

Zdisk

для Windows 2000/XP

Система защиты персонального компьютера

Руководство пользователя

Внимание!

Данный Продукт (программное обеспечение, включая носители информации, документацию, другие печатные материалы, электронные ключи и/или смарт-карты, устройства для работы с ними и пр.) передается Вам на условиях Лицензионного соглашения.

Перед вскрытием пакета с диском внимательно ознакомьтесь с Лицензионным соглашением. Вскрытие пакета рассматривается как Ваше полное согласие с условиями Лицензионного соглашения.

Если Вы не согласны с каким-либо из условий Лицензионного соглашения, то, не вскрывая пакет с диском, в течение семи дней со дня приобретения продукта верните его в организацию, в которой Вы его приобрели, и Вам будут возвращены деньги, которые Вы за него уплатили.

Программное обеспечение, описанное в данном Руководстве, поставляется в соответствии с Лицензионным соглашением и может использоваться лишь в строгом соответствии с условиями Лицензионного соглашения. Копирование программного обеспечения на какой-либо носитель, если на это нет специального разрешения в Лицензионном соглашении, является нарушением Закона Российской Федерации "О правовой охране программ для ЭВМ и баз данных" и норм международного права.

Никакая часть настоящего Руководства ни в каких целях не может быть воспроизведена или передана в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование и запись на магнитные или иные носители, если на то нет письменного разрешения компании SecurIT.

Условия использования Продукта

Условия использования приобретенной Вами системы Zdisk зафиксированы в Лицензионном соглашении, которое входит в состав данного Руководства. Лицензионное соглашение рассматривается как Договор между Вами и компанией SecurIT и имеет юридическую силу. Все споры, связанные с нарушением Лицензионного договора, решаются в судебном порядке.

Авторское право и торговые марки

Авторское право на систему Zdisk и ее документацию принадлежит компании SecurIT, © с 2001 г. по настоящее время. Все права защищены.

SecurIT является зарегистрированной торговой маркой компании SecurIT.

Все прочие изделия и торговые марки, упоминаемые в данном документе, являются торговыми марками своих законных владельцев.

Компания SecurIT®

129090 Москва

Проспект Мира, д.5 стр. 4

Телефон: (095) 208-9141

Тел./Факс: (095) 208-9784

Е-mail: info@securit.ru

HTTP: www.securit.ru

Лицензионное соглашение

Настоящее Лицензионное соглашение является соглашением между Вами, Конечным пользователем (физическим или юридическим лицом), и компанией SecurIT.

Программное обеспечение (далее по тексту ПО) или Продукт - это комплекс программ для компьютера, баз данных, документации (печатные материалы, носители и файлы с информацией), аппаратные средства, предназначенные для идентификации пользователя (электронные ключи, брелки, смарт-карты и пр.) и средства ввода информации в компьютер (идентификаторов пользователя), являющихся неотъемлемой частью Продукта.

Продукт, включая все дальнейшие усовершенствования, является объектом авторского права и охраняется законом.

1. Предмет Договора

Предметом настоящего Договора является передача Правообладателем (компания SecurIT) Конечному пользователю неисключительного авторского права на использование Продукта.

Все условия, оговоренные далее, относятся как к Продукту в целом, так и ко всем его компонентам в отдельности.

2. Имущественные права

Имущественные права на данный продукт принадлежат исключительно компании SecurIT.

Конечному Пользователю предоставляется неисключительное право, т.е. именная, непередаваемая и неисключительная Лицензия на использование Продукта в указанных в документации целях и при соблюдении приведенных ниже условий.

Лицензия предоставляется Вам и никому больше, если на то нет письменного согласия компании SecurIT.

3. Условия использования

Вы можете установить Продукт на нескольких компьютерах и использовать его одновременно при условии приобретения необходимого количества Лицензий.

В случае если ПО одновременно поставляется на различных носителях (например, дискеты и CD-ROM), то Вы можете использовать один из них, наиболее удобный для Вас. При этом считается, что оба комплекта содержат один и тот же экземпляр ПО.

Конечный пользователь не имеет права распространять Продукт, т.е. передавать его для последующего использования третьим лицам. Под распространением Продукта понимается предоставление доступа третьим лицам к воспроизведенным в любой форме компонентам Продукта, в том числе сетевыми и иными способами, а также путем их продажи, проката, сдачи внаем или предоставления взаймы.

Конечный пользователь не имеет права осуществлять самостоятельно или разрешать другим лицам осуществлять следующую деятельность:

- § Допускать использование Продукта людьми и организациями, не имеющими прав на использование данного Продукта и работающими в одной сети или многопользовательской системе с Вами;
- § Пытаться дизассемблировать, декомпилировать (преобразовывать объектный код в исходный) программы, драйверы, базы данных и другие компоненты Продукта;
- § Вносить какие-либо изменения в исходный код программ, драйверов или баз данных к ним, за исключением тех, которые вносятся штатными средствами, включенными в комплект поставки Продукта и описанными в документации, а также разбирать и анализировать аппаратные средства (оборудование), выяснять их устройство и принципы работы;
- § Предоставлять авторские права на использование программ или другие права на Продукт третьим лицам;
- § Совершать относительно Продукта другие действия, нарушающие российское законодательство и нормы международных договоров по авторскому праву, включая использование программных средств.

4. Срок действия Договора

Настоящий Договор вступает в силу с момента вскрытия запечатанного пакета с дисками и действует на протяжении всего срока использования Продукта.

В случае нарушения Вами условий настоящего Договора или неспособности далее выполнять его условия, Вы обязуетесь уничтожить все копии ПО (включая архивные, файлы с информацией, носители ПО, печатные материалы) или вернуть все материалы Продукта организации, в которой Вы его приобрели. После этого Договор прекращает свое действие.

5. Ответственность

Нелегальное использование, распространение и воспроизведение (копирование) ПО является нарушением Закона РФ "О правовой охране программ для электронных вычислительных машин и баз данных" и преследуется по закону.

В случае нарушения настоящего Договора компания SecurIT лишает Конечного пользователя Лицензии на использование Продукта. При этом компания SecurIT полностью отказывается от своих гарантийных обязательств на обслуживание и на бесплатные поставки обновлений ПО.

6. Гарантии

Компания SecurIT гарантирует работоспособность Продукта в течение 12 (двенадцати) месяцев со дня его покупки при условии, что он используется с аппаратными средствами и операционными системами, для которых был разработан, и в полном соответствии с Руководством по эксплуатации.

Компания SecurIT гарантирует качество записанных на носителях данных, работоспособность оборудования и программ, входящих в комплект поставки Продукта, при выполнении Конечным пользователем условий, оговоренных в документации, соответствие компонентов ПО спецификациям, а также качество печатной документации.

В случае если Продукт используется совместно с нелегальным программным обеспечением, гарантийные обязательства компании SecurIT не действуют.

7. Ограниченная гарантия

Продукт поставляется "таким, каков он есть". Компания SecurIT не гарантирует, что ПО будет отвечать ожиданиям Конечного пользователя в части выполнения функций, не предусмотренных техническими условиями.

Компания SecurIT не несет ответственность за убытки (реальный ущерб и/или упущенную выгоду), понесенные Конечным пользователем вследствие эксплуатации Продукта или его отдельных компонент с нарушением условий применения, определенных техническими условиями.

Компания SecurIT не гарантирует совместную работу Продукта с программным обеспечением или оборудованием других производителей, в особенности с моделями, выпущенными позднее, чем данная версия Продукта.

Ограниченная гарантия действует в течение 60 (шестидесяти) дней со дня приобретения Продукта. В течение этого времени принимаются все претензии к качеству поставки Продукта.

8. Обязательства по гарантии

Обязательством компании SecurIT по гарантии является бесплатная замена или ремонт всего Продукта или его неисправной компоненты. Доставка Продукта или его неисправных компонент в SecurIT и обратно оплачивается Конечным пользователем.

Гарантийные заявки должны подаваться в письменном виде до истечения гарантийного срока. Заявки должны быть подтверждены свидетельствами неисправности.

Ответственность компании SecurIT за возможные убытки, понесенные Конечным пользователем или третьей стороной по любой причине, не может превышать цену, уплаченную Конечным пользователем за Лицензию на Продукт, использование или невозможность использования которого нанесло фактический ущерб или является предметом иска. Компания SecurIT не несет ответственности за убытки, понесенные вследствие невыполнения Конечным пользователем своих обязательств, а также за потерю данных, прибыли, сбережений, нарушение работы аппаратных средств, сетей и другие последствия или случайности (даже если Конечный пользователь ранее сообщал о такой возможности), а также по претензиям, предъявляемым Конечным пользователем на основании претензий третьей стороны.

За исключением вышесказанного, не существует никаких других явно выраженных или подразумеваемых гарантий в отношении Продукта или его составных частей, в том числе, гарантий пригодности использования Продукта для конкретных целей Конечного пользователя.

Содержание

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ.....	3
ВВЕДЕНИЕ.....	8
Краткий обзор глав.....	8
Условные обозначения.....	8
Порядок оказания технической поддержки.....	9
ГЛАВА 1 О СИСТЕМЕ ZDISK.....	10
1.1 Для чего служит ZDISK.....	10
1.2 Комплект поставки.....	10
1.3 Краткое описание системы.....	11
1.4 Требования к компьютеру и программному обеспечению.....	11
ГЛАВА 2 УСТАНОВКА СИСТЕМЫ.....	12
2.1 Подготовка аппаратного обеспечения.....	12
2.2 Установка программного обеспечения системы.....	12
2.3 Мастер первого запуска.....	12
2.4 Удаление системы.....	12
ГЛАВА 3 ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС.....	14
3.1 ZDISK Администратор.....	14
3.1.1 Меню.....	14
3.1.2 Панель инструментов.....	14
3.1.3 Рабочая область.....	14
3.2 Системное меню ZDISK.....	15
3.3 Описание меню и панели инструментов ZDISK Администратор.....	16
ГЛАВА 4 ОСНОВНЫЕ ОПЕРАЦИИ С СИСТЕМОЙ.....	17
4.1 Активация электронного идентификатора.....	17
4.2 Создание секретных дисков.....	18
4.3 Подключение секретных дисков.....	21
4.4 Отключение секретных дисков.....	23
4.5 Блокировка операционной системы.....	24
ГЛАВА 5 РАБОТА С СЕКРЕТНЫМИ ДИСКАМИ.....	25
5.1 РАБОТА СО СВОЙСТВАМИ СЕКРЕТНОГО ДИСКА.....	25
5.1.1 Настройка параметров секретного диска.....	26
5.1.2 Изменение пароля доступа и (или) электронного идентификатора.....	27
5.1.3 Увеличение объема секретного диска.....	27
5.2 МНОГОПОЛЬЗОВАТЕЛЬСКИЙ РЕЖИМ.....	28
5.2.1 Использование секретного диска в многопользовательском режиме.....	28
5.2.2 Добавление нового пользователя секретного диска.....	28
5.2.3 Изменение атрибутов пользователя.....	29
5.2.4 Удаление пользователя.....	30
5.3 ВЕДЕНИЕ ЖУРНАЛА ОБРАЩЕНИЙ К СЕКРЕТНОМУ ДИСКУ.....	30
5.3.1 Журнал работы с диском.....	30
5.3.2 Настройка свойств журнала секретного диска.....	30
5.3.3 Просмотр журнала.....	31
5.3.4 Экспорт и очистка журнала.....	32
5.4 МОМЕНТАЛЬНОЕ ОТКЛЮЧЕНИЕ ВСЕХ ПОДКЛЮЧЕННЫХ ДИСКОВ.....	32
5.5 УДАЛЕНИЕ СЕКРЕТНЫХ ДИСКОВ.....	32
ГЛАВА 6 УПРАВЛЕНИЕ КЛЮЧАМИ.....	33
6.1 Личный ключ, рабочие ключи и пароли.....	33
6.2 Запись личного ключа пользователя в файл.....	33
6.3 Загрузка личного ключа пользователя из файла.....	34
6.4 Действия в случае утери электронного идентификатора и (или) пароля.....	35

ГЛАВА 7	РЕЗЕРВНОЕ КОПИРОВАНИЕ И РАБОТА С ЗАЩИЩЕННЫМИ АРХИВАМИ	38
7.1	ОБЗОР ВОЗМОЖНОСТЕЙ РЕЗЕРВНОГО КОПИРОВАНИЯ	38
7.2	РЕЗЕРВНОЕ КОПИРОВАНИЕ СЕКРЕТНЫХ ДИСКОВ.....	38
7.2.1	<i>Расположение резервных копий файлов секретных дисков.....</i>	<i>38</i>
7.2.2	<i>Настройка параметров резервного копирования файла секретного диска.....</i>	<i>39</i>
7.3	ВОССТАНОВЛЕНИЕ СЕКРЕТНЫХ ДИСКОВ ИЗ РЕЗЕРВНЫХ КОПИЙ.....	40
7.4	СОЗДАНИЕ ЗАШИФРОВАННОГО АРХИВА	40
7.5	РАСПАКОВКА ЗАЩИЩЕННОГО АРХИВА.....	43
ГЛАВА 8	НАСТРОЙКА ZDISK.....	44
8.1	ОБЩИЕ ПАРАМЕТРЫ СИСТЕМЫ.....	44
8.2	НАСТРОЙКА БЛОКИРОВКИ КОНСОЛИ	44
8.3	РАБОТА ПОД ПРИНУЖДЕНИЕМ.....	45
8.4	НАСТРОЙКА “КРАСНОЙ КНОПКИ”	46

ВВЕДЕНИЕ

Целью данного Руководства является описание системы Zdisk, что позволит максимально полно и правильно использовать возможности продукта.

