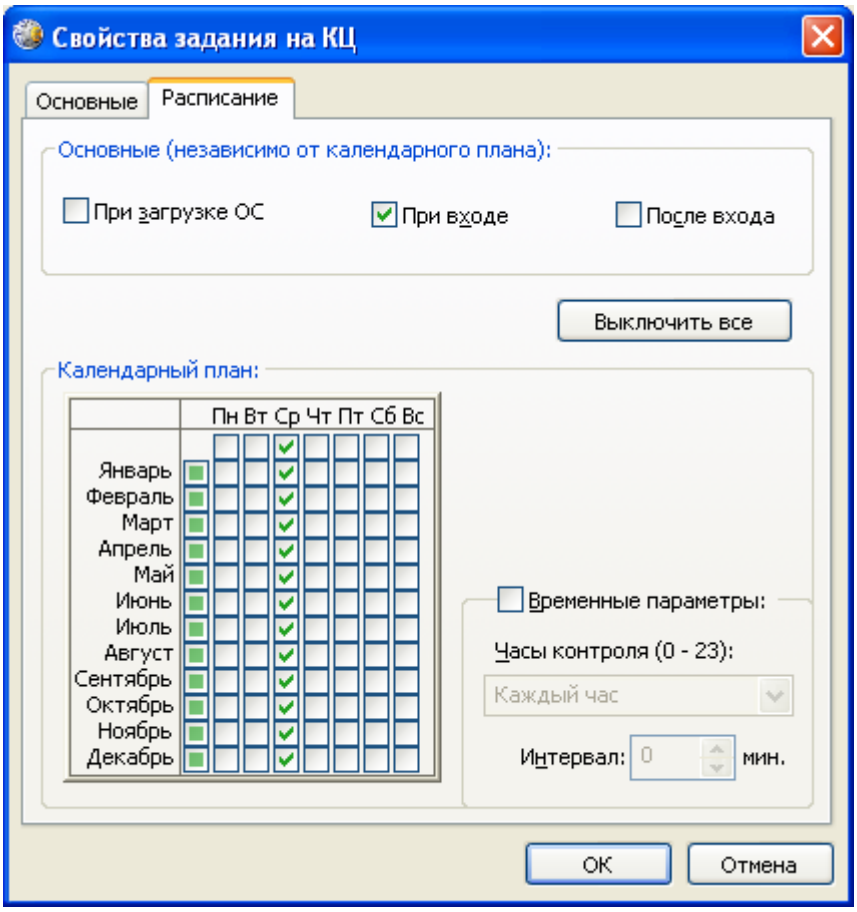


Рис. 3.57. Настройка контроля целостности в СЗИ «Secret Net 5.0-C»

ВЫПОЛНИТЬ!

24. Зарегистрироваться администратором, создать в каталоге «C:\База данных» короткий текстовый файл «DB.txt». Настроить контроль целостности этого файла с указанием контроля содержимого объекта по алгоритму ГОСТ Р 34.11–94 с регистрацией в журнале безопасности и блокировкой компьютера (рис. 3.58). Указать проведение контроля при входе.

25. Изменить содержимое файла «DB.txt». Завершить сеанс работы администратора. Можно ли зарегистрироваться иным пользователем, кроме администратора?
26. Выполнить пересчет эталонов контролируемых параметров ресурса «DB.txt».
27. Войти в систему пользователем Клинов, убедиться в отсутствии сообщения о нарушении контроля целостности.

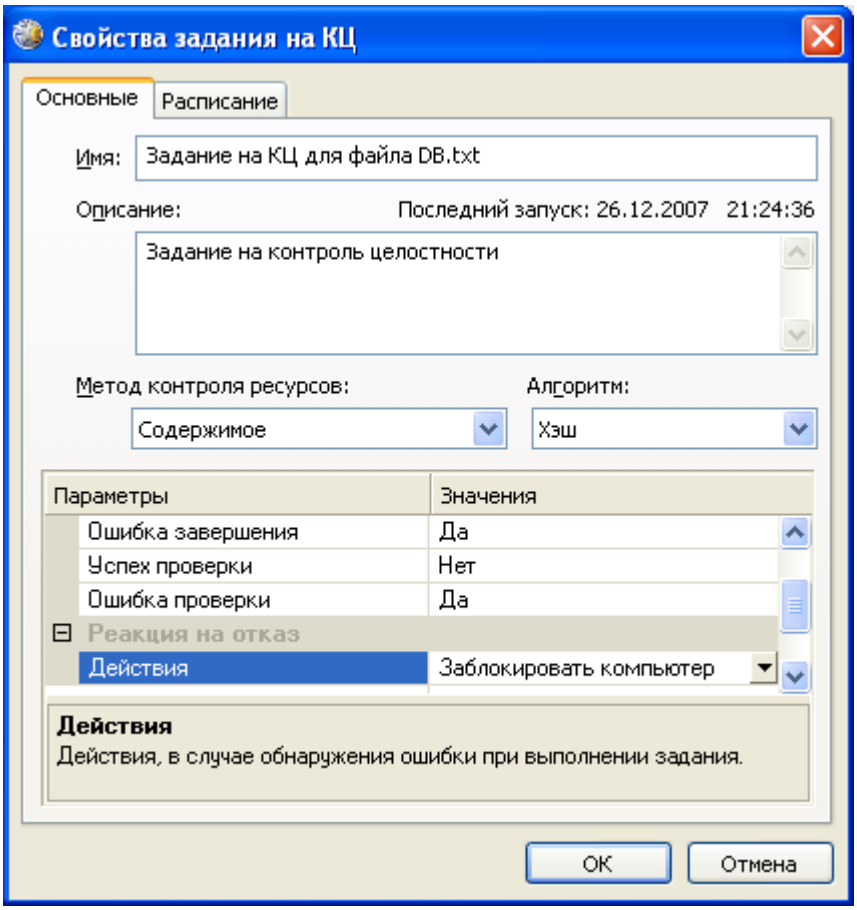


Рис. 3.58. Создание задания контроля целостности

3.4.8. Регистрация событий

СЗИ «Secret Net 5.0-C» для регистрации событий использует стандартные средства, присутствующие в ОС Windows NT, дополняя их возможностью регистрации ряда специальных событий. Важной особенностью реализации механизма регистрации событий является возможность использования как общего для всех пользователей перечня регистрируемых событий, так и персонального перечня, составляемого индивидуально для каждого пользователя.

Настройка политики аудита производится в оснастке ***«Локальные параметры безопасности» ⇒ «Параметры Secret Net» ⇒ «Регистрация событий»*** (рис. 3.59).

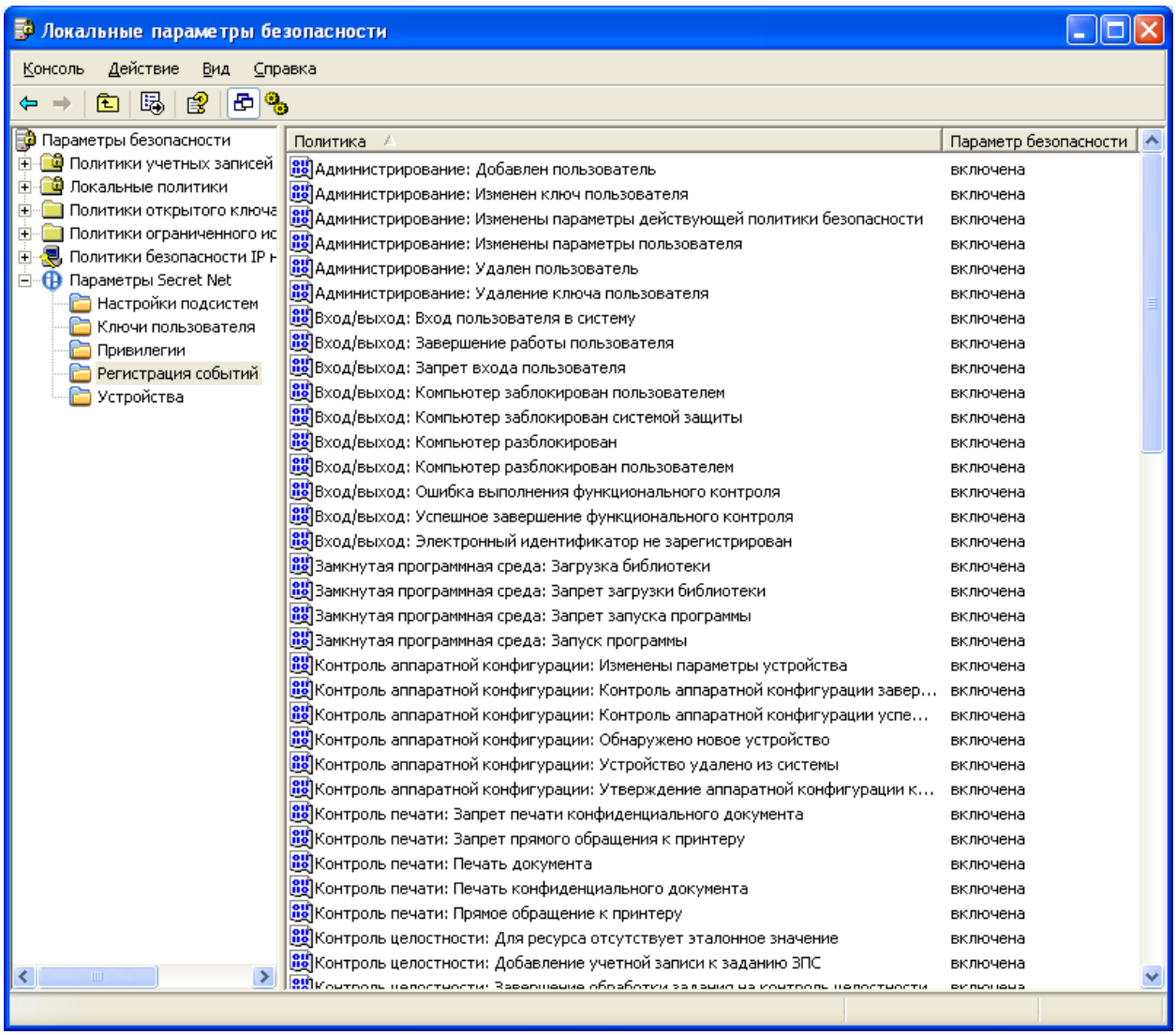


Рис. 3.59. Настройка политики аудита в СЗИ «Secret Net 5.0-C»

Анализ событий безопасности может производиться в стандартном окне «Просмотр событий» ОС Windows NT или с использованием специального средства «Журналы» СЗИ: ***«Пуск» ⇒ «Программы» ⇒ «Secret Net 5» ⇒ «Журналы»***. В этом окне (рис. 3.60) доступен просмотр журналов регистрации запуска приложений, системных событий и событий безопасности. Кроме того, имеется специальный журнал «Secret Net», в котором регистрируются критически важные для защищаемой системы и самого СЗИ события.

ВЫПОЛНИТЬ!

28. Зарегистрироваться администратором и в журнале событий найти событие, связанное нарушением целостности файла «DB.txt».
29. Найти записи, связанные с получением доступа к каталогу «C:\Проекты\Полет\Текстовые документы\Секретно» пользователем Клинов. Установить фильтр по типу события – «Доступ к конфиденциальному документу» и по имени пользователя – Клинов.

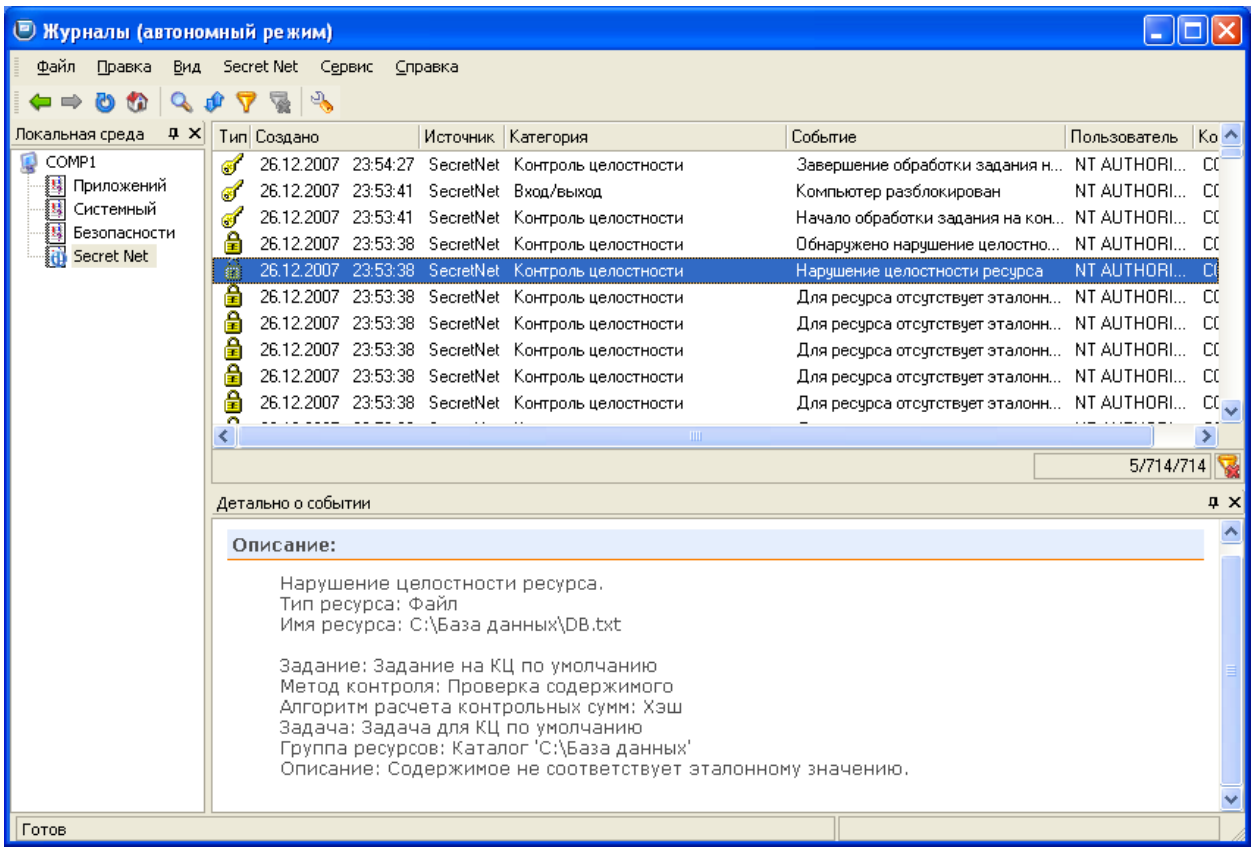


Рис. 3.60. Просмотр журналов регистрации событий

3.4.9. Печать штампа

СЗИ «Secret Net 5.0-C» позволяет создавать штамп на конфиденциальных документах, отправляемых на печать при использовании редактора MS Word и таблиц Excel. В процессе печати СЗИ дополняет колонтитулы печатаемого документа рядом полей. Перечень заполняемых полей формируется в файле – шаблоне STAMP.RTF, находящемся в каталоге «C:\Program Files\Infosec\ SecretNet5\Client».

Особенностью работы СЗИ «Secret Net 5.0-C» с конфиденциальными документами программ MS Word и Excel является создание временных технологических файлов в каталоге «C:\Documents and Settings\ %имя_пользователя%\Local Settings\Temp». В связи с тем, что при открытии конфиденциальных документов программа MS Word получает соответствующую метку конфиденциальности, то создаваемые временные файлы также должны получать соответствующие метки полномочного доступа. В соответствии с правилами полномочного доступа, каталог «C:\Documents and Settings\%имя_пользователя%\Local Settings\Temp», в котором создаются временные файлы, должен иметь метку конфиденциальности не ниже открываемых документов. Для этого необходимо в параметре HKLM\SYSTEM\ CurrentControlSet\Services\SnMC5xx\Params\SourceRedirect реестра ОС Windows добавить строку «\Local Settings\Temp».

Работа с конфиденциальными документами в режиме печати должна быть начата с включения параметра «Полномочное управление доступом: Режим контроля печати конфиденциальных документов» в оснастке «Локальные политики безопасности» ⇒ «Настройки подсистем» (рис. 3.61).

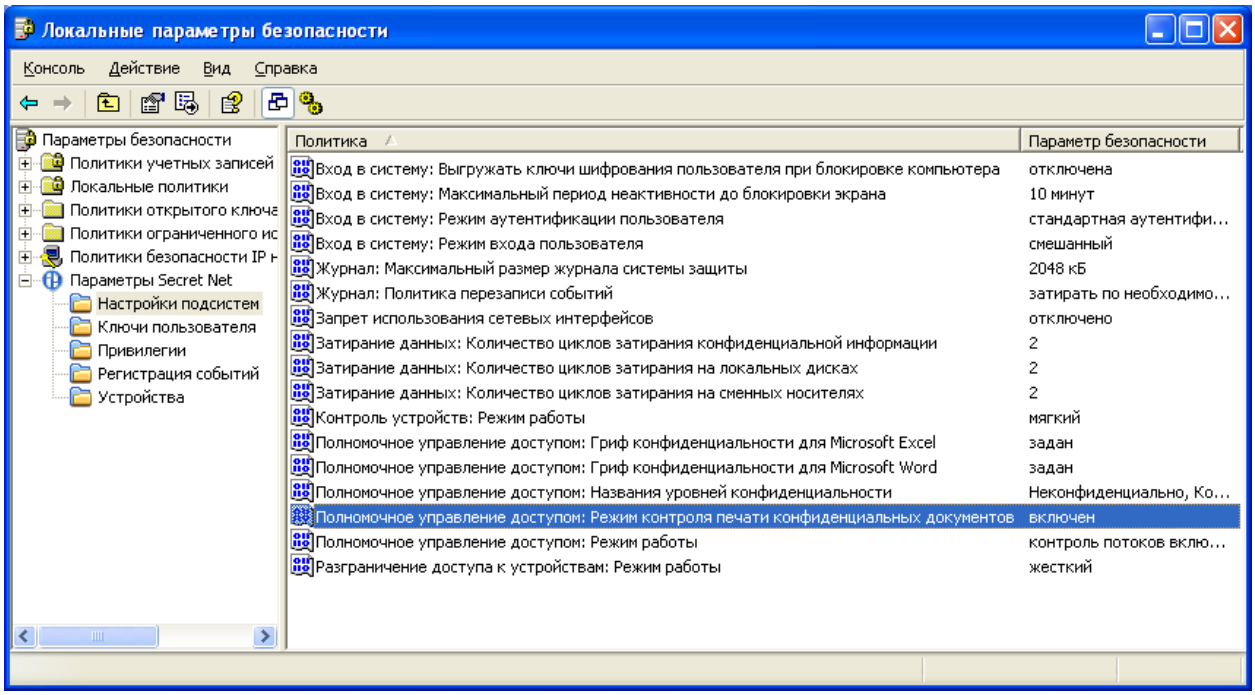


Рис. 3.61. Установка параметра «Полномочное управление доступом: Режим контроля печати конфиденциальных документов»

ВЫПОЛНИТЬ!

30. Установить параметр «Полномочное управление доступом: Режим контроля печати конфиденциальных документов».
31. Открыть редактор реестра, в параметре HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\SnMC5xx\Params\SourceRedirect добавить строку «\Local Settings\Temp».

Если параметр «Полномочное управление доступом: Режим контроля печати конфиденциальных документов» установлен и компьютер перезагружен, то нажатием кнопки «Редактировать» (***«Локальная политика безопасности» ⇒ «Параметры Secret Net» ⇒ «Настройки подсистем» ⇒ «Полномочное управление доступом: Гриф конфиденциальности для Microsoft Word»***) может быть запущена программа MS Word в режиме редактирования файла STAMP.RTF. Перейдя в режим редактирования колонтитулов, можно изменить содержание штампа, добавив в него требуемые поля (рис. 3.62). В шаблоне предусмотрено два варианта штампа, выбор варианта производится в процессе работы с документом при помощи панели инструментов «Грифы Secret Net». Часть полей в штампе заполняется автоматически, а часть требует заполнения пользователем в процессе вывода конфиденциального документа на печать.

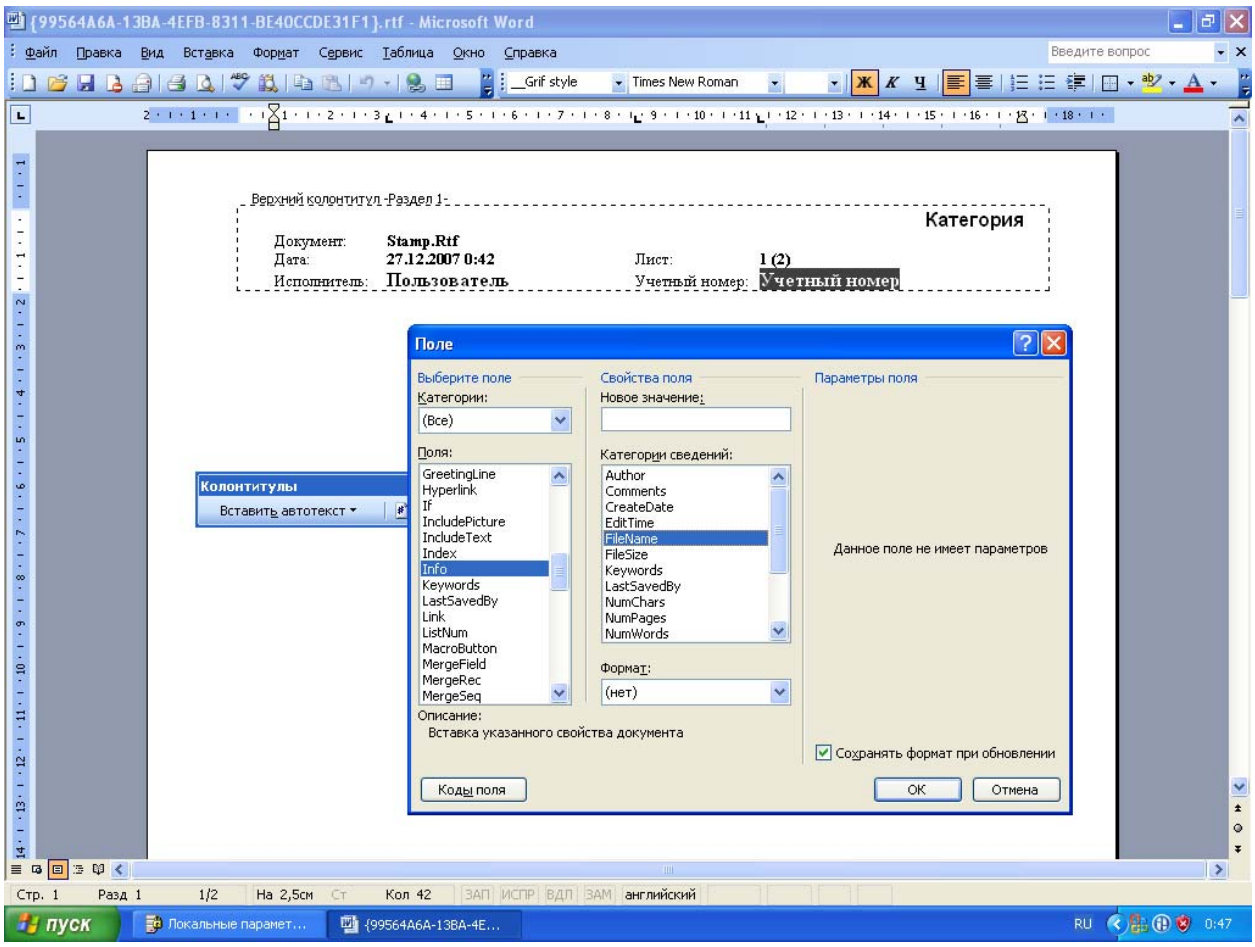


Рис. 3.62. Редактирование штампа конфиденциального документа

ВЫПОЛНИТЬ!

32. Зарегистрироваться пользователем Клинов с максимальным уровнем конфиденциальности, создать в каталоге «C:\Проекты\ Полет\Текстовые документы\Секретно» документ в формате MS Word.
33. Открыть созданный документ, выбрать «Гриф #2» в списке грифов Secret Net, выполнить предварительный просмотр печати документа.

3.4.10. Гарантированное удаление данных

Для включения механизма гарантированного уничтожения данных необходимо в оснастке ***«Локальные политики безопасности» ⇒«Параметры Secret Net» ⇒ «Настройки подсистем»*** изменить параметры «Затирание данных: Количество циклов затирания конфиденциальной информации», «Затирание данных: Количество циклов затирания на локальных дисках» и «Затирание данных: Количество циклов затирания на сменных носителях», указав в них ненулевое значение (рис. 3.63). Количество циклов затирания может варьироваться от 1 до 10.

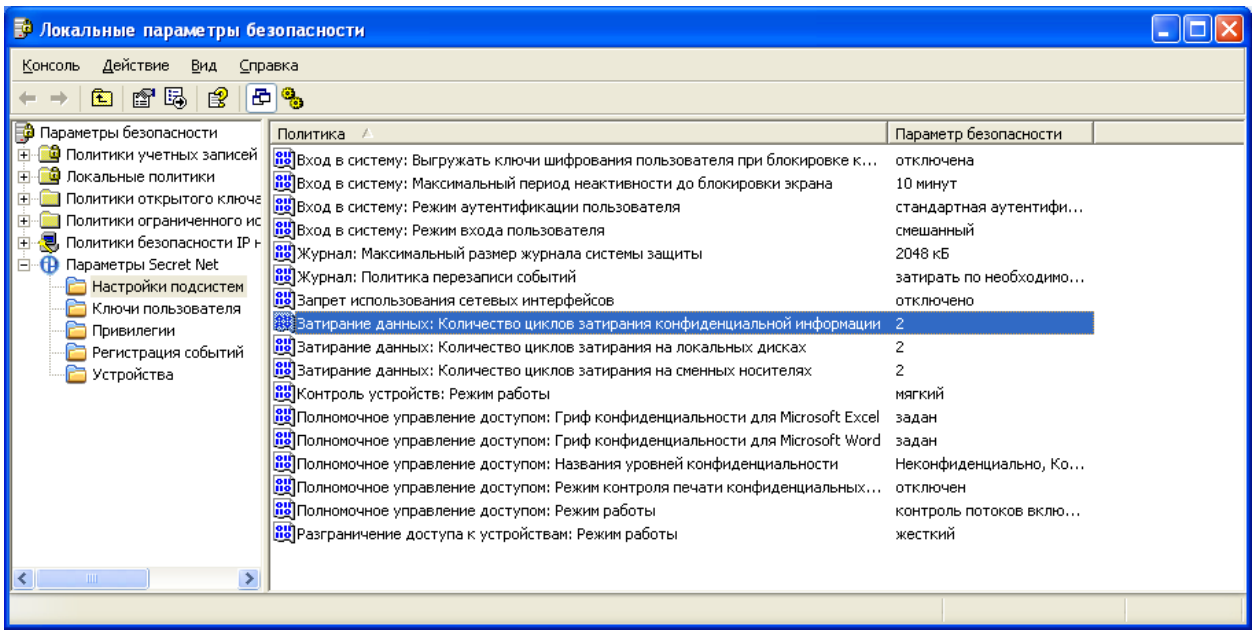


Рис. 3.63. Установка количества циклов затирания данных

ВЫПОЛНИТЬ!

34. Зарегистрироваться Администратором, включить параметры «Затирание данных: Количество циклов затирания конфиденциальной информации», «Затирание данных: Количество циклов затирания на локальных дисках».
35. Зарегистрироваться пользователем Клинов, создать короткий текстовый документ в каталоге «Секретно».
36. Зарегистрироваться Администратором, с помощью дискового редактора найти файловую запись созданного документа, отметить номер кластера, в котором хранятся данные.
37. Зарегистрироваться пользователем Клинов, удалить документ без помещения его в «Корзину».
38. Зарегистрироваться Администратором, открыть содержимое отмеченного кластера. Отметить изменения, произошедшие в кластере.

3.4.11. Настройка механизма шифрования

Являясь комплексной системой защиты компьютерной информации, СЗИ «Secret Net 5.0-C» позволяет пользователям шифровать персональные данные. В системе используется классический подход к организации криптозащиты данных, при котором информация зашифровывается на основе симметричных ключей, а те в свою очередь зашифровываются открытыми ключами пользователей и хранятся в заголовках зашифрованных файлов. Открытые ключи пользователей хранятся в локальной базе данных «Secret Net 5.0-C», закрытые ключи – в его персональном идентификаторе. Доступ к зашифрованным файлам могут иметь несколько пользователей, если их заголовок содержит ключ шифрования данных, зашифрованный несколькими персональными ключами.

В системе «Secret Net 5.0-C» управление шифрованием файлов и доступ к зашифрованным файлам осуществляются на уровне каталогов. Зашифрованные файлы располагаются только в шифрованных каталогах. Шифрованные каталоги могут содержать нешифрованные файлы и подкаталоги. Для пользователей, обладающих доступом к зашифрованным файлам, подсистема автоматически (на лету) расшифровывает содержимое зашифрованного файла при его чтении и автоматически зашифровывает содержимое файла при его сохранении. Расшифрование файла, находящегося в шифрованном каталоге, переводит его в открытое состояние, оставляя его в том же каталоге. Расшифрование каталога переводит в открытое состояние все находящиеся в нем зашифрованные файлы.

Пользователь, не имеющий доступа к шифрованному каталогу, может только просматривать его содержимое. Порядок работы с нешифрованными файлами, находящимися в таком каталоге, не отличается от обычного порядка работы с открытым каталогом. При этом пользователь не имеет доступа к содержимому зашифрованных файлов в каталоге и не может копировать, перемещать и удалять зашифрованные файлы.

Пользователи, имеющие доступ к шифрованному каталогу, получают разные права в зависимости от той роли, которую они играют в системе:

a. роль владельца ресурса, которым является пользователь, создавший шифрованный каталог (создавать шифрованные каталоги может пользователь, обладающий на данном компьютере привилегией «Создание шифрованного ресурса»);
b. роль пользователя ресурса, имеющего право доступа к зашифрованным файлам чужого шифрованного каталога.

Для того чтобы пользователи компьютера могли защищать свои файлы, используя механизм шифрования, и имели возможность работать с зашифрованными файлами других пользователей, администратор безопасности должен выполнить в системе следующие настройки:

a. предоставить пользователям привилегию на создание шифрованных ресурсов;
b. присвоить пользователям персональные идентификаторы;
c. выдать пользователям криптографические ключи;
d. настроить параметры смены криптографических ключей;
e. настроить регистрацию событий, связанных с работой механизма шифрования.

После выполнения указанных процедур необходимо довести до сведения пользователей порядок работы с зашифрованными ресурсами.

В «Secret Net 5.0-C» используются 2 привилегии, связанные с шифрованием файлов. Привилегия «Создание шифрованного ресурса» позволяет создавать каталоги для хранения зашифрованных файлов. После установки «Secret Net 5.0-C» эта привилегия по умолчанию предоставляется двум стандартным группам пользователей: «Администраторы» и «Пользователи». Привилегия «Удаление шифрованного ресурса при отсутствии ключа» позволяет удалять зашифрованные файлы и каталоги без их расшифрования и по умолчанию предоставляется группе «Администраторы».

Предоставление привилегий осуществляется в оснастке «Локальная политика безопасности» ⇒ «Параметры Secret Net» ⇒ «Привилегии». При этом в правой части окна появится список привилегий «Secret Net 5.0-C». Здесь необходимо вызвать контекстное меню для строки «Шифрование файлов: Создание шифрованного ресурса», выбрать в нем команду «Свойства» и добавить пользователей, которым необходимо разрешить шифрование данных (рис. 3.64). Таким же образом следует поступить с привилегией «Удаление шифрованного ресурса при отсутствии ключа».

Персональный идентификатор – отдельное аппаратное устройство, предназначенное для хранения персональных данных, которые необходимы для идентификации и аутентификации пользователя. В идентификаторе так же хранятся криптографические ключи пользователя. Для хранения криптографических ключей также могут использоваться сменные носители, такие как дискеты, Flash-карты, USB Flash-накопители и т. п.