В Руководстве описаны процедуры установки и настройки системы, а также способы решения основных проблем связанных с настройкой, эксплуатацией и администрированием системы Zdisk.

Система Zdisk предназначена для защиты информации, хранимой и обрабатываемой на персональных компьютерах, работающих под управлением операционных систем Windows 2000/XP.

Система Zdisk разработана исключительно на базе документированных возможностей, изложенных в соответствующих материалах компании Microsoft. В руководстве не содержится информация по работе с Microsoft Windows.

Важные сведения о последних изменениях в программе, не учтенные в настоящем Руководстве, приведены в файле **readme.txt**, находящемся на дистрибутивном компакт-диске.

Система Zdisk не содержит встроенных криптографических средств, но имеет открытый интерфейс для подключения внешних библиотек шифрования. В Руководстве не рассматриваются используемые алгоритмы шифрования и вопросы, связанные с криптографией.

Краткий обзор глав

Глава 1. О системе Zdisk– содержит сведения, описывающие основные принципы работы системы Zdisk, а также возможности, требования к оборудованию и программному обеспечению компьютера.

Глава 2. Установка системы - пошаговое описание процесса установки системы Zdisk.

Глава 3. Пользовательский интерфейс - основные элементы интерфейса Zdisk.

Глава 4. Основные операции с системой - генерация ключа, создание диска, открытие диска и закрытие диска, а также блокировка система.

Глава 5. Работа с секретными дисками - подробное описание прочих операций с секретными дисками.

Глава 6. Управление ключами - работа с электронными идентификаторами, восстановление доступа к данным.

Глава 7. Резервное копирование и работа с защищенными архивами

Глава 8. Настройка Zdisk - настройки блокировки, "Красной кнопки" и прочих параметров системы.

Условные обозначения

В данной документации для выделения различных смысловых частей текста используются специальные условные обозначения, приведенные в таблице 1.

Таблица 1. Условные обозначения

Обозначение	Описание
Шрифт Courier New	Строки, вводимые пользователем с клавиатуры
• Перечисление	Пункт перечисления
1. Выберите в меню...	Шаг процедуры, выполняемой пользователем
2 Для того чтобы...	Описание выполняемой пользователем последовательности действий
i На заметку	Полезная информация, на которую желательно обратить внимание
! Важная информация	Информация, на которую мы рекомендуем обратить особое внимание
M Внимание!	Предупреждение об опасности потери данных, выхода оборудования из строя и т. п.
“Диск”	Названия меню, пунктов меню, окон, их элементов и т. п.

Порядок оказания технической поддержки

Пользователям системы Zdisk предоставляется бесплатная техническая поддержка в форме консультаций по телефону или по электронной почте. Если, устанавливая систему Zdisk или используя ее, Вы столкнетесь с теми или иными проблемами, обратитесь в службу технической поддержки компании SecurIT:

Телефон: (095) 208-9141

Тел./Факс: (095) 208-9784

E-mail: support@securit.ru

HTTP: www.securit.ru

! Для оказания оперативной технической поддержки, пожалуйста, будьте готовы сообщить следующую информацию:

- регистрационный номер Вашей копии;
- пытались ли Вы найти решение проблемы в документации, в справочной системе или в файле readme.txt;
- версию операционной системы и установленное программное обеспечение;
- аппаратную конфигурацию компьютера;
- полный номер версии системы Zdisk;
- тип используемого электронного идентификатора;
- точную последовательность Ваших действий, вызывающих возникновение проблемы.

Глава 1 О системе Zdisk

1.1 Для чего служит Zdisk

Система Zdisk предназначена для защиты от несанкционированного доступа к информации, хранимой и обрабатываемой на персональных компьютерах под управлением Windows 2000/XP.

Система Zdisk позволяет создавать и использовать защищенные логические диски, которые представляют собой специальные файлы-контейнеры на жестком, съемном или сетевом диске. Информация на защищенном диске хранится в зашифрованном виде и недоступна для посторонних даже при изъятии диска или компьютера.

Основные возможности системы:

- § использование при создании защищенного диска криптостойких алгоритмов шифрования с длиной ключа от 128 бит;
- § использование средств аппаратной аутентификации с применением USB-ключей;
- § мгновенное отключение всех защищенных дисков и уничтожения ключа шифрования при нажатии комбинации клавиш - "красная кнопка";
- § блокирование консоли в случае отключения электронного идентификатора;
- § введение отдельного пароля, который используется в экстремальных ситуациях. Пароль на короткое время подключает защищенный диск, при этом, уничтожается личный ключ пользователя и имитируется сбой в операционной системе. После этого получить доступ к диску будет невозможно, даже при использовании личного ключа.
- § работа в сети. Защищенный диск является ресурсом, который может быть предоставлен для работы в сети. При этом есть возможность заблокировать общий доступ;
- § режим совместного использования. Возможность доступа к одному защищенному диску нескольких пользователей. Для работы в данном режиме каждому пользователю потребуется персональный электронный ключ и пароль;
- § создание нескольких защищенных дисков. Возможность создания любого количества защищенных дисков;
- § работа с зашифрованными архивами. Обмен информацией, записанной с защищенного диска на иной носитель в зашифрованном и сжатом виде. Для использования архива на другом ПК потребуется пароль либо электронный ключ;
- § увеличение объема защищенного диска в любой момент после его создания;
- § резервное копирование. Возможность создания защищенной копии всего защищенного диска как в ручном, так и в автоматическом режиме;
- § восстановление данных осуществляется с аварийной дискеты, на которой хранятся резервные копии ключей доступа;
- § журнал обращений к защищенному диску автоматически ведет протокол всех обращений к секретному диску (как удачных, так и неудачных). Контролирует работу журнала системный администратор.

1.2 Комплект поставки

В комплект поставки системы Zdisk входит:

- § компакт-диск с дистрибутивом системы;
- § данная документация;
- § USB-ключ и удлинительный USB-кабель;
- § рекламно-информационные материалы.

1.3 Краткое описание системы

Система защиты персонального компьютера Zdisk предназначена для создания, использования и обслуживания секретных дисков. Секретный диск — это логический диск, информация на котором хранится в зашифрованном виде. Секретный диск становится доступен пользователю только после того, как он подключит к компьютеру USB-ключ и введет пароль. Такие диски не являются реальными физическими устройствами, они виртуальны, то есть их существование — это результат работы специальной программы, а именно системного драйвера Zdisk. Система Zdisk создает на одном из уже имеющихся дисков специальный файл — файл секретного диска — и с помощью своего драйвера “подключает” его на правах физического устройства.

Самая важная особенность секретного диска состоит в том, что при записи на него данные автоматически шифруются, в дальнейшем хранятся в зашифрованном виде и для посторонних недоступны. При чтении с секретного диска данные автоматически расшифровываются. Подключив секретный диск, Вы можете работать с ним, как с любым другим. Например, запускать находящиеся на нем программы, создавать и открывать на нем документы, базы данных, файлы бухгалтерских систем и любые другие файлы. Пока диск, на котором они находятся, подключен, приложения могут обращаться к ним, как к файлам на обычном диске. Иными словами, использование системы Zdisk равносильно встраиванию функций шифрования данных во все приложения, с которыми Вы работаете. Отключив секретный диск, Вы закрываете доступ к находящимся на нем файлам.

Естественно, пользователь может подключить секретный диск и работать с ним только в том случае, если он будет опознан системой Zdisk как “владелец” этого диска. Для идентификации пользователя необходимо:

- § Ввести пароль доступа к секретному диску. Пароль указывается при создании секретного диска и впоследствии может быть неоднократно изменен.
- § Присоединить к компьютеру свой USB-ключ.

Систему Zdisk можно использовать в качестве архиватора, который не только сжимает, но и надежно шифрует данные. Это бывает очень полезно, если необходимо перенести конфиденциальную информацию на сменном носителе или переслать ее по электронной почте.

1.4 Требования к компьютеру и программному обеспечению

Для работы с системой Zdisk требуется:

- § PC-совместимый компьютер на базе процессора Pentium или выше с 128 Мб оперативной памяти и приблизительно 6 Мб свободного дискового пространства для размещения программных модулей Zdisk.
- § Операционная система Windows 2000 Professional или Windows XP.
- § Устройство чтения компакт-дисков (для установки системы).
- § Свободный USB-порт.

Глава 2 Установка системы

2.1 Подготовка аппаратного обеспечения

В комплект поставки системы входит USB-ключ.

i Не подключайте USB-ключ до установки системы Zdisk.

2.2 Установка программного обеспечения системы

i Перед установкой Zdisk завершите работу со всеми документами и запущенными приложениями.

2 Для установки системы:

1. Запустите с установочного диска программу **SETUP.EXE** из папки **SETUP**.
2. Нажмите кнопку "**Далее >**" в появившемся диалоговом окне.
3. Изучите Лицензионное Соглашение. Если Вы согласны с предлагаемыми условиями, нажмите "**Да**".
4. На следующем этапе Вам предлагается указать каталог для установки файлов, нажав кнопку "**Обзор**", или воспользоваться папкой по умолчанию. Нажмите "**Далее >**".
5. Система готова к установке. Нажмите "**Далее >**" для начала процесса инсталляции.

i В процессе копирования и регистрации файлов может инициироваться установка **Менеджера ключей – Key Manager**, если он не был установлен ранее. Установка происходит в фоновом режиме и не требует никаких дополнительных действий пользователя.

! Если Вы устанавливаете Zdisk не с компакт-диска, для фоновой установки **Key Manager** необходимо разместить каталог **Keymgr** с его дистрибутивом в папке с установочными файлами Zdisk.

6. Дождитесь окончания процесса копирования и перезагрузите компьютер, выбрав пункт "**Да, перезагрузить компьютер сейчас**" и нажав "**Готово**". Вы можете отложить перезагрузку, если выберете "**Нет, перезагрузить компьютер позже**".

2.3 Мастер первого запуска

После перезагрузки операционной системы программа установки предложит Вам выполнить первоначальную настройку системы Zdisk с помощью Мастера первого запуска.

Следуя указаниям Мастера, Вы сможете активировать электронный идентификатор (см. п. 4.1), настроить параметры системы (см. гл. 8), создать и подключить новый секретный диск (см. пп. 4.2 и 4.3).

i Мастер первого запуска можно запустить в любое время из Zdisk Администратора, выбрав пункт "**Мастер первого запуска**" из меню "**Помощь**".

2.4 Удаление системы

i В процессе удаления файлы-контейнеры секретных дисков, их резервные копии и файлы зашифрованных архивов не удаляются.

2 Для удаления Zdisk:

1. Откройте "**Панель управления**" ("**Control Panel**").
2. Дважды щелкните по значку "**Установка и удаление программ**" ("**Add/Remove Programs**").
3. Выберите в списке пункт "**Zdisk**" и нажмите кнопку "**Добавить/Удалить...**" ("**Add/Remove...**").
4. Подтвердите Ваши намерения, нажав кнопку "**ОК**" в появившемся диалоговом окне.
5. После перезагрузки система Zdisk будет полностью удалена с компьютера.


Глава 3 Пользовательский интерфейс

3.1 Zdisk Администратор

Практически все операции с секретными дисками выполняются в окне “Zdisk Администратор”.

2

Для запуска Администратора:

- Подведите курсор мыши к значку  в правой части панели задач Windows.
- Нажмите на правую клавишу мыши и выберите в системном меню Zdisk пункт “Администратор”.

i

Для вызова на экран окна “Zdisk Администратор” можно также использовать меню, которое появляется при нажатии на кнопку “Пуск” в панели задач Windows или воспользоваться ярлыком на рабочем столе.

В окне “Zdisk Администратор” находятся:

- § меню;
- § панель инструментов;
- § разделенная на две панели рабочая область.

3.1.1 Меню

Выполняемые с помощью системы Zdisk операции в большинстве своем могут быть иницированы выбором соответствующего пункта в одном из меню

3.1.2 Панель инструментов

В панели инструментов находятся кнопки, каждая из которых соответствует определенному пункту меню.



3.1.3 Рабочая область

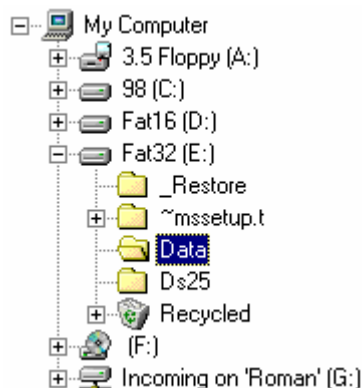
Большую часть главного окна “Zdisk Администратор” занимает рабочая область. Она разделена на две части: иерархический список (слева) и список секретных дисков (справа). В иерархическом списке в виде дерева дисков и каталогов отображается все доступное Вам в данный момент дисковое пространство.

На верхнем уровне иерархии находится пункт “Мой компьютер”. Он включает в себе все доступные в данный момент диски, в том числе дисководы, внешние накопители и сетевые диски. Каждый диск может содержать в себе каталоги, а те в свою очередь — другие каталоги. Иерархический список предназначен для навигации по дисковому пространству, поэтому файлы в нем не отображаются.



i


Сетевые диски отображаются в рабочей области только в том случае, если они подключены и им присвоены буквы.

Каждый пункт иерархического списка может быть открыт или закрыт. Если пункт открыт, в иерархическом списке видны все находящиеся в нем пункты.



В списке, который расположен в правой части рабочей области, отображаются файлы секретных дисков и файлы зашифрованных архивов, находящиеся в каталоге (или на диске), выделенном в иерархическом списке. Файлы подключенных в данный момент дисков обо-

значаются значком , а неподключенных — значком , файлы зашифрованных

архивов обозначаются значком . Кроме того, в списке всегда присутствует значок




, двойной щелчок мышью по которому инициирует процесс создания нового секретного диска.

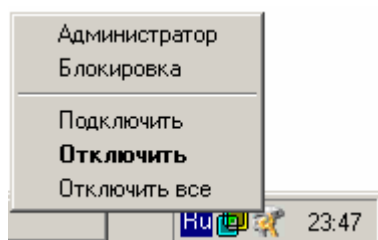
3.2 Системное меню Zdisk




Основные функции системы Zdisk доступны через системное меню.

2



Для вызова на экран системного меню

1. Подведите курсор мыши к значку  в правой части панели задач Windows.
2. Нажмите на правую клавишу мыши. После этого на экране появится системное меню Zdisk.



i В зависимости от состояния системы значок в панели задач меняет свой вид. Если нет ни одного открытого диска и электронные идентификаторы не подсоединены, значок выглядит так: , и пункты “Отключить” и “Отключить все” временно недоступны. При подсоединении USB-ключа значок изменит свой вид на , а после подключения хотя бы одного секретного диска значок будет выглядеть так: , и все пункты в контекстном меню станут активными.

3.3 Описание меню и панели инструментов Zdisk Администратор

Кнопка	Меню - пункт меню	Описание
	Диск - Создать новый диск	Запускает мастер создания секретного диска. См п. 4.2
	Диск - Подключить диск	Подключает секретный диск. См п. 4.3
	Диск - Отключить диск	Отключает секретный диск. См п. 4.4
	Диск - Удалить диск	Удаляет файл-контейнер. См п. 5.5
	Диск - Свойства диска	Открывает свойства секретного диска. См п. 5.1
	Диск - Пользователи диска	Открывает управление пользователями. См п. 5.2
	Резервное копирование - Сохранить данные	Запускает мастер создания защищенного архива. См п. 7.4
	Резервное копирование - Восстановить данные	Распаковывает защищенный архив. См п. 7.5

Глава 4 Основные операции с системой

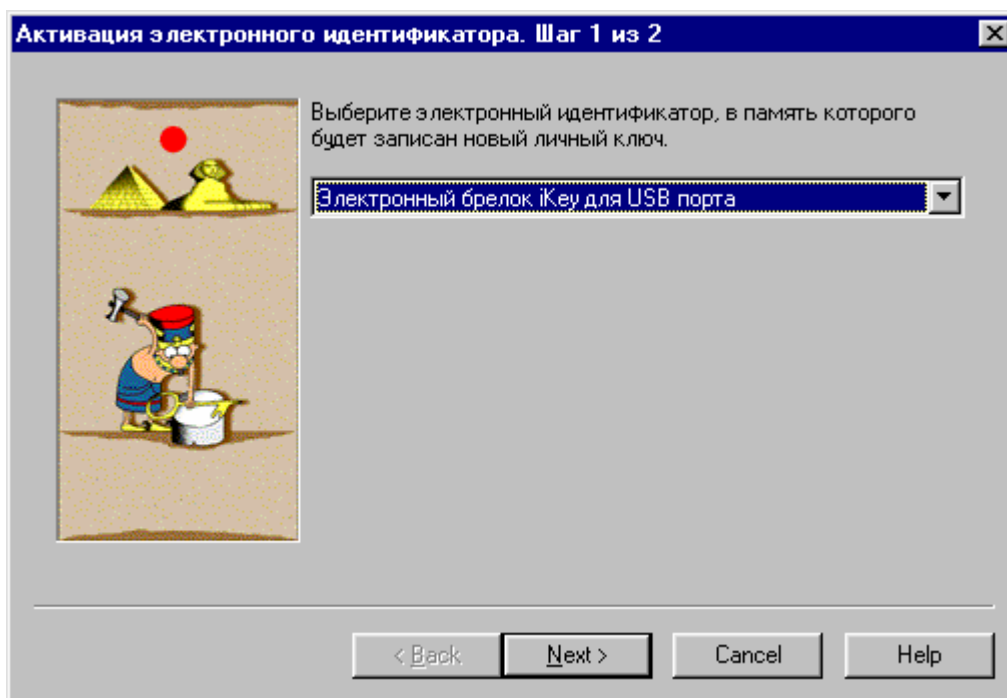
4.1 Активация электронного идентификатора

При выполнении данной операции система Zdisk генерирует новый личный ключ и записывает его в электронный идентификатор.

2

Для активации электронного идентификатора:

1. Выберите в меню “Электронный идентификатор” пункт “Активация”.
2. В диалоговом окне “Активация... Шаг 1 из 2” в раскрывающемся списке выберите тип электронного идентификатора, который Вы намереваетесь активировать, и нажмите на кнопку “Далее >”.



3. В диалоговом окне “Активация шаг 2 из 2” примите участие в построении Вашего личного ключа. Нажимайте на клавиши в произвольном порядке или перемещайте курсор мыши по диалоговому окну до тех пор, пока один из имеющихся индикаторов не окажется заполненным и в поле “Генерация ключа” не высветится надпись “Готово”.
4. Нажмите на кнопку “Готово”.
5. Далее Вам будет предложено сохранить копию только что созданного личного ключа в файл. В диалоговом окне “Обзор папок” выберите диск и каталог, куда будет записан файл, содержащий копию Вашего личного ключа. Выбрав в иерархическом списке диск и каталог, нажмите на кнопку “ОК”. После этого новый личный ключ будет записан в память электронного идентификатора, а в выбранном каталоге будет создан файл с его копией.

i Файл, содержащий копию личного ключа, всегда имеет уникальное имя, соответствующее используемому экземпляру Вашего электронного идентификатора, и расширение **.key**. Если такой файл уже существует, система допишет новый ключ в него же (то есть такой файл может содержать несколько личных ключей, сгенерированных для данного электронного идентификатора).

! Личный ключ рекомендуется сразу сохранять на сменный носитель: дискету, диск ZIP и т.п. Если Вы сохраните личный ключ на жесткий диск, потом скопируете на аварийную дискету и затем сотрете файл на жестком диске, то у заинтересованных лиц будет возможность впоследствии восстановить его.


4.2 Создание секретных дисков

Секретные диски могут создаваться и храниться на жестком диске локального компьютера, на сетевых дисках, а также на съемных носителях типа ZIP, CD-RW и магнитооптических дисках.

2 Для создания секретного диска

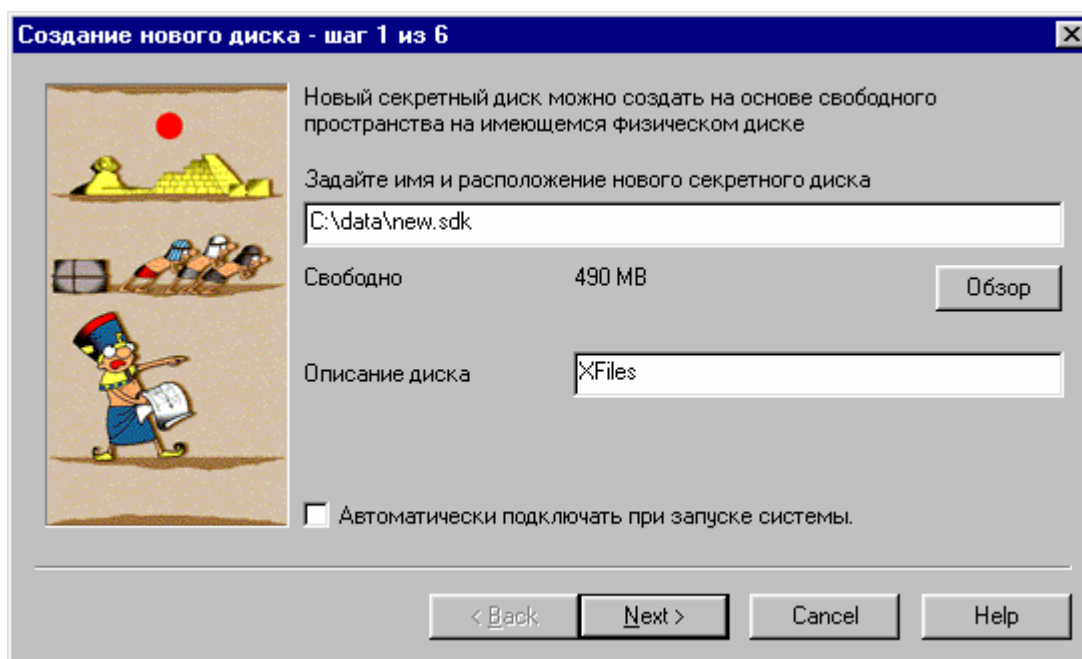
1. В окне **“Zdisk Администратор”** в иерархическом списке выберите диск или каталог, в котором Вы хотите поместить файл секретного диска.
2. В окне **“Zdisk Администратор”** выберите в меню **“Диск”** пункт **“Создать новый**



диск” или нажмите на кнопку  в панели инструментов. Кроме того, Вы можете дважды щелкнуть мышью по такому же значку в правом списке.

i Для создания секретного диска можно также воспользоваться контекстным меню стандартной программы Проводник. Для этого в программе Проводник нажмите на правую кнопку мыши, выберите в динамическом меню пункт **“Создать”**, а в следующем меню – пункт **“Файл секретного диска”**.

3. В диалоговом окне **“Создание нового диска - шаг 1 из 6”** в поле **“Задайте...”** введите имя файла секретного диска. Имя файла может включать в себя полный путь к нему, независимо от того, какой диск и какой каталог является текущим в рабочей области.

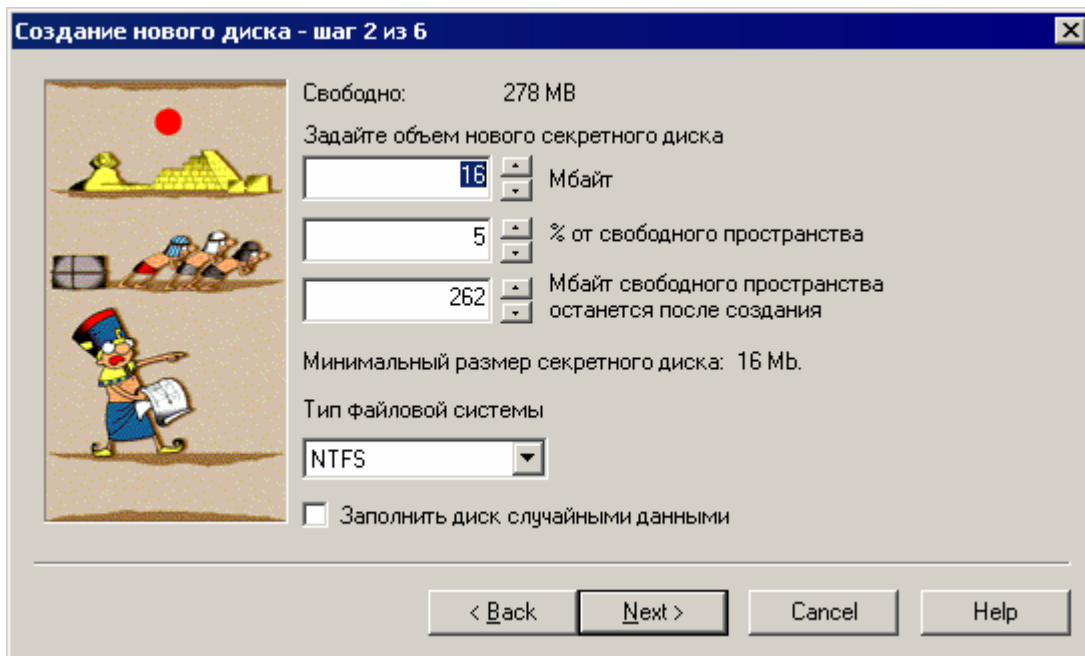


- § В поле **“Описание диска”** можно ввести произвольный комментарий. В дальнейшем он будет отображаться при просмотре свойств секретного диска.
- § Если Вы хотите, чтобы создаваемый диск автоматически подключался при запуске системы, установите во включенное состояние переключатель

“Автоматически подключать...”. При запуске система выводит окно подключения каждого из автоматически подключаемых дисков.