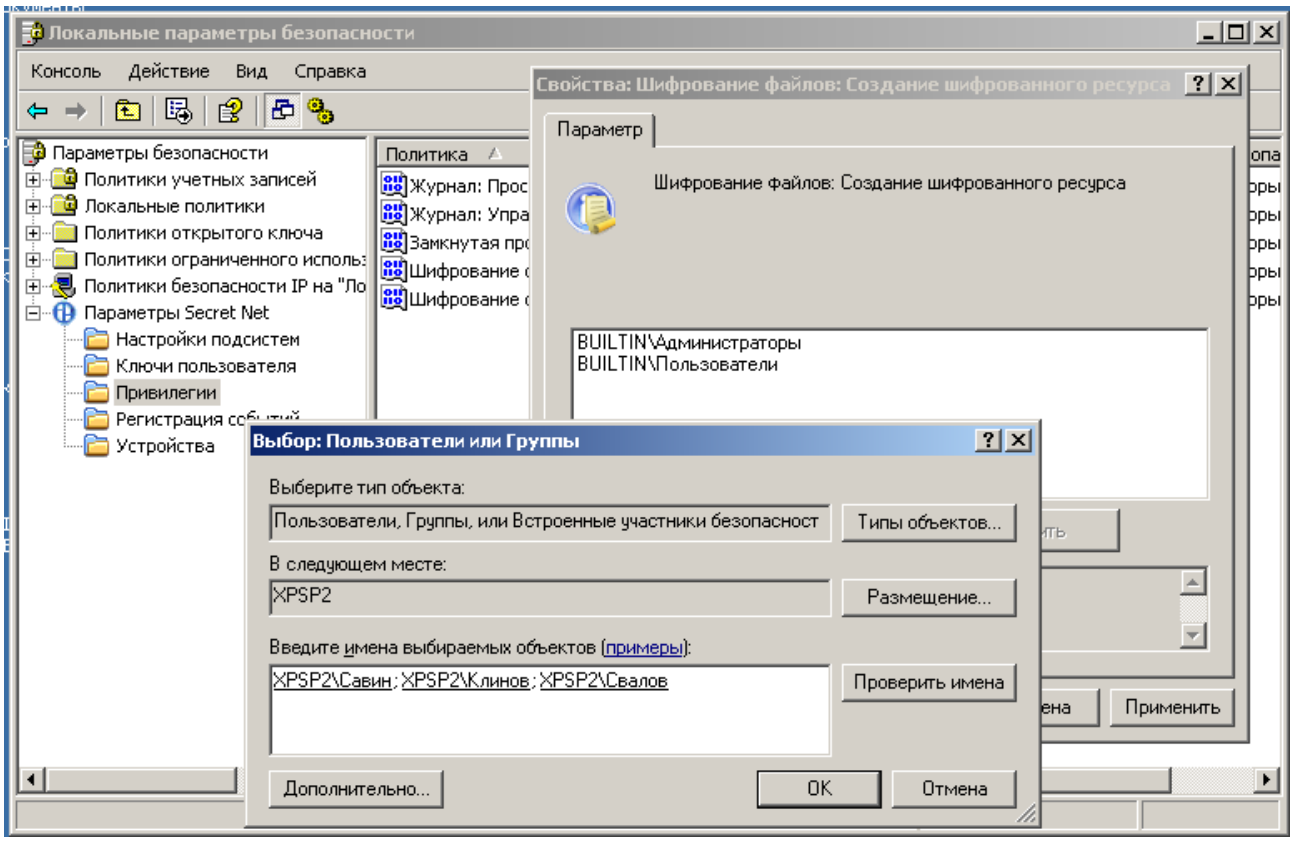


Рис. 3.64. Предоставление пользователям привилегий шифрования

Персональный идентификатор выдается пользователю компьютера администратором безопасности. Идентификаторы должны быть присвоены и выданы каждому пользователю, работающему с шифрованными ресурсами. Один и тот же персональный идентификатор не может быть выдан нескольким пользователям. В то же время администратор может выдать пользователю несколько персональных идентификаторов для работы на одном или нескольких компьютерах с установленной системой «Secret Net 5.0-C».

Работа с персональными идентификаторами осуществляется из окна настройки свойств пользователя на вкладке «Secret Net 5.0-C» в режиме «Идентификатор» и предполагает выполнение следующих операций:

a. просмотр сведений об идентификаторах;
b. инициализация идентификатора;
c. присвоение идентификатора;
d. отмена присвоения идентификатора;
e. включение (отключение) режима хранения пароля в идентификаторе;
f. включение (отключение) режима интеграции с программно-аппаратным комплексом «Соболь»;
g. запись (удаление) закрытых ключей;
h. проверка принадлежности.

Все основные операции с персональными идентификаторами, за исключением инициализации и проверки принадлежности, выполняются применительно к конкретному пользователю (рис. 3.65).

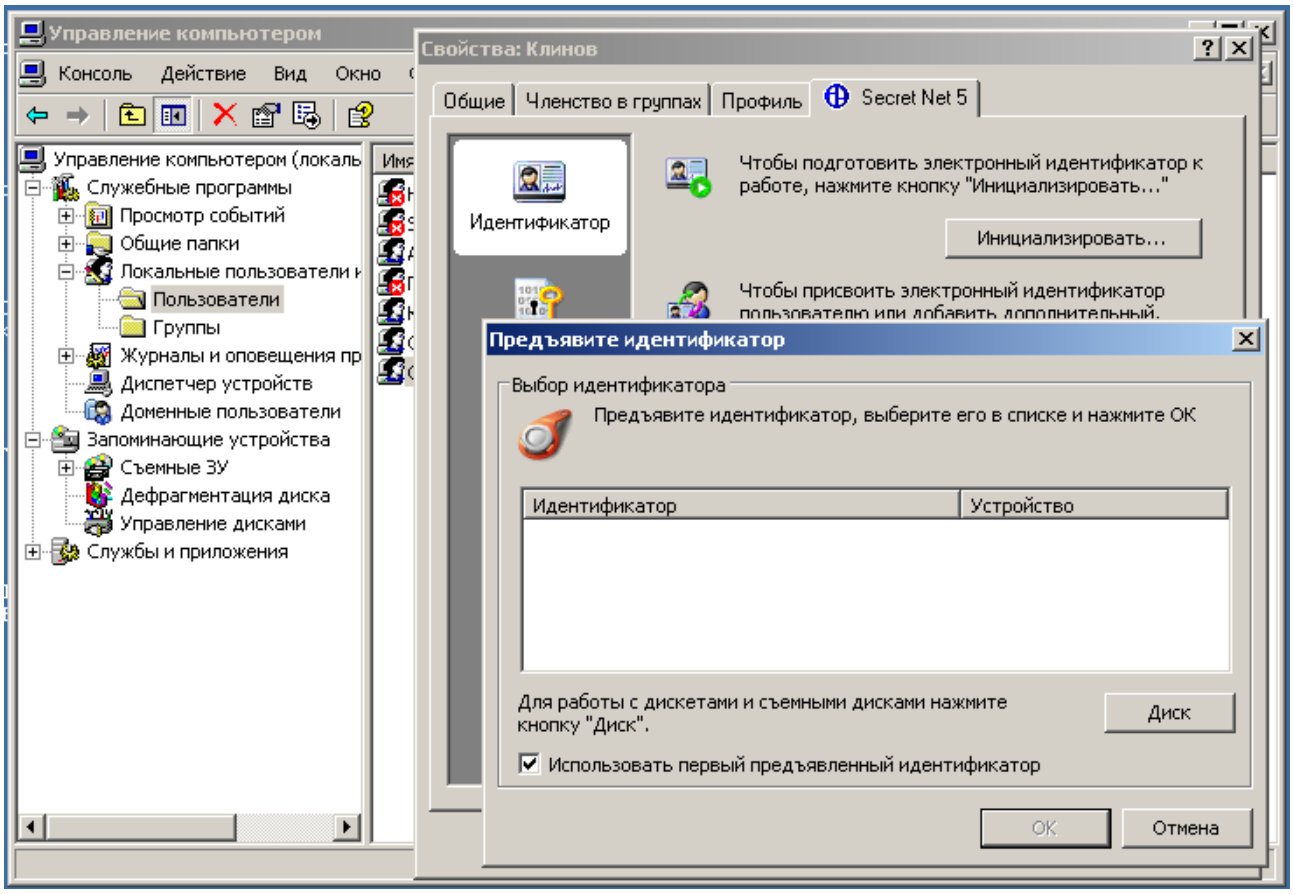


Рис. 3.65. Инициализация персонального идентификатора

При первом обращении к диску-идентификатору в окне «предъявите идентификатор» происходит подготовка к размещению на нем персональных данных (в частности, форматирование дискеты). При повторном – появляется запрос на присвоение персонального идентификатора, где следует выбрать требуемые поля «включить режим хранения пароля» и «записать в идентификатор закрытый ключ пользователя». Если идентификатор предполагается использо-

вать только для организации криптографической защиты, то следует активизировать только последнее поле. При нажатии клавиши «Далее» система инициализирует соответствующему пользователю персональный ключ и поместит его в идентификатор (рис. 3.66). Информация о присвоенных идентификаторах будет теперь отображаться в окне настройки свойств пользователя на вкладке «Secret Net 5.0-C».

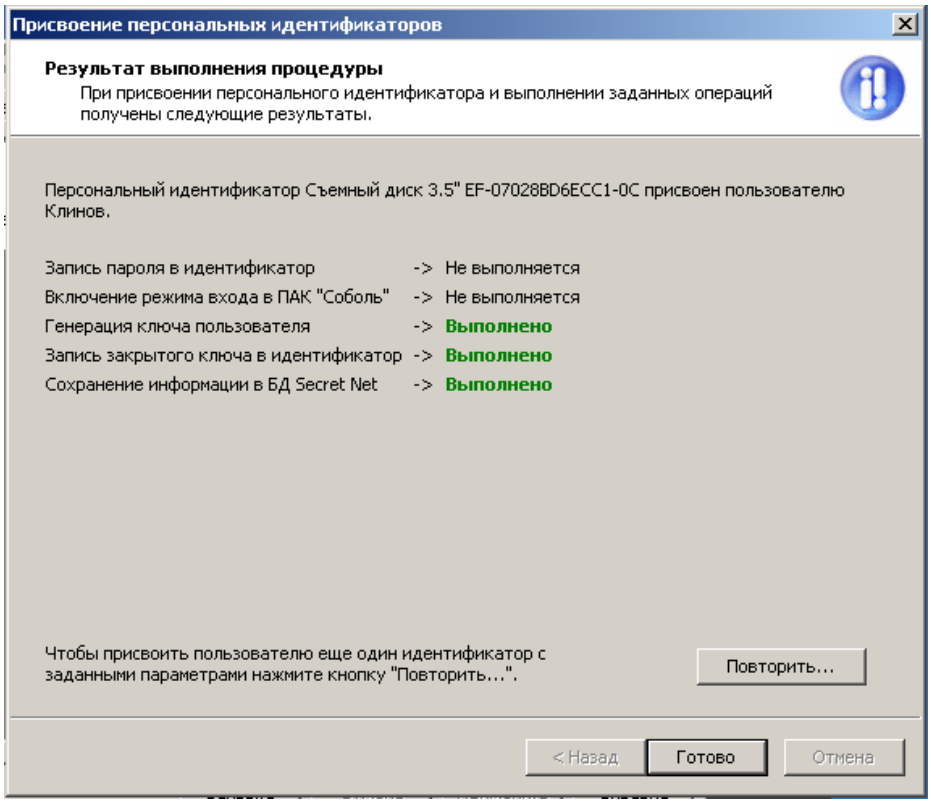


Рис. 3.66. Запись закрытого ключа пользователя в персональный идентификатор

Для проведения аудита, связанного с работой механизма шифрования, необходимо выполнить настройку регистрации событий. Для этого следует указать, какие события категории «Шифрование файлов» должны регистрироваться в журнале безопасности «Secret Net 5.0-C» (рис. 3.67).

Выполнение различных операций с зашифрованными ресурсами можно осуществлять только после того, как в систему будут загружены пользовательские ключи. Для загрузки ключей необходимо вызвать контекстное меню пиктограммы «Secret Net 5.0-C», находящееся в системной области панели задач Windows, и активировать команду «Загрузить ключи» (рис. 3.68). В диалоговом окне «Загрузка ключей» отображается список идентификаторов, предъявленных системе в данный момент. Наименование идентификатора включает в себя тип идентификатора и его серийный номер. При разрыве контакта между считывающим устройством и персональным идентификатором соответствующая идентификатору строка удаляется из списка.

При использовании в качестве идентификаторов iButton или eToken возможные действия пользователя и реакция на них системы зависят от состояния выключателя «Использовать первый предъявленный идентификатор». Если поле выключателя содержит соответствующую отметку, то после предъявления

персонального идентификатора произойдет чтение ключевой информации из этого идентификатора в память компьютера.

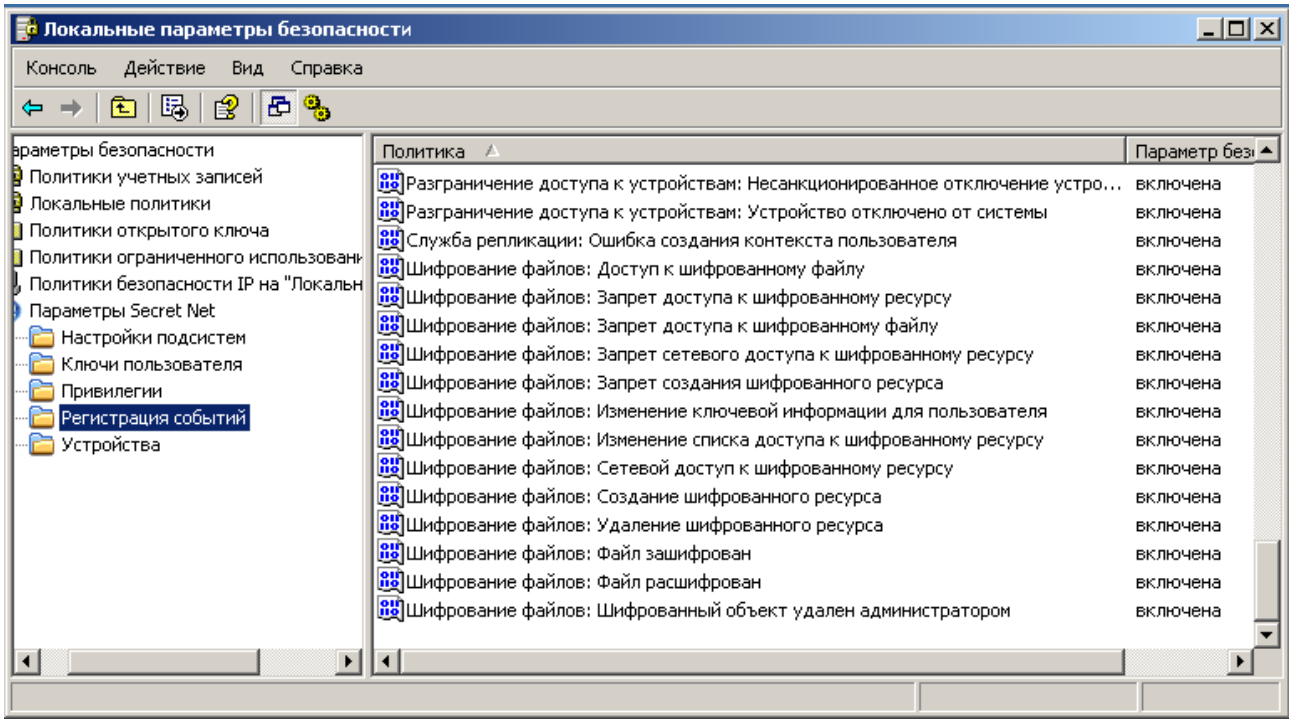


Рис. 3.67. Настройка регистрации событий шифрования данных

Если одновременно предъявлено более одного идентификатора, то указанное выше действие с ключевой информацией будет выполнено для одного из них. Если поле выключателя не содержит отметки, то после предъявления персонального идентификатора в списке идентификаторов отображается наименование персонального идентификатора. При этом чтение ключевой информации не выполняется. Для чтения ключевой информации, не разрывая контакт между считывающим устройством и персональным идентификатором, выберите в списке нужную строку и нажмите кнопку «ОК». Если в систему загружены ключи, то пиктограмма «Secret Net 5.0-C» дополняется знаком замка, а во всплывающем окне появляется краткая информация о загруженных ключах.

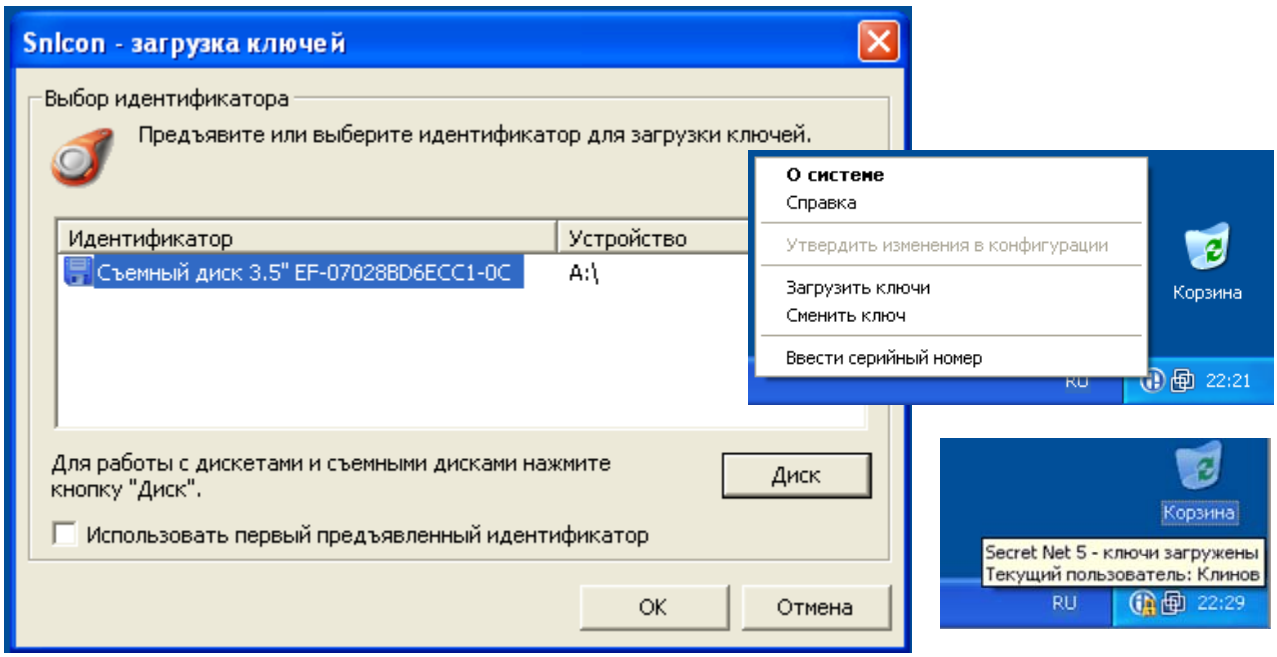


Рис. 3.68. Загрузка криптографических ключей пользователей

В системе «Secret Net 5.0-C» под созданием шифрованного каталога подразумевается включение режима шифрования файлов в этом каталоге. При этом сам каталог должен уже существовать в файловой системе. Включать режим шифрования имеют право пользователи, обладающие привилегией «Создание шифрованного ресурса», которая предоставляется администратором. Включение режима шифрования осуществляется в окне «Secret Net» свойств выбранного каталога в поле «Шифровать содержимое папки» (рис. 3.69). После чего в списке пользователей, которым разрешен доступ к шифрованному каталогу, появится строка с именем текущего пользователя. При необходимости список пользователей может быть отредактирован. Если рабочий каталог уже содержит подкаталоги и файлы, на экране появится диалог, позволяющий зашифровать имеющиеся в каталоге объекты.

ВЫПОЛНИТЬ!

При выполнении практических заданий в качестве сменных носителей информации (идентификаторов) следует использовать электронные образы дискет, хранящиеся в одном каталоге вместе с образом самой системы в виде файлов с именем «дискета» и «дискета_1». Дискеты-идентификаторы рекомендуется назначить различным пользователям системы, например, администратору (Чистякову) и руководителю предприятия (Клинову). При смене пользователя в программе VMware необходимо монтировать соответствующий образ дискеты.

39. Зарегистрироваться Администратором, создать в корне диска c:\ каталог с именем «Зашифрованные данные», в каталоге создать несколько текстовых документов. К каталогу разрешить полный доступ всем пользователям системы.

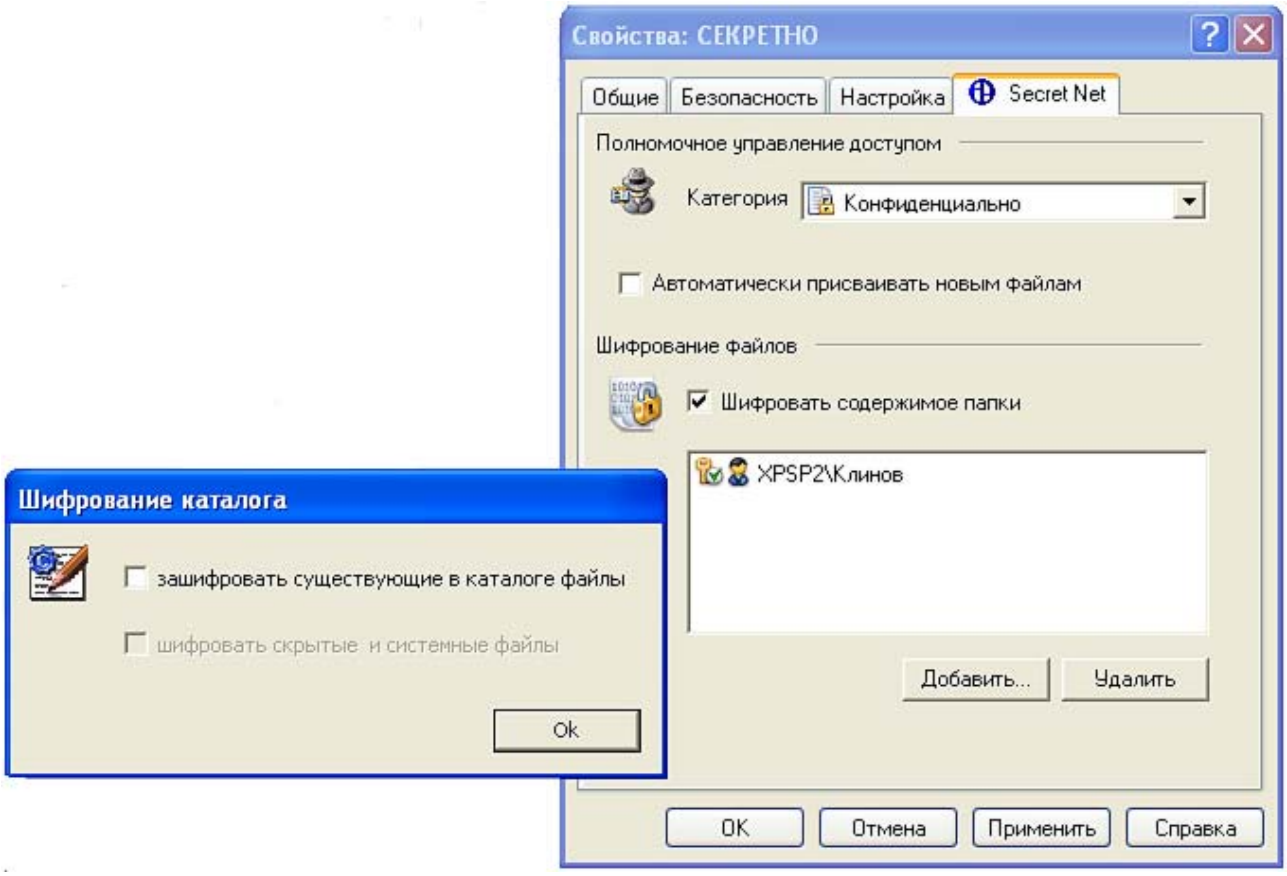


Рис. 3.69. Создание шифрованного каталога

40. В свойствах пользователя Клинов инициировать и присвоить электронный идентификатор (дискету) и назначить пользователю закрытый ключ шифрования. Поместить ключ на дискету.
41. Зарегистрироваться пользователем Клинов с минимальным уровнем допуска, загрузить ключ активного пользователя в систему.
42. От имени пользователя Клинов «создать» зашифрованный каталог «Зашифрованные данные», включив поле «зашифровать существующие в каталоге файлы». Создать в каталоге файл, убедиться, что он помечен как зашифрованный.
43. Зарегистрироваться Администратором, убедиться, что доступ к зашифрованным файлам не возможен. Просмотреть журнал регистрации событий.
44. Подмонтировать к системе VMware образ следующей дискеты, назначить ее в качестве идентификатора администратора и записать на нее закрытый ключ администратора.
45. Зарегистрироваться Клиновым. В окне «Secret Net» свойств зашифрованного каталога разрешить доступ к зашифрованному каталогу администратору системы. Убедиться в возможности доступа.

4. СРЕДСТВА ОРГАНИЗАЦИИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

4.1. Задачи, решаемые VPN

Защищенные компьютерные сети на сегодняшний день применяют технологию защиты информации, включающую в себя как элементы межсетевого экранирования, так и механизмы криптографической защиты сетевого трафика. Такая технология получила название VPN — Virtual Private Network (виртуальная частная сеть). В литературе (см. [30]) встречаются различные определения виртуальной частной сети. Мы будем использовать следующее. VPN — это технология, объединяющая доверенные сети, узлы и пользователей через открытые сети, к которым нет доверия. Основная идея данного определения приведена на схеме (рис. 4.1).

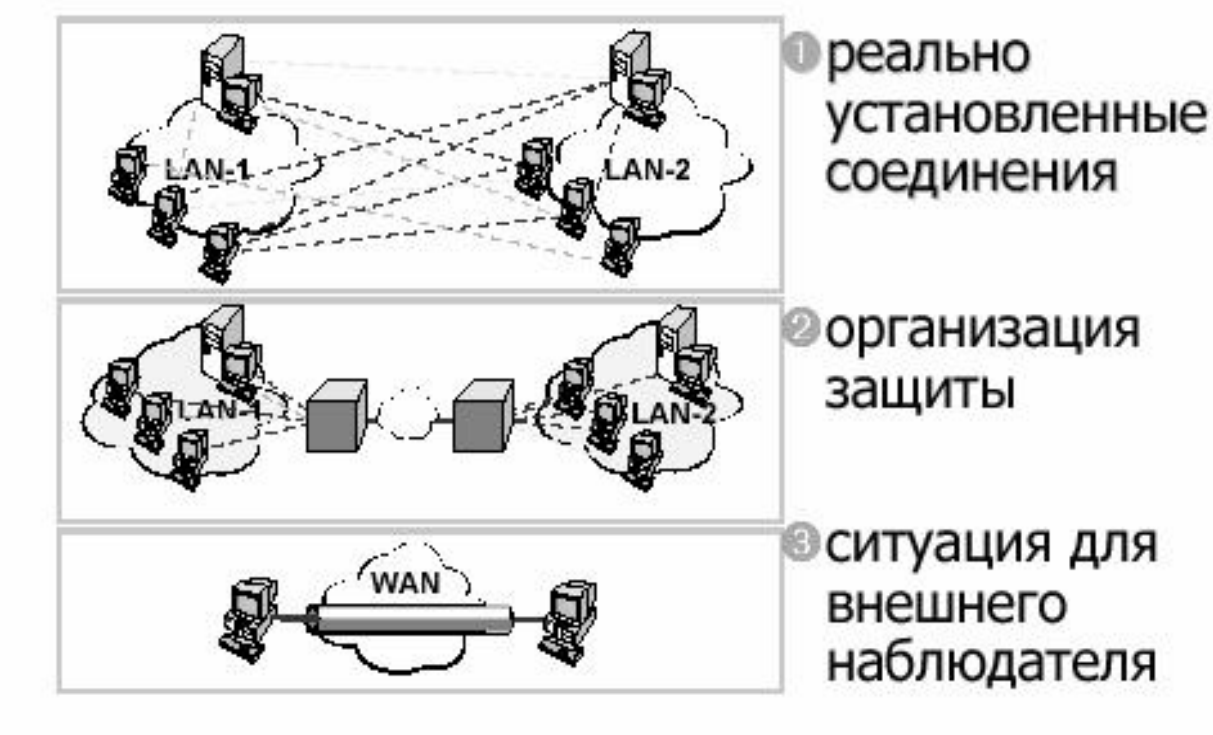


Рис. 4.1. Схема VPN

Предположим, имеются две локальных сети (LAN-1 и LAN-2, рис. 4.1), принадлежащие одной организации (например, головной офис и филиал). Обе эти локальные сети объединены при помощи иной сети, в большинстве случаев для этого используется Интернет. С точки зрения пользователей соединения могут устанавливаться между любыми узлами этих локальных сетей. На самом же деле реальные соединения устанавливаются через посредников, неких «черных ящиков», устанавливаемых на входе в каждую из них. Задача этих «черных ящиков» так обработать идущий между ними сетевой трафик, чтобы злоумышленник или просто внешний наблюдатель не мог совершить с передаваемой информацией какого-либо действия, приводящего к ущербу. А именно, не должен нарушить конфиденциальность, целостность и подлинность информации. Иными словами, передаваемая информация, включая адреса ее получателя и

отправителя, должна быть зашифрована и криптографически подписана. Кроме того, задача «черных ящиков» — защищать сами локальные сети от несанкционированного доступа к ним из глобальной сети. Таким образом, внешний наблюдатель должен увидеть в сети лишь зашифрованный обмен информацией между двумя «черными ящиками» и ничего более.

Таким образом, можно сформулировать, что VPN призвана решать следующие задачи:

− обеспечивать защиту (конфиденциальность, целостность, подлинность) передаваемой по сетям информации[1]. Как указывалось выше, данная задача решается применением криптографического метода защиты передаваемой информации;

− выполнять защиту внутренних сегментов сети от НСД извне. Решение задачи возможно благодаря встроенным в VPN-системы функциям межсетевого экранирования, а также криптографическим механизмам, запрещающим незашифрованный сетевой трафик;

− обеспечивать идентификацию и аутентификацию пользователей. Данная задача возникает вследствие того, что, как сказано в определении VPN, в сети должны взаимодействовать лишь доверенные узлы, доверие к которым возможно после прохождения процедур идентификации и аутентификации.

Отдельно стоящей задачей, решаемой VPN, является экономия финансовых ресурсов организации, когда для обеспечения защищенной связи с филиалами применяются не защищенные выделенные каналы связи, а Интернет.

Сформулируем ряд требований, которые предъявляются к программно-аппаратным комплексам, реализующим VPN:

− масштабируемость, т. е. возможность со временем подключать новые локальные сети без необходимости изменения структуры имеющейся VPN;

− интегрируемость, т. е. возможность внедрения VPN-системы в имеющуюся технологию обмена информацией;

− легальность и стойкость используемых крипоалгоритмов, т. е. система должна иметь соответствующий сертификат, позволяющий ее использовать на территории Российской Федерации с целью защиты информации ограниченного доступа;

− пропускная способность сети, т. е. система не должна существенно увеличивать объем передаваемого трафика, а также уменьшать скорость его передачи;

− унифицируемость, т. е. возможность устанавливать защищенные соединения с коллегами по бизнесу, у которых уже установлена иная VPN-система;

− общая совокупная стоимость, т. е. затраты на приобретение, развертывание и обслуживание системы не должны превосходить стоимость самой информации, особенно если речь идет о защите коммерческой тайны.

[1] Заметим, что классическую задачу защиты информации в виде обеспечения ее доступности технология VPN самостоятельно решать не может.

4.2. Туннелирование в VPN

Как указывалось выше, основная задача, решаемая VPN, — скрыть передаваемый трафик. При этом необходимо скрыть как передаваемые данные, так и адреса реальных отправителя и получателя пакетов. И кроме того, необходимо обеспечить целостность и подлинность передаваемых данных. Для защиты передаваемых данных и реальных IP-адресов применяются криптографические алгоритмы. При отправке пакетов применяется туннелирование, т. е. в пакетах, которые идут в открытой сети, в качестве адресов фигурируют только адреса «черных ящиков». Кроме того, туннелирование предполагает, что внутри локальных сетей трафик передается в открытом виде, а его защита осуществляется только тогда, когда он попадает в «туннель».

Итак, пусть у нас имеется пакет, содержащий данные и IP-заголовок, которые подлежат защите (рис. 4.2). Для защиты применим криптографические методы и зашифруем и данные, и заголовок вместе. Так как необходимо обеспечить скорость обработки информации, то для зашифрования, естественно, будем использовать симметричный алгоритм.

Известно, что применение симметричных алгоритмов шифрования требует решения задачи распространения симметричных ключей. Поэтому поступим следующим образом: прикрепим симметричный ключ прямо к зашифрованным с его использованием данным. Назовем симметричный ключ пакетным ключом (его еще называют сеансовым ключом). Этот пакетный ключ будем генерировать случайным образом при отправлении каждого нового пакета (тогда он действительно «пакетный» ключ). Либо будем его генерировать также случайно при каждом сеансе обмена. Тогда данные всех пакетов, передаваемых в данном сеансе связи, будут шифроваться одним и тем же ключом, и это уже «сеансовый» ключ.

Конечно, нельзя отправлять пакетный ключ в открытом виде, прикрепляя его к зашифрованным им данным. Следует его зашифровать. Воспользуемся тем, что ключ, в отличие от данных, — это лишь пара сотен бит (в зависимости от реализации, например, 256 бит — длина ключа алгоритма ГОСТ 28147-89, 56 бит — длина ключа алгоритма DES). Таким образом, можем применить более медленные асимметричные алгоритмы и зашифровать с их помощью пакетный ключ. Вместе с тем, для шифрования пакетного ключа может быть применен и симметричный алгоритм. Ключ алгоритма шифрования пакетного ключа назовем ключом связи.

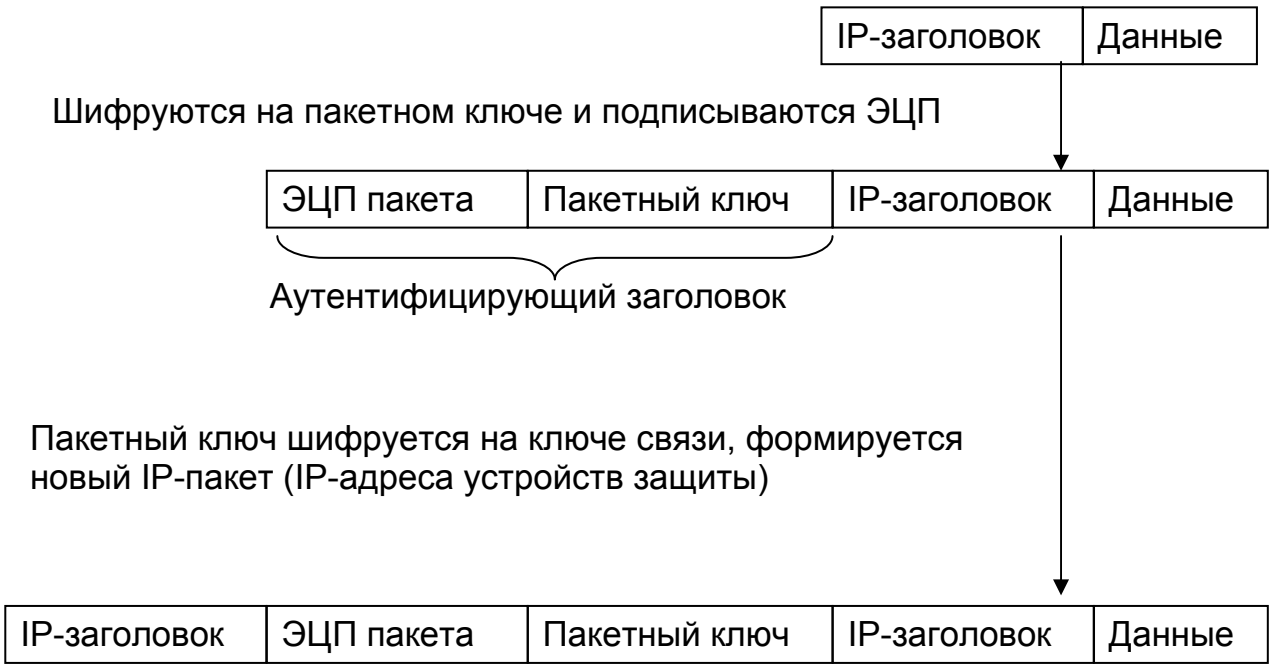


Рис. 4.2. Преобразование отправляемого пакета

Кроме того, для обеспечения целостности пакетов сгенерируем электронно-цифровую подпись (ЭЦП) нашего пакета и прикрепим ее к формируемому пакету.

Совокупность ЭЦП и зашифрованного пакетного ключа называют аутентифицирующим заголовком.

Для того чтобы отправить сгенерированный нами пакет, необходимо добавить к нему IP-адреса источника и приемника. В случае туннеля этими адресами будут адреса пограничных VPN-узлов. Если же защищается трафик между двумя узлами без применения туннеля, то эти адреса совпадут с адресами в исходном пакете.

Таким образом, исходный пакет защищен. Осталось выяснить ряд моментов. Во-первых, каким образом будет осуществлен обмен ключом связи и, во-вторых, что будем понимать под шифруемыми данными: только лишь данные прикладного уровня либо относящиеся к транспортному или сетевому уровню.

Чтобы ответить на второй вопрос, рассмотрим уровни защищенных каналов.

4.3. Уровни защищенных каналов

Итак, необходимо разобраться, данные какого уровня модели OSI подлежат шифрованию в процессе организации VPN.

Рассмотрим упрощенную модель OSI, реализованную в стеке протоколов TCP/IP. Эта модель предполагает наличие четырех уровней: прикладного, транспортного, сетевого и канального. Соответственно, для каждого уровня возможность шифрования передаваемой информации различна. Так, на прикладном уровне можно скрыть данные, например, электронного письма или получаемой web-страницы. Однако факт передачи письма, т. е. диалог по протоколу SMTP скрыть невозможно. На транспортном уровне может быть вместе с

данными скрыт и тип передаваемой информации, однако IP-адреса получателя и приемника остаются открытыми. На сетевом уровне уже появляется возможность скрыть и IP-адреса. Эта же возможность имеется и на канальном уровне.

Чем ниже уровень, тем легче сделать систему, функционирование которой будет незаметно для приложений высокого уровня, и тем большую часть передаваемой информации можно скрыть.

Для каждого уровня модели разработаны свои протоколы (табл. 5.1).

Таблица 5.1

Уровни защищенных каналов и протоколы

Уровень	**Протоколы**
Прикладной	S/MIME / PGP / SHTTP
Транспортный (TCP/UDP)	SSL / TLS / SOCKS
Сетевой (IP)	IPSec / SKIP
Канальный	PPTP / L2F / L2TP

Так, на прикладном уровне для защиты электронной почты применяется протокол S/MIME (Secure Multipurpose Internet Mail Extension) либо система PGP. Для защиты обмена по протоколу HTTP применяется протокол SHTTP (Secure HTTP). На данном уровне шифруется текст передаваемого почтового сообщения или содержимое HTML-документа. Недостатками организации VPN на базе протоколов прикладного уровня является узкая область действия, для каждой сетевой службы должна быть своя система, способная интегрироваться в соответствующие приложения. В пособии мы не будем подробно рассматривать системы этого уровня.

На транспортном уровне чаще всего применяются протоколы SSL (Secure Socket Layer) и его более новая реализация — TSL (Transport Layer Security). Также применяется протокол SOCKS. Особенность протоколов транспортного уровня — независимость от прикладного уровня, хотя чаще всего шифрование осуществляется для передачи по протоколу HTTP (режим HTTPS). Недостатком является невозможность шифрования IP-адресов и туннелирования IP-пакетов.

На сетевом уровне используются два основных протокола: SKIP (Simple Key management for Internet Protocol – простое управление ключами для IP-протокола) и IPSec. На данном уровне возможно как шифрование всего трафика, так и туннелирование, включающее скрытие IP-адресов. На сетевом уровне строятся самые распространенные VPN системы.

Канальный уровень представлен протоколами PPTP (Point-to-Point Tunneling Protocol), L2F (Layer-2 Forwarding) и L2TP (Layer-2 Tunneling Protocol). Достоинством данного уровня является прозрачность не только для приложений прикладного уровня, но и для служб сетевого и транспортного уровня. В частности, достоинством является независимость от применяемых протоколов сетевого и транспортного уровня — это может быть не только IP-протокол, но и протоколы IPX (применяется в локальных сетях с серверами на основе ОС

Novell Netware) и NetBEUI (применяется в локальных сетях Microsoft). Шифрованию подлежат как передаваемые данные, так и IP-адреса.

В каждом из указанных протоколов по-разному реализованы алгоритмы аутентификации и обмена ключами шифрования.

4.4. Защита данных на канальном уровне

На канальном уровне применяются упомянутые выше протоколы PPTP (разработчик Microsoft), L2F (разработчик Cisco Systems) и L2TP (совместная разработка Microsoft и Cisco Systems).

Протоколы PPTP и L2TP основываются на протоколе Point-to-Point Protocol (PPP). PPP — протокол канального уровня, разработан для инкапсуляции данных и их доставки по соединениям типа точка-точка.

В основе протокола PPTP лежит следующий алгоритм: сначала производится инкапсуляция данных с помощью протокола PPP, затем протокол PPTP выполняет шифрование данных и инкапсуляцию. PPTP инкапсулирует PPP-кадр в пакет Generic Routing Encapsulation (протокол GRE). Схема инкапсуляции приведена на рис. 4.3.

Рис. 4.3. Инкапсуляция в протоколе PPTP

К исходному отправляемому IP-пакету (обозначенному на рисунке серым цветом) последовательно добавляются PPP-, GRE- и IP-заголовки. В новом IP-пакете в качестве адресов указываются адреса туннелирующих узлов.

Протокол PPTP очень часто используется провайдерами Интернет при организации прямого кабельного подключения пользователей. В этом случае пользователям назначается IP-адрес из диапазона «домашних» сетей (например, 10.1.1.189 или 192.168.1.1). Сервер провайдера имеет два адреса — внутренний (для «домашней» сети) и внешний («настоящий»). Когда пользователь авторизуется на PPTP-сервере провайдера, ему динамически выделяется реальный IP-адрес.

Внутри локальной сети между пользователем и PPTP-сервером циркулируют IP-пакеты с внутренними IP-адресами, внутри которых инкапсулированы пакеты с внешними адресами.

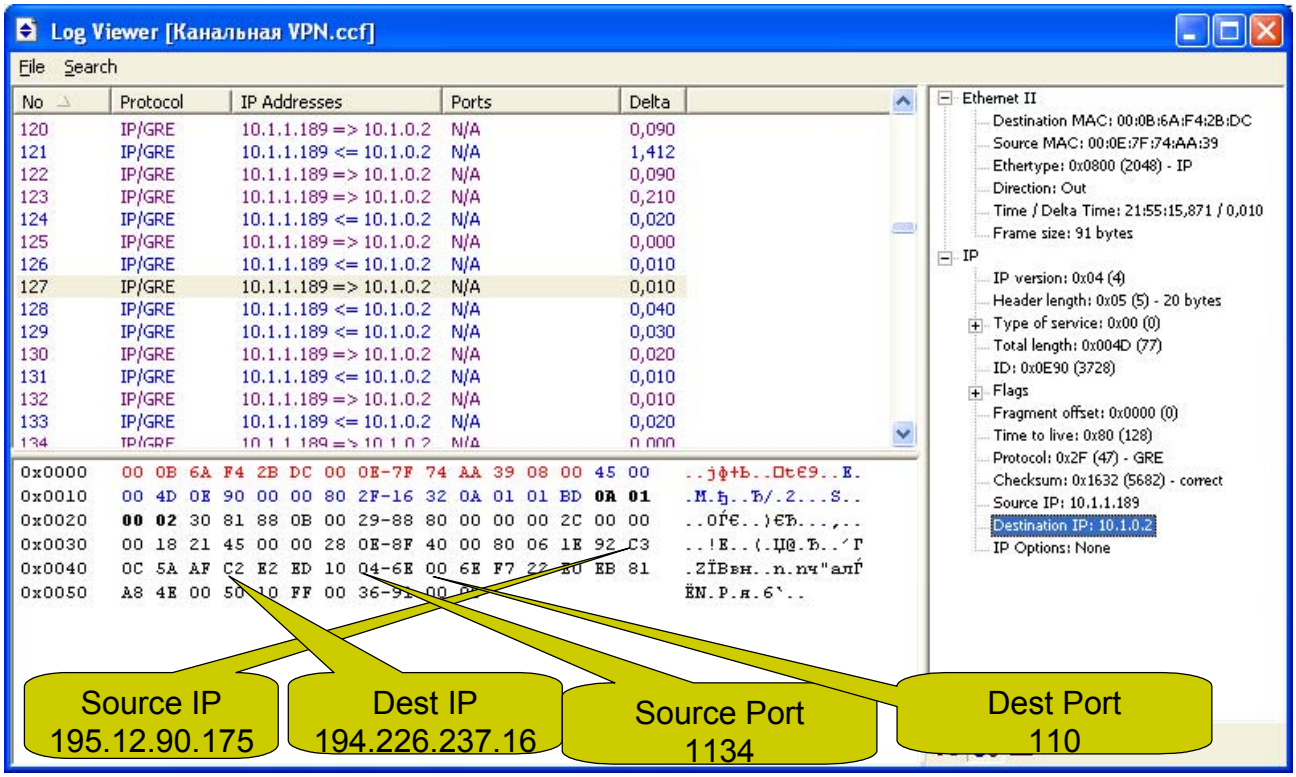


Рис. 4.4. Пакет протокола PPTP

На рис. 4.4 приведен пример обмена по протоколу POP3 (порт приемника 110), осуществляемого между удаленным POP3-сервером с адресом 194.226.237.16 и пользователем, которому назначен динамический адрес 195.12.90.175. В локальной сети видны пакеты протокола IP/GRE, проходящие между узлами 10.1.1.189 (внутренний адрес пользователя) и 10.1.0.2 (внутренний адрес PPTP-сервера).

Обычно провайдеры не включают возможность шифрования и сжатия инкапсулируемых пакетов, поэтому при анализе трафика в локальной сети содержимое IP/GRE-пакетов легко распознать и увидеть адреса, протокол и передаваемые данные.

Для шифрования передаваемых данных с использованием клиентов с ОС Windows XP необходимо в настройках подключения указать пункт «Require Data Encryption» («Требовать шифрование данных», рис. 4.5).

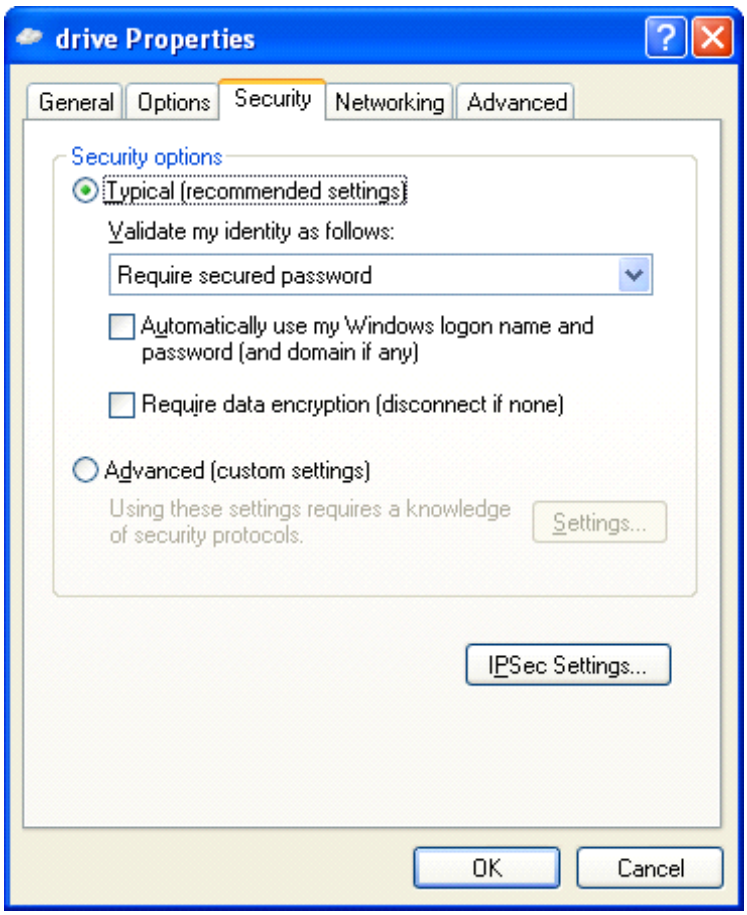


Рис. 4.5. Настройка клиента протокола PPTP

В протоколе PPTP для аутентификации предусматриваются различные протоколы аутентификации:

- Extensible Authentication Protocol (EAP),
- Microsoft Challenge Handshake Authentication Protocol (MSCHAP),
- Challenge Handshake Authentication Protocol (CHAP),
- Shiva Password Authentication Protocol (SPAP)
- Password Authentication Protocol (PAP)

Наиболее стойким является протокол MSCHAP версии 2, требующий взаимную аутентификацию клиента и сервера. В протоколе MSCHAP могут быть использованы три различных варианта передачи пароля:

- клиент передает серверу пароль в открытом текстовом виде;
- клиент передает серверу хэш пароля;
- аутентификация сервера и клиента с использованием вызова и ответа.

Последний вариант наиболее защищенный, алгоритм его состоит в следующем (рис. 4.6).

- Клиент запрашивает вызов сетевого имени.
- Сервер возвращает 8-байтовый случайный вызов (например, «01234567», рис. 4.7).
- Клиент вычисляет хэш-функцию пароля алгоритмом «Lan Manager» (например, «C2 34 1A 8A A1 E7 66 5F AA D3 B4 35 B5 14 04 EE»), добавляет пять нулей для создания 21-байтовой строки и делит строку на три 7-байтовых ключа. Каждый ключ используется для шифрования вызова с использованием алго-

ритма DES, что приводит к появлению 24-байтного шифрованного значения (например, «AA AA AA AA AA AA AA AA BB BB BB BB BB BB BB BB CC CC CC CC CC CC CC CC»). Клиент выполняет то же самое с хэш-функцией пароля, получаемой алгоритмом хэширования, реализованном в ОС семейства Windows NT. В результате формируется 48-байтное значение, которое возвращается серверу как ответ.

− Сервер ищет значение хэш-функции в своей базе данных, шифрует запрос с помощью хэш-функции и сравнивает его с полученными шифрованными значениями. Если они совпадают, аутентификация заканчивается.

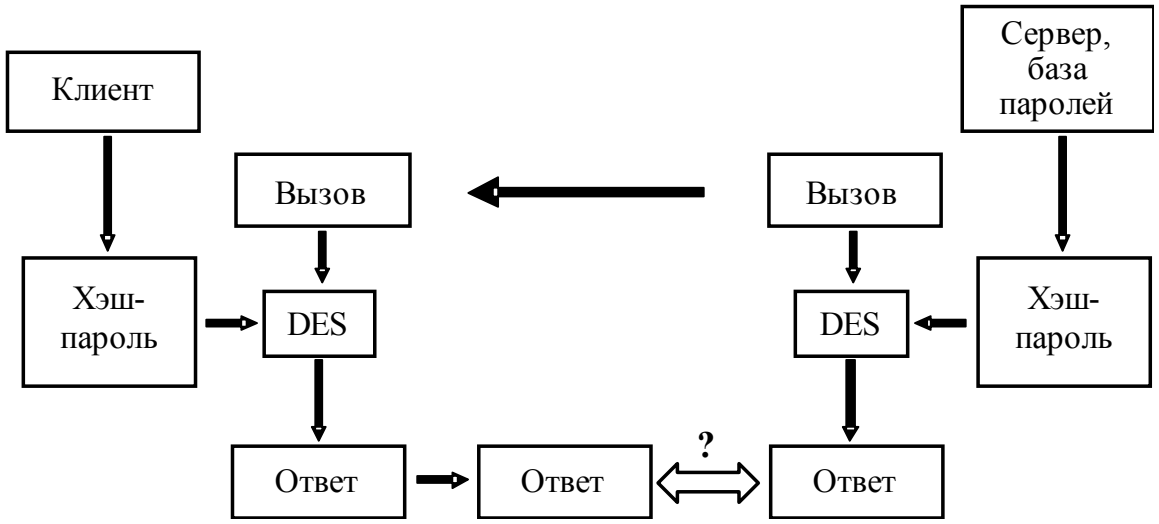


Рис. 4.6. Аутентификация в протоколе MSCHAP

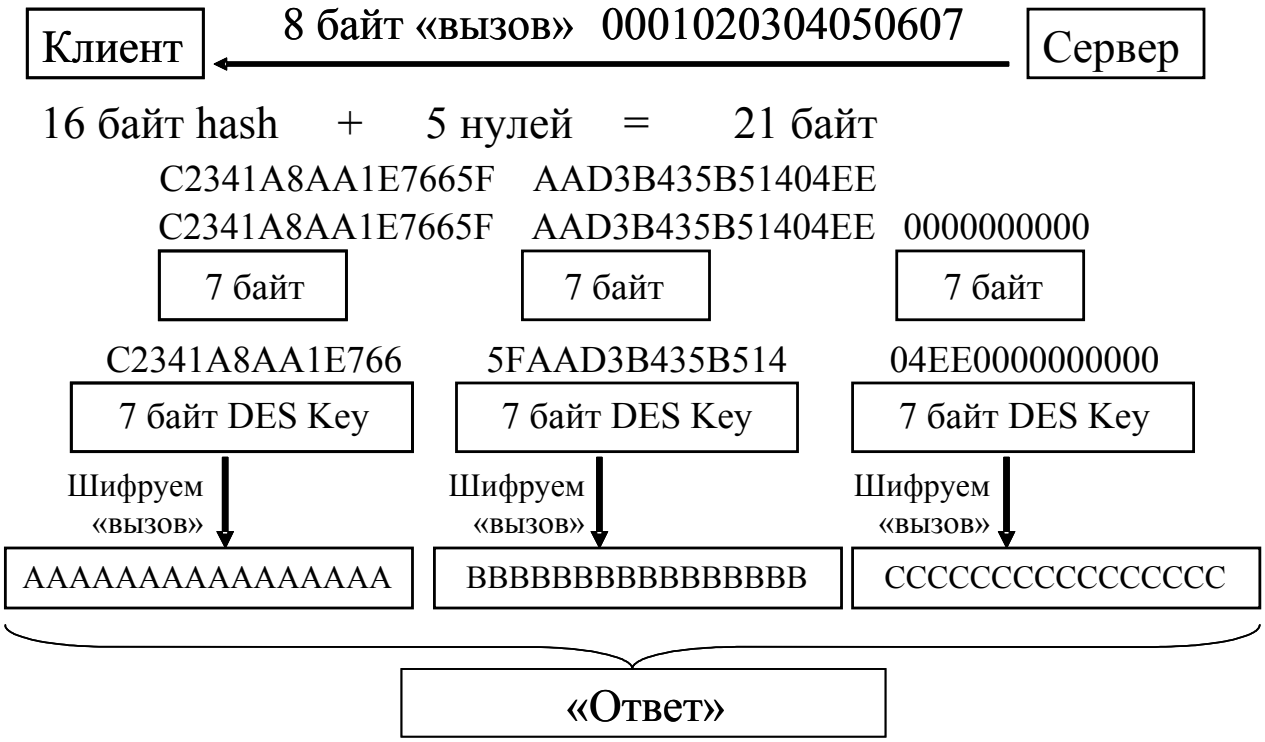


Рис. 4.7. Схема формирования «ответа» в протоколе MSCHAP

Для шифрования передаваемых данных применяется поточный шифр RC4 с 40- либо 128-разрядным ключом. Алгоритм предполагает существование секретного ключа, известного обоим участникам соединения. Данный ключ формируется из хэш-функции «Lan Manager» пароля пользователя, известного и клиенту, и серверу.

4.5. Организация VPN средствами протокола PPTP

4.5.1. Постановка задачи

Предлагается организовать соединение по протоколу PPTP между двумя сетевыми узлами. При этом имитируется соединение, которое пользователь Интернет устанавливает с сервером провайдера в том случае, когда используется подключение по выделенному каналу на основе Ethernet. В результате подключения пользователю выделяется IP-адрес, который может быть известен пользователю заранее либо выделяться динамически. Динамическое выделение адресов позволяет затруднить идентификацию узла пользователя из Интернет, сделав его в какой-то степени анонимным. Кроме того, это дает возможность провайдеру более эффективно использовать выделенное ему адресное пространство.

Для имитации предполагается использовать два рабочих места. Первое рабочее место (рис. 4.8) имитирует PPTP-сервер Интернет-провайдера, этим сервером является компьютер под управлением ОС Windows 2000/XP. На этом же рабочем месте имитируется пользовательский компьютер, который выполняется в виде виртуальной машины VMWare с установленной Windows 2000.

Второе рабочее место (им может быть любой компьютер в локальной сети) имитирует удаленный web-сервер.

Предполагается, что удаленный web-сервер имеет IP-адрес 192.168.1.1, основной компьютер имеет два интерфейса — внутренний с адресом 192.168.200.1 и внешний с адресом 192.168.1.128. Пользовательский компьютер имеет внутренний адрес 192.168.200.2. Пройдя авторизацию на PPTP-сервере, пользовательский компьютер получит адрес внешней сети 192.168.1.129. В дальнейшем пользовательский компьютер будет обращаться к внешнему web-серверу по протоколу HTTP.

Анализ трафика будет осуществляться в локальной сети между пользовательским компьютером и PPTP-сервером.

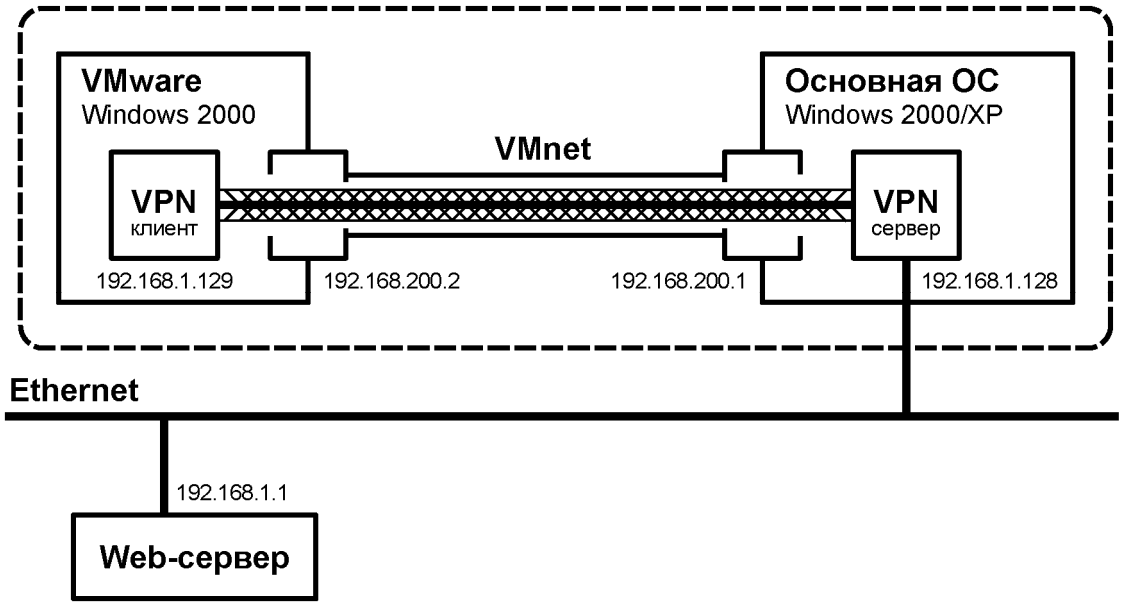


Рис. 4.8. Схема имитируемой VPN-сети

4.5.2. Установка и настройка VPN

ВЫПОЛНИТЬ!

1. Настроить виртуальную сеть между основной ОС и виртуальной машиной Windows 2000. Для этого выполнить следующие действия.
2. В общих настройках виртуальной сети включить адаптер VMnet1 (опция «Enable adapter», рис. 4.9).

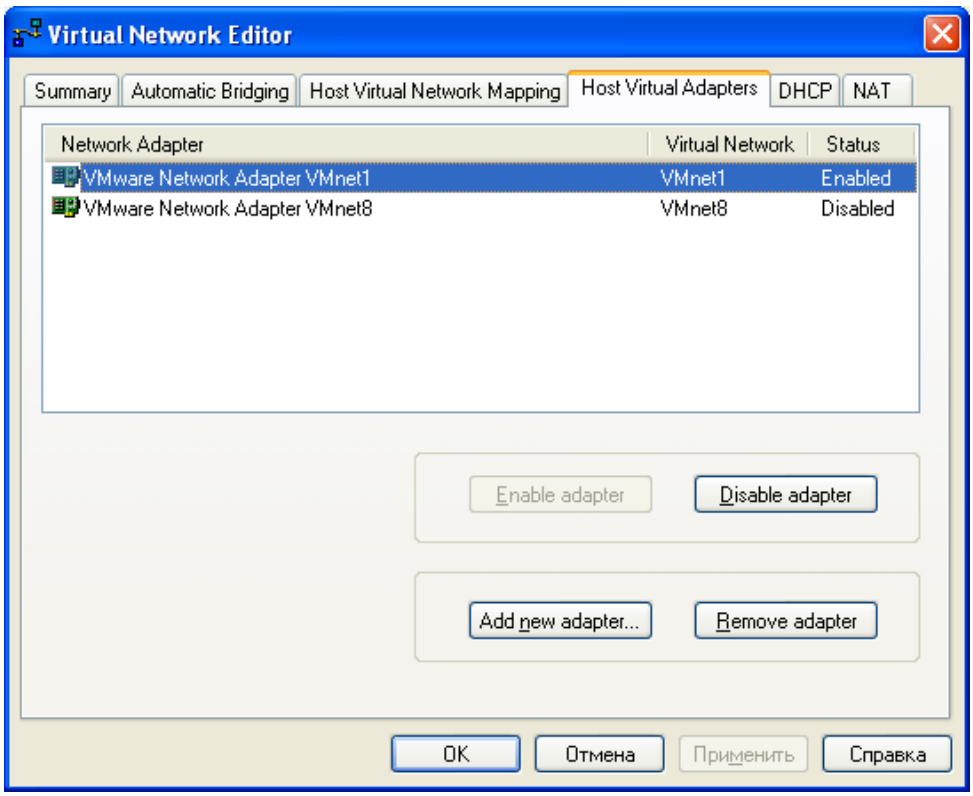


Рис. 4.9. Активация адаптера VMnet1

3. В разделе «Host Virtual Network Mapping» настроить свойства адаптера VMnet1, указав подсеть 192.168.200.0 (рис. 4.10).

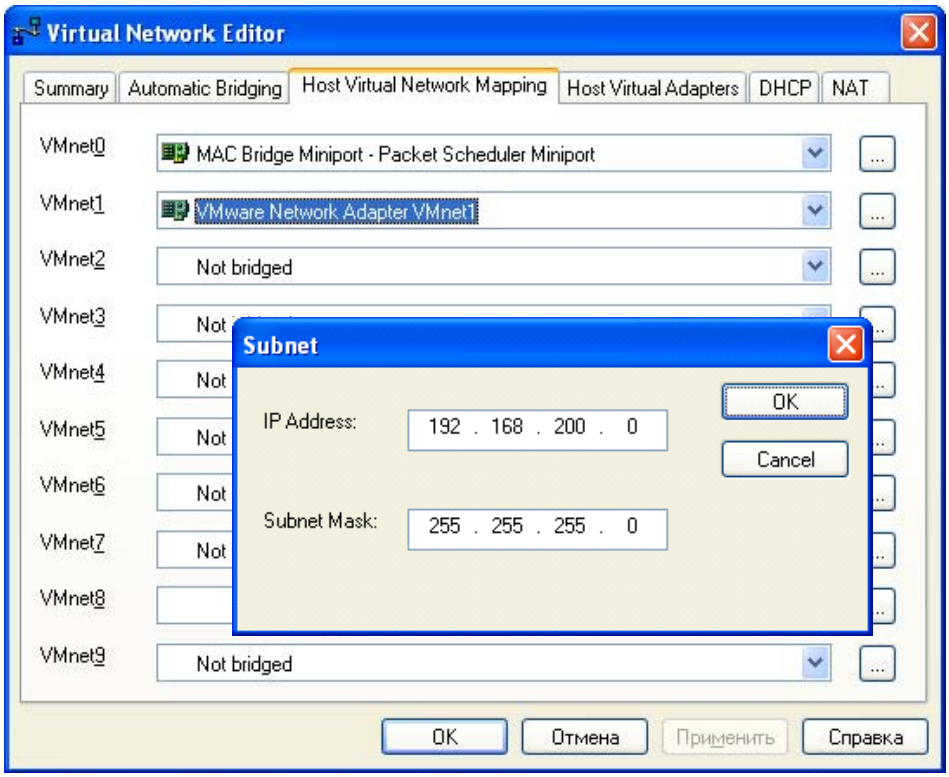


Рис. 4.10. Настройка подсети адаптера VMnet1

4. В настройках загружаемой виртуальной машины указать подключение к адаптеру VMnet1 (рис. 4.11).

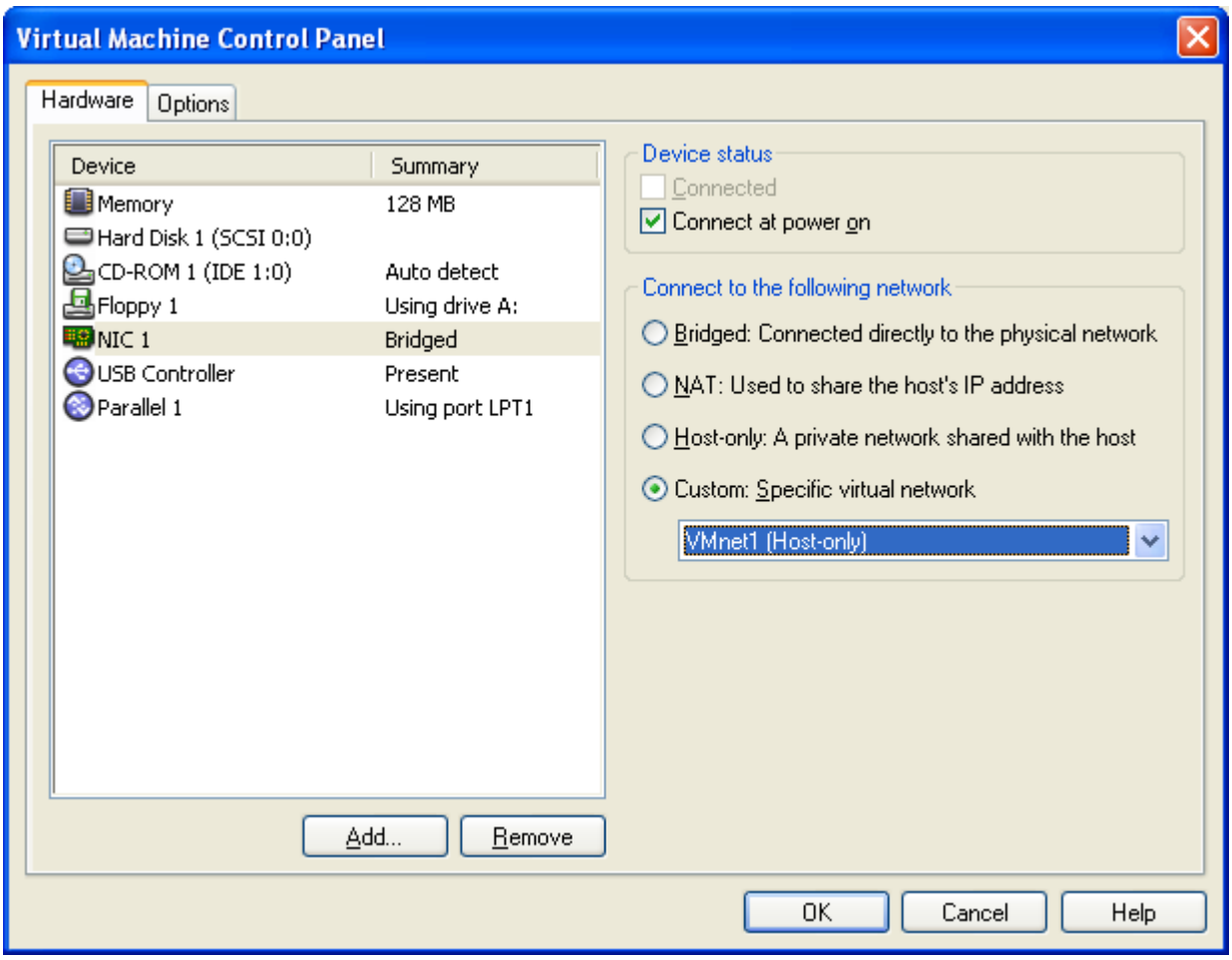


Рис. 4.11. Настройка адаптера виртуальной машины на адаптер VMnet1

5. Установить IP-адрес виртуальной машины 192.168.200.2.
6. Установить IP-адрес адаптера VMnet1 основной ОС (VMware Network Adapter VMnet1) 192.168.200.1.
7. Подключение по локальной сети основной ОС настроить на IP-адрес 192.168.1.128.
8. Добавить в основной ОС входящее подключение VPN, для чего в свойствах «Сетевого окружения» запустить «Мастер новых подключений». С помощью мастера последовательно установить следующие параметры: «Установить прямое подключение к другому компьютеру»; «Принимать входящие подключения»; «Разрешить виртуальные частные подключения»; указать учетную запись, которая будет использована для подключения.
9. Настроить в основной ОС входящее подключение VPN в разделах:
   «Общие» ⇒ «Разрешить другим пользователям устанавливать частное подключение к моему компьютеру с помощью туннеля в Интернете или другой сети» (установлен).
   «Пользователи» ⇒ «Все пользователи должны держать в секрете свои пароли и данные» (сброшен)
   «Сеть» ⇒ «Протокол Интернета (TCP/IP)» ⇒ «Разрешить звонящим доступ к локальной сети» (установлен)
   «Сеть» ⇒ «Протокол Интернета (TCP/IP)» ⇒ «Указать IP-адреса явным образом» (192.168.1.128 — 192.168.1.254)

«Сеть» ⇒ «Клиент для сетей Microsoft» (установлен)

«Сеть» ⇒ «Служба доступа к файлам и принтерам сетей Microsoft» (установлен)

Остальные параметры оставить по умолчанию.