§ Нажмите на кнопку “Далее >”.

4. В диалоговом окне “Создание нового диска - шаг 2 из 6” в раскрывающемся списке “Создать секретный диск, расширяемый до” укажите емкость создаваемого диска.



§ Используя любое из трех расположенных ниже взаимосвязанных полей, задайте начальный объем файла создаваемого секретного диска. По мере заполнения секретного диска данными объем файла секретного диска можно увеличивать от начального размера до максимального. Выразить начальный объем файла секретного диска можно любым из следующих способов:

- ввести в поле “Мбайт” начальный объем файла секретного диска в мегабайтах;
- ввести в поле “% от свободного пространства” начальный объем файла секретного диска, выраженный в процентах от свободного пространства на том логическом диске, где создается секретный диск, — например, если Вы хотите, чтобы секретный диск изначально занимал 60% свободного пространства, введите в это поле значение 60;
- ввести в поле “Мбайт свободного пространства останется...” объем в мегабайтах, который должен остаться свободным после создания секретного диска, — например, если Вы хотите, чтобы после создания секретного диска на логическом диске осталось 100 свободных мегабайт, введите в это поле значение 100.

i Если файл-контейнер секретного диска располагается на разделе с файловой системой FAT32, максимальный объем секретного диска не может превышать 4 Гб.

§ В раскрывающемся списке “Тип файловой системы” выберите тип файловой системы.

i Для FAT32 максимальный объем секретного диска не может превышать 20 Гб.

§ При необходимости включите опцию **“Заполнить диск случайными данными”**. Эта процедура займет достаточно большое количество времени, но не даст злоумышленнику возможность определить объем зашифрованных данных.

§ Нажмите на кнопку **“Далее >”**.

5. В диалоговом окне **“Создание нового диска - шаг 3 из 6”** в поле **“Пароль”** введите пароль доступа к создаваемому секретному диску. Паролем может быть любая последовательность символов.

§ В раскрывающемся списке **“Выберите электронный идентификатор”** укажите тип используемого Вами электронного идентификатора.

§ В раскрывающемся списке **“Выберите алгоритм шифрования”** выберите алгоритм, который Вы хотели бы использовать для шифрования данных на создаваемом секретном диске.

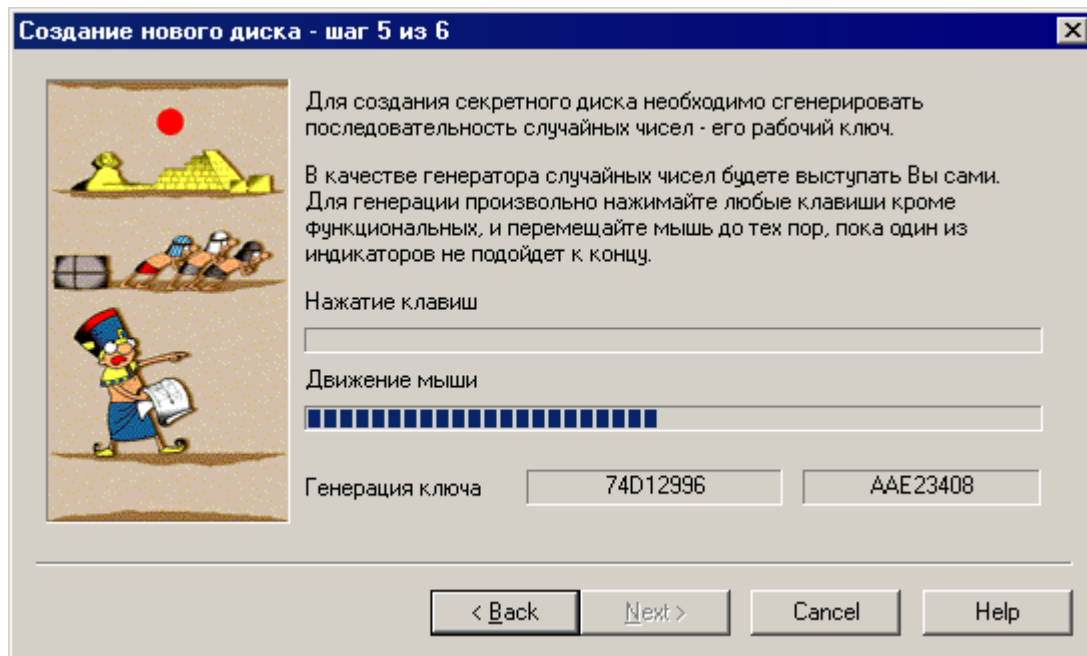
§ Нажмите на кнопку **“Далее >”**.

6. В диалоговом окне **“Создание нового диска - шаг 4 из 6”** в поле **“Пароль для входа под принуждением”** введите соответствующий пароль.

! Пароль входа под принуждением обязательно должен отличаться от пароля доступа

7. В диалоговом окне **“Создание нового диска - шаг 5 из 6”** примите участие в построении рабочего ключа создаваемого секретного диска. Рабочий ключ представляет собой случайную последовательность чисел (см. п. 6.1). Для ее создания можно было бы использовать встроенный в операционную систему генератор случайных чисел, но это не очень надежный способ, потому что на самом деле генератор выдает не случайные, а псевдослучайные числа, получаемые по определенной формуле. В статистическом смысле внутри каждой последовательности эти числа случайны, то есть выглядят как случайные и, скажем, могут использоваться во всевозможных численных экспериментах в качестве исходных данных. Однако сами последовательности нередко бывают одинаковыми. Таким образом, не исключено, что компьютер будет каждый раз при создании нового секретного диска генерировать один и тот же ключ, и, более того, разные компьютеры могут порождать одинаковые ключи. Поэтому необходим генератор по-настоящему случайных чисел. Этим генератором будете Вы.

§ Нажимайте на клавиши в произвольном порядке или водите мышью до тех пор, пока один из имеющихся в диалоговом окне индикаторов не окажется заполненным, а в поле **“Генерация ключа”** не появится надпись **“Готово”**. Затем нажмите на кнопку **“Далее >”**.



8. В диалоговом окне “Создание нового диска - шаг 6 из 6” укажите диск или каталог, в который в виде файла будет записан рабочий ключ создаваемого диска. Этот файл следует надежно спрятать и хранить на тот случай, если Вы забудете пароль или потеряете (или намеренно испортите) электронный идентификатор. Тогда с помощью этого файла Вы сможете изменить пароль доступа и "прописать" другой электронный идентификатор данного диска (см. п. 5.1.2).

Система не случайно по умолчанию предлагает записать рабочий ключ секретного диска именно на дискету. Если Вы запишете его на жесткий диск, потом скопируете на дискету, а потом сотрете файл на жестком диске, его в принципе можно будет восстановить.

i При сохранении рабочего ключа система Zdisk создает на указанном Вами диске (в указанном Вами каталоге) файл **zdisk.key** и записывает в него рабочий ключ. Если на том диске (в том каталоге), куда сохраняется рабочий ключ, такой файл уже существует, система дописывает в него рабочий ключ, то есть в одном файле может храниться несколько рабочих ключей.

9. Нажмите на кнопку “Готово”, после чего будет запущена процедура создания нового секретного диска. Эта процедура может занять некоторое время. После того как секретный диск будет создан, система сразу предложит Вам подключить его.

4.3 Подключение секретных дисков


Приложения могут работать с файлами, находящимися на секретном диске, только если этот диск подключен. При отключенном диске все находящиеся на нем файлы и приложения недоступны системе.

i Подключенный диск можно предоставить для использования в локальной сети. Правда, при этом данные будут передаваться по сети в незашифрованном виде.

2


Для подключения секретного диска

1. Убедитесь в том, что электронный идентификатор подключен к компьютеру.
2. В окне “Zdisk Администратор” в иерархическом списке выберите диск или каталог, в котором находится подключаемый секретный диск.

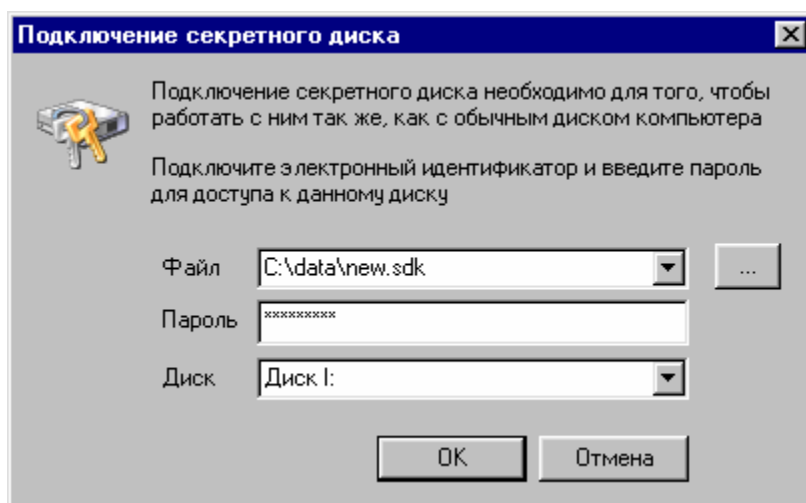
3. В правом списке щелчком мыши выделите диск, который Вы собираетесь подключать. Неподключенные диски изображаются значком .
4. Выберите в меню “Диск” пункт “Подключить диск” или нажмите на кнопку



в панели инструментов.

i Для подключения секретного диска можно дважды щелкнуть мышью по значку  в правой части панели задач Windows.

5. В диалоговом окне “Подключение секретного диска” в редактируемом раскрывающемся списке “Файл” будет автоматически введено имя файла секретного диска, включая полный путь. Если Вы хотите подключить другой диск, Вы можете нажать на кнопку “...” справа от этого раскрывающегося списка и выбрать в стандартном диалоговом окне другой файл секретного диска. Кроме того, в раскрывающемся списке “Файл” можно выбрать один из дисков, которые подключались в последнее время.



- § В поле “Пароль” введите пароль доступа к подключаемому диску.
- § В раскрывающемся списке “Диск” выберите свободную букву, которой Вы хотели бы обозначить подключаемый диск. Например, если Вы хотите, чтобы операционная система воспринимала подключаемый диск как I:, выберите в раскрывающемся списке пункт “Диск I:”.
- § Нажмите на кнопку “ОК”.

После этого, если, конечно, Вы подключили нужный электронный идентификатор и правильно ввели пароль, секретный диск будет подключен и останется доступным всем приложениям до тех пор, пока Вы его не отключите (см. п. 4.4) или не завершите работу Windows.

i

В правом списке для обозначения подключенных дисков используется значок .

i

Если файл-контейнер имеет расширение, отличное от .sdk, он не будет восприниматься системой как файл секретного диска. Поэтому для его подключения придется вручную набирать в поле “Файл” в окне “Подключение секретного диска” полный путь к нему.


4.4 Отключение секретных дисков

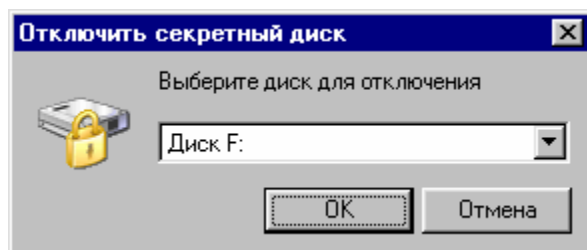
Отключив секретный диск, Вы сделаете его недоступным операционной системе и приложениям, однако при просмотре файловых каталогов файл-контейнер секретного диска будет виден.

! Прежде чем отключить секретный диск, убедитесь в том, что ни одно приложение не работает с находящимися на нем файлами. Отключение диска, на котором находятся открытые файлы, может привести к потере данных или к их рассекречиванию.

i Отключить секретный диск может любой пользователь, даже если он не обладает электронным идентификатором и не знает пароль.

2 Для отключения секретного диска

1. Выберите в меню “Диск” пункт “Отключить диск” или нажмите на кнопку  в панели инструментов.
2. В диалоговом окне “Отключить секретный диск” выберите в раскрывающемся списке диск, который Вы хотели бы отключить и нажмите кнопку “ОК”.



! Если в момент отключения диска вы все еще работали с его файлами, то Вы увидите диалоговое окно, в котором будет предложено принудительно закрыть диск, что чревато потерей данных, или прекратить работу с файлами и повторить попытку.

i Для вызова диалогового окна отключения секретного диска достаточно дважды щелкнуть мышью по его значку в правом списке (тогда в диалоговом окне “Отключить секретный диск” в раскрывающемся списке будет выбран именно этот диск). Вы можете также воспользоваться контекстным меню соответствующего отключаемому секретному диску пункта левого (иерархического) или правого списка. Для этого подведите курсор мыши к значку диска, который Вы собираетесь отключить, нажмите на правую клавишу мыши и выберите в контекстном меню пункт “Отключить” или “Отключить диск” соответственно.

i Секретный диск можно отключить, не запуская Администратор. Для этого:

1. Подведите курсор мыши к значку файла секретного диска в Проводнике Windows.
2. Нажмите на правую клавишу мыши и выберите в динамическом меню файла пункт “Zdisk”, в следующем меню выберите пункт “Отключить”. После этого будет открыто диалоговое окно “Отключить секретный диск”

! Перед завершением сеанса работы с Windows необходимо отключить все подключенные секретные диски.