10. Добавить в ОС виртуальной машины подключение к виртуальной частной сети через Интернет со следующими параметрами:

«IP-адрес компьютера, к которому осуществляется подключение» (IP-адрес назначения): 192.168.200.1

«Безопасность» ⇒ «Требуется шифрование данных» (сброшен)

«Сеть» ⇒ «Тип вызываемого сервера VPN» ⇒ «Туннельный протокол точка-точка (PPTP)»

«Сеть» ⇒ «Тип вызываемого сервера VPN» ⇒ «Настройка» ⇒ «Программное сжатие данных» (сброшен)

«Сеть» ⇒ «Клиент для сетей Microsoft» (установлен)

«Сеть» ⇒ «Служба доступа к файлам и принтерам сетей Microsoft» (установлен)

11. Чтобы предотвратить возможность сетевого доступа к файлам и каталогам основной ОС с виртуальной машины в обход туннеля VPN, необходимо дополнительно установить следующие параметры для соединения VMnet1 в основной ОС:

«Общие» ⇒ «Протокол Интернета (TCP/IP)» ⇒ «Дополнительно» ⇒ «WINS» ⇒ «Отключить NetBIOS через TCP/IP»

«Общие» ⇒ «Клиент для сетей Microsoft» (сброшен)

«Общие» ⇒ «Служба доступа к файлам и принтерам сетей Microsoft» (сброшен)

Аналогичные параметры должны быть установлены для подключения к локальной сети в ОС виртуальной машины (тоже, фактически, VMnet1):

«Общие» ⇒ «Протокол Интернета (TCP/IP)» ⇒ «Дополнительно» ⇒ «WINS» ⇒ «Отключить NetBIOS через TCP/IP»

«Общие» ⇒ «Клиент для сетей Microsoft» (сброшен)

«Общие» ⇒ «Служба доступа к файлам и принтерам сетей Microsoft» (сброшен)

12. Установить виртуальное частное подключение. Выяснить адрес, выделенный клиенту, а также адрес сервера. При установленном параметре «Разрешить звонящим доступ к локальной сети» подключившийся таким образом клиент становится узлом локальной сети, но только на сетевом уровне модели OSI и выше.

4.5.3. Анализ защищенности передаваемой информации

Предлагается изучить степень защищенности передаваемой по туннельному соединению информации с использованием анализатора сетевого трафика.

ВЫПОЛНИТЬ!

13. На втором рабочем месте запустить произвольный web-сервер.
14. Запустить анализатор трафика и настроить его на перехват пакетов, передаваемых виртуальным сетевым адаптером VMnet1.
15. Отправить из ОС виртуальной машины несколько ECHO-запросов в адрес сервера двумя способами: сначала напрямую через сеть VMnet1 (адрес сервера 192.168.200.1), а затем через туннельное соединение (адрес сервера необходимо выяснить при помощи диалогового окна состояния соединения). Обратите внимание, что пакеты, посылаемые через туннельное соединение, не опознаются как ICMP-пакеты. Поскольку шифрование передаваемой информации и программное сжатие отключены, то содержимое исходного IP-пакета сохраняется в первоначальном виде. Изменения в передаваемой информации заключаются только в том, что к исходному пакету добавляется заголовок протокола PPTP, который затем снимается при выходе пакета из туннеля.
16. Перевести IP-адреса источников и приемников ECHO-запросов (всего 4 различных адреса) в шестнадцатеричную систему исчисления. Найти эти адреса в перехваченных пакетах. Убедиться, что при туннелировании IP-адреса остаются неизменными и могут быть восстановлены в случае перехвата трафика. Привести пакеты ECHO-запросов, отправленных напрямую и через туннель, и выделить в них соответствующие IP-адреса.
17. Запустить на виртуальной машине Internet Explorer и подключиться к запущенному в локальной сети web-серверу. При помощи анализатора трафика посмотреть пакеты, передаваемые через интерфейс VMnet1. Найти HTTP-запросы, отправляемые на 80 (50h) порт web-сервера, а также ответы сервера, отправляемые с 80 порта. Текст HTTP-запроса начинается со слова GET, следующего за ним пробела и далее URL запрашиваемого ресурса. Сравнить эти пакеты с пакетами, передаваемыми по локальной сети. В чем выражено отличие этих пакетов?
18. Разорвать виртуальное соединение.
19. Включить шифрование передаваемой информации, для этого в свойствах соединения в ОС виртуальной машины установить следующий параметр:
    Безопасность ⇒ Шифрование данных
20. Установить виртуальное соединение. Отправить из ОС виртуальной машины несколько ECHO-запросов через туннельное соединение. Просмотреть перехваченный трафик, есть ли возможность установить, пакеты какого содержания передавались? Зашифрованы ли поля заголовков? Какая информация может быть перехвачена злоумышленником в случае его подключения к линии связи?

4.6. Защита данных на сетевом уровне

На сетевом уровне применяются два основных алгоритма: SKIP и IPSec. Различие в алгоритмах, главным образом, состоит в способе генерации и передачи ключей для шифрования содержимого пакетов.

4.6.1. Протокол SKIP

Протокол SKIP (Simple Key management for Internet Protocol – простое управление ключами для IP-протокола) разработан компанией Sun Microsystems в 1994 году. Основными его свойствами являются: аппаратная независимость, прозрачность для приложений и независимость от системы шифрования. Последнее очень важно ввиду того, что в большинстве стран мира, включая и Россию, существуют ограничения на применяемые в данной стране стандарты шифрования передаваемых данных. Таким образом, при реализации алгоритма в каждой стране может быть применен свой стандарт шифрования, в частности в России применяется симметричный алгоритм ГОСТ 28147-89. Широко известная реализация — линейка программных продуктов «Застава» российской компании «ЭЛВИС+».

В основе алгоритма лежит система открытых ключей Диффи-Хелмана. В этой системе предполагается наличие у каждого из пользователей пары ключей. Каждый пользователь системы защиты информации имеет секретный ключ *Кс*, известный только ему, и открытый ключ *Ко*. Открытые ключи могут быть выложены на любом общедоступном сервере.

Особенностью схемы является то, что открытый ключ *Ко* вычисляется из секретного ключа **Кс**. Вычисление осуществляется следующим образом: $Ko = gKc \bmod n$, где g и n — некоторые заранее выбранные достаточно длинные простые целые числа.

При этом если узел *J* устанавливает соединение с узлом *I*, то они легко могут сформировать общий ключ для симметричного алгоритма шифрования данных, воспользовавшись возможностью вычисления общего для них разделяемого секрета *Kij*:

$Kij = Koj * Kci = (gKcj) * Kci \bmod n = (gKci) * Kcj \bmod n = Koi * Kcj = Kij$.

Иными словами, отправитель и получатель пакета могут вычислить разделяемый секрет на основании собственного секретного ключа и открытого ключа партнера.

Полученный ключ *Kij* является долговременным разделяемым секретом для любой пары абонентов *I* и *J* и не может быть вычислен третьей стороной, так как секретные ключи *Kci* и *Kcj* в сетевом обмене не участвуют и третьей стороне не доступны.

Таким образом, разделяемый секрет не требуется передавать по линии связи для организации соединения, и он пригоден в качестве ключа для симметричного алгоритма шифрования. Однако на практике для шифрования отдельных пакетов применяют так называемый пакетный ключ, который помещают в заголовок SKIP-пакета и зашифровывают с помощью разделяемого секрета.

Далее полученный пакет дополняется новым IP-заголовком, адресами в котором являются адреса туннелирующих узлов (рис. 4.12).

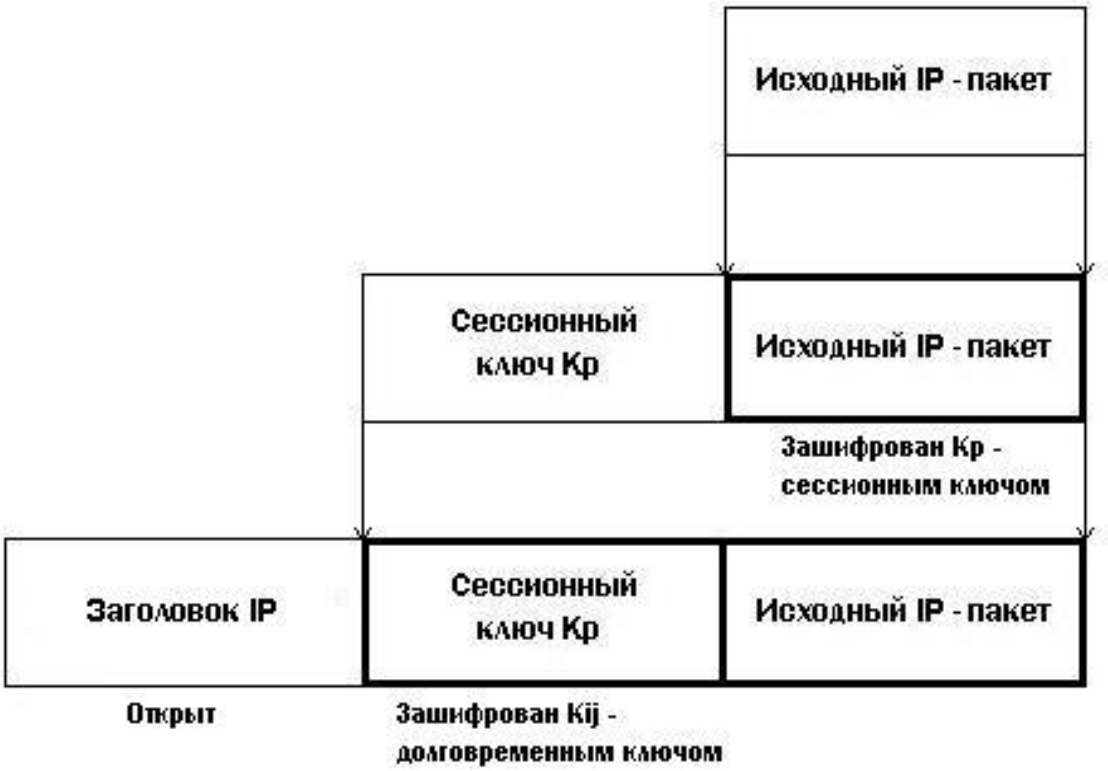


Рис. 4.12. Схема создания SKIP-пакета

Преимуществами такого решения являются, во-первых, дополнительная защита разделяемого секрета, так как он используется для шифрования малой части трафика (только лишь пакетного ключа) и не даёт вероятному противнику материал для статистического криптоанализа в виде большого количества информации, зашифрованного им; во-вторых, в случае компрометации пакетного ключа ущерб составит лишь небольшая группа пакетов, зашифрованных им.

В том случае, когда отсутствует необходимость шифрования или подписывания данных, соответствующие элементы, а именно пакетный ключ и ЭЦП пакета, могут отсутствовать. Необходимость шифрования и/или подписывания указывается при установке параметров SKIP-соединения. Так, в примере настроек SKIP-протокола в СЗИ «Застава», приведенном на рис. 4.13 (в нижней части рисунка), указано на необходимость шифрования данных пакетов с использованием алгоритма DES, требование аутентификации, т. е. применения ЭЦП пакета, отсутствует.

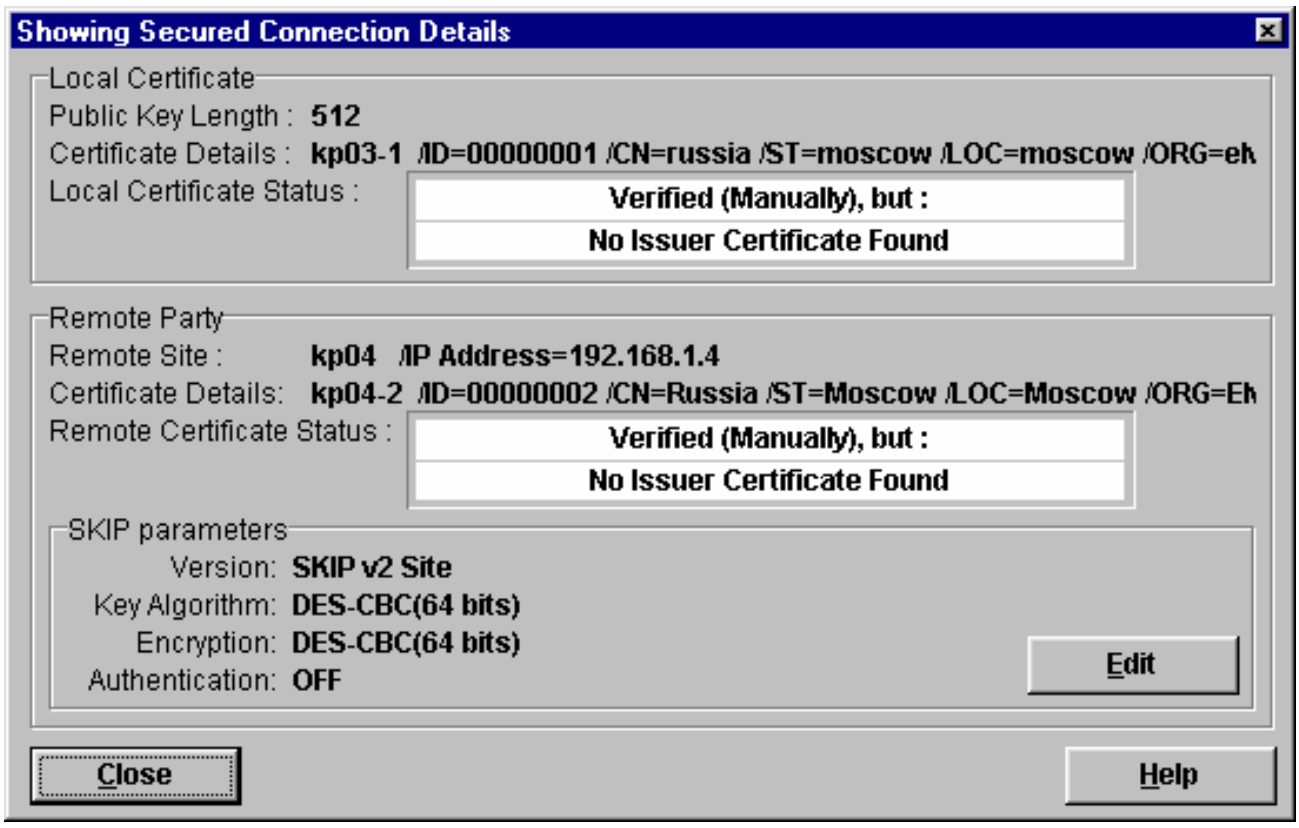


Рис. 4.13. Настройки параметров протокола SKIP

Технология, применяющая протокол SKIP, не свободна от ряда организационных проблем:

− необходимо обеспечить безопасное хранение секретных ключей *Kc* и кэширования разделяемых секретов *Kij*;

− необходимо обеспечить безопасный способ генерации и хранения (в течение относительно короткого времени жизни) пакетных ключей *Kp*;

− обеспечить сертификацию открытых ключей.

Проблема обеспечения сертификации открытых ключей возникает вследствие возможности проведения известной атаки «man-in-the-middle». Идея данной атаки не нова и состоит в следующем. Атакующая сторона находится внутри сети, где обмениваются информацией пользователи *i* и *j*. Цель атаки — хакер должен предложить от своего имени пользователю i «поддельный» открытый ключ *Koj*, а пользователю *j*, соответственно, «поддельный» ключ *Koi*. Данное действие вполне возможно вследствие того, что открытые ключи пользователей должны располагаться в общедоступном месте, где обязательно должна быть разрешена запись файлов (иначе никто не сможет поместить туда свой открытый ключ). После того, как подмена ключей осуществится, третья сторона сможет принимать весь шифрованный трафик от одного абонента, расшифровывать, читать, шифровать под другим ключом и передавать другому абоненту. Иными словами, весь зашифрованный трафик пойдет через «человека в центре».

В качестве защиты от подобной атаки применяется сертификация открытых ключей. Смысл сертификации заключается в создании электронного документа — сертификата открытого ключа. В данном документе кроме самого

электронного ключа должна содержаться информация о том, кому данный сертификат выдан, каков срок его действия, кем выдан, и, самое важное, должна присутствовать ЭЦП открытого ключа, сгенерированная организацией, выдавшей сертификат. Зная эту организацию, любой пользователь, желающий проверить подлинность сертификата, может получить ее открытый ключ и проверить ЭЦП, хранящуюся в сертификате.

Таблица 5.2

Пример сертификата открытого ключа

Поле	**Пример значения**
Версия сертификата	1, 2, 3
Серийный номер сертификата	40:00:00:00:00:00:00:ab:38:1e:8b:e9:00:31:0c:60
Идентификатор алгоритма ЭЦП	ГОСТ Р 34.10-94
Имя издателя сертификата	C=RU, ST=Moscow,O=PKI, CN=Certification Authority
Срок действия сертификата	Действителен с: Ноя 2 06:59:00 1999 GMT Действителен по: Ноя 6 06:59:00 2004 GMT
Имя владельца сертификата	C=RU, ST=Moscow, O=PKI, CN=Sidorov
Открытый ключ владельца	тип ключа: Открытый ключ ГОСТ длина ключа: 1024 значение: AF:ED:80:43.....
Уникальный идентификатор издателя	
Уникальный идентификатор владельца	
ЭЦП Центра сертификации	

Предполагается, что распределением открытых ключей должна заниматься заслуживающая доверия сторона. В зарубежной литературе для подобного органа используется термин Certificate Authority («Нотариус»), в российских документах он именуется Центром сертификации (ЦС).

Как уже говорилось, сертификат — файл определенного формата. Наибольшее распространение получил формат сертификата, установленный Международным телекоммуникационным союзом — ITU Rec. X.509. Электронный сертификат стандарта X.509 содержит: имя издателя сертификата; имя владельца сертификата; открытый ключ владельца; срок действия открытого (секретного) ключа издателя и владельца; дополнения; списки отозванных сертификатов.

Пример сертификата открытого ключа в формате X.509 приведен в табл. 5.2.

Протокол SKIP содержит механизмы защиты от следующих видов атак.

− Атаки из сети на сервисы ОС и на прикладные программы, подключение неавторизованных узлов к сети. Механизм: в защищаемую сеть или компьютер пропускаются пакеты только от владельца разделяемого секрета.

− Прослушивание трафика. Механизм: передаваемые пакеты могут быть прочитаны только владельцем разделяемого секрета.

− Повторение пакетов. Механизм: в аутентифицирующую часть заголовка SKIP-пакета перед вычислением криптосуммы пакета подставляется, в частности, текущее время.

− Подмена/маскарад. Механизм: все пакеты и их адресная информация аутентифицируются и защищаются от подделки криптосуммой по пакету, разделяемому секрету и текущему времени.

− Перехват сессий. Механизм: в сеть может войти только владелец разделяемого секрета.

− Атака Man-in-the-middle. Механизм: подписанные ЦС сертификаты.

− Анализ топологии сети. Механизм: топология сети полностью скрывается туннелированием всех исходящих из сети пакетов.

− Криптоанализ. Механизм: большая длина пакетных ключей (до 256 бит); частая смена пакетных ключей – через каждые 5-10 IP- пакетов; отсутствие данных для криптоанализа разделяемого секрета — он не используется непосредственно для криптообработки.

− Атака: отказ в обслуживании. Механизм: нейтрализуется для всех DoS атак, ведущихся на уровне выше чем IP. В сеть пропускаются пакеты только от владельца разделяемого секрета.

Вместе с тем, защита от ряда атак протоколом не реализуется:

− осуществляется защита лишь части трафика, например направленного в удаленный филиал. Остальной трафик (например, к web-серверам) проходит через VPN-устройство без обработки;

− нет защиты от действий пользователей, имеющих санкционированный доступ в корпоративную сеть.

4.6.2. Протокол IPSec

Протокол IPSec позволяет осуществлять две важнейшие функции сетевой защиты — осуществлять криптографическую защиту трафика и выполнять фильтрацию входящих/исходящих пакетов. Протокол реализован в ОС Windows 2000/XP. Протокол обеспечивает аутентификацию участников сетевого обмена (протокол IKE — Internet Key Exchange), защиту целостности (заголовок аутентификации AH — Authentication Header) и шифрование (ESP — Encapsulating Security Payload)

Аутентифицирующий заголовок (AH) выполняет защиту от атак, связанных с несанкционированным изменением содержимого пакета. Для этого особым образом применяется алгоритм MD5: в процессе формирования AH после-

довательно вычисляется хэш-функция от объединения самого пакета и некоторого предварительно согласованного ключа, затем от объединения полученного результата и преобразованного ключа.

Заголовок ESP служит для обеспечения конфиденциальности данных, предполагает возможность использования любого симметричного алгоритма шифрования.

Протокол обмена ключами IKE отвечает за первоначальный этап установки соединения, способ инициализации защищенного канала, процедуры обмена секретными ключами, выбор метода шифрования. Предполагает три различных способа аутентификации: технологию «вызов-ответ» с использованием хэш-функции с общим секретным ключом, применение сертификатов открытых ключей и использование протокола Керберос.

4.7. Организация VPN средствами СЗИ VipNet

4.7.1. Постановка задачи

Рассмотрим некоторую гипотетическую организацию, ведущую проектирование инженерной документации, составляющей коммерческую тайну. Готовые проекты передаются по защищенному каналу в удаленные филиалы.

Внедряемая система защиты должна обеспечить защиту от несанкционированного доступа к передаваемым данным, удовлетворяя следующим требованиям:

− только зарегистрированные пользователи могут иметь возможность входа в систему и обмена конфиденциальной информацией;

− передаваемая конфиденциальная информация должна быть защищена криптографическими методами, обеспечивающими её конфиденциальность, целостность и подлинность;

− в целях расследования возможных инцидентов должна вестись регистрация в журналах наиболее важных событий, связанных с передачей защищаемой информации по каналам связи;

− должна быть обеспечена безопасная работа пользователей в Интернет средствами межсетевого экранирования.

Пусть в данной организации работают администратор безопасности и два пользователя. Один пользователь работает в головном офисе, другой в удаленном филиале. Задачами администратора безопасности являются: создание логической структуры сети, определение необходимых соединений между узлами, создание ключевых наборов и генерация пользовательских паролей, установка различных уровней защиты сетевого трафика. Задачей пользователей, имеющих допуск к клиентской части ViPNet, является обмен конфиденциальной информацией.

В ходе работы имитируется функционирование четырех рабочих станций: две станции для работы пользователей и две станции для работы администратора безопасности. Администратор использует два функционально различных компьютера: ViPNet Менеджер и ViPNet Координатор.

Кроме того, имитируется работа компьютера стороннего наблюдателя (злоумышленника), имеющего возможность захватывать сетевой трафик на пути его следования. Задачей стороннего наблюдателя является анализ возможности получения доступа к конфиденциальной информации.

Лабораторная работа выполняется двумя слушателями на двух рабочих местах с использованием технологии виртуальных машин (см. Приложение 1). Первое рабочее место имитирует компьютер пользователя основного офиса и компьютер «ViPNet Менеджер» администратора безопасности. Второе рабочее место имитирует компьютер пользователя филиала и компьютер «ViPNet Координатор» администратора безопасности. На каждом рабочем месте запускаются две виртуальные машины с ОС Windows 2000 для установки СЗИ VipNet.

Основные операционные системы на обоих рабочих местах имитируют компьютеры сторонних наблюдателей и используются для анализа сетевого трафика.

Для исследования применяется демонстрационная версия СЗИ VipNet.

4.7.2. Настройка сетевых соединений виртуальных машин

Задача данного этапа — подготовить сетевые настройки виртуальных компьютеров для обеспечения сетевого взаимодействия между ними. Сетевые настройки виртуальных машин устанавливаются для имитации присутствия в сети независимого компьютера с отдельным IP-адресом (рис. 4.14).

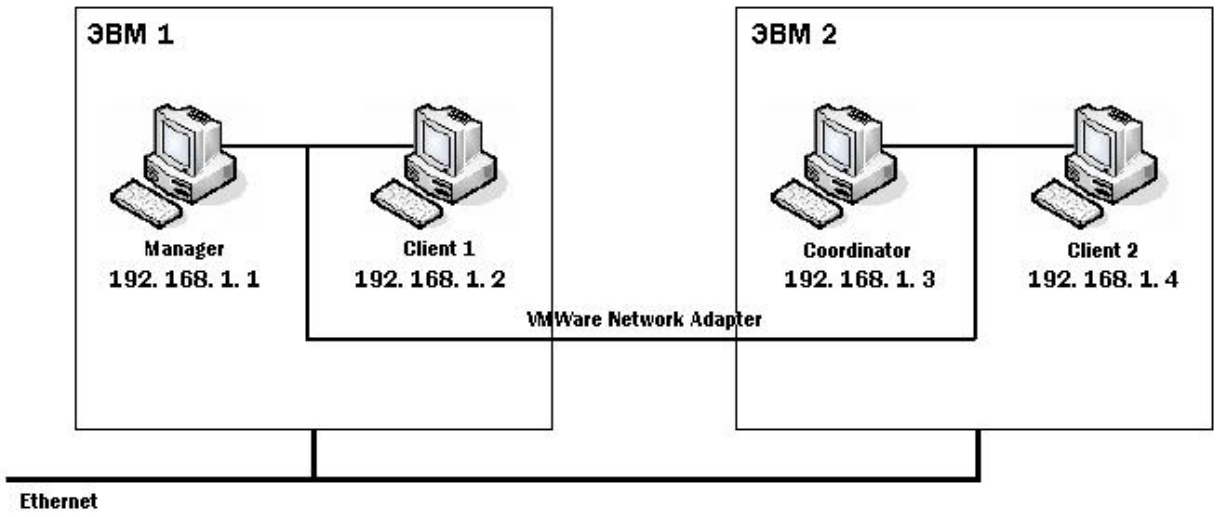


Рис. 4.14. Схема организации VPN с помощью виртуальных машин

ВЫПОЛНИТЬ!

1. На каждом рабочем месте в системе VMware открыть по два образа ОС Windows 2000. Для каждого образа на вкладке Edit выбрать меню «Virtual Machine Settings» и установить размер потребляемой памяти (Guest size) — 64 MB, а тип сетевого подключения — «bridged». Запустить все четыре виртуальные машины.
2. Назначить виртуальным ОС уникальные сетевые имена («Manager», «Client1» — для первого рабочего места, «Coordinator», «Client2» — для второго). Для этого в каждой из виртуальных ОС следует перейти на вкладку «Сетевая идентификация» окна «Свойства системы», в графе «Имя компьютера» ввести сетевое имя данной виртуальной машины.
3. Настроить IP-адреса запущенных виртуальных машин следующим образом. Назначить для первого рабочего места адреса: 192.168.1.1 (для «ViPNet Менеджера» на узле «Manager»), 192.168.1.2 (для «ViPNet Клиента1» на узле «Client1») и 192.168.1.5 (для основной ОС). Для второго рабочего места назначьте адреса: 192.168.1.3 (для «ViPNet Координатора» на узле «Coordinator»), 192.168.1.4 (для «ViPNet Клиента2» на узле «Client2») и 192.168.1.6 (для основной ОС). Для этого необходимо в каждой из виртуальных ОС зайти в свойства подключения по локальной сети, выбрать пункт «Протокол Интернета (TCP/IP)» и ввести IP-адрес.
4. С помощью программ ipconfig и ping убедитесь в правильной настройке сетевых адресов, а именно, в возможности получить ICMP-ответ от каждого из узлов.
5. Осуществите захват трафика в основных ОС, убедитесь в возможности анализа ICMP-пакетов.
6. Организуйте передачу текстового файла с одного клиентского компьютера («Client1») на другой («Client2»). Убедитесь в возможности захвата трафика и получения передаваемого документа.

4.7.3. Установка СЗИ VipNet

Установка ViPNet Office осуществляется в три этапа: сначала инсталлируется модуль менеджера, затем модуль координатора и в последнюю очередь – модули клиентов.

В идеологии данной версии СЗИ VipNet предполагается, что на компьютерах пользователей устанавливаются модули клиентов (рис. 4.15). Координаторы — это компьютеры, выполняющие функции туннелирующих узлов. Менеджер — это центральный узел, хранящий ключи и пароли всех пользователей.

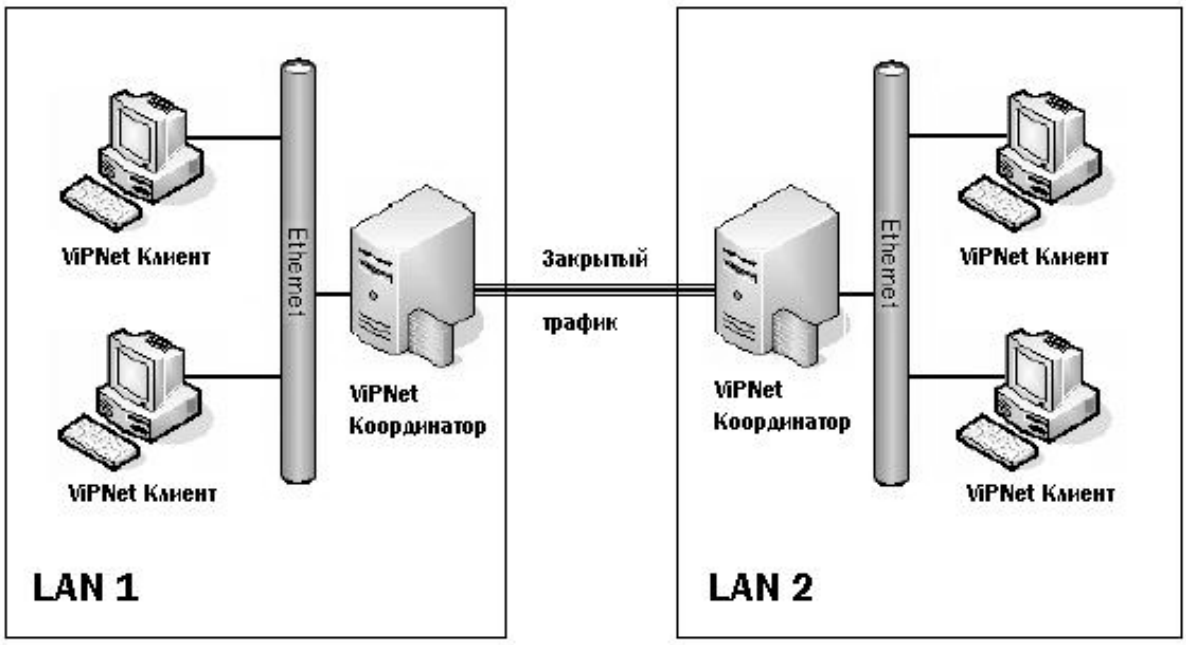


Рис. 4.15. Схема взаимодействия компонентов ViPNet в сети

Для построения имитируемой сети необходим один менеджер, один координатор и два клиента.

Для установки модуля «ViPNet Manager» необходимо запустить мастер (файл «Setup.exe» из каталога «\Soft\ViPNet Manager»). После перезагрузки компьютера следует активизировать программу «ViPNet Manager», нажав иконку на рабочем столе, и создать структуру сети при помощи «Мастера создания сети ViPNet». С помощью мастера создается структура ViPNet сети, ключевые наборы и начальные пароли для всех пользователей в режиме автоматической генерации структуры с использованием готового сценария (рис. 4.16).

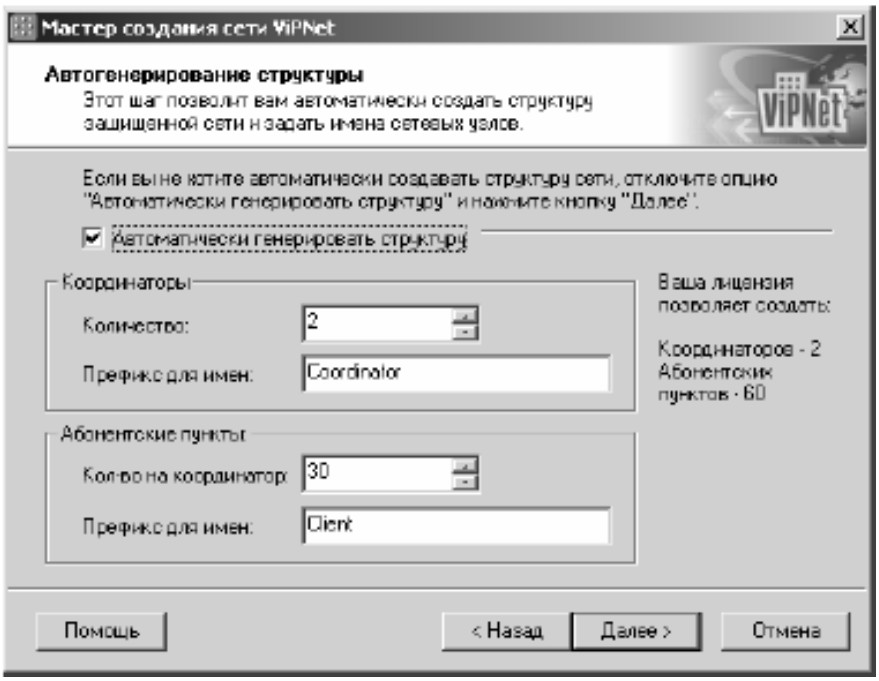


Рис. 4.16. Окно «Автогенерирование структуры»

По умолчанию префиксы имен Координаторов — «Coordinator», а префиксы имен Клиентов — «Client». Изменение вышеуказанных значений возможно при соблюдении следующих правил:

− количество Координаторов не должно быть не менее одного и не может быть больше, чем это определено лицензией;

− количество Клиентов может быть равно нулю, но не более количества определенных лицензией;

− префиксы имен сетевых узлов не должны содержать более 40 символов.

− После коррекции предложенных значений следует нажать кнопку Далее и перейти в окно «Автоматическое создание связей», в котором производится выбор стандартных сценариев для разрешенных соединений между узлами сети ViPNet.

Существуют следующие варианты установления связи:

− Связать все сетевые узлы — установлено по умолчанию. Все Клиенты и Координаторы будут иметь разрешенные VPN-соединения между собой.

− Связать все абонентские пункты каждого координатора — Клиенты, лицензированные для данного Координатора, будут иметь разрешенные VPN-соединения между собой и с соответствующим Координатором. Координаторы будут связаны VPN-соединениями между собой.

− Связать каждый абонентский пункт со своим координатором — каждый Клиент будет иметь разрешенное соединение только со своим Координатором. Координаторы будут по-прежнему иметь VPN-соединение по схеме «каждый с каждым».

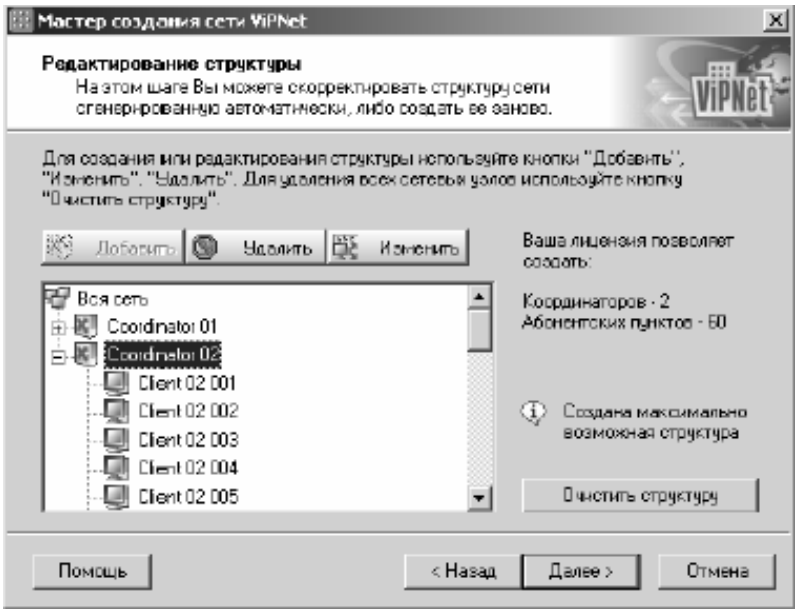


Рис. 4.17. Окно «Редактирование структуры»

После выбора оптимального варианта появляется окно «Редактирование структуры» (рис. 4.17). На этом шаге предоставляется возможность модернизации созданной структуры, а также создания новой. В окне можно осуществлять следующие действия: добавлять новые сетевые узлы, переименовывать и уда-

лять существующие узлы, переносить Клиента под обслуживание другим Координатором, удалять сетевую структуру.

После завершения редактирования структуры появляется окно, в котором следует сгенерировать системный пароль, затем, следуя инструкциям мастера установки, необходимо создать дистрибутив ключей. В процессе генерации появится окно «Электронная рулетка» — специальное приложение для генерации случайных значений.

Дистрибутив ключей для каждого сетевого узла размещен в файле с расширением «*.DST». Исходные ключи зашифрованы на парольной фразе и потому недоступны третьим лицам непосредственно из DST-файла.

Все наборы ключей и пароли к ним будут сохранены в подкаталоге «\NCC\KEYS» для каталога, куда был установлен «ViPNet Manager». Файлы с ключевыми наборами сохраняются в каталогах с именами сетевых узлов и имеют расширение «*.DST». Также будет создан файл «ViPNet.txt», в котором будут указаны пароли для соответствующих ключевых наборов.

ВЫПОЛНИТЬ!

7. Установить модуль «ViPNet Manager» на диск виртуальной машины с сетевым именем «Manager».
8. После перезагрузки виртуальной машины выполнить автоматическую генерацию структуры сети. Установить: количество координаторов — 1; количество клиентов — 2; все клиенты и координаторы должны иметь разрешенные VPN-соединения между собой (пункт «Связать все сетевые узлы»).
9. Сгенерировать наборы ключей и пароли к ним, основываясь на требованиях: словарь — английский, слов в парольной фразе — 6, используемых букв — 3.
10. После завершения работы мастера скопировать все наборы ключей и пароли к ним из каталога «C:\Program Files\InfoTeCS\ViPNet Manager\NCC\KEYS» на отдельную дискету (ключевую дискету).

Для установки «ViPNet Координатор» необходимо запустить файл «Setup.exe» из каталога «\Soft\ViPNet Coordinator\» и следовать указаниям мастера установки. В ходе последующей загрузки компьютера «ViPNet Координатор» автоматически попросит ввести соответствующий пароль из списка, находящегося в файле «ViPNet.txt», еще до появления запроса на пароль входа в ОС Windows (рис. 4.18).

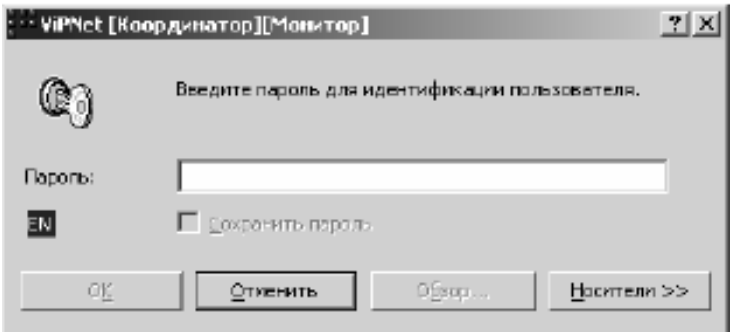


Рис. 4.18. Окно ввода пароля VipNet

В компьютер необходимо поместить внешний носитель (дискету), на котором предварительно в процессе работы с «ViPNet Manager» были записаны наборы ключей. При нажатии кнопки «Носители» появляется проводник, в котором указывается путь, где хранятся ключи на внешнем носителе. Соответствующие данному узлу ключи будут скопированы автоматически на системный диск. Путь к ним будет указан, как представлено на рис. 4.19. В дальнейшем для входа на этот же узел ViPNet внешний носитель уже не понадобится.

Установка «ViPNet Клиента» осуществляется аналогично.

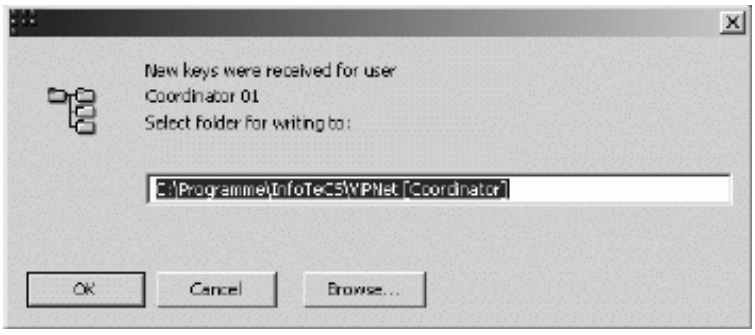


Рис. 4.19. Окно с указанием пути к файлам ключей

ВЫПОЛНИТЬ!

11. Установить модуль «ViPNet Координатор» на диск виртуальной машины с сетевым именем «Coordinator», модули «ViPNet Клиент» на диски узлов «Client1» и «Client2».

4.7.4. Настройка СЗИ VipNet

Как указывалось выше, узлы ViPNet могут быть подключены к сети непосредственно либо могут располагаться за межсетевыми экранами и другими устройствами. Для каждого узла может быть указан один из способов подключения:

- непосредственное соединение с другими узлами;
- соединение с другими узлами через локальный Координатор, обеспечивающий технологию преобразования сетевых адресов (NAT — Network Address Translation) для трафика данного Клиента;
- соединение через межсетевой экран/NAT систему, NAT-правила которой могут быть модифицированы;
- соединение через межсетевой экран/NAT систему, установки которой не могут быть модифицированы.

После запуска каждый сетевой узел ViPNet посылает соответствующую информацию Координатору. В изучаемой лабораторной установке каждый сетевой узел имеет IP-адрес, свободно доступный другим ViPNet-узлам, поскольку все виртуальные машины находятся в одном сегменте сети. Таким образом, любому клиенту для организации взаимодействия достаточно послать Координатору только свой IP-адрес. Таким образом, при настройке узлов-клиентов

достаточно для них выбрать соединение первого типа — «Непосредственное соединение с другими узлами».

Настройка модуля «ViPNet Manager» может осуществляться для модернизации структуры сети, изменения сетевых узлов, создания ключевых наборов и просмотра параметров всей сети или отдельных сетевых узлов. Главное окно программы разделено на левую и правую части (рис. 4.20). На левой стороне приведена древовидная структура сети с отображением сетевых узлов. Просмотр информации о каждом отдельном объекте осуществляется посредством выбора этого объекта на изображении дерева.

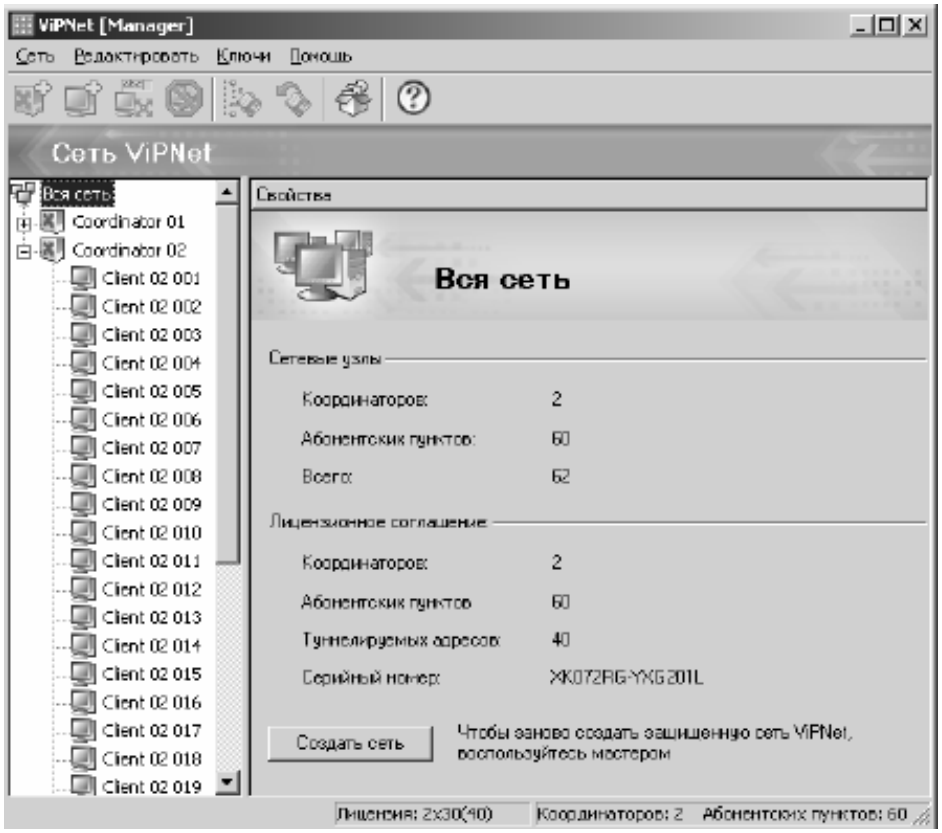


Рис. 4.20. Окно «Вся сеть» модуля «ViPNet Manager»

При выборе корневого объекта дерева «Вся сеть» появляется информация о сети, в частности количество фактически созданных сетевых узлов, включая количество Клиентов, Координаторов и общее количество узлов.

Кнопка «Создать сеть» используется для создания абсолютно новой сети, но при этом все ранее созданные конфигурации теряются.

Информация о конкретном сетевом узле появляется в правой части главного окна после выбора этого узла на дереве структуры сети (рис. 4.21) и содержит следующие данные:

- тип узла — Координатор или Клиент;
- имя узла;
- максимально возможное количество туннелируемых соединений через Координатор (если в качестве узла выбран Координатор);
- пароль и соответствующая парольная фраза (если существует);
- путь к месту, где хранятся ключи сетевого узла (если они существуют).

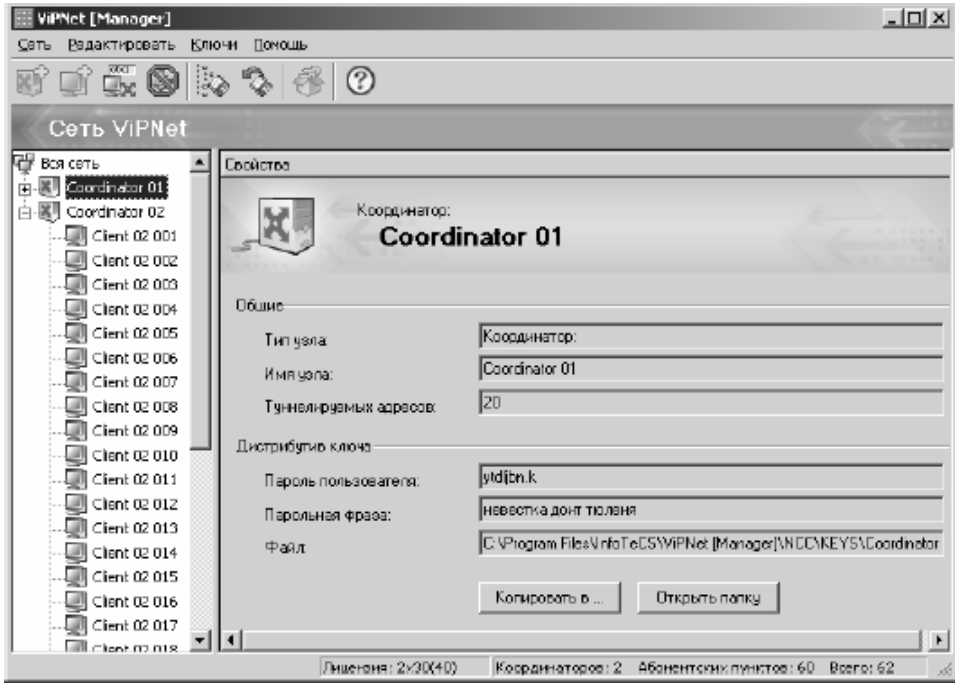


Рис. 4.21. Окно свойств сетевого узла модуля «ViPNet Manager»

Кнопка «Открыть папку» открывает подкаталог, содержащий DST-файл дистрибутива ключей для выбранного сетевого узла.

Кнопка «Копировать в…» запускает процедуру копирования ключевого набора в определенное администратором место.

Настройка модулей «ViPNet Координатор» и «ViPNet Клиент» осуществляется с помощью окна Монитора (рис. 4.22), для открытия которого следует воспользоваться иконкой , расположенной в области системного трея. Левая часть окна содержит средства конфигурирования и администрирования в виде каталогизированного дерева.

Сразу после открытия окна по умолчанию выбрана секция «Защищенная сеть». В правой части окна показаны все сетевые узлы ViPNet, VPN соединение с которыми было разрешено на этапе создания структуры сети с помощью «ViPNet Manager». Сетевые узлы будут высвечиваться разными цветами:

- серый — сетевой узел отключен (находится в состоянии off-line);
- голубой — обозначает данный локальный узел;
- красный — обозначает доступные Координаторы;
- фиолетовый — ViPNet Клиенты в состоянии on-line.
- Дополнительно статус узла показан с помощью следующих символов:
- — локальный узел;
- — узел в состоянии off-line;
- — Клиент в состоянии on-line;
- — Координатор в состоянии on-line.

Значительная часть настроек в секциях «Защищенная сеть», «Открытая сеть», «Блокированные IP-пакеты» и «Режимы связана» с настройкой работы интегрированного межсетевого экрана. Секция «Настройки» позволяет выбрать и настроить тип соединения в зависимости от реализованного физического способа подключения сетевого узла. Остальные элементы дерева содержат инст-

рументы для получения статистической информации, создания готовых конфигураций, расширения возможностей администрирования и т. п.

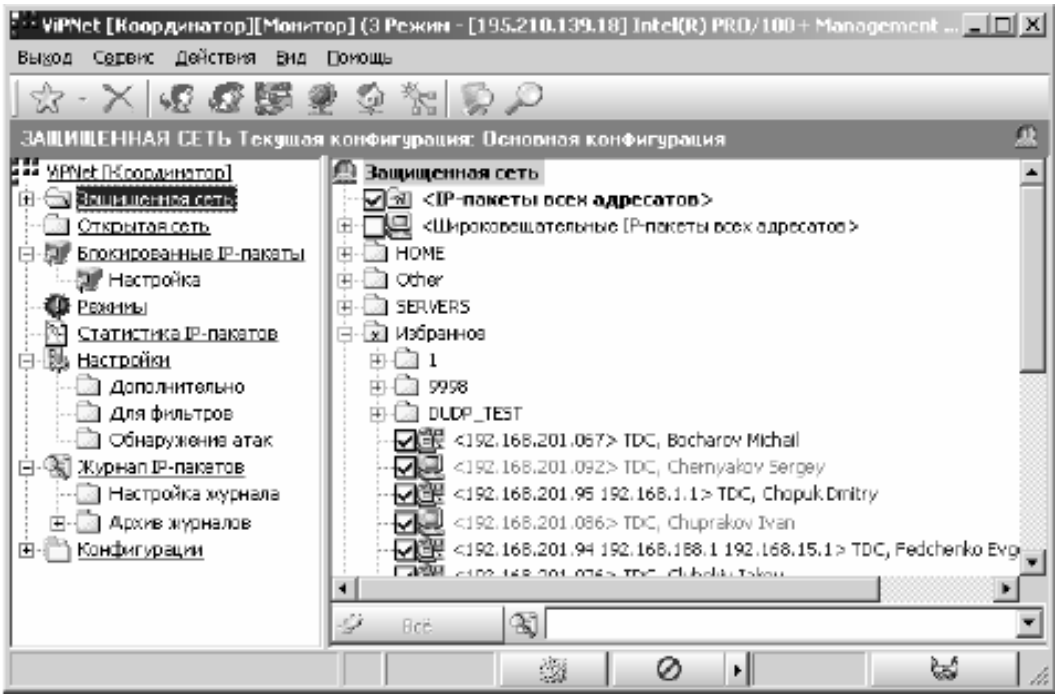


Рис. 4.22. Окно Монитор модуля «ViPNet Координатор»

ВЫПОЛНИТЬ!

12. Создать и проверить соединения между координатором и клиентами. Для этого необходимо загрузить программу «Координатор Монитор» на виртуальной машине с сетевым именем «Coordinator». В списке узлов «Защищенная сеть» выбрать соответствующего клиента, дважды кликнув на нем мышью открыть окно «Правило доступа», выбрать закладку «IP-адреса», нажать кнопку «Добавить» и ввести IP-адрес данного клиента (192.168.1.2 (для «ViPNet Клиента1» на узле «Client1») и 192.168.1.4 (для «ViPNet Клиента2» на узле «Client2»).
13. Загрузить программу «Клиент — Монитор» на виртуальных машинах «Client1» и «Client2». Провести аналогичные операции, введя IP-адрес координатора.
14. Убедиться в том, что соединение Координатор — Клиенты установлено. Для этого следует вернуться в секцию «Защищенная сеть» на виртуальной машине «Coordinator», выбрать соответствующего клиента в списке сетевых узлов, вызвать контекстное меню и выполнить команду «Проверить соединение».
15. Подготовить компьютеры «Client1» и «Client2» к файловому обмену. Для этого на «Client1» следует запустить программу «Клиент Монитор», вызвать программу «Деловая почта», нажав кнопку  на нижней панели. На верхней панели окна ViPNet [Клиент][Деловая почта] нажать кнопку «Отправить/Получить письма».

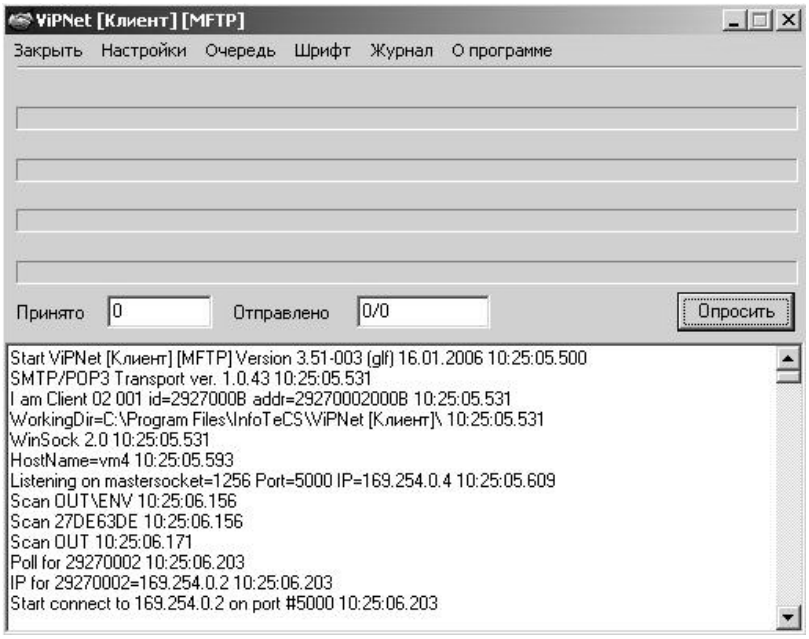


Рис. 4.23. Окно ViPNet [Клиент][Деловая почта]

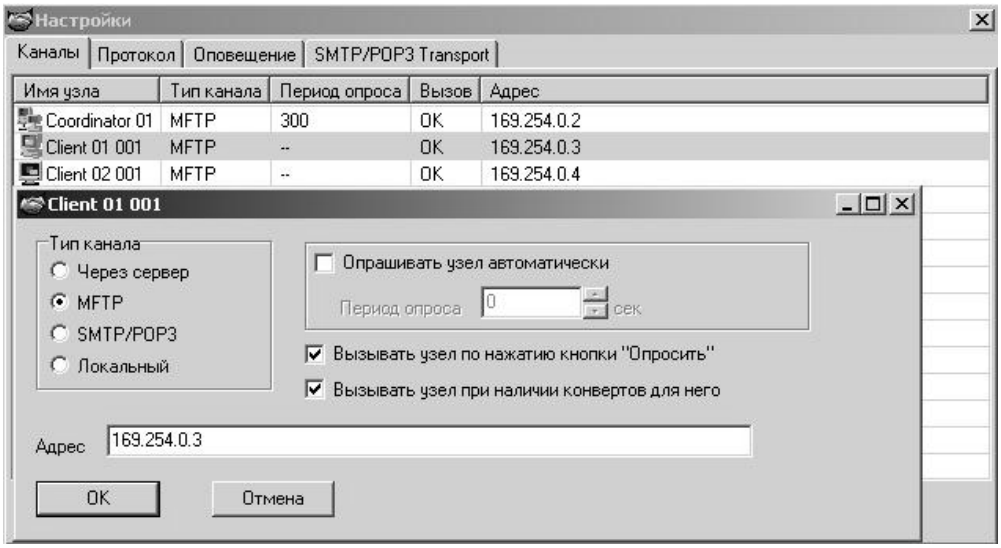


Рис. 4.24. Окно настроек почтового соединения

16. На панели инструментов появившегося окна (рис. 4.23) нажать кнопку «Настройки», чтобы появился список узлов ViPNet сети.
17. В появившемся списке узлов кликнуть два раза мышью на узле «Client1», чтобы появилось окно настроек почтового соединения (рис. 4.24). Установить следующие параметры:
   – Тип канала: MFTP;
   – Вызывать узел по нажатию кнопки «Опросить» (включить);
   – Ввести IP-адрес данного узла (192.168.1.2) (см. выше).

   Выполнить аналогичные операции для узла «Client2» (IP-адрес 192.168.1.4).
18. На узле «Client2» выполнить аналогичные настройки.
19. На компьютере «Client1» создать небольшой текстовый файл с произвольной информацией. Запустить анализатор трафика в режиме захвата пакетов. Запустить программу «Клиент Монитор», в папке «Защищенная сеть» выбрать получателя файла — «Client2», вызвать программу «Файловый об-

мен», нажав кнопку  на верхней панели. В программе «Файловый обмен» ввести получателя (Client2) в поле «Адрес», присоединить текстовый файл нажатием кнопки «Добавить» и отправить письмо.

20. На компьютере «Client2» в программе «Клиент Монитор» нажать кнопку «Принято» и просмотреть полученный текстовый файл.
21. Убедиться в невозможности нахождения имени и содержимого текстового файла в захваченных сетевых пакетах.

4.8. Использование протокола IPSec для защиты сетей

4.8.1. Шифрование трафика с использованием протокола IPSec

ВЫПОЛНИТЬ!

1. Проверьте возможность анализа сетевого трафика при отключенном протоколе IPSec. Запустите анализатор сетевого трафика. Отправьте текстовый файл (набранный латинскими буквами) на виртуальный компьютер. Просмотрите захваченные пакеты. Убедитесь, что файл передается по протоколу SMB, текст файла передается в открытом виде.
2. Осуществите настройку протокола IPsec. ***Администрирование ⇒ Локальная политика безопасности ⇒ Политики безопасности IP***.
3. Обратите внимание на существование трех шаблонов: «Безопасность сервера» (при использовании данного шаблона не допускается нешифрованный трафик), «Клиент (Только ответ)» (при использовании данного шаблона возможен нешифрованный трафик, если сервер его не требует) и «Сервер (Запрос безопасности)» (при использовании данного шаблона возможен нешифрованный трафик, если клиент не поддерживает шифрование).
4. Выполните настройку шаблона «Безопасность сервера». Измените настройку фильтра «Весь IP-трафик» (рис. 4.25).
5. В разделе «Методы проверки подлинности» измените метод Kerberos.
6. Выберите пункт «Использовать данную строку для защиты обмена ключами» и введите произвольную текстовую строку.
7. Примените внесенные изменения и активизируйте политику, выбрав из контекстного меню данного шаблона пункт «Назначить».
8. Аналогичные действия осуществите на соседнем компьютере. Убедитесь, что ключ шифрования (текстовая строка) совпадает.

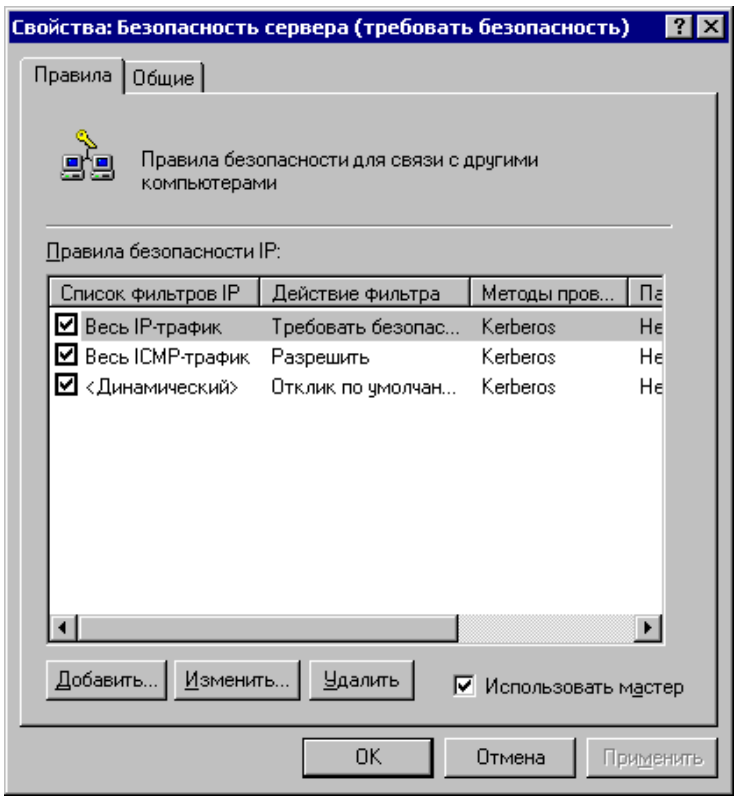


Рис. 4.25. Окно настройки шаблона «Безопасность сервера»

4.8.2. Проверка защиты трафика

9. Убедитесь, выполняя команду PING, что для проверки присутствия в сети вашего компьютера возможны ICMP-пакеты как от соседнего компьютера (на котором также включено шифрование), так и от любого другого.
10. Убедитесь, что в сетевом окружении вам доступен только соседний компьютер. При обращении к другим системам появляется ошибка.
11. Убедитесь путем анализа сетевого трафика при отправке на соседний компьютер текстового файла, что весь IP-трафик идет в зашифрованном виде.
12. Проверьте функционирование IPSec при использовании шаблонов «Клиент (Только ответ)» и «Сервер (Запрос безопасности)».
13. По окончании отключите шифрование трафика.

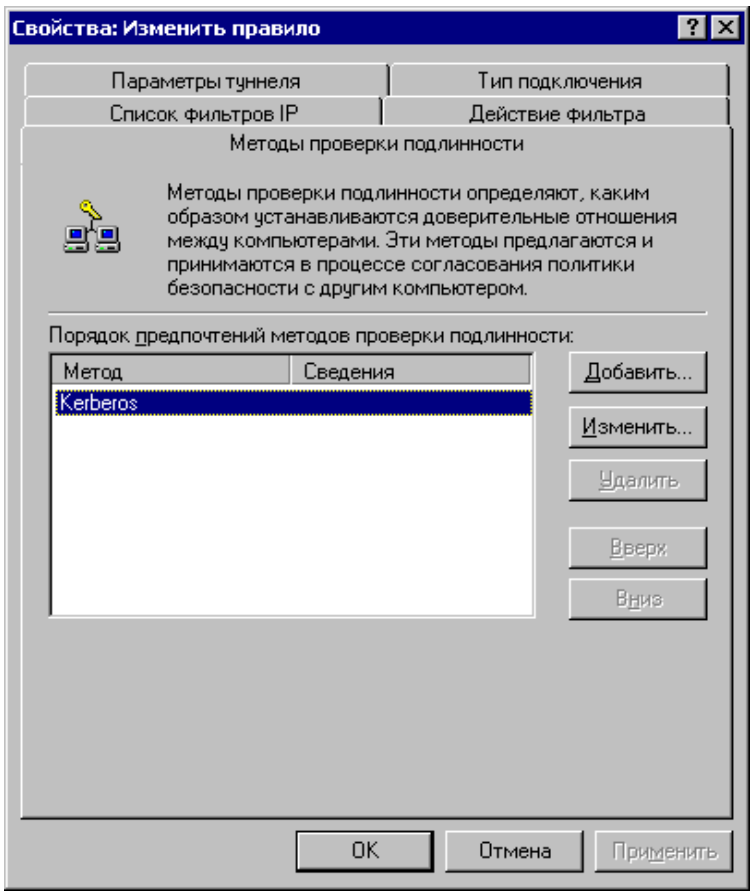


Рис. 4.26. Окно раздела «Методы проверки подлинности»

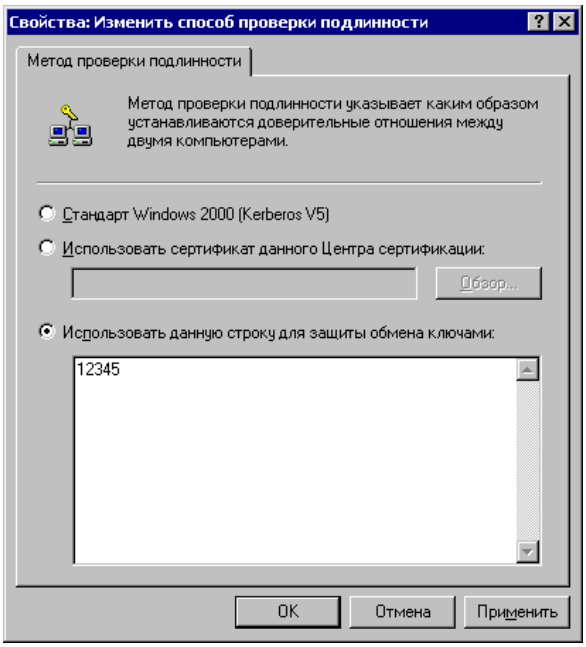


Рис. 4.27. Окно ввода ключевой строки

4.8.3. Настройка политики межсетевого экранирования с использованием протокола IPSec

Задача. Разработать политику для web-сервера, на котором разрешен только трафик через порты TCP/80 и TCP/443 из любой точки.