4.5 Блокировка операционной системы

Под блокировкой операционной системы подразумевается блокирование консоли рабочей станции, и для снятия блокировки необходимо будет дополнительно ввести пароль учетной записи текущего пользователя Windows. Подключенные на момент блокировки секретные диски не отключаются, а все приложения продолжают работать, т.е. угрозы потери данных при блокировке системы нет.

Блокировка операционной системы может происходить при следующих условиях:

- Пользователь выбрал пункт **“Блокировка”** в системном меню Zdisk.
- Пользователь нажал заданную в настройках системы Zdisk комбинацию клавиш.
- Пользователь отключил электронный идентификатор.
- Пользователь заблокировал консоль рабочей станции.

Снятие блокировки происходит стандартным для Windows образом, с помощью нажатия <Ctrl>+<Alt>+ и ввода пароля текущего пользователя. Прежде чем консоль разблокируется, Zdisk проверяет, присоединен ли к компьютеру электронный идентификатор, который использовался при подключении всех подключенных на момент снятия блокировки секретных дисков. Если подключенных дисков нет, то проверка электронных идентификаторов производиться не будет.


Глава 5 Работа с секретными дисками

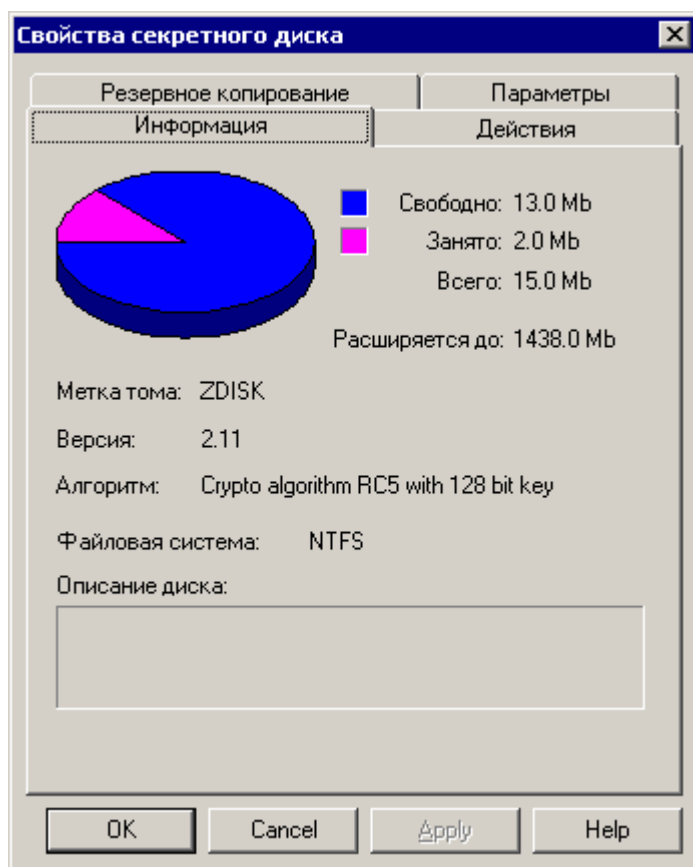
i Основные операции с секретными дисками - создание, подключение и отключение - описаны в Главе 4.

5.1 Работа со свойствами секретного диска

Просматривать и изменять свойства можно только у отключенных (см. п. 4.4) секретных дисков. Эта возможность доступна только **“администратору”** - создателю данного диска.

2 Для просмотра и изменения свойств секретного диска

1. Убедитесь в том, что электронный идентификатор подключен к компьютеру.
2. В окне **“Zdisk Администратор”** в иерархическом списке выберите тот диск или каталог, где находится секретный диск, свойства которого Вас интересуют.
3. В правом списке щелчком мыши выделите нужный диск.
4. Выберите в меню **“Диск”** пункт **“Свойства диска”** или нажмите на кнопку  в панели инструментов.
5. В диалоговом окне **“Пароль”** введите пароль доступа к диску и нажмите на кнопку **“ОК”**. После этого будет открыто окно **“Свойства секретного диска”**.



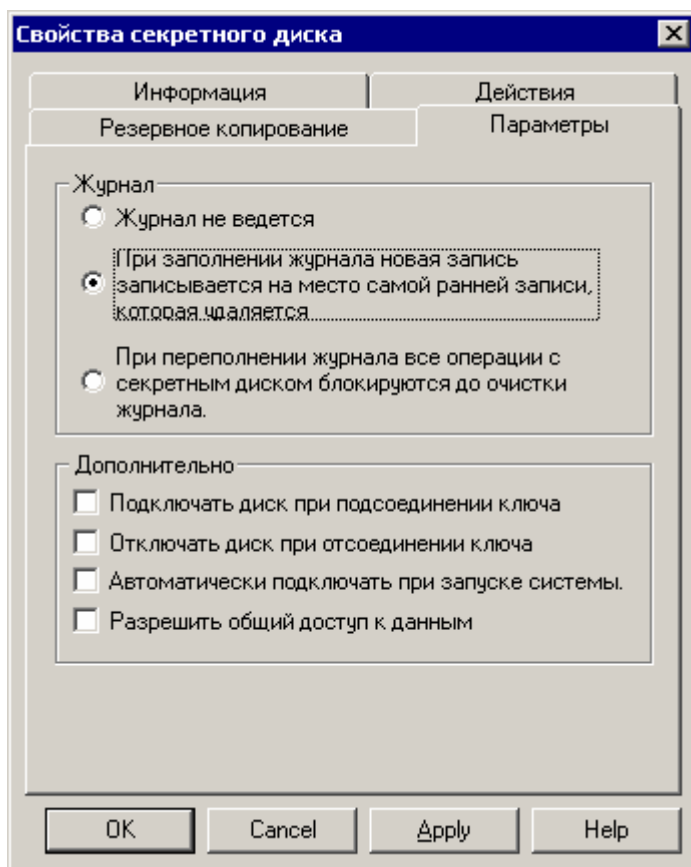
На закладке **“Информация”** представлены следующие сведения о секретном диске:

- § Объем свободного пространства на секретном диске (поле **“Свободно”**), объем, занятый на нем файлами (поле **“Занято”**) и общий объем диска (поле **“Всего”**). В поле **“Расширяется до:”** отображается максимально возможный объем диска.
- § Метка тома для этого диска (поле **“Метка тома”**).
- § Используемый алгоритм шифрования (поле **“Алгоритм”**).
- § Тип файловой системы (поле **“Файловая система”**).

- § В поле **“Описание диска”** — комментарий, введенный при создании диска в первом диалоговом окне.

5.1.1 Настройка параметров секретного диска

На вкладке **“Параметры”** находятся дополнительные настройки секретного диска.



i Группа настроек **“Журнал”** описывается в п. 5.3 **“Ведение журнала обращений к секретному диску”**.

- Для секретного диска можно установить режим автоподключения. Тогда при запуске Windows система Zdisk каждый раз будет предлагать пользователю ввести пароль доступа к этому диску и подключить его. Для того чтобы установить (отменить) для секретного диска режим автоподключения, установите во включенное (выключенное) состояние переключатель **“Автоматически подключать при запуске системы”**;
- Опция **“Подключать диск при подсоединении ключа”** означает, что при подсоединении электронного идентификатора будет выводиться диалоговое окно **“Подключение секретного диска”** с предложением ввести пароль для данного файлового контейнера;
- Включение опции **“Отключать диск при отсоединении ключа”** приведет к тому, что при отсоединении электронного идентификатора открытый секретный диск закроется, без участия пользователя;

M Автоматическое отключение секретного диска во время работы с ним приложений может привести к потере информации.

- Параметр **“Разрешить общий доступ к данным”** отвечает за предоставление общего доступа к открытому секретному диску пользователям сети. Если он отключен, создать общий ресурс невозможно.

5.1.2 Изменение пароля доступа и (или) электронного идентификатора

2

Для изменения параметров доступа к диску

1. В диалоговом окне **“Свойства секретного диска”** переключитесь на закладку **“Действия”**.
2. В группе **“Изменить пароль или личный ключ”** нажмите на кнопку **“Изменить”**.
3. В диалоговом окне **“Изменение личного ключа и пароля - шаг 1 из 2”**
 - § Установите во включенное состояние кнопку выбора **“Пароль”**.
 - § Введите в расположенное справа от нее поле текущий пароль доступа к диску.
 - § Нажмите на кнопку **“Далее >”**.
4. В диалоговом окне **“Изменение личного ключа и пароля - шаг 2 из 2”**
 - § В поле **“Пароль”** введите новый пароль доступа к диску.
 - § Выберите в раскрывающемся списке тип электронного идентификатора, который вы хотите использовать для доступа к этому секретному диску.
 - § Нажмите на кнопку **“Готово”**.

После этого секретному диску будет присвоен новый пароль доступа и электронный идентификатор.

i

На этой же закладке возможно изменить пароль для входа под принуждением, нажав кнопку **“Изменить”** в группе **“Пароль для входа под принуждением”**.

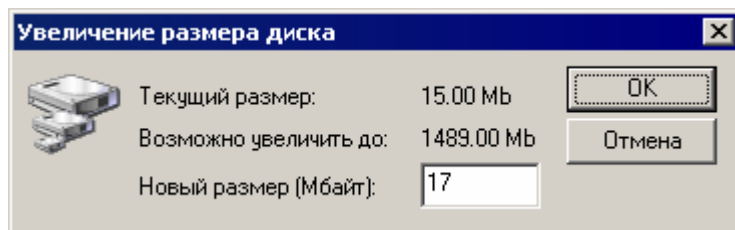
5.1.3 Увеличение объема секретного диска

Вы можете увеличивать емкость секретного диска вплоть до максимального возможного объема, который зависит от свободного места на диске, файловой системы и прочих параметров. Максимальный объем можно узнать на вкладке **“Информация”** в свойствах секретного диска.

2

Для увеличения объема секретного диска

1. В диалоговом окне **“Свойства секретного диска”** переключитесь на закладку **“Действия”**.
2. В группе **“Изменить размер диска”** нажмите на кнопку **“Изменить”**.
3. В диалоговом окне **“Увеличение размера диска”** в поле **“Новый размер”** введите новый объем секретного диска в мегабайтах. Обратите внимание: в поле **“Текущий размер”** отображается текущий объем диска, а в поле **“Возможно увеличить до”** — максимальный объем диска, который был задан при его создании.



4. Нажмите на кнопку **“ОК”**.

5.2 Многопользовательский режим

5.2.1 Использование секретного диска в многопользовательском режиме

В системе Zdisk реализована возможность многопользовательского режима доступа к секретному диску.

Пользователь, создавший секретный диск, получает права администратора этого секретного диска. Он может не только работать с этим секретным диском, но также добавлять и удалять других пользователей, которые могут только подключать диск, работать с ним и отключать его. Кроме того, администратор диска может просматривать журнал обращений пользователей к диску.

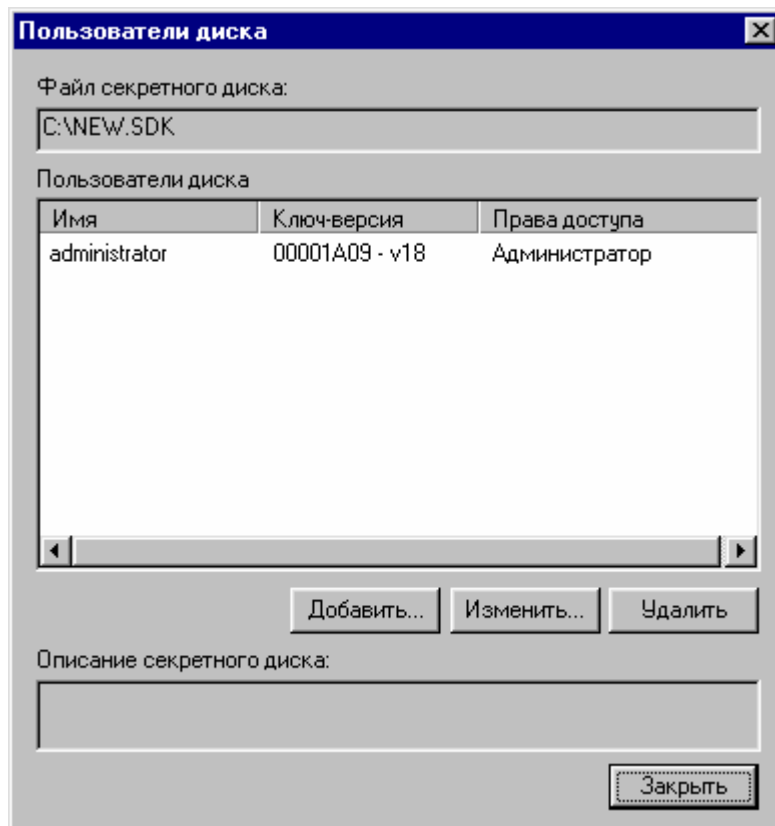
5.2.2 Добавление нового пользователя секретного диска

! В системе Zdisk невозможно создание нескольких пользователей одного секретного диска, имеющих один и тот же (или одинаковый) электронный идентификатор. Поэтому для того чтобы предоставить доступ к секретному диску, предположим, двум пользователям необходимо иметь в распоряжении два электронных идентификатора.