ВЫПОЛНИТЬ!

14. Запустите на своем узле web-сервер. Проверьте его функционирование, обратившись с другого узла.
15. Запустите утилиту настройки протокола IPSec: ***Администрирование ⇒ Локальная политика безопасности ⇒ Политики безопасности IP***.
16. Из контекстного меню выберите «Управление списками IP-фильтра и действиями фильтра». Создайте два действия (сначала сбросьте флажок «Использовать мастер»): «Разрешение» (определяющее допустимый метод безопасности) и «Блокировка» (заблокированный метод безопасности) (рис. 4.28).

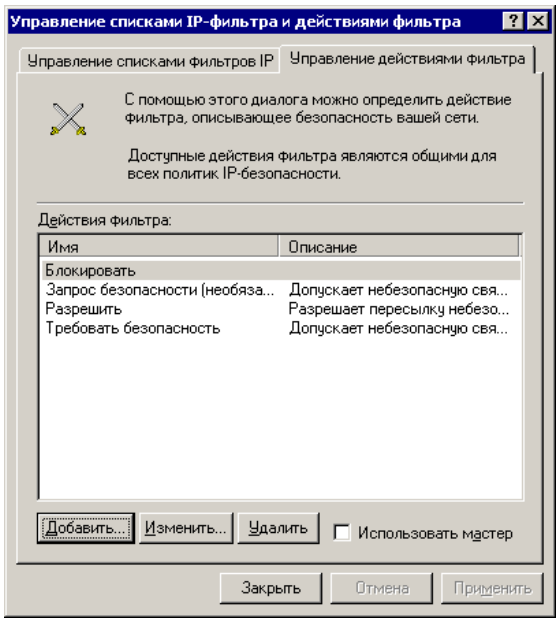


Рис. 4.28. Окно создания действий

17. Создайте список фильтров под названием «Любой», имеющий настройки по умолчанию, которые соответствуют всему трафику (рис. 4.29).
18. Создайте список фильтров под названием «web-доступ» (рис. 4.30) для web-сервера, разрешающего трафик на портах TCP/80 и TCP/443 из любой точки, основываясь на правилах:
    Правило 1. Источник – Любой IP-адрес. Назначение – Мой IP-адрес. Отображаемый – Да. Протокол – TCP. Порт источника – Любой (ANY). Порт назначения – 80.
    Правило 2. Источник – Любой IP-адрес. Назначение – Мой IP-адрес. Отображаемый – Да. Протокол – TCP. Порт источника – Любой (ANY). Порт назначения – 443.

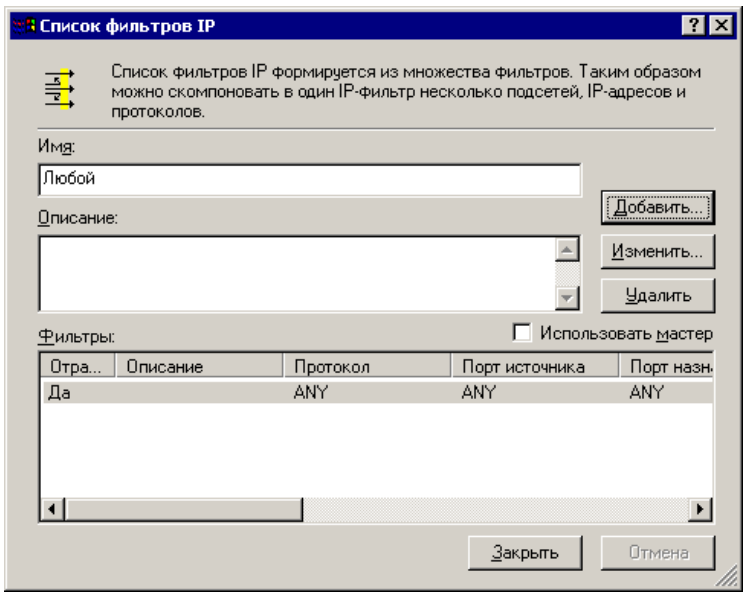


Рис. 4.29. Окно создания списка фильтров «Любой»

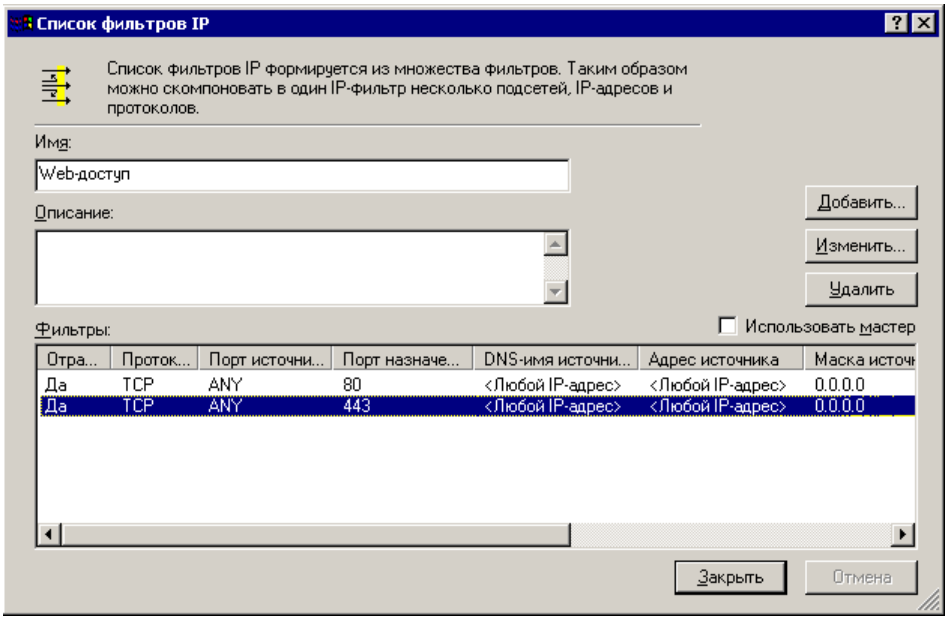


Рис. 4.30. Окно создания списка фильтров «Web-доступ»

19. Создайте новую политику под названием «Web-доступ». Из контекстного меню окна «Политики безопасности IP» выберите «Создание политики безопасности IP». Воспользуйтесь мастером. Не активизируйте пункт «Использовать правило по умолчанию».
20. Добавьте в созданную политику правило доступа «Web-доступ», использующее список фильтров «Web-доступ» и действие «Разрешение».
21. Добавьте в созданную политику правило доступа «Любой», использующее список фильтров «Любой» и действие «Блокировка» (рис. 4.31). Обратите внимание на последовательность правил.

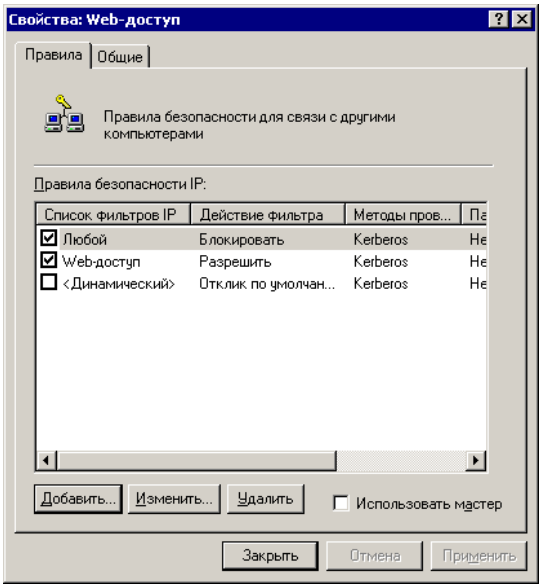


Рис. 4.31. Окно создания правила доступа

22. Примените политику «Web-доступ» (из контекстного меню политики «Web-доступ» выберите пункт «Применить», рис. 4.32).

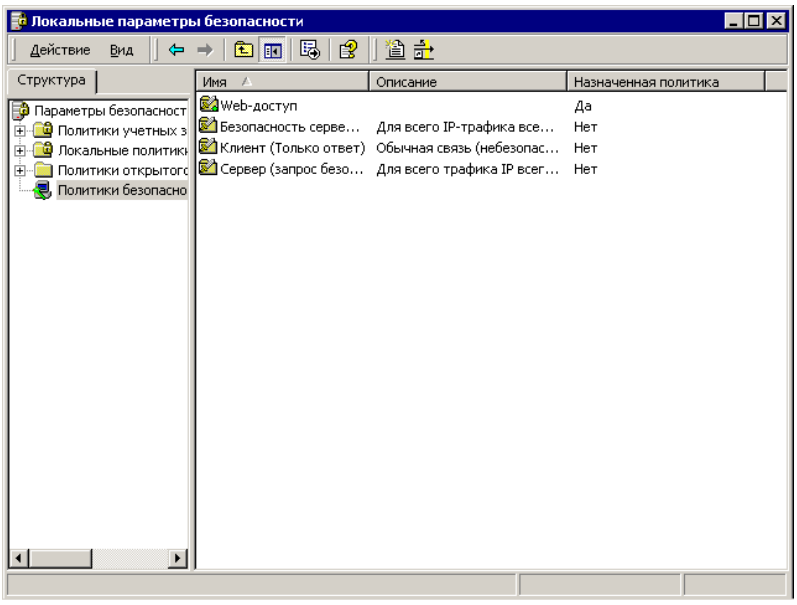


Рис. 4.32. Окно применения политики

23. Проверьте политику «Web-доступ», осуществив подключение к 80-ому порту с другого узла.

4.9. Организация VPN средствами СЗИ StrongNet

4.9.1. Описание системы

Система StrongNet предназначена для построения защищенных виртуальных частных сетей, позволяет создать защищенный канал для передачи данных между компьютерами в локальной сети или Интернет. Вся информация передается по этому каналу с использованием туннелирования в зашифрованном виде.

Система StrongNet основана на предварительном распределении ключей. Принцип работы следующий: все данные, передаваемые по защищенному каналу, шифруются с помощью симметричных алгоритмов шифрования. При этом ключи шифрования (сеансовые ключи) передаются между компьютерами при установлении защищенного соединения и шифруются с помощью асимметричного алгоритма шифрования RSA. Открытые и личные ключи, использующиеся при установлении соединения, хранятся в базе данных ключей. Распределение ключей между пользователями осуществляется системным администратором с помощью центра генерации ключей. Таким образом, пользователи сети к моменту установления соединения уже имеют все необходимые ключи.

Кроме защиты данных, передаваемых между двумя компьютерами по сети, StrongNet предоставляет функции персонального межсетевого экрана, который осуществляет фильтрацию входящих и исходящих IP-пакетов по определенным критериям.

Для работы с системой StrongNet необходимо сгенерировать и распределить между пользователями открытые и личные ключи. У каждого пользователя системы StrongNet есть набор ключей, в который входит его личный ключ и открытые ключи других пользователей системы, с которыми он обменивается данными через защищенные каналы. Набор ключей может храниться в файле либо на электронном ключе.

Программа «StrongNet Центр генерации ключей» предназначена для создания базы данных ключей, составления из них наборов, записываемых в файл или на электронный ключ, и распределения этих наборов между пользователями системы. Генерация ключей происходит один раз при создании базы данных.

4.9.2. Постановка задачи

Пусть существует некая организация, в которой в удаленных друг от друга офисах работают два пользователя. Требуется с использованием технологии виртуальных машин создать структуру сети, состоящую из двух виртуальных узлов, и установить защищенное соединение (рис. 4.33). Основная ОС имитирует работу компьютера стороннего наблюдателя и используется для анализа сетевого трафика.

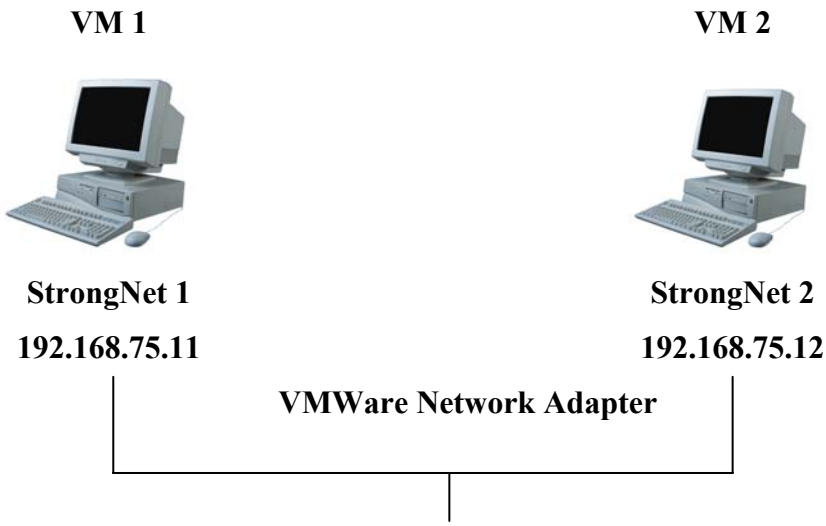


Рис. 4.33. Схема соединения виртуальных узлов

ВЫПОЛНИТЬ!

1. На рабочем месте открыть два образа ОС Windows 2000. Для каждого образа на вкладке Edit выбрать меню «Virtual Machine Settings» и установить размер потребляемой памяти (Guest size) — 64 MB, а тип сетевого подключения — «VMNet1 (Host Only)». Для обоих образов настроить виртуальные дисководы на единый файл. Запустить виртуальные ОС.
2. Настроить IP-адреса виртуальных машин (например, для первой ОС — 192.168.75.11, для второй ОС — 192.168.75.12). С помощью программ ipconfig и ping убедиться в правильной настройке сетевых адресов.
3. Осуществить захват трафика в основной ОС, убедиться в возможности анализа передаваемых ICMP-пакетов.
4. Установить систему StrongNet в обе виртуальные ОС, следуя указаниям установочной программы.

4.9.3. Генерация и распространение ключевой информации

Для успешной работы системы StrongNet необходимо создать базу данных ключей. Дистрибутив ключей для каждого сетевого узла размещен в файле с расширением «DST». Исходные ключи зашифрованы на парольной фразе и потому недоступны третьим лицам непосредственно из DST-файла. Чтобы создать базу данных ключей нужно запустить программу «Центр генерации ключей».

ВЫПОЛНИТЬ!

5. На одной из систем запустить программу «StrongNet Центр генерации ключей». В меню «Действие» выбрать пункт «Создать БД ключей». В появившемся окне установить количество генерируемых ключей — 2. Сохранить базу данных ключей.
6. Сгенерировать ключи для двух пользователей с учетом их дальнейшего взаимодействия. Для этого в правой части главного окна дважды щелкнуть

левой кнопкой мыши на элементе «Пользователь 1». В появившемся окне «Создание КК» ввести имя, в списке «Все» выбрать Пользователь 2 и нажать кнопку « >> ». Нажать кнопку «Далее». В появившемся диалоговом окне «Запись КК» выбрать тип внешнего ключа — «Файл». Указать путь и имя файла, в котором будет храниться созданный набор ключей для Пользователя 1 и открытый ключ Пользователя 2. Аналогичные действия произвести для Пользователя 2.

7. После завершения работы мастера скопировать набор ключей Пользователя 2 на дискету (виртуальную дискету).

4.9.4. Настройка СЗИ StrongNet

ВЫПОЛНИТЬ!

8. В одной из виртуальных систем открыть главное окно программы StrongNet и нажать кнопку «Развернуть» (рис. 4.34).

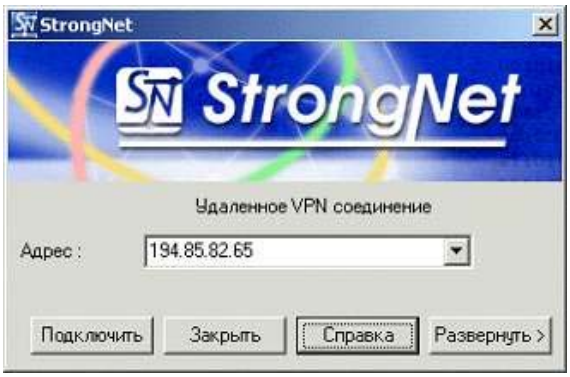


Рис. 4.34. Главное окно программы «StrongNet»

9. На вкладке «Ключи» (рис. 4.35) выбрать тип внешнего ключа – файл. Указать файл с набором ключей Пользователя 2 и нажать кнопку «Загрузить». Переключатель «Загружать ключи при старте» поставить в состояние «Включено».
10. Во второй ОС аналогично загрузить набор ключей Пользователя 2, сохраненный на дискете.
11. Используя вкладку «Настройки» (рис. 4.36) сделать так, чтобы сеансовый ключ в процессе работы защищенного соединения периодически менялся. Он может меняться по истечении некоторого промежутка времени, для этого переключатель «Генерировать ключ каждые» устанавливается во включенное состояние и в поле «Секунды» указывается длина соответствующего временного интервала. Чтобы защищенное соединение периодически проверялось на предмет активности, переключатель «Подтверждать соединение» устанавливается во включенное состояние и в поле «Секунды» указывается длина периода в секундах. Для вступления в силу сделанных изменений нажать кнопку «Применить».

Рис. 4.35. Загрузка ключевой информации

Рис. 4.36. Настройка параметров обновления ключевой информации

4.9.5. Установка защищенного соединения

ВЫПОЛНИТЬ!

12. Создать и проверить соединение между виртуальными ОС. Для этого на вкладке «Соединение» (рис. 4.37) одного из узлов указать IP-адрес второго узла и нажать кнопку «Подключить».
13. Убедиться в том, что соединение установлено. Для этого зайти на вкладку «Сессии» (рис. 4.38), подвести указатель мыши к соединению в списке, в контекстном меню выбрать пункт «Информация о соединении». Просмотреть информацию об установленном соединении.
14. Осуществить захват трафика в основной ОС, убедиться в том, что трафик является защищенным, проанализировать его тип.

Рис. 4.37. Настройка параметров соединения

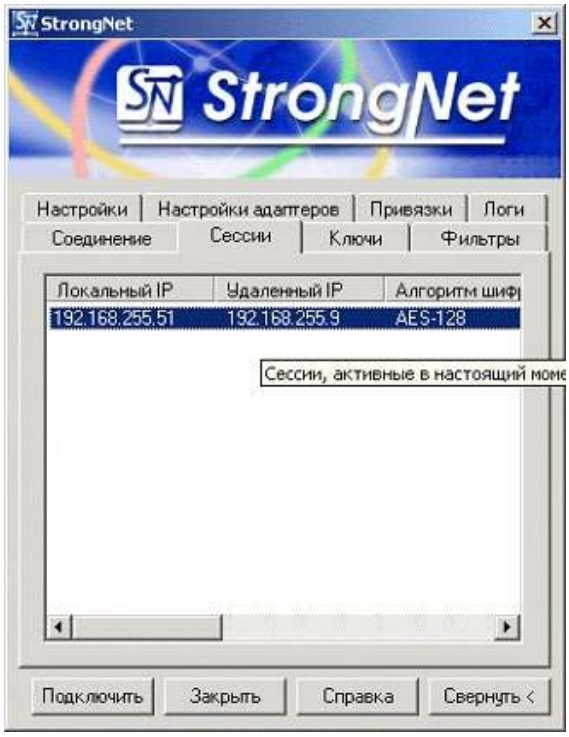


Рис. 4.38. Проверка информации о соединении

4.10. Защита на транспортном уровне

Для защиты на транспортном уровне применяются протоколы TLS и SSL. Особенностью защиты на данном уровне является независимость от прикладного уровня, однако чаще всего технология применяется для защиты данных, передаваемых по протоколу HTTP (режим HTTPS).

Подробнее рассмотрим функционирование протокола SSL. Протокол часто применяется для установки защищенного соединения, когда пользователь, обратившийся к web-серверу, передает или получает конфиденциальные сведения, например об объеме и стоимости покупки в Интернет-магазине, либо получает статистику своих соединений у Интернет-провайдера. В этом случае web-клиент, например Internet Explorer, автоматически переходит в защищенный режим, о чем свидетельствует пиктограмма «замок» в правой нижней части окна.

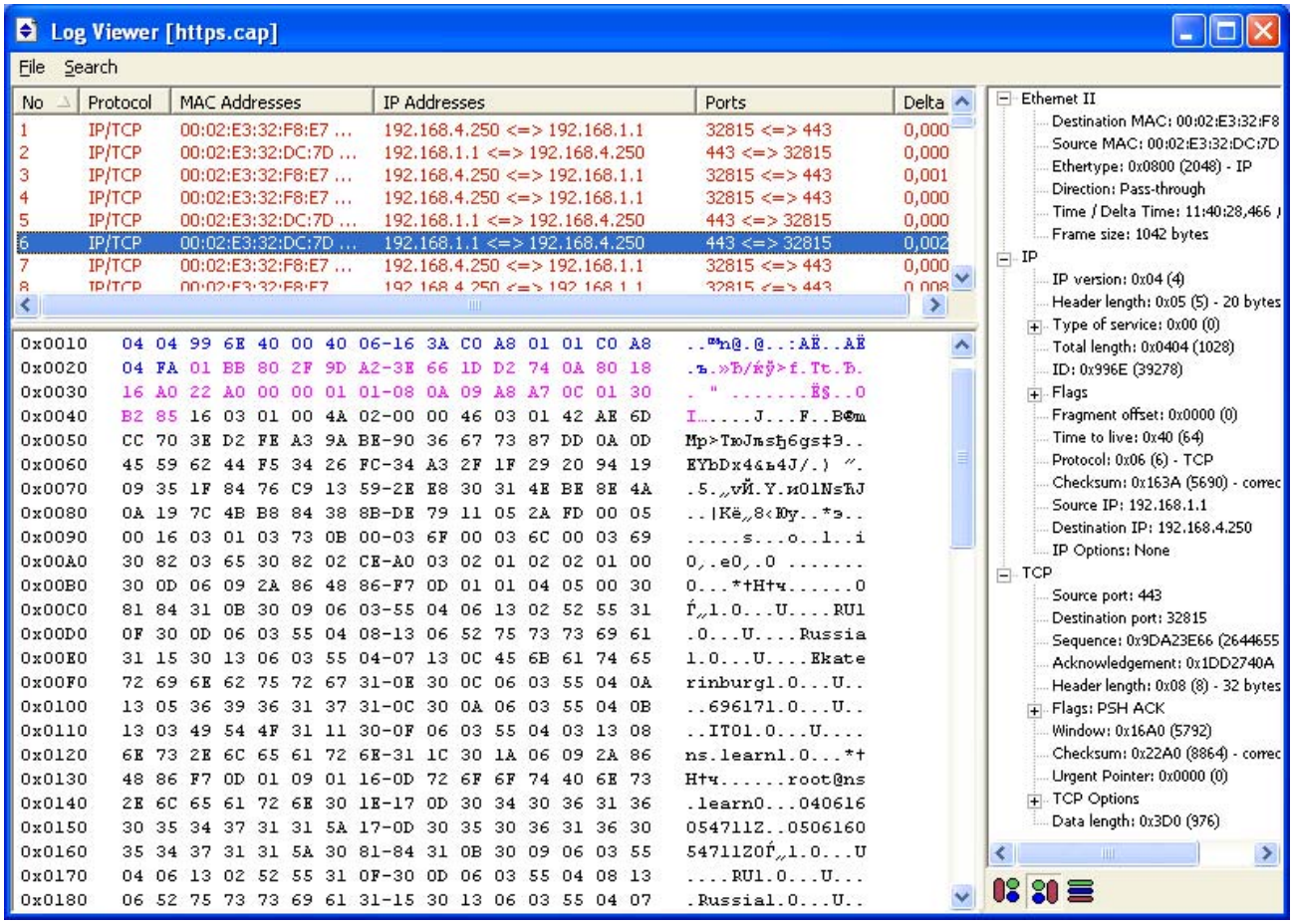


Рис. 4.39. Сетевой пакет с сертификатом открытого ключа сервера

Протокол SSL предусматривает функции аутентификации, шифрования данных и обеспечения целостности данных. Аутентификация осуществляется путем обмена цифровыми сертификатами при установлении соединения (сессии). Так как web-сервер обычно принимает запросы от произвольных клиентов, то чаще всего аутентифицируется только сервер. Для шифрования данных применяется стандартный для VPN-соединений подход: для шифрования данных применяется симметричный сеансовый ключ. Обмен симметричными се-

ансовыми ключами происходит при установлении соединения, при передаче сеансовые ключи шифруются с помощью открытых ключей. Для обеспечения целостности к сообщению добавляется его хэш-код.

Рассмотрим этапы установки SSL-соединения. Сначала устанавливается стандартное TCP-соединение с портом сервера 443. Далее клиент передает сообщение «Client-Hello», в котором сообщает поддерживаемую им версию протокола SSL и случайную последовательность «Challenge_Data». В ответ сервер передает сообщение «Server-Hello», в котором указывает версию SSL, идентификатор соединения «Connection_id», список базовых шифров (протоколов) и сертификат сервера (подписанный открытый ключ).

Цель следующего сообщения, отправляемого клиентом (сообщение «Client_Master_Key»), — передача симметричного сеансового ключа, зашифрованного открытым ключом сервера. Таким образом, только сервер может расшифровать переданный симметричный ключ.

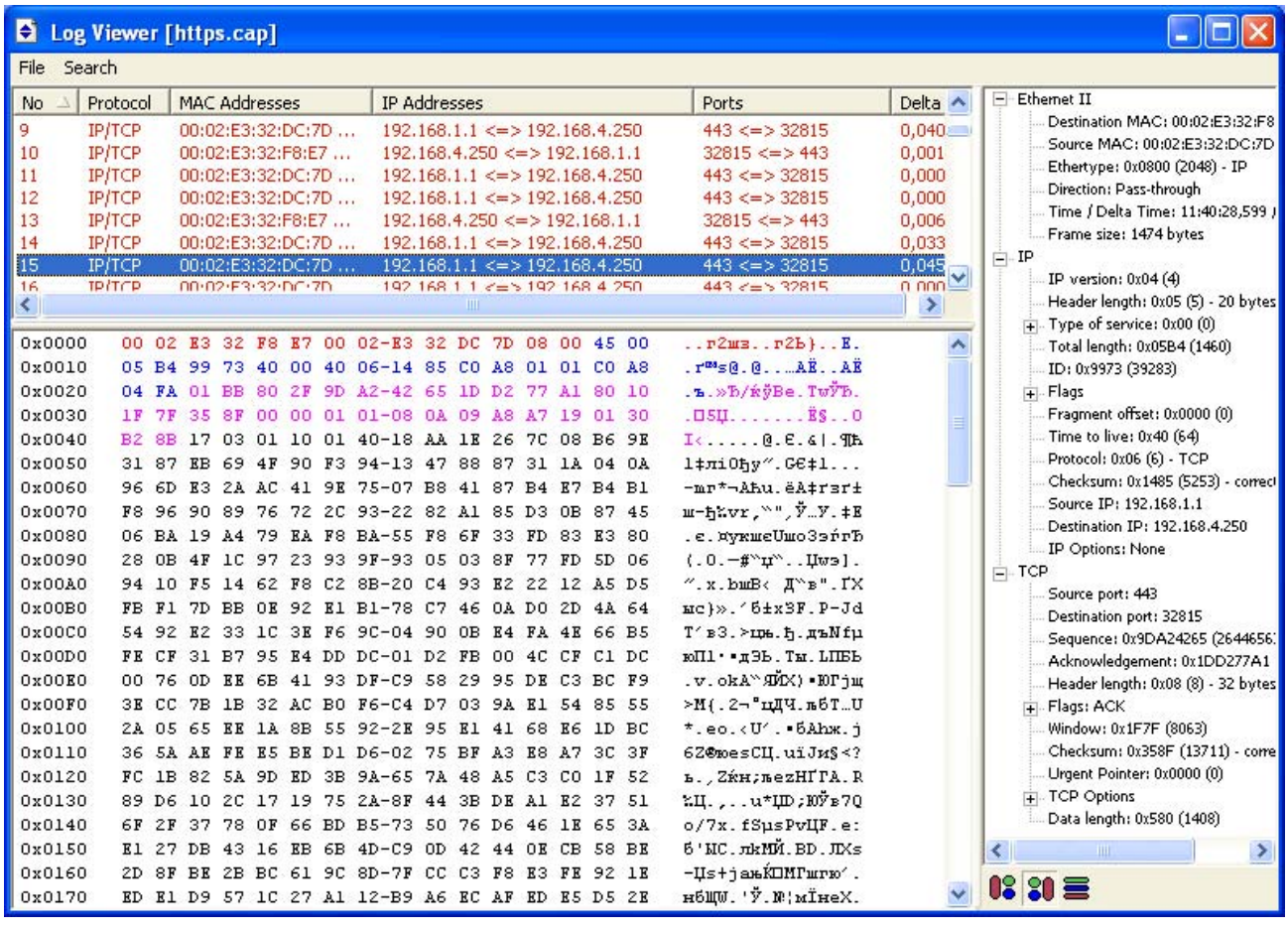


Рис. 4.40. Зашифрованный HTTP-трафик

Получив ключ, сервер зашифровывает этим ключом отправленную ранее последовательность «Challenge_Data» и передает ее в сообщении «Server-Verify». Получив и расшифровав данное сообщение, клиент уверен, что сеансовый ключ получен и расшифрован сервером правильно. Для того чтобы сервер также мог убедиться в правильности полученного им сеансового ключа, клиент зашифровывает этим ключом идентификатор соединения «Connection_id», полученный от сервера, и передает его в сообщении «Client-Finished».

Таким образом, соединение установлено, сервер проверен, сеансовый ключ передан. Теперь весь трафик может передаваться в зашифрованном виде. Для внешнего наблюдателя виден трафик, идущий по 443 TCP-порту между двумя узлами с известными IP-адресами.

4.11. Организация VPN средствами протокола SSL в Windows Server 2003

Предположим, нам необходимо организовать защищенный обмен информацией между web-сервером и произвольным клиентом. Для организации воспользуемся ОС Windows Server 2003, в качестве web-сервера будем использовать встроенный в ОС компонент IIS (Internet Information Services).

Поставленная задача разбивается на три этапа: активизация IIS, генерация сертификата открытого ключа для web-севера и настройка SSL-соединения.

4.11.1. Активизация IIS

Компонент IIS по умолчанию в ОС Windows Server 2003 не установлен, целью данного этапа является его установка и проверка его функционирования с автоматически генерируемой web-страницей.

ВЫПОЛНИТЬ!

1. Установить компонент Internet Information Services (***Control Panel*** ⇒ ***Administrative Tools*** ⇒ ***Manage Your Server***).

В открывшемся диалоговом окне необходимо выбрать пункт «Add or remove a role», после чего ОС автоматически определит текущие сетевые настройки и отобразит диалоговое окно со списком возможных задач, выполняемых сервером (рис. 4.41). В этом списке необходимо выбрать пункт «Application servers (IIS, ASP.NET)». Установка дополнительных компонентов сервера FrontPage Extensions и ASP.NET не является обязательной, поэтому может быть пропущена. В результате указанных действий будут установлены компоненты, необходимые, в том числе для запуска web-сервера. Процесс установки может занять несколько минут, и для его успешного завершения понадобится дистрибутив Windows Server 2003.