2

Для того чтобы добавить нового пользователя некоторого секретного диска,

1. В окне **“Zdisk Администратор”** в иерархическом списке выберите тот диск или каталог, где находится секретный диск, доступ к которому нового пользователя Вы хотите организовать.
2. В правом списке щелчком мыши выделите нужный секретный диск.
3. Выберите в меню **“Диск”** пункт **“Пользователи диска”** или нажмите на кнопку в панели инструментов.
4. Убедитесь в том, что Ваш электронный идентификатор подключен к компьютеру и в диалоговом окне **“Пароль”** введите пароль доступа к секретному диску и нажмите на кнопку **“ОК”**. После этого на экране отобразится диалоговое окно **“Пользователи диска”**.



5. Нажмите на кнопку **“Добавить”**.
6. В появившемся на экране диалоговом окне **“Добавление нового пользователя — шаг 1 из 2”** в поле **“Введите имя нового пользователя”** введите имя нового пользователя.

§ В раскрывающемся списке **“Выберите тип электронного идентификатора нового пользователя”** укажите тип используемого новым пользователем электронного идентификатора.

§ Отключите Ваш электронный идентификатор и подключите электронный идентификатор того пользователя, которому Вы хотите предоставить доступ к секретному диску.

! Электронный идентификатор пользователя обязательно должен быть активирован.

§ Нажмите на кнопку **“Далее >”**.

7. В диалоговом окне **“Добавление нового пользователя - шаг 2 из 2”** в поле **“Введите пароль нового пользователя”** должен быть задан пароль доступа к секретному диску для нового пользователя.
8. Нажмите на кнопку **“Готово”**. На экране появится сообщение **“Пользователь успешно добавлен”**.
9. Нажмите на кнопку **“ОК”**.

5.2.3 Изменение атрибутов пользователя

2 Для того чтобы задать имя, пароль или тип личного идентификатора пользователя,

1. В поле **“Пользователи диска”** диалогового окна **“Пользователи диска”** щелкните мышью по строке с именем пользователя, атрибуты которого Вы собираетесь изменить.
2. Нажмите на кнопку **“Изменить”**.

3. В появившемся на экране диалоговом окне **“Изменение пользователя — шаг 1 из 2”** в поле **“Введите имя нового пользователя”** измените имя пользователя. Если с момента добавления пользователя его электронный идентификатор был заменен или повторно активизирован, в раскрывающемся списке **“Выберите тип электронного идентификатора нового пользователя”** укажите тип электронного идентификатора пользователя. Отключите Ваш электронный идентификатор и подключите электронный идентификатор того пользователя, атрибуты которого Вы задаете.
4. Нажмите на кнопку **“Далее >”**.
5. В диалоговом окне **“Изменение пользователя - шаг 2 из 2”** в поле **“Введите пароль нового пользователя”** измените пароль доступа к создаваемому секретному диску. Паролем может быть любая последовательность символов.
6. Нажмите на кнопку **“Готово”**. На экране появится сообщение **“Пользователь успешно изменен”**.
7. Нажмите на кнопку **“ОК”**.

5.2.4 Удаление пользователя

2

Для того чтобы исключить пользователя из числа имеющих доступ к данному диску,

1. В поле **“Пользователи диска”** диалогового окна **“Пользователи диска”** щелкните мышью по строке с именем пользователя, которого Вы хотите лишить права доступа к данному секретному диску.
2. Нажмите на кнопку **“Удалить”**.
3. На экране появится диалоговое окно с запросом подтверждения удаления пользователя. Для подтверждения удаления нажмите на кнопку **“Да”**.
4. На экране появится сообщение **“Пользователь успешно удален”**.
5. Нажмите на кнопку **“ОК”**.

Имя удаленного пользователя исчезнет из списка в поле **“Пользователи диска”**.

5.3 Ведение журнала обращений к секретному диску

5.3.1 Журнал работы с диском

Система Zdisk предоставляет возможность контроля работы пользователей с секретными дисками. С этой целью для каждого диска ведется отдельный журнал. В журнале фиксируются следующие события:

- § подключение диска;
- § подключение диска под принуждением;
- § отключение диска;
- § смена пароля и (или) электронного идентификатора;
- § изменение размера диска;
- § добавление пользователя;
- § удаление пользователя;
- § очистка журнала.


Для каждого события в журнал записывается системное время и дата, а также имя и полномочия пользователя, выполнившего действие.

В журнале фиксируются не только имевшие место события, но и неудачные попытки операций с дисками.

5.3.2 Настройка свойств журнала секретного диска

В зависимости от конкретных условий использования секретного диска Вы можете по-разному настроить порядок занесения записей в журнал.

2 Для просмотра и изменения свойств журнала

1. В окне **“Zdisk Администратор”** в иерархическом списке выберите диск или каталог, содержащий файл секретного диска, журнал которого Вы хотели бы настроить.
2. В правом списке щелчком мыши выделите нужный секретный диск.
3. Выберите в меню **“Диск”** пункт **“Свойства диска”** или нажмите на кнопку  в панели инструментов.
4. В диалоговом окне **“Пароль”** введите пароль доступа к секретному диску и нажмите на кнопку **“ОК”**. После этого будет открыто окно **“Свойства секретного диска”**.
5. Переключитесь на закладку **“Параметры”**.
6. Выберите один из возможных способов ведения журнала в группе настроек **“Журнал”** или откажитесь от ведения журнала (кнопка выбора **“Журнал не ведется”**).
7. Нажмите на кнопку **“ОК”**.

5.3.3 Просмотр журнала

i Содержимое журнала секретного диска может просматривать только администратор секретного диска.

2 Для того чтобы просмотреть содержимое журнала

1. Подключите электронный идентификатор, использованный при создании данного диска.
2. В окне **“Zdisk Администратор”** в иерархическом списке выберите тот диск, журнал которого Вы хотите просмотреть.
3. Выберите в меню **“Диск”** пункт **“Журнал”**.
4. В появившемся диалоговом окне **“Пароль”** введите пароль администратора диска.
5. Нажмите на кнопку **“ОК”**. На экране появится диалоговое окно **“Журнал”**.

Журнал			
Время-дата	Событие	Пользователь	Ключ
11:20:47 05.04.2002	Создание	administrator	
11:20:51 05.04.2002	Подключение	administrator	6665
11:22:41 05.04.2002	Отключение		6665
11:22:45 05.04.2002	Подключение	administrator	6665
11:22:59 05.04.2002	Отключение		6665
11:23:03 05.04.2002	Подключение	administrator	6665
11:23:17 05.04.2002	Отключение		6665
11:26:58 05.04.2002	Подключение	administrator	6665
11:27:48 05.04.2002	Отключение		6665
11:29:02 05.04.2002	Подключение	administrator	6665
11:29:31 05.04.2002	Отключение		6665
11:31:51 05.04.2002	Подключение		6665
11:32:04 05.04.2002	Подключение	administrator	6665
11:32:05 05.04.2002	Отключение		6665

Очистить Экспорт... ОК

5.3.4 Экспорт и очистка журнала

i Эта функция доступна только создателю (администратору) секретного диска. Данные, заносимые в журнал, могут Вам понадобиться для работы в других приложениях (например, для занесения в базу данных). Для этого в системе Zdisk предусмотрена возможность экспорта содержимого журнала в текстовый файл.

- 2** Для того чтобы экспортировать содержимое журнала в текстовый файл,
1. В диалоговом окне **“Журнал”** нажмите на кнопку **“Экспорт”**.
 2. В появившемся на экране диалоговом окне **“Сохранение”** выберите путь и имя файла, в который Вы хотите экспортировать записи из журнала.
 3. Нажмите на кнопку **“Сохранить”**.

После экспорта журнала его можно очистить.


- 2** Для того чтобы очистить журнал,
1. В диалоговом окне **“Журнал”** нажмите на кнопку **“Очистить”**.
 2. В появившемся на экране диалоговом окне подтверждения **“Экспортировать журнал в текстовый файл перед его очисткой?”** нажмите на кнопку **“Нет”**.
 3. На экране появится сообщение **“Журнал очищен”**. Нажмите на кнопку **“ОК”**.

Из журнала удалятся все записи.

5.4 Моментальное отключение всех подключенных дисков


Возможность моментального отключения всех секретных дисков предусмотрена в основном для использования в исключительных ситуациях.

M Моментальное отключение секретных дисков может привести к потере информации. Это особенно относится к сложно организованным данным, в частности к файлам баз данных.

Для моментального отключения всех секретных дисков в окне **“Zdisk Администратор”** выберите пункт **“Отключить все диски”** в меню **“Диск”** или в системном меню Zdisk, открываемом при щелчке мыши по значку  в правой части панели задач Windows.

5.5 Удаление секретных дисков

Удалить секретный диск — означает удалить его файл-контейнер. Эта операция, может быть выполнена двумя способами: стандартными средствами среды Windows или в окне **“Zdisk Администратор”**.

- 2** Для удаления секретного диска
1. В окне **“Zdisk Администратор”** в правом списке выделите диск, который Вы собираетесь удалить. Можно выделить сразу несколько дисков.
 2. Выберите в меню **“Диск”** пункт **“Удалить диск”** или нажмите на кнопку  в панели инструментов.
 3. Нажмите в диалоговом окне подтверждения на кнопку **“Да”**. Для отказа от удаления нажмите на кнопку **“Нет”**.

! Удаление секретных дисков без подключенного электронного идентификатора посредством модуля **“Zdisk Администратор”** невозможно.

Глава 6 Управление ключами

6.1 Личный ключ, рабочие ключи и пароли

Каждый секретный диск защищен тремя ключами: рабочим ключом диска, личным ключом пользователя и паролем доступа к диску.

i Рабочий ключ секретного диска генерируется при создании последнего и тогда же может быть записан в файл.

У каждого секретного диска свой *рабочий ключ*. Рабочий ключ используется для шифрования данных на диске и хранится в заголовке файла секретного диска в зашифрованном виде. *Личный ключ* пользователя генерируется при активации электронного идентификатора и хранится в нем. Активация электронного идентификатора заключается в построении случайной последовательности чисел и ее записи в электронный идентификатор. Вместе с паролем доступа личный ключ пользователя используется для шифрования рабочих ключей в заголовках файлов секретных дисков. Для того чтобы подключить секретный диск, необходимо, чтобы был подключен активированный Вами электронный идентификатор.

i Рекомендуется сохранить личный и рабочий ключи на специально выделенную для этого аварийную дискету и хранить ее в надежном месте.

Пароль доступа к диску наряду с электронным идентификатором используется для шифрования рабочих ключей в заголовках файлов секретных дисков. Для каждого секретного диска рекомендуется задать свой пароль доступа. Если Вы забыли пароль, его можно задать заново с помощью рабочего ключа данного диска.

При открытии диска происходит следующее:

1. Из электронного идентификатора считывается личный ключ пользователя.
2. На основе личного ключа и введенного пароля формируется дополнительный идентификационный ключ.
3. С помощью полученного ключа система расшифровывает рабочий ключ диска, находящийся в заголовке файла-контейнера.
4. Расшифрованный рабочий ключ загружается в память.
5. Данные становятся доступными для пользователя.

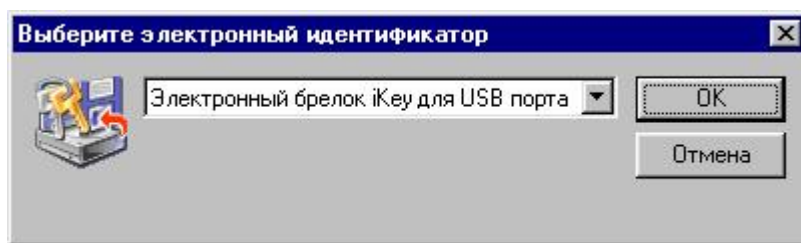
Операция по генерации личного ключа - активация электронного идентификатора - описана в п. 4.1.

6.2 Запись личного ключа пользователя в файл

Суть данной операции состоит в следующем: система Zdisk считывает из памяти электронного идентификатора личный ключ и записывает его в файл. Записанный в файл личный ключ затем можно оттуда загрузить обратно в этот (и только этот) электронный идентификатор.