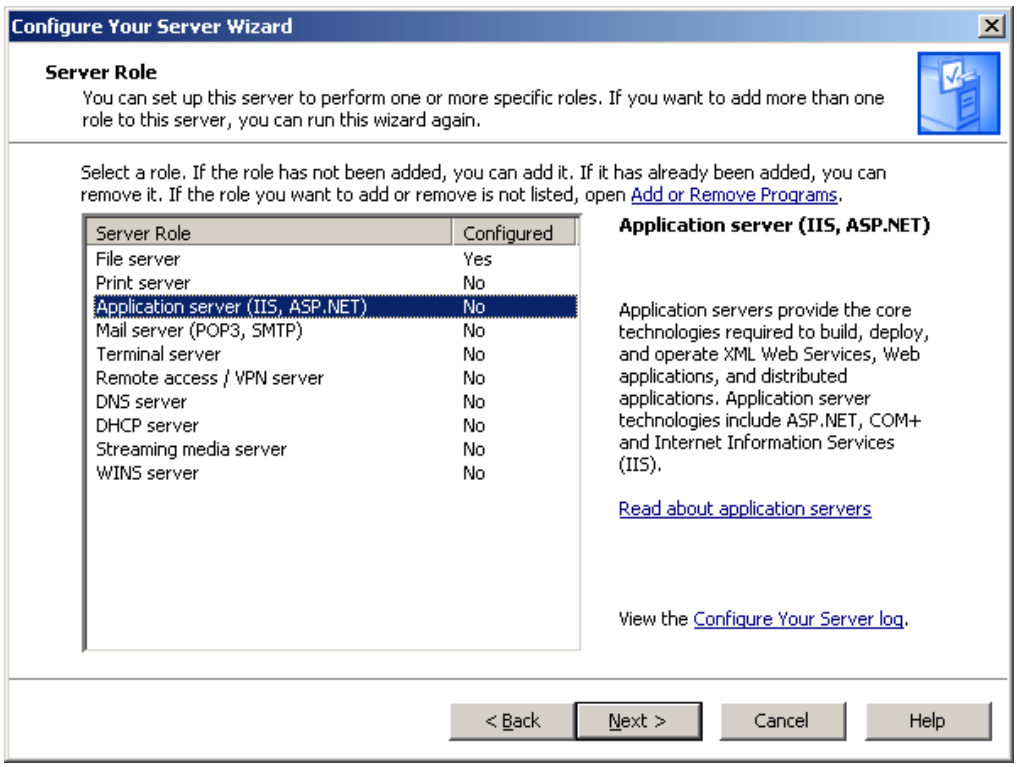


Рис. 4.41. Выбор пункта «Application servers (IIS, ASP.NET)»

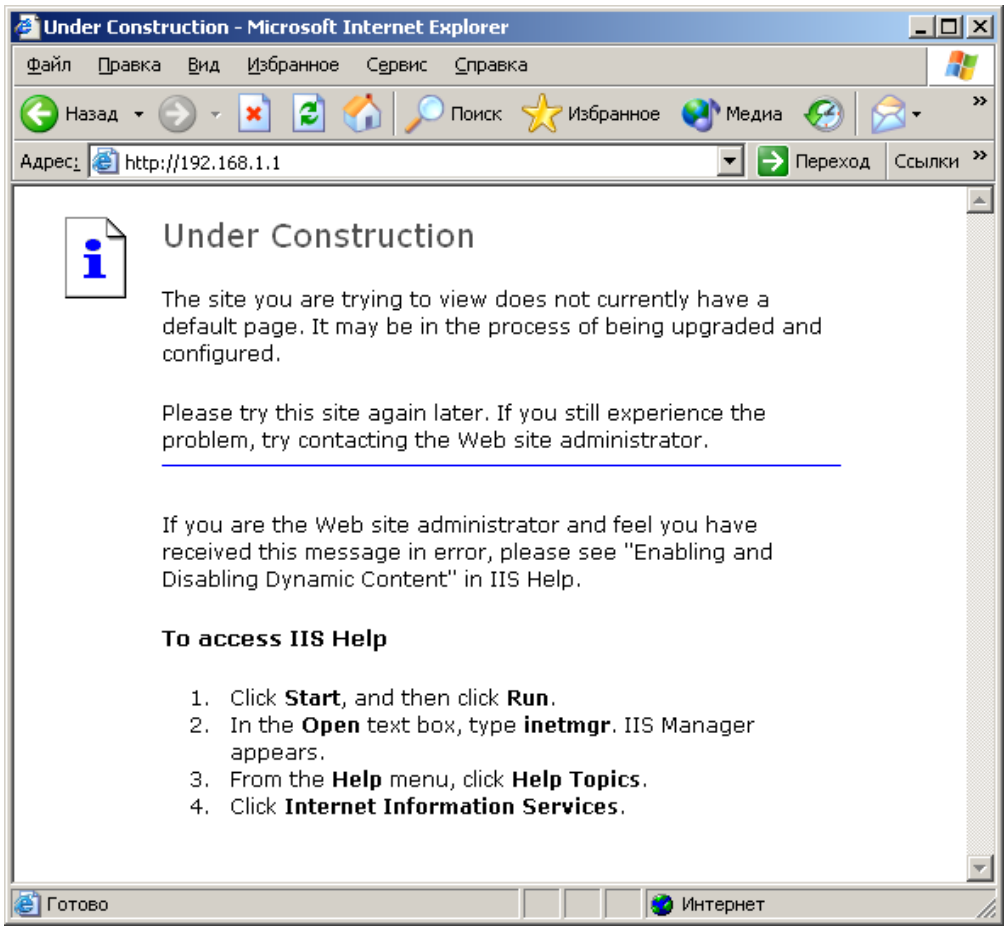


Рис. 4.42. Отображение web-страницы при обращении к серверу

После установки и перезагрузки web-сервер IIS автоматически запускается, в качестве стартовой используется автоматически генерируемая web-

страница (рис. 4.42). Отображение этой страницы при обращении к серверу по его IP-адресу с указанием протокола HTTP говорит о том, что сервер отвечает на HTTP-запросы клиента (программы Internet Explorer). В результате выполнения данного этапа мы получили функционирующий web-сервер под управлением IIS.

ВЫПОЛНИТЬ!

2. Запустить анализатор сетевого трафика и просмотреть содержимое передаваемой между клиентом и сервером информации. Убедиться, что HTTP-запрос и HTTP-ответ передаются в открытом виде.

4.11.2. Генерация сертификата открытого ключа для web-сервера

Как указывалось выше, для шифрования передаваемой информации клиент и сервер должны получить общий ключ симметричного шифрования. В протоколе транспортного уровня данный ключ генерирует клиент и отправляет серверу. Однако для отправки ключа клиент применяет его зашифрование с использованием открытого ключа сервера, который должен быть известен клиенту. Для передачи открытого ключа применяется механизм сертификатов, цель которого обеспечить подлинность передаваемого открытого ключа. Таким образом, сервер должен иметь сертификат своего открытого ключа, который в общем случае должен быть подписан одним из доверенных центров сертификации.

В связи с тем, что мы организуем VPN-соединение в локальной сети учебного компьютерного класса, то в процессе работы самостоятельно сгенерируем сертификат открытого ключа и создадим его ЭЦП. Для этой цели нам понадобится Центр сертификации, для работы с которым необходимо добавить компонент Certificate Services (Службы сертификации). В процессе установки необходимо будет указать имя Центра сертификации (например, «Mycompany»), остальные настройки можно оставить по умолчанию.

ВЫПОЛНИТЬ!

3. Установить компонент Certificate Services (***Control Panel ⇒ Add or Remove Programs ⇒ Add/Remove Windows Components***, рис. 4.43).

После установки Центра сертификации необходимо от имени web-сервера выполнить запрос на получение нового сертификата.

ВЫПОЛНИТЬ!

4. Запустить оснастку Internet Information Services (IIS) Manager (***Control Panel ⇒ Administrative Tools ⇒ Internet Information Services (IIS) Manager***).
5. В разделе «Web Sites» (рис. 4.44) выбрать компонент «Default Web Site», щелкнуть на нем правой кнопкой и выбрать пункт «Properties» в контекстном меню. Далее выбрать вкладку «Directory Security» и нажать кнопку «Server Certificate…» в открывшемся окне (рис. 4.45).

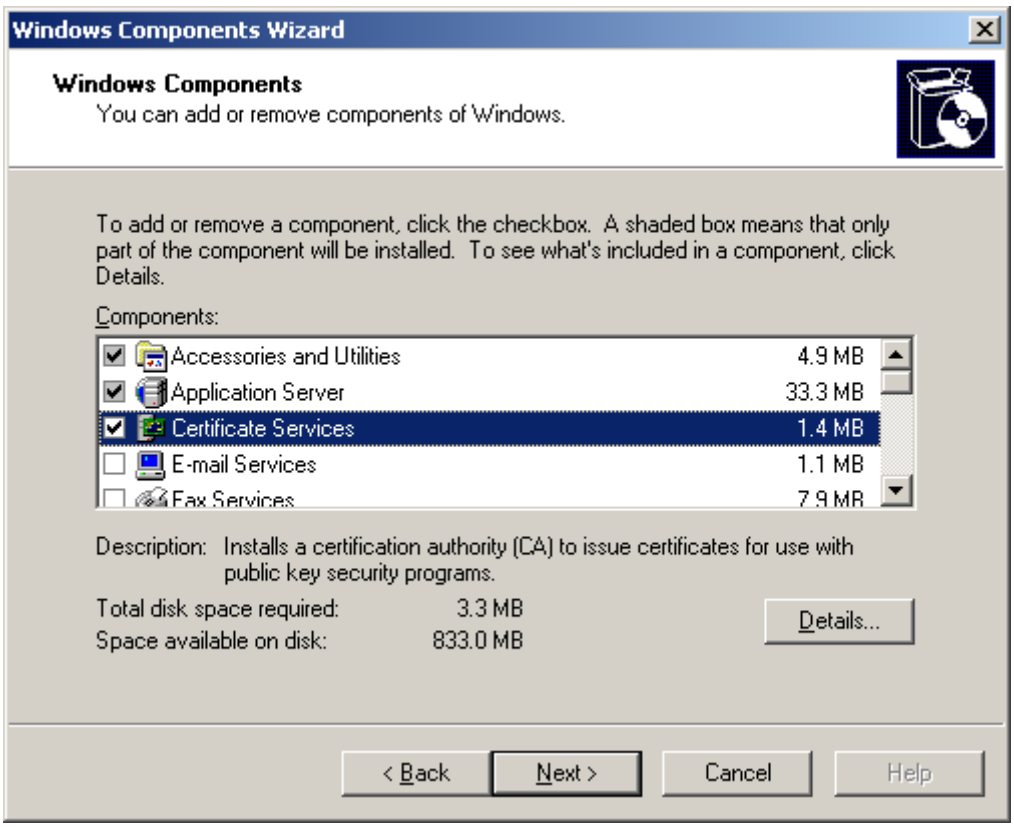


Рис. 4.43. Выбор компонента Certificate Services

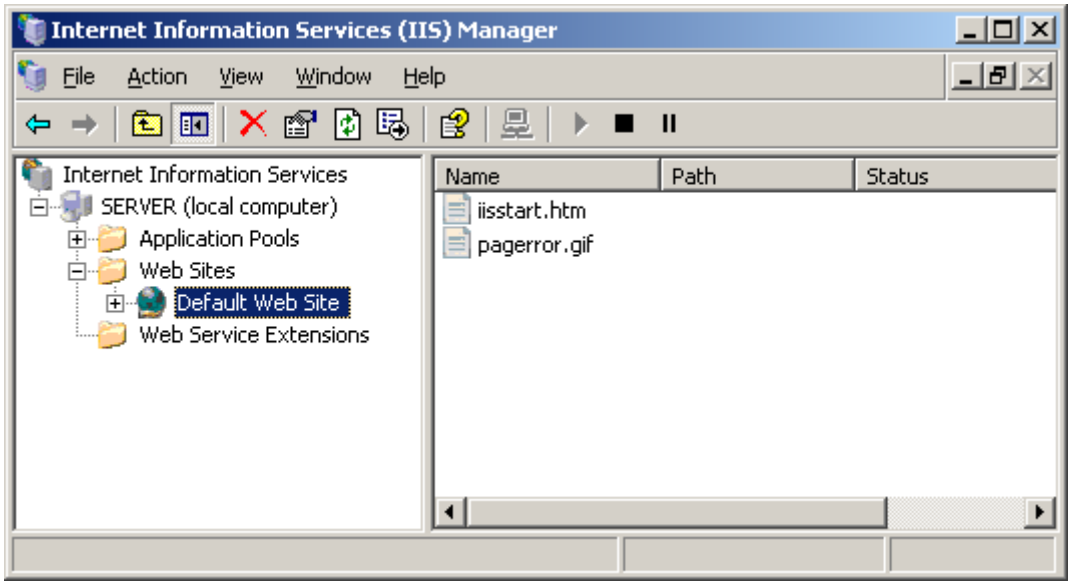


Рис. 4.44. Оснастка Internet Information Services (IIS) Manager

Будет запущен «мастер», позволяющий сформировать запрос на выдачу сертификата открытого ключа к Центру сертификации (Certification Authority). Необходимо выбрать опцию «Create a new certificate» (создать новый сертификат), а затем «Prepare the request, but send it later» (подготовить запрос, но отправить его позже). Будет предложено заполнить исходные данные, на основании которых будет выдан сертификат, в том числе наименования организации (Organization) и организационного подразделения (Organizational unit). Кроме того, необходимо указать доменное имя web-сайта (например,

«www.mycompany.com») и его географическое местонахождение. Затем будет предложено сохранить текст запроса в виде текстового файла (рис. 4.46), содержимое которого необходимо отправить в Центр сертификации. Данный файл содержит открытый ключ web-сервера и заполненные сведения.

Так как Центром сертификации также является наш узел, то процесс отправки полученного текстового файла упрощается и заключается лишь в обработке данного файла с использованием оснастки Certification Authority (рис. 4.47). Результатом обработки будет создание файла-сертификата открытого ключа в формате X.509.

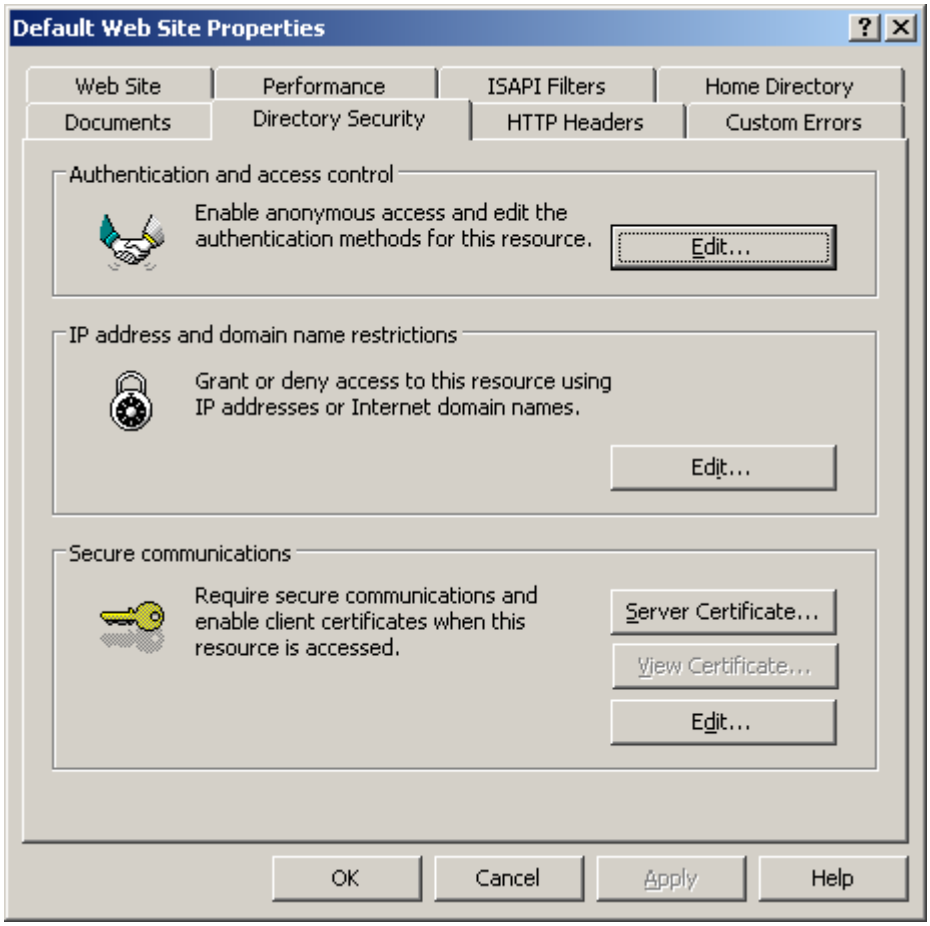


Рис. 4.45. Вкладка «Directory Security» окна свойств web-сайта

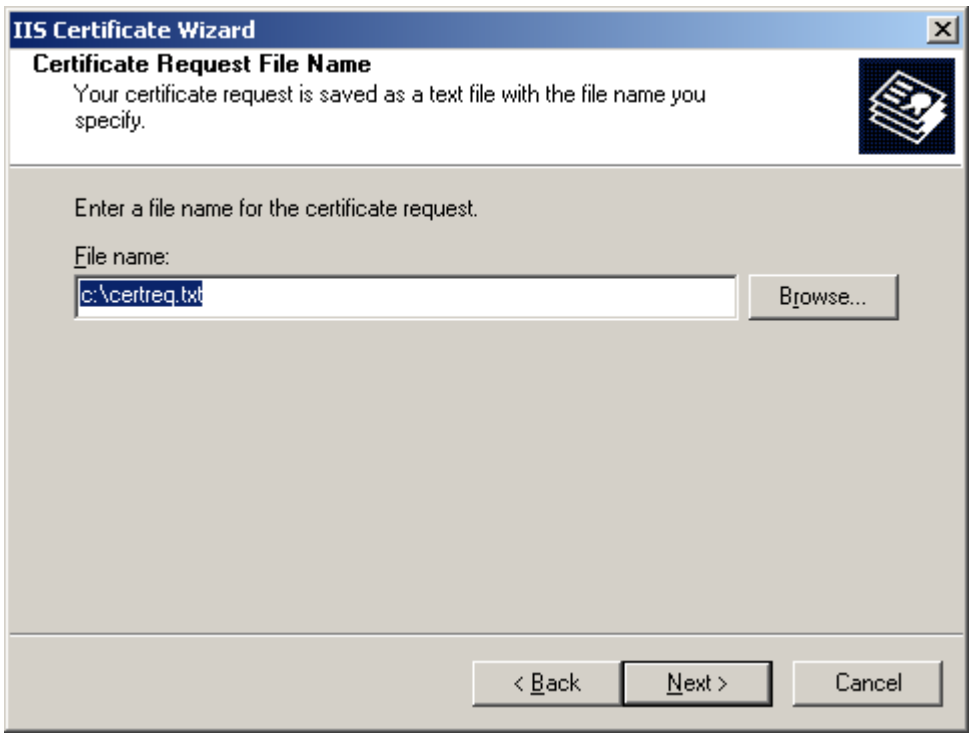


Рис. 4.46. Сохранение запроса сертификата

ВЫПОЛНИТЬ!

6. Запустить оснастку Certification Authority (***Control Panel ⇒ Administrative Tools ⇒ Certification Authority***).

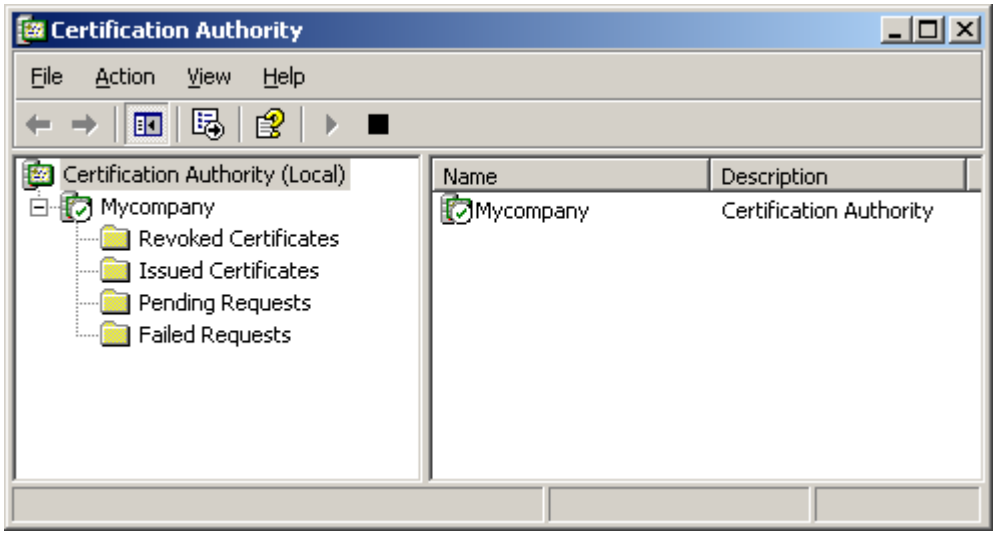


Рис. 4.47. Оснастка Certification Authority

Для добавления запроса необходимо из контекстного меню компонента «Mycompany» (в рассматриваемом примере) выбрать пункт ***All Tasks ⇒ Submit new request…*** Будет предложено выбрать файл с текстом запроса (он был создан ранее). Запрос добавляется в каталог «Pending Requests», чтобы обработать его, нужно из контекстного меню его записи выбрать пункт ***All Tasks ⇒ Issue***. Обработанный сертификат помещается в каталог «Issued Certificates». Чтобы сохранить сертификат в виде файла на жесткий диск, необходимо дважды

щелкнуть на нем, перейти на вкладку «Details» и нажать кнопку «Copy to File…». Будет запущен «Мастер экспорта сертификатов», в котором нужно выбрать формат экспортируемого файла (выбрать «DER encoded binary X.509»), а также указать его имя (например, «c:\certnew.cer»).

ВЫПОЛНИТЬ!

7. Создать файл-сертификат открытого ключа.

Таким образом, сгенерирован файл-сертификат открытого ключа, который теперь может быть использован для организации VPN-соединения.

4.11.3. Настройка SSL-соединения

Настройка SSL-соединения заключается в установке на web-сервере сгенерированного сертификата и активизации SSL-соединения с указанием номера порта. Общепринятым номером порта для SSL-соединения является порт 443.

ВЫПОЛНИТЬ!

8. Запустить оснастку Internet Information Services (IIS) Manager и открыть окно свойств компонента «Default Web Site». На вкладке «Directory Security» нажать кнопку «Server Certificate…» и выбрать пункт «Process the pending request and install the certificate» (обработать находящийся на рассмотрении запрос и установить сертификат).

Будет предложено выбрать файл, содержащий указанный сертификат, а также указать SSL-порт, который будет использоваться web-сайтом (по умолчанию 443). В результате на данном web-сервере будет установлен сертификат открытого ключа.

Чтобы включить шифрование информации, передаваемой между клиентом и сервером, необходимо указать номер порта SSL на вкладке «Web Site», а затем на вкладке «Directory Security» нажать кнопку «Edit…» в разделе «Secure communications» и в открывшемся окне (рис. 4.48) установить отметку «Require secure channel (SSL)». Остальные настройки данного окна можно оставить без изменений. В частности, так как для web-сервера в общем случае не важно, имеется ли у клиента сертификат открытого ключа, то устанавливается значение «Игнорировать сертификаты клиентов» (Ignore client certificates).

Для активизации сделанных изменений необходимо нажать кнопку «Apply» (применить) в диалоговом окне «Default Web Site Properties».

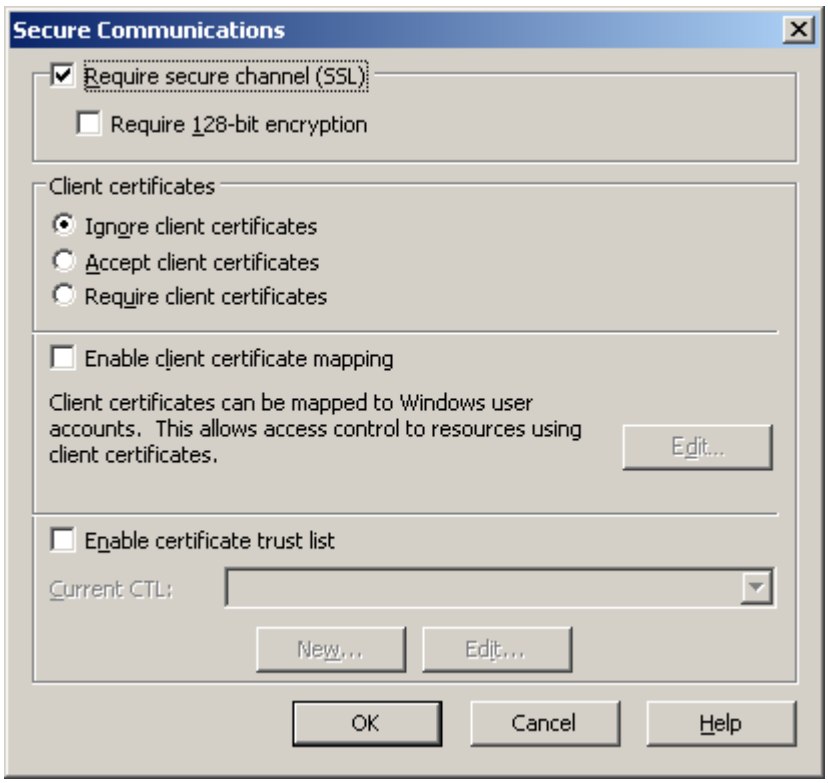


Рис. 4.48. Окно «Secure communications»

После применения выполненных настроек web-сервер готов к осуществлению VPN-соединения с произвольным клиентом, обратившимся к ресурсам сервера с использованием режима HTTPS. Передаваемая информация будет зашифрована симметричным алгоритмом с 56- либо 128-битным ключом.

ВЫПОЛНИТЬ!

9. Запустить анализатор сетевого трафика и включить перехват пакетов.
10. Запустить в основной операционной системе программу «Internet Explorer» и обратиться к серверу по протоколу SSL, для этого ввести в строке адреса: «https://<IP-адрес_сервера>». Будет предложено согласиться с использованием сертификата, подписанного неизвестной удостоверяющей компанией, после чего должна быть открыта стартовая страница web-сайта (см. выше).

Выключить захват пакетов в анализаторе трафика. Проследить порядок установления соединения по протоколу SSL. Найти момент передачи текста сертификата от сервера к клиенту. Убедиться, что передача HTTP-запросов и HTTP-ответов происходит в зашифрованном виде.

4.12. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP

Предположим, нам необходимо организовать защищенный обмен почтовой информацией между двумя пользователями. В процессе организации воспользуемся двумя узлами. Один узел под управлением ОС Windows 2000 Professional будет выполнять роль почтового сервера, реализуемого сервером Eserv, этот же узел будет являться рабочим местом первого пользователя (u1) для отправки почтовой корреспонденции с использованием программы Outlook Express. Второй узел под управлением ОС Windows Server 2003 будет рабочим местом второго пользователя (u2), дополнительно этот узел будет решать задачу по выдаче сертификатов открытых ключей. Шифрование почтовых сообщений будет осуществляться с помощью алгоритма ГОСТ 28147-89, реализуемого средствами СКЗИ КриптоПро CSP.

Поставленная задача разбивается на несколько этапов: организация почтового обмена без применения шифрования, активизация Web-сервера Internet Information Services (IIS) в ОС Windows Server 2003, установка СКЗИ КриптоПро CSP, установка Центра сертификации в ОС Windows Server 2003, получение сертификатов открытых ключей, организация защищенного обмена электронной почтой.

Для работы потребуются виртуальные образы систем Windows 2000 Professional (с установленным почтовым сервером Eserv) и Windows Server 2003, а также диски с дистрибутивами ОС Windows Server 2003 и СКЗИ КриптоПро CSP. Дополнительно требуется чистая дискета (может быть использована виртуальная дискета).

Предварительной операцией является настройка сетевого соединения виртуальных машин, имитирующих оба сетевых узла. Рекомендуется установить виртуальные сетевые адаптеры в режим Bridged и назначить сетевым узлам уникальные сетевые адреса, например, 192.168.*x*.1 и 192.168.*x*.2, где *x* — номер компьютера в учебном классе.

ВЫПОЛНИТЬ!

1. Открыть и запустить виртуальные образы, назначить IP-адреса, проверить установку связи с использованием команды ping.
2. С целью анализа сетевого трафика добавить в ОС Windows Server 2003 компонент Network Monitor (Control Panel ⇒ Add or Remove Programs ⇒ Add/Remove Windows Components ⇒ Management and Monitoring Tools ⇒ Network Monitor Tools).
3. Запустить установленную программу Network Monitor, убедиться в возможности захвата и анализа сетевого трафика.

4.12.1. Организация почтового обмена

Данный этап предусматривает настройку почтовых программ Outlook Express на двух узлах для отправки и получения электронной почты по протоколам SMTP и POP3 с сервера Eserv, установленного на узле с ОС Windows 2000.

4. Запустить сервер Eserv на узле с ОС Windows 2000, для чего выполнить командный файл Run.bat, находящийся на диске C: образа.
5. Проверить настройки сервера Eserv и убедиться в наличии учетных записей u1 и u2 (меню Общие настройки ⇒ Пользователи), установить пароли для указанных пользователей (задав и применив значение поля Password), убедиться в наличии настроек, указывающих в качестве локального домена адрес mail.ru (меню Почтовый сервер ⇒ SMTPсервер ⇒ Локальные домены).
6. Настроить почтовые программы Outlook Express на обоих узлах, создав учетные записи электронной почты для пользователей u1 (на ОС Windows 2000) и u2 (на ОС Windows Server 2003). В настройках указать адреса электронной почты, соответственно u1@mail.ru и u2@mail.ru, в качестве адресов SMTP- и POP3-серверов указать IP-адрес узла с ОС Windows 2000 (192.168.*x*.1).
7. Проверить функционирование почтового обмена путем отправки и получения почтовых сообщений. В процессе обмена в ОС Windows Server 2003 выполнить захват сетевого трафика, убедиться, что текст отправляемых и получаемых сообщений передается в открытом виде.
8. Убедиться в настройках учетных записей почты программы Outlook Express (Сервис ⇒ Учетные записи ⇒ Почта ⇒ Свойства ⇒ Безопасность) в наличии возможности шифрования с использованием алгоритмов DES, 3DES, RC2, а также в отсутствии сертификатов открытого ключа для подписи и шифрования.

4.12.2. Активизация IIS

Процесс активизации IIS подробно рассмотрен в разделе «Организация VPN средствами протокола SSL в ОС Windows Server 2003» учебного пособия. Приведем лишь перечень требуемых для выполнения команд.

ВЫПОЛНИТЬ!

9. Установить компонент Internet Information Services (Control Panel ⇒ Administrative Tools ⇒ Manage Your Server ⇒ Add or remove a role ⇒ Custom Configuration ⇒ Application servers (IIS, ASP.NET)).
10. Проверить функционирование Web-сервера, обратившись в ОС Windows 2000 с помощью программы Internet Explorer по адресу http://192.168.*x*.2.

4.12.3. Установка СКЗИ КриптоПро CSP

Установка СКЗИ КриптоПро CSP выполняется на обоих узлах с дистрибутивного диска. Применяется полнофункциональная версия СКЗИ без регистрации, что позволяет использовать ее в течение 30 дней. Инсталляция СКЗИ осуществляется стандартным образом. Настройки СКЗИ КриптоПро CSP доступны через Панель управления.

ВЫПОЛНИТЬ!

11. Установить СКЗИ КриптоПро CSP в ОС Windows 2000 и Windows Server 2003. Выполнить требуемую перезагрузку. После перезагрузки ОС Windows 2000 запустить сервер Eserv.
12. Проанализировать настройки учетных записей почты программы Outlook Express, выяснить изменения в разделе «Безопасность» свойств учетных записей, произошедшие после установки СКЗИ КриптоПро CSP.
13. Выполнить настройку считывателей программы КриптоПро CSP (Панель управления ⇒ КриптоПро CSP ⇒ Настроить считыватели). В ОС Windows 2000 в качестве считывателя использовать дисковод A:. В ОС Windows Server 2003 в качестве считывателя добавить реестр пользователя (User registry).

4.12.4. Установка Центра сертификации в ОС Windows Server 2003

В процессе выполнения данного пункта необходимо установить Службу сертификации отдельно стоящего корневого Центра сертификации. Установка Службы сертификации (Certificate Services) в ОС Windows Server 2003 подробно описана в разделе «Организация VPN средствами протокола SSL в ОС Windows Server 2003» учебного пособия.

ВЫПОЛНИТЬ!

14. Установить компонент Certificate Services (Control Panel ⇒ Add or Remove Programs ⇒ Add/Remove Windows Components). В процессе установки указать имя Центра сертификации (например, «Mycompany»), остальные настройки можно оставить по умолчанию.

4.12.5. Получение сертификатов открытых ключей

Одним из доступных способов получения сертификатов открытых ключей является обращение от имени каждого из пользователей к Центру сертификации через Web-интерфейс. Получение сертификата осуществляется в два этапа – сначала Пользователь обращается к Центру сертификации с запросом, а затем получает готовый сертификат и его инсталлирует в своей ОС. Между этими этапами администратор Центра сертификации должен осуществить обработку полученных запросов (издание сертификатов). Особенностью данного

этапа будет получение сертификата, позволяющего работать с СКЗИ Крипто-Про CSP. Сертификат должен быть сгенерирован для алгоритма ГОСТ Р 34.11-94.

ВЫПОЛНИТЬ!

15. От имени пользователя u1 в ОС Windows 2000 с помощью браузера Internet Explorer обратиться по адресу http://192.168.*x*.2/certsrv. Среди перечня задач выбрать пункт «Request a certificate».
16. При выборе типа запрашиваемого сертификата указать «advanced certificate request» и в следующем окне выбрать пункт «Create and submit a request to this CA».
17. В полученном информационном окне указать параметры пользователя, обязательными являются: имя пользователя (user1), точный адрес электронной почты (u1@mail.ru), тип сертификата «E-Mail Protection Certificate», настройки ключей (Key options) «CSP: Crypto-Pro Cryptographic Service Provider». Остальные параметры могут быть введены произвольно. Обратите внимание на то, что в параметрах алгоритма хэш-функции указан вариант «GOST R 34.11-94».
18. Для выполнения дальнейших действий разрешить выполнение элемента ActiveX, получаемого от сервера. В качестве носителя выбрать дисковод A: и поместить в него чистую дискету. Указать пароль, защищающий секретный ключ на носителе.
19. Выполнить аналогичный запрос от имени пользователя u2 в ОС Windows Server 2003, указав адрес почты u2@mail.ru. В качестве носителя выбрать «User registry». Указать пароль, защищающий секретный ключ в реестре.
20. В ОС Windows Server 2003 с помощью оснастки Certification Authority осуществить выдачу сертификатов. Для этого запустить оснастку Certification Authority (Control Panel ⇒ Administrative Tools ⇒ Certification Authority). В разделе «Pending Requests» найти запросы на получение сертификатов и обработать их, выбрав из контекстного меню записи запросов пункт «All Tasks ⇒ Issue».
21. Оснастку Certification Authority можно закрыть.
22. Повторно в каждой ОС с помощью Internet Explorer обратиться по адресу http://192.168.*x*.2/certsrv. В перечне задач выбрать «View the status of a pending certificate request».
23. Инсталлировать полученные сертификаты. В процессе инсталляции потребуется ввод пароля для доступа к секретным ключам на соответствующих носителях.
24. В каждой из ОС выполнить настройку почтовых учетных записей программы Outlook Express, подключив полученные сертификаты защиты электронной почты в разделе «Безопасность» свойств учетных записей.