2 Для записи личного ключа пользователя в файл

1. Выберите в меню “Электронный идентификатор” пункт “Сохранение”.
2. В диалоговом окне “Выберите электронный идентификатор” выберите в раскрываемом списке электронный идентификатор, из которого Вы собираетесь скопировать личный ключ и нажмите на кнопку “ОК”.



3. В диалоговом окне **“Обзор папок”** выберите диск и каталог, куда будет записан файл, содержащий считанный из электронного идентификатора ключ. Выбрав в иерархическом списке диск и каталог, нажмите на кнопку **“ОК”**. После этого в выбранном каталоге будет создан файл с именем ***.key**, содержащий записанный в электронном идентификаторе личный ключ. Если такой файл уже существует, система допишет новый ключ в него же (то есть в нем может храниться несколько ключей).

Личный ключ рекомендуется сразу сохранять на сменный носитель: аварийную дискету, диск ZIP и т.п. Если Вы сохраните личный ключ на жесткий диск, затем скопируете на дискету, а затем сотрете файл, то у заинтересованных лиц будет возможность восстановить его.

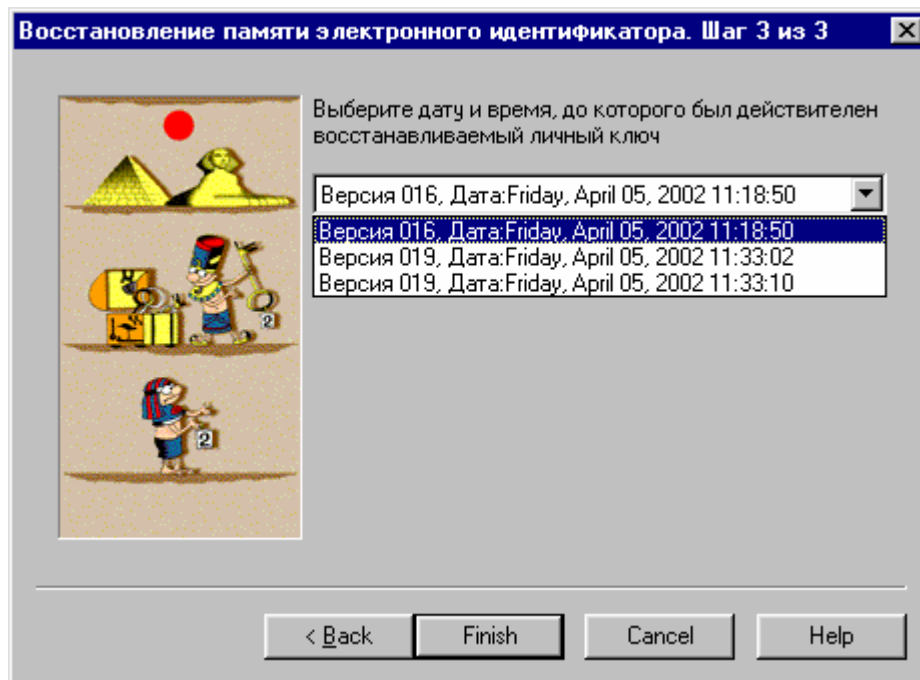
6.3 Загрузка личного ключа пользователя из файла

Суть данной операции состоит в следующем: система Zdisk считывает личный ключ из файла и замещает им тот личный ключ, который на тот момент записан в электронном идентификаторе.

i Личный ключ пользователя можно загрузить только в тот электронный идентификатор, из которого он был считан.

2 Для загрузки личного ключа пользователя из файла

1. Выберите в меню **“Электронный идентификатор”** пункт **“Восстановление”**.
2. В диалоговом окне **“Восстановление... Шаг 1 из 3”** в раскрывающемся списке выберите электронный идентификатор, в который Вы собираетесь записать личный ключ из файла и нажмите на кнопку **“Далее >”**.
3. В диалоговом окне **“Восстановление... Шаг 2 из 3”** в поле ввода наберите имя (включая полный путь) к файлу, в котором записан нужный Вам личный ключ. Вы можете выбрать файл в диалоговом окне, которое открывается при нажатии на кнопку **“Выбрать”**. Нажмите на кнопку **“Далее >”**.
4. В диалоговом окне **“Восстановление... Шаг 3 из 3”** в раскрывающемся списке выберите личный ключ, который Вы хотите записать в электронный идентификатор. Ключ идентифицируется датой и временем создания.



МПо окончании следующего этапа считанный из файла личный ключ будет записан в электронный идентификатор. Тот личный ключ, который записан там сейчас (текущий ключ), будет затерт. Если текущий ключ не был записан в файл, то доступ к секретным дискам, которые были созданы с его использованием, можно будет получить, только воспользовавшись их рабочими ключами. Прежде чем записывать в электронный идентификатор новый личный ключ, убедитесь в том, что в случае необходимости Вы сможете найти текущий личный ключ.

5. Нажмите на кнопку “Готово”.

6.4 Действия в случае утери электронного идентификатора и (или) пароля


Рассмотрим несколько характерных ситуаций, которые могут возникнуть при работе с системой Zdisk, и объясним, каким образом следует действовать для того, чтобы снова получить доступ к данным на секретных дисках.

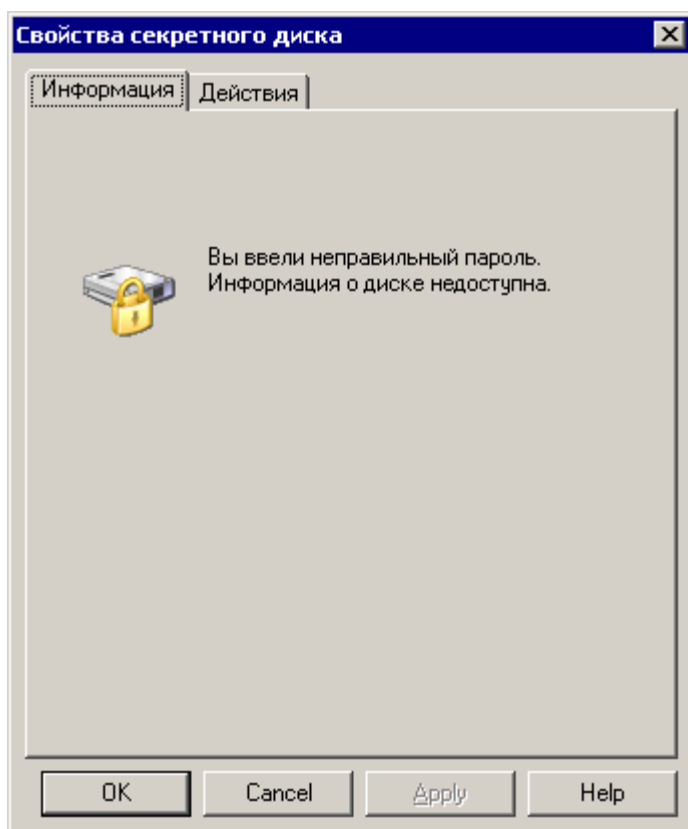
Ситуация 1. Вы забыли пароль доступа к диску.

Решение. В этом случае следует, используя записанный на аварийной дискете рабочий ключ диска, заново задать для этого диска пароль доступа и личный ключ.

2

Для этого необходимо

1. В окне “Zdisk Администратор” в иерархическом списке выберите тот диск или каталог, где находится Ваш секретный диск.
2. В правом списке щелчком мыши выделите нужный диск.
3. Выберите в меню “Диск” пункт “Свойства диска” или нажмите на кнопку  в панели инструментов.
4. В диалоговом окне “Пароль” нажмите на кнопку “ОК” не вводя пароль. После этого будет открыто окно “Свойства секретного диска” с предупреждением о неправильном вводе ключа.



5. В диалоговом окне **“Свойства секретного диска”** переключитесь на закладку **“Действия”**.
6. В группе **“Изменить пароль или личный ключ”** нажмите на кнопку **“Изменить”**.
7. В диалоговом окне **“Изменение личного ключа и пароля - шаг 1 из 2”**
 - § Установите во включенное состояние кнопку выбора **“Файл”**.
 - § Введите полный путь и имя файла сохраненной копии рабочего ключа или нажмите кнопку **“...”** и выберите этот файл в появившемся диалоговом окне.
 - § Нажмите на кнопку **“Далее >”**.
8. В диалоговом окне **“Изменение личного ключа и пароля - шаг 2 из 2”**
 - § В поле **“Пароль”** введите новый пароль доступа к диску.
 - § Выберите в раскрывающемся списке тип электронного идентификатора, который вы хотите использовать для доступа к этому секретному диску.
 - § Нажмите на кнопку **“Готово”**.

Ситуация 2. Вы потеряли электронный идентификатор.

Решение. В этом случае следует:

1. Приобрести новый электронный идентификатор.
2. Подключить его к компьютеру.
3. Активировать новый электронный идентификатор (см. п. 4.1).
4. Используя записанный на аварийной дискете рабочий ключ диска, заново задать для диска пароль доступа и личный ключ (аналогично ситуации 1).

Ситуация 3. Вы затерли записанный в электронном идентификаторе личный ключ. У Вас есть аварийная дискета, на которой записан потерянный личный ключ.

Решение. В этом случае следует с аварийной дискеты загрузить в электронный идентификатор личный ключ.

Ситуация 4. Вы затерли записанный в электронном идентификаторе личный ключ. При этом у Вас в распоряжении нет файла с записанным в нем личным ключом.

Решение. В этом случае следует:

1. Заново активировать электронный идентификатор (см. п. 4.1).
2. Используя записанный на аварийной дискете рабочий ключ диска, заново задать для этого диска пароль доступа и личный ключ (аналогично ситуации 1).

Глава 7 Резервное копирование и работа с защищенными архивами

7.1 Обзор возможностей резервного копирования

Систему Zdisk можно использовать для создания резервных копий секретных дисков и для работы с зашифрованными архивами. Доступ к зашифрованному архиву может быть ограничен либо только паролем, либо только электронным идентификатором. Возможность работы с зашифрованными архивами очень полезна в тех случаях, когда конфиденциальные данные требуется передать на сменном носителе или переслать по электронной почте.

7.2 Резервное копирование секретных дисков

Данная возможность предназначена для регулярного автоматического или ручного резервного копирования файлов секретных дисков. Для каждого файла секретного диска может быть задан свой режим резервного копирования, который включает в себя:

- § Расположение резервной копии файла секретного диска (диск, каталог и т.д.).
- § Периодичность резервного копирования (один раз в N дней).
- § Момент резервного копирования (при запуске Windows, при завершении работы, перед подключением диска, после отключения диска).

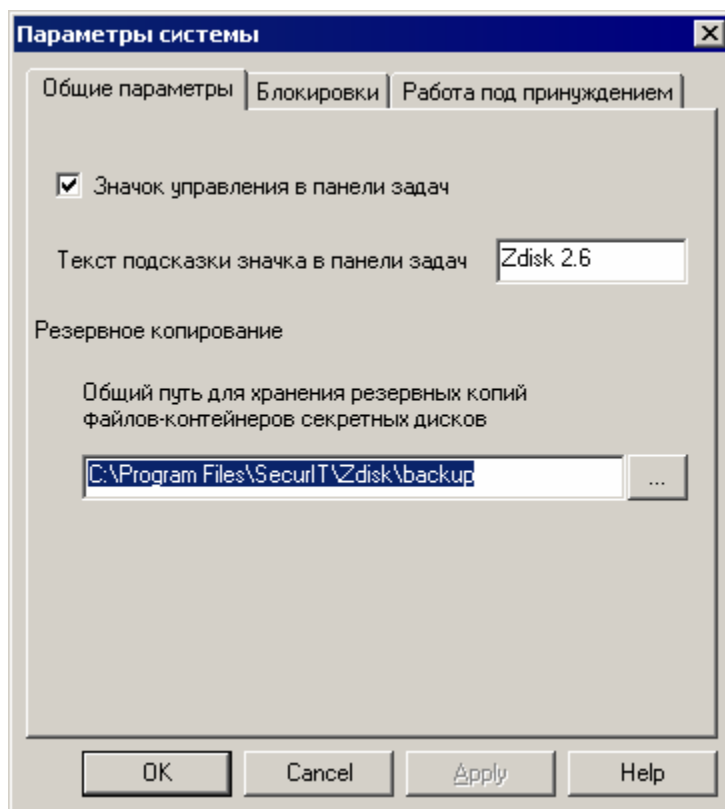
7.2.1 Расположение резервных копий файлов секретных дисков

Общий для всех файлов секретных дисков каталог хранения резервных копий должен быть задан в ходе работы Мастера первого запуска.

Позже Вы сможете изменить путь к этому каталогу.

2 Для того чтобы назначить общий для всех файлов-контейнеров каталог хранения резервных копий:

1. Выберите в меню “Диск” пункт “Параметры системы”.
2. В диалоговом окне “Параметры системы” переключитесь на закладку “Общие параметры”. На этой закладке в поле ввода “Общий каталог для хранения резервных копий файлов-контейнеров” введите путь к каталогу, в котором будут сохраняться резервные копии файлов секретных дисков или, нажав на кнопку “...” справа от этого поля, Вы можете выбрать этот каталог в иерархическом списке в появившемся диалоговом окне “Обзор папок”.