4.12.6. Организация защищенного обмена электронной почтой

Для того чтобы два пользователя могли отправлять друг другу зашифрованные сообщения, они должны обменяться сертификатами открытых ключей. Самым простым способом обмена является отправка писем, подписанных каждым из пользователей. После получения подписанного письма его отправитель должен быть добавлен в адресную книгу.

ВЫПОЛНИТЬ!

25. Создать, подписать (Сервис ⇒ Цифровая подпись) и отправить сообщение от имени пользователя u1, адресуемое пользователю u2.
26. Включить захват сетевого трафика. От имени пользователя u2 получить указанное сообщение. Остановить захват трафика.
27. Проанализировать захваченный сетевой обмен по протоколу POP3, убедиться в передаче открытого текста сообщения и его электронной цифровой подписи.
28. Открыть полученное сообщение, добавить пользователя u1 и его сертификат в адресную книгу пользователя u2.
29. Выполнить аналогичные действия, направив подписанное письмо от пользователя u2 к пользователю u1.
30. Осуществить обмен зашифрованными сообщениями, выполнив захват сетевого трафика в процессе отправки либо получения зашифрованного письма. Сделать вывод о том, какие из атрибутов письма передаются в зашифрованном виде.
31. Проанализировать свойства полученных зашифрованных писем и сделать вывод о том, какие алгоритмы и ключи применяются в процессе отправки зашифрованных сообщений, какие алгоритмы и ключи применяются при прочтении зашифрованных писем.
32. Дать ответ на вопрос, почему при формировании подписи требуется вводить пароль для доступа к ключевому носителю, а при отправке зашифрованного сообщения пароль вводить не требуется?
33. В ОС Windows 2000 с помощью программы-настройки СКЗИ КриптоПро CSP в окне «Сертификаты на носителе» выяснить состав сертификата пользователя. Указать назначение и содержимое полей: серийный номер, алгоритм подписи, поставщик, субъект, тип открытого ключа, идентификатор ключа субъекта, использование ключа.
34. Проанализировать свойства и содержимое ключевой дискеты. Проанализировать содержимое значений ключей реестра и их параметров в разделе реестра HKLM\Software\Crypto Pro\Setings\USERS\ Идентификатор_пользователя\Keys в ОС Windows Server 2003. Сделать вывод о необходимости организационной защиты ключевых носителей.
35. В ОС Windows 2000 с помощью оснастки «Сертификаты – текущий пользователь» (mmc ⇒ Консоль ⇒ Добавить/удалить оснастку ⇒ Сертификаты ⇒ Моей учетной записи) найти личный сертификат и сертификаты других пользователей.

ЗАКЛЮЧЕНИЕ

Гарантия надежной и безопасной работы любого информационного объекта базируется на сплаве самых разнообразных защитных технологий. Комплексный подход к обеспечению информационной безопасности подразумевает разумное и согласованное сочетание организационных, режимных, программных, аппаратных, социально-психологических и других методов и средств. Но все же основой стройной системы защиты компьютерной информации являются программные, аппаратные или программно-аппаратные средства. Мы надеемся, что пособие сформирует у читателя убеждение в целесообразности применения для организации системы защиты мощных профессиональных программно-аппаратных СЗИ.

В настоящее время на рынке систем безопасности представлен весьма широкий выбор СКЗИ, СЗИ от НСД и СЗИ сетевого действия. В пособии рассмотрены только наиболее распространенные средства защиты, получившие заслуженное признание во многих организациях и учреждениях. Большинство из этих средств имеет соответствующие сертификаты на обработку служебной и государственной тайны. Разработчики средств защиты постоянно совершенствуют свои изделия, расширяя их номенклатуру, придавая им все больше функциональных возможностей.

Надеемся, что, прочитав наше пособие, читатель получит достаточную методическую базу, познакомится с основными методами защиты компьютерной информации, овладеет приведенными в пособии СЗИ, разберется с их особенностями. Полученные теоретические знания и практические навыки будут хорошим подспорьем не только для текущей работы по администрированию защищенных автоматизированных систем. Они помогут свободно осваивать новые средства защиты и их версии, которые позволят создавать защищенные автоматизированные системы, удовлетворяющие всем основным принципам защиты: системности, комплексности, непрерывности, разумной достаточности, гибкости управления, открытости механизмов защиты и простоты применения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий [Текст] : РД: утв. Гостехкомиссией России. – М., 2002.
2. ГОСТ Р 51275–99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию [Текст]. – Введ. 2000–01–01 – М.: Изд-во стандартов, 1999. – 8 с.
3. ГОСТ Р 50922–96. Защита информации. Основные термины и определения [Текст]. М.: Изд-во стандартов, 1996.
4. ГОСТ Р 51624–2000. [Текст]. М.: Изд-во стандартов, 2000.
5. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации [Текст] : РД : утв. Гостехкомиссией России. – М.: Изд-во стандартов, 1992.
6. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации [Текст] : РД : утв. Гостехкомиссией России. – М.: Изд-во стандартов, 1992.
7. Защита от несанкционированного доступа к информации. Термины и определения [Текст] : РД : утв. Гостехкомиссией России. – М.: Изд-во стандартов, 1992.
8. ГОСТ Р 15408–02. Критерии оценки безопасности информационных технологий [Текст]. – Введ. 2004–01–01 – М.: Изд-во стандартов, 2002.
9. ISO/IEC 17799:2000. Информационные технологии. Свод правил по управлению защитой информации. Международный стандарт [Текст] / ISO/IEC, 2000.
10. Зегжда Д. П. Как построить защищенную информационную систему. Технология создания безопасных систем [Текст] / Д. П. Зегжда, А. М. Ивашко ; под научн. ред. П. Д. Зегжды, В. В. Платонова. – СПб.: Мир и Семья-95, Интерлайн, 1998. – 256 с. : ил. ; 20 см. – 500 экз.
11. Девянин П. Н. Теоретические основы компьютерной безопасности [Текст]: учеб. пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков. – М.: Радио и связь, 2000. – 192 с. : ил. ; 21 см.
12. Ресурсы Microsoft Windows NT Workstation 4.0 [Текст] : [пер. с англ.] / Корпорация Майкорософт. – СПб. : BHV – Санкт-Петербург, 1998. – 800 с. : ил. ; 28 см. + 1 электрон. опт. диск. – Перевод изд.: Microsoft Windows NT Workstation 4.0 Resource Kit / Microsoft Corporation, 1996.
13. Проскурин В. Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах [Текст]: учеб. пособие для вузов / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. – М.: Радио и связь, 2000. – 168 с. : ил.
14. Гайдамакин Н. А. Автоматизированные системы, базы и банки данных. Вводный курс [Текст]: учеб. пособие / Н. А. Гайдамакин. – М.: Гелиос АРВ, 2002. – 368 с. : ил.

15. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах [Текст] / Н. А. Гайдамакин. – Екатеринбург: Изд-во Урал. Ун-та, 2003. – 328 с. : ил.
16. Хорев П. Б. Методы и средства защиты информации в компьютерных системах [Текст]: учеб. пособие для вузов / П. Б. Хорев. – М.: Академия, 2005. – 256 с. : ил.
17. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа [Текст] / А. Ю. Щеглов ; под ред. М. В. Финкова. – СПб: Наука и Техника, 2004. – 384 с. : ил.
18. Система защиты информации от несанкционированного доступа «СТРАЖ NT». Версия 2.0. Описание применения. УИМ.00025-01 31 [Электронный ресурс]. – 53 с. : ил.
19. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0». Руководство по эксплуатации [Электронный ресурс]. – 88 с. : ил.
20. Система защиты информации «Secret Net 2000. Автономный вариант для Windows 2000». Руководство по администрированию [Электронный ресурс]. – 142 с. : ил.
21. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-NT/2000» (версия 2.0). Описание применения [Электронный ресурс]. – 30 с. : ил.
22. Система защиты конфиденциальной информации StrongDiskPro. Версия 2.8.5. Руководство пользователя [Электронный ресурс]. – 31 с. : ил.
23. Система защиты конфиденциальной информации Secret Disk. Версия 2.0. Руководство пользователя [Электронный ресурс]. – 116 с. : ил.
24. Петров А. А. Компьютерная безопасность. Криптографические методы защиты [Текст] / А. А. Петров – М.: ДМК, 2000. – 448 с. : ил.
25. Молдовян А.А. Криптография [Текст] / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов. СПб.: Лань, 2000. – 224 с. : ил.
26. Алферов А. П. Основы криптографии [Текст]: учеб. пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос АРВ, 2001. – 480 с. : ил.
27. Брассар Ж. Современная криптология. Руководство [Текст] : [пер. с англ.] / Ж. Брассар. – М.: ПОЛИМЕД, 1999. – 176 с. : ил.
28. Разработка политики безопасности организации в свете новейшей нормативной базы / А. С. Марков, С. В. Миронов, В. Л. Цирлов // Защита информации. Конфидент. – 2004. – № 2 – С. 20–28.
29. Синадский Н. И. Угрозы безопасности компьютерной информации [Текст]: учеб. пособие / Н. И. Синадский, О. Н. Соболев – Екатеринбург: Изд-во Урал. ун-та, 2000. – 85 с. : ил.
30. Запечников, С.В. Основы построения виртуальных частных сетей [Текст]: Учеб. пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. — М.: Горячая линия–Телеком, 2003. — 249 с. ; 20 см. — 3000 экз. — ISBN 5-93517-139-2

ПРИЛОЖЕНИЕ

Рекомендации по проведению практических занятий

Для проведения практических занятий в компьютерных классах рекомендуется использовать технологию виртуальных машин (система VMware Workstation), позволяющую осуществлять одновременный запуск на одном компьютере нескольких операционных систем.

Работа с образами систем решает ряд методических проблем при проведении занятий. В частности, решается проблема необходимости присутствия разных систем на одном рабочем месте. Изучение принципов работы СЗИ при проведении практических занятий требует развертывания каждой из систем на отдельном компьютере. Установленные механизмы защиты полностью блокируют возможность проведения на данном компьютере занятий по изучению других тем. Для проведения занятий средствами VMware Workstation заранее создается образ операционной системы MS Windows 2000, который может быть сохранен и размножен для дальнейшей установки различных СЗИ. Каждое СЗИ устанавливается и сохраняется в отдельном файле-образе. Размер файла-образа — до 2 Гб, что позволяет на одном рабочем месте в компьютерном классе иметь более десятка различных систем в разных конфигурациях. После сжатия файла-образа программой-архиватором его объем уменьшается до 500-600 Мб, что позволяет сохранять и переносить образы систем на обычных CD-ROM дисках.

Второй решаемой проблемой является необходимость использования в компьютерных классах разнотипных компьютеров. Особенностью виртуальных машин VMware Workstation является возможность работы образа на любом компьютере, удовлетворяющем определенным требованиям по объему свободного дискового пространства и оперативной памяти (от 128 Мб ОЗУ). Таким образом, полученный образ системы с установленным СЗИ может быть легко размножен практически в любом компьютерном классе.

Третьей решаемой проблемой является то, что для изучения одного СЗИ требуется до 6 часов лабораторных работ, в то время как чаще всего в расписании учебных групп отведено 4, а то и 2 часа в неделю. Следовательно, лабораторная работа должна быть прервана на определенном этапе с возможностью ее продолжения на очередном занятии. Система VMware Workstation предоставляет возможность «усыпить» (команда ***Power*** $\Rightarrow$ ***Suspend***) операционную систему в определенном состоянии и «разбудить» ее, возобновив изучение с этого же момента. Таким образом, слушателям при возобновлении занятий не приходится повторно выполнять настройки ОС и СЗИ и, следовательно, нет необходимости искусственно прерывать ход лабораторной работы.

Четвертой проблемой, легко решаемой с применением системы VMware Workstation, является необходимость деления группы слушателей на подгруппы и проведения занятий в разное время на одних и тех же рабочих местах, что требует для каждой подгруппы имитации собственного отдельного компьюте-

ра. Проблема решается простым дополнительным копированием исходного образа ОС с СЗИ для очередной подгруппы.

Кроме того, система VMware Workstation позволяет в реальном режиме времени с использованием дискового редактора исследовать изменения, происходящие на жестком диске в ходе активизации защитных механизмов СЗИ.

Организация дисковой памяти. Главная загрузочная запись

Главная загрузочная запись Master Boot Record (MBR) создается при организации первого раздела на жестком диске. MBR всегда занимает первый сектор нулевой дорожки нулевой стороны. MBR содержит таблицу разделов жесткого диска (Partition Table) и небольшую программу, в задачи которой входят анализ таблицы разделов и определение системного раздела для последующей передачи управления загрузчику (Partition Boot Sector) системного раздела.

```
Physical Sector: Cyl 0, Side 0, Sector 1
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000000  33 C0 8E D0 BC 00 7C FB  50 07 50 1F FC BE 1B 7C   3ÀŽÐ¼.|ûP.P.ü¾.|
000000010  BF 1B 06 50 57 B9 E5 01  F3 A4 CB BD BE 07 B1 04   ¿..PW¹å.ó¤Ë½¾.±.
000000020  38 6E 00 7C 09 75 13 83  C5 10 E2 F4 CD 18 8B F5   8n.|.u.ƒÅ.âôÍ.‹õ
000000030  83 C6 10 49 74 19 38 2C  74 F6 A0 B5 07 B4 07 8B   ƒÆ.It.8,tö µ.´.‹
000000040  F0 AC 3C 00 74 FC BB 07  00 B4 0E CD 10 EB F2 88   ð¬<.tü».´.Í.ëòˆ
000000050  4E 10 E8 46 00 73 2A FE  46 10 80 7E 04 0B 74 0B   N.èF.s*þF.€~..t.
000000060  80 7E 04 0C 74 05 A0 B6  07 75 D2 80 46 02 06 83   €~..t. ¶.uÒ€F..ƒ
000000070  46 08 06 83 56 0A 00 E8  21 00 73 05 A0 B6 07 EB   F..ƒV..è!.s. ¶.ë
000000080  BC 81 3E FE 7D 55 AA 74  0B 80 7E 10 00 74 C8 A0   ¼□>þ}Uªt.€~..tÈ
000000090  B7 07 EB A9 8B FC 1E 57  8B F5 CB BF 05 00 8A 56   ·.ë©‹ü.W‹õË¿..ŠV
0000000A0  00 B4 08 CD 13 72 23 8A  C1 24 3F 98 8A DE 8A FC   .´.Í.r#ŠÁ$?˜ŠÞŠü
0000000B0  43 F7 E3 8B D1 86 D6 B1  06 D2 EE 42 F7 E2 39 56   C÷ã‹Ñ†Ö±.ÒîB÷â9V
0000000C0  0A 77 23 72 05 39 46 08  73 1C B8 01 02 BB 00 7C   .w#r.9F.s.¸..».|
0000000D0  8B 4E 02 8B 56 00 CD 13  73 51 4F 74 4E 32 E4 8A   ‹N.‹V.Í.sQOtN2äŠ
0000000E0  56 00 CD 13 EB E4 8A 56  00 60 BB AA 55 B4 41 CD   V.Í.ëäŠV.`»ªU´AÍ
0000000F0  13 72 36 81 FB 55 AA 75  30 F6 C1 01 74 2B 61 60   .r6□ûUªu0öÁ.t+a`
000000100  6A 00 6A 00 FF 76 0A FF  76 08 6A 00 68 00 7C 6A   j.j.ÿv.ÿv.j.h.|j
000000110  01 6A 10 B4 42 8B F4 CD  13 61 61 73 0E 4F 74 0B   .j.´B‹ôÍ.aas.Ot.
000000120  32 E4 8A 56 00 CD 13 EB  D6 61 F9 C3 49 6E 76 61   2äŠV.Í.ëÖaùÃInva
000000130  6C 69 64 20 70 61 72 74  69 74 69 6F 6E 20 74 61   lid partition ta
000000140  62 6C 65 00 45 72 72 6F  72 20 6C 6F 61 64 69 6E   ble.Error loadin
000000150  67 20 6F 70 65 72 61 74  69 6E 67 20 73 79 73 74   g operating syst
000000160  65 6D 00 4D 69 73 73 69  6E 67 20 6F 70 65 72 61   em.Missing opera
000000170  74 69 6E 67 20 73 79 73  74 65 6D 00 00 00 00 00   ting system.....
000000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
0000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
0000001B0  00 00 00 00 00 2C 44 63  12 F4 12 F4 00 00 80 01   .....,Dc.ô.ô..€.
0000001C0  01 00 07 EF FF FF 3F 00  00 00 11 DC FF 00 00 00   ...ïÿÿ?....Üÿ...
0000001D0  C1 FF 0F EF FF FF 50 DC  FF 00 F0 85 3E 00 00 00   Áÿ.ïÿÿPÜÿ.ð…>...
0000001E0  C1 FF 07 EF FF FF 40 62  3E 01 E0 0B 7D 00 00 00   Áÿ.ïÿÿ@b>.à.}...
0000001F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA   ..............Uª
```

Листинг П. 1. Пример MBR

Рассмотрим пример главной загрузочной записи (листинг п. 1), представленной в виде двух частей. Первая часть — несистемный загрузчик, занимающий первые 446 байт сектора (до смещения 0x1BE). Вторая часть, занимающая

64 байта, — таблица разделов. Последние два байта представляют собой сигнатуру сектора и всегда имеют значение «55AA».

Информация о главном и расширенном разделах жесткого диска хранится в таблице разделов, которая представляет собой структуру данных длиной 64 байта, расположенную по адресу 0x1BE (листинг п. 1). Таблица разделов имеет 4 записи по 16 байт каждая, описывающие четыре возможных раздела жесткого диска. Каждая запись содержит поля:

- загрузочный индикатор (1 байт, значение 0x80 — загрузочный (активный) раздел, 0x00 — незагрузочный раздел),
- начальная головка (1 байт),
- начальный сектор (6 бит),
- начальный цилиндр (10 бит),
- системный идентификатор (1 байт),
- завершающая головка (1 байт),
- завершающий сектор (6 бит),
- завершающий цилиндр (10 бит),
- относительный сектор (DWORD – 4 байта),
- общее количество секторов (DWORD – 4 байта).

Ниже приведены некоторые значения поля системного идентификатора, описывающего файловую систему, имеющуюся на томе (таблица).

Таблица

Примеры значений поля системного идентификатора

Значение	Описание
0x01	12-битный раздел FAT или логический диск
0x04	16-битный раздел FAT или логический диск
0x05	Расширенный раздел
0x06	Раздел или логический диск BIGDOS FAT
0x07	Раздел или логический диск NTFS

Основными параметрами записи таблицы разделов являются: загрузочный индикатор, системный идентификатор и относительный сектор, указывающий на адрес, по которому система должна передать управление.

Главная загрузочная запись может содержать информацию о двух типах разделов — главных (primary — первичный, основной) и расширенных (extended — дополнительный). Главных разделов может быть несколько, что позволяет устанавливать и запускать операционные системы, использующие разные файловые системы (например, Windows NT и UNIX). Расширенный раздел на диске один, на нем могут быть создан один или несколько логических дисков. Каждый из логических дисков может быть отформатирован для использования конкретной файловой системы.

На жестком диске могут быть только три главных раздела и один расширенный, или четыре главных. В примере (листинг п. 1) описывается жесткий диск, содержащий три раздела с файловой системой NTFS. Структура разделов, отображаемая оснасткой «Computer Management», приведена на рис. п. 1. Рас-

ширенный раздел (диск D) находится в примере между главными разделами (диски C и E). Дисковое пространство в конце диска, не принадлежащее ни одному из разделов, не используется.

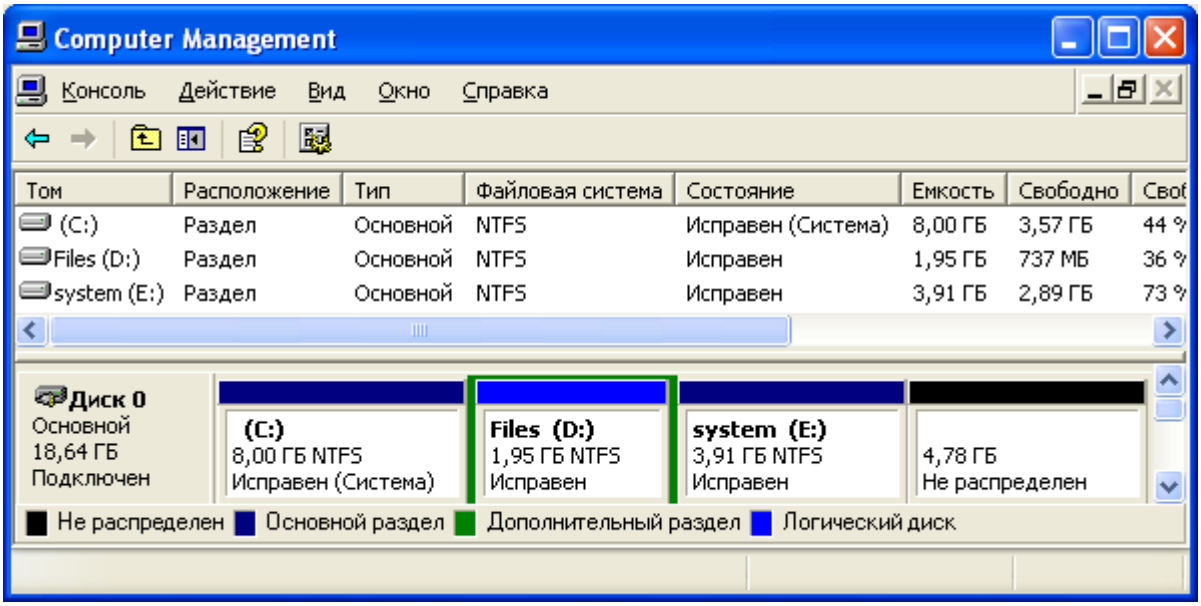


Рис. П. 1. Пример структуры разделов

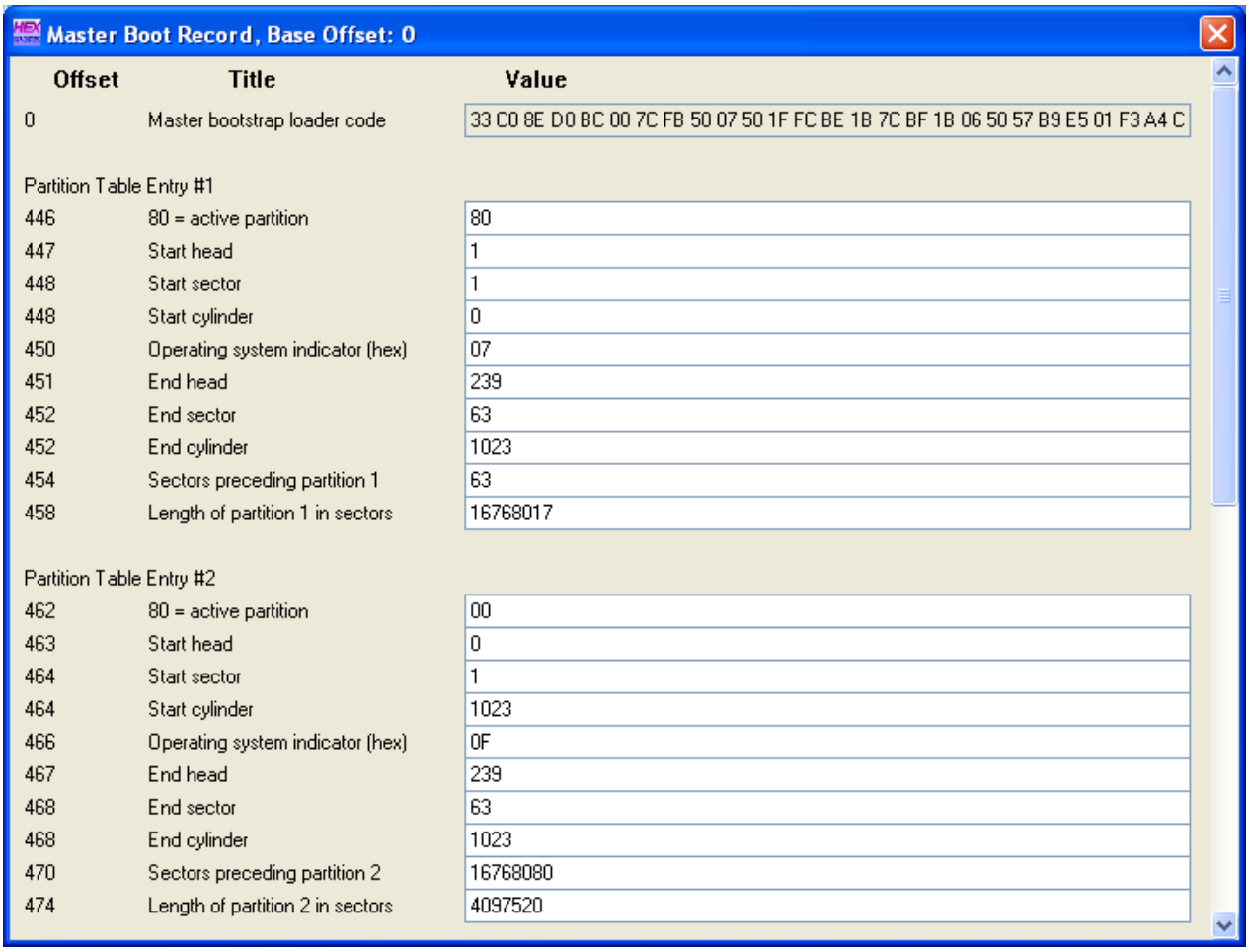


Рис. П. 2. Таблица разделов

Вид записи таблицы разделов, полученный в режиме просмотра «Master Boot Record» дискового редактора WinHex, представлен на рис. п. 2. Разберем поля записи первого раздела (Partition Table Entry 1). Загрузочный индикатор (0x80) указывает, что раздел является загрузочным. Начальная головка — 1 (0x01), начальный сектор — 1, начальный цилиндр — 0 (0x0100), системный идентификатор — NTFS (0x07), завершающая головка — 239 (0xEF), завершающий сектор — 63, завершающий цилиндр — 1023 (0xFFFF), относительный сектор — 63 (0x0000003F), общее количество секторов — 16768017 (0x00FFDC11).

Если на диске имеется расширенный раздел, то в первом секторе нулевой стороны дорожки, в которой он начинается, содержится запись аналогичная MBR. Эта запись содержит таблицу разделов для расширенного раздела.

Загрузчик, находящийся в MBR, определяет активный раздел (раздел с установленным значением загрузочного индикатора 0x80) и передает управление загрузочной записи активного раздела.

Электронные идентификаторы

Электронные ключи Touch Memory

Электронные ключи iButton или «Далласские таблетки» часто (по названию наиболее распространенных изделий) называют устройствами «Touch Memory». Записанная в устройство информация считывается контактным методом при прикосновении ключа к считывателю. Ключи выпускаются в пяти различных модификациях DS1990 – DS1994. Они имеют одинаковое конструктивное исполнение (цилиндрический корпус толщиной 3 – 5 мм) и отличаются друг от друга емкостью и организацией памяти. Для удобства применения впрессовываются в пластмассовый брелок (рис. п. 3). Устройства сохраняют работоспособность в диапазоне температур от –20 до $+70^0$C, имеют 10-летний срок хранения данных.

Рис. П. 3. Внешний вид электронных ключей Touch Memory

Электронные ключи ***DS1990 Touch Serial Number*** представляют собой постоянное неперепрограммируемое, прожигаемое лазером, запоминающее устройство емкостью 48 бит. Ключи содержат 6-байтный уникальный серийный номер устройства присваиваемый при изготовлении чипа. Первый байт памяти содержит код семейства ключей, для DS1990 он тождественно равен 01. Восьмой байт — контрольная сумма (CRC) первых семи байтов, необходимая

для контроля правильности считанной информации. Чаще всего устройства серии DS1990 используются в системах управления и контроля физического доступа сотрудников на предприятия или в режимные помещения. Ключи не способны запоминать собственный, сгенерированный лично код пользователя, и в СЗИ не применяются.

Электронные ключи с «защищенной» памятью ***DS1991 Touch MultiKey***, как и DS1990, имеют 48-битный уникальный серийный номер с байтом кода семейства и байтом CRC. Кроме этого имеют дополнительную энергонезависимую память, организованную в виде 4-х страниц. Первые три страницы объемом по 48 байт каждая имеют защиту от доступа с помощью 8-ми байтного идентификационного поля и 8-ми байтного пользовательского пароля. Четвертая страница объемом 64 байта не защищена. MultiKey могут работать как три отдельных электронных ключа, имеющих защищенную энергонезависимую память, доступную на чтение/запись. При доступе к защищенной памяти проверяется поле ключевого слова. Такая внутренняя структура ключей DS1991позволяет организовывать на базе одного устройства двухфакторную аутентификацию (пароль + индивидуальная кодовая последовательность) и создавать системы разграничения доступа к различным объектам.

Электронные ключи ***DS1992 Touch Memory 1K-bit*** имеют память суммарной емкостью 1 Кбит. Внутренняя энергонезависимая перезаписываемая память размером 128 байт организована в виде 4-х страниц по 32 байта. Чтение памяти можно производить с произвольного байта для любой страницы. Запись в DS1992 осуществляется только через специальную буферную 32-х байтную страницу. Для идентификации самого устройства ключи Touch Memory имеют дополнительный служебный байт с кодом семейства (для DS1992 равный 08), 6-ти байтный уникальный серийный номер и байт CRC для проверки считанной информации.

Электронные ключи ***DS1993 Touch Memory 4K-bit*** аналогичны устройствам DS1992, но отличаются повышенной емкостью (4 Кбита) и организацией памяти. Перепрограммируемая доступная память выполнена в виде 16-ти страниц по 32 байта, плюс одна буферная 32-х байтная страница. Чтение памяти возможно с произвольного байта для любой страницы, запись – только через буферную страницу. Код семейства (первый байт в уникальном серийном номере для DS1993) равен 06.

Электронные ключи ***DS1994 Touch Memory 4K-bit Plus Time*** также имеют энергонезависимую память объемом 4 Кбита, доступную для чтения и записи. Основная память DS1994 сегментируется на 256-битовые страницы для пакетизированных данных. Сохранность каждого пакета данных обеспечивается соблюдением строгих протоколов чтения/записи. DS1994 имеют встроенные механизмы аудита критичных событий и программируемую реакцию на некоторые из них. Устройство включает в себя часы/календарь реального времени, работающий в двоичном формате (точность часов лучше, чем 1 мин/месяц). Специальный интервальный таймер может автоматически сохранять время, когда к устройству было приложено питание. Программируемый счетчик может накапливать количество циклов включения/выключения системного питания.

Программируемые аварийные действия могут быть установлены при генерации прерываний интервальным таймером, часами реального времени и/или счетчиком циклов. Например, программируемое истечение времени ограничивает доступ к страницам памяти и событиям хронометража.

Электронные ключи eToken

Электронные ключи eToken, выпускаемые фирмой «ALADDIN Software Security R.D.», представляют собой устройства, содержащие небольшой объем перезаписываемой памяти, а также микроконтроллер, аппаратно реализующий ряд криптографических функций. В настоящее время выпускается две модификации ключей: eToken R2 и eToken PRO.

Электронные ключи **eToken R2** (рис. п. 4) построены на базе микроконтроллера Cypress CY7C63413 и выполнены в виде брелока, который имеет разъем для подключения к USB-порту персонального компьютера. Доступны версии с разным объемом перезаписываемой памяти (EEPROM): 8 КБ, 16 КБ и 32 КБ. Микроконтроллер реализует аппаратное шифрование по симметричному алгоритму на базе DES, а также осуществляет поддержку связи с ПЭВМ по протоколу USB. Для защиты информации, хранящейся во внешней микросхеме EEPROM, она подвергается криптографическому преобразованию и хранится в зашифрованном виде. Для получения доступа к этой информации необходимо предъявить PIN-код.

Рис. П. 4. Внешний вид электронных ключей eToken R2

Электронные ключи **eToken PRO** построены на основе микросхем смарт-карт Infineon SLE66CX160S и SLE66CX320P и имеют 16 или 32 КБ внутренней перезаписываемой памяти (EEPROM) соответственно. eToken PRO выпускаются в виде брелока с USB-разъемом или в виде смарт-карты (пластиковая карта с впрессованной в нее микросхемой). Для работы с eToken, выполненным в виде смарт-карты, необходимо устройство считывания. Микросхема смарт-карты реализует следующие функции: хранение информации во внутренней защищенной памяти, аппаратную реализацию алгоритмов шифрования (RSA, DES, 3DES), хэширования (SHA-1), а также аппаратную реализацию генератора ключевой пары на основе аппаратно сгенерированных случайных чисел. Так как EEPROM, в которой хранится защищаемая информация, является внутренней, она доступна только с использованием внутренних средств микросхемы смарт-карты. Для получения доступа к этой информации необходимо предъявить PIN-код.