7.2.2 Настройка параметров резервного копирования файла секретного диска

2

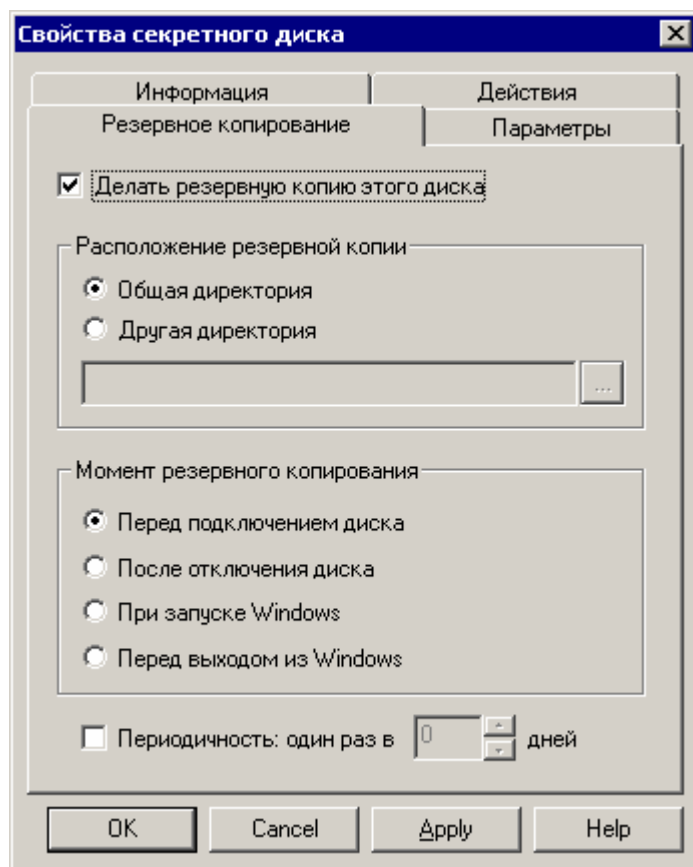
Чтобы настроить параметры резервного копирования секретного диска,

1. Вызовите на экран диалоговое окно **“Свойства секретного диска”**. Для этого выделите в правой части рабочей области нужный секретный диск и выберите в меню **“Диск”** или в контекстном меню диска пункт **“Свойства диска”**. После этого откроется диалоговое окно **“Пароль”**. Наберите в нем пароль доступа к диску и нажмите на кнопку **“ОК”**.
2. В диалоговом окне **“Свойства секретного диска”** переключитесь на закладку **“Резервное копирование”**.
3. Установите переключатель **“Делать резервную копию этого диска”** во включенное состояние.
4. В группе **“Расположение резервной копии”** установите во включенное состояние кнопку выбора **“Общая директория”**.

i

Если Вы хотите назначить для хранения резервной копии файла данного секретного диска другой каталог, это можно сделать, установив во включенное состояние кнопку выбора **“Другая директория”** и введя в поле ввода под этой кнопкой путь к нужному каталогу.

5. В группе **“Момент резервного копирования”**, установив во включенное состояние соответствующую кнопку, можно указать, в какой момент система должна производить резервное копирование файла данного секретного диска.
6. Установив переключатель **“Периодичность”** во включенное состояние и указав в поле ввода нужное число дней, Вы можете задать периодичность автоматического сохранения резервной копии. Например, если Вы хотите, чтобы резервное копирование файла секретного диска происходило каждые 10 дней, введите в это поле значение 10.



Кроме того, сохранить резервную копию файла выделенного диска Вы можете, выбрав пункт **“Сохранить файл-контейнер”** в меню **“Резервное копирование”**.

7.3 Восстановление секретных дисков из резервных копий

2


Чтобы восстановить содержимое секретного диска из резервной копии,

1. Выделите в правой части рабочей области нужный секретный диск.
2. В меню **“Резервное копирование”** выберите пункт **“Восстановить файл-контейнер”**.
3. В появившемся диалоговом окне подтвердите необходимость восстановления секретного диска из его резервной копии, нажав на кнопку **“Да”**.
4. После завершения восстановления секретного диска на экране появится диалоговое окно с сообщением об успешном завершении восстановления. Нажмите на кнопку **“ОК”**.

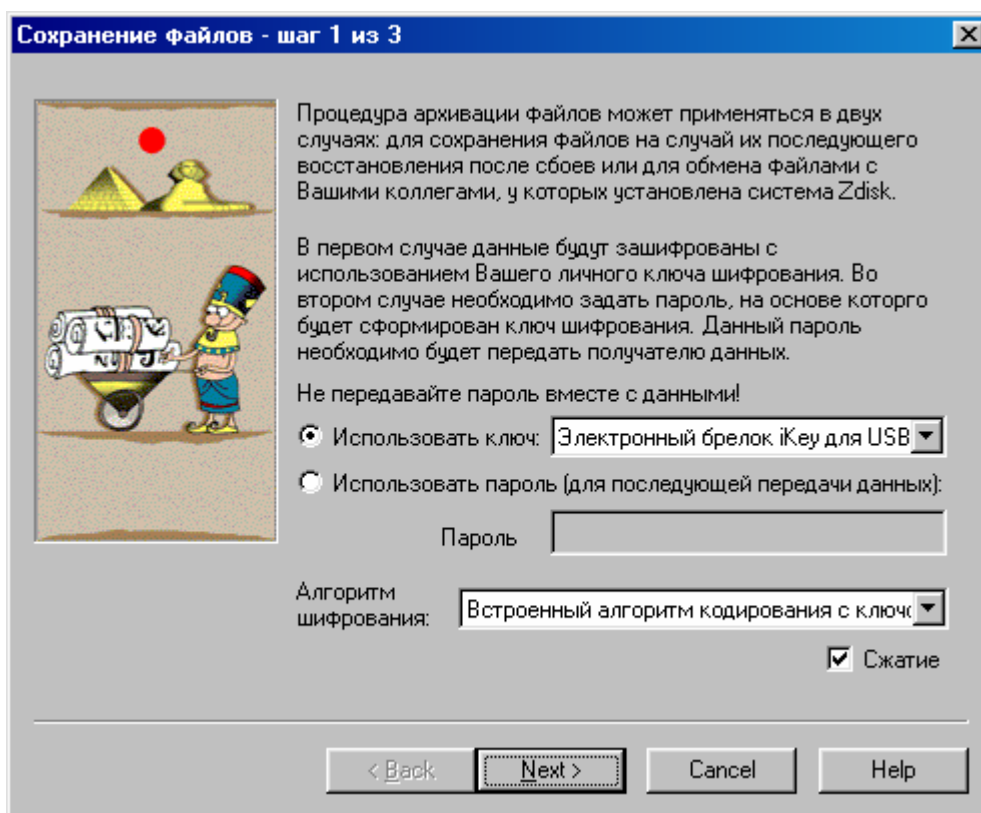
7.4 Создание зашифрованного архива

2

Для создания зашифрованного архива

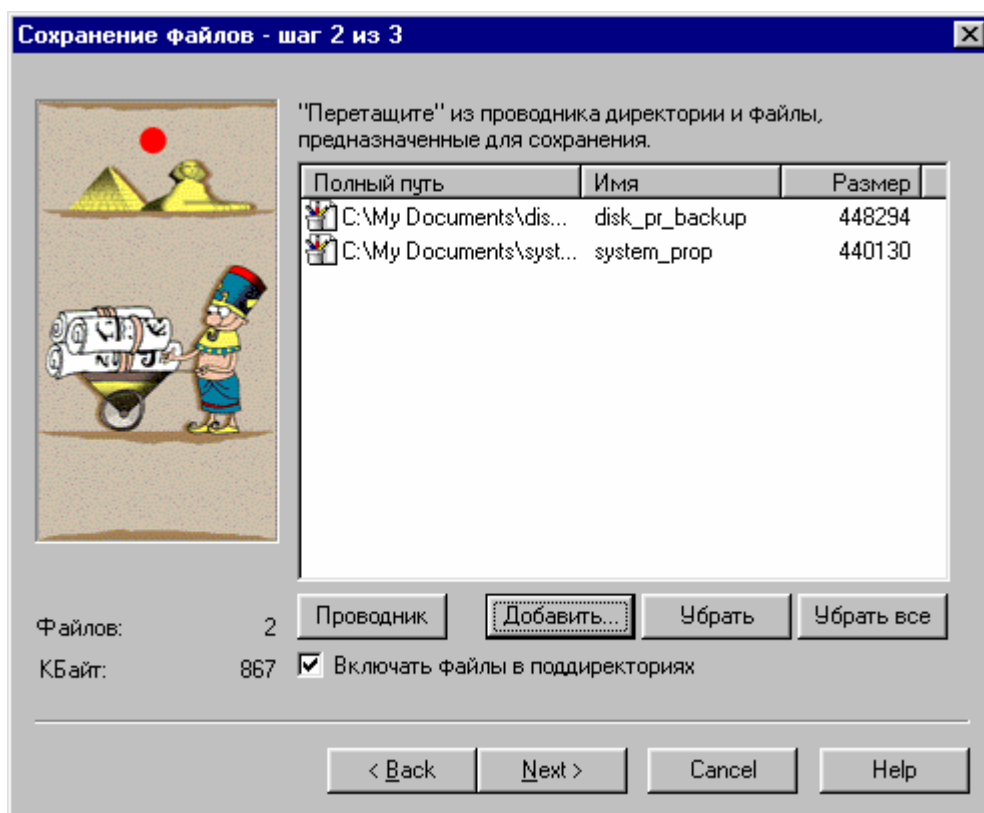
1. Выберите в меню **“Резервное копирование”** пункт **“Сохранить данные”** или нажмите на кнопку  в панели инструментов.
2. В диалоговом окне **“Сохранение файлов - шаг 1 из 3”** выберите способ защиты архива. Чтобы защитить архив электронным идентификатором, установите во включенное состояние кнопку выбора **“Использовать ключ”** и выберите в раскрывающемся списке электронный идентификатор. Для того чтобы защитить архив паро-

лем, установите во включенное состояние кнопку выбора **“Использовать пароль”**. Затем введите пароль доступа к архиву в поле **“Пароль”**.



- § В раскрывающемся списке **“Алгоритм шифрования”** выберите алгоритм шифрования, который Вы хотели бы использовать для защиты архива.
 - § Если Вы хотите не только зашифровать, но и сжать данные, установите во включенное состояние переключатель **“Сжатие”**.
 - § Нажмите на кнопку **“Далее >”**.
3. В диалоговом окне **“Сохранение файлов - шаг 2 из 3”** сформируйте список файлов, которые Вы хотите поместить в архив. Для того чтобы поместить файл в архив, его следует перетащить в список из какого-нибудь окна Windows или с Рабочего стола.

i Чтобы облегчить поиск нужных файлов, Вы можете непосредственно из этого диалогового окна вызвать программу Проводник — для этого нажмите на кнопку **“Проводник”**, расположенную под списком.



Для того чтобы исключить один или несколько файлов из списка добавляемых в архив, выделите их в списке и нажмите на кнопку **“Убрать”**. Чтобы выделить в списке файл, щелкните по нему (точнее, по его изображению) мышью. Чтобы выделить несколько файлов, щелкните мышью по каждому из них, удерживая нажатой клавишу <Ctrl>. Чтобы выделить в списке несколько файлов, расположенных подряд, щелкните мышью по верхнему, а затем, удерживая нажатой клавишу <Shift>, — по нижнему (можно наоборот).

Для того чтобы очистить список, нажмите на кнопку **“Убрать все”**.

і В список можно добавлять не только файлы, но и каталоги. Если отбуксировать в список каталог, то в архив будут добавлены все находящиеся в нем файлы. Если Вы хотите, чтобы при этом в архив попали еще и файлы, расположенные в подкаталогах добавляемого каталога, установите во включенное состояние переключатель **“Включать файлы в поддиректориях”**.

§ Нажмите на кнопку **“Далее >”**.

4. В диалоговом окне **“Сохранение файлов - шаг 3 из 3”** в верхнем поле ввода наберите имя файла архива (включая полный путь к нему). Диск и каталог для размещения архива можно выбрать в диалоговом окне, которое открывается при нажатии на кнопку **“Выбрать”**.

§ В многострочном поле ввода наберите, если нужно, комментарий к создаваемому архиву.

§ Нажмите на кнопку **“Готово”**.

5. Создание архива может потребовать некоторого времени. Пока этот процесс не завершится, на экране будет находиться диалоговое окно **“Резервное копирование”**. Вы можете прервать создание архива, нажав на кнопку **“Отмена”** в этом окне. После того как архив будет создан, кнопка изменит свое название на **“ОК”**. Нажмите на кнопку **“ОК”**.

7.5 Распаковка защищенного архива

2

Для того чтобы извлечь файлы из зашифрованного архива,

1. Выберите в меню **“Резервное копирование”** пункт **“Восстановить данные”** или

нажмите на кнопку  в панели инструментов.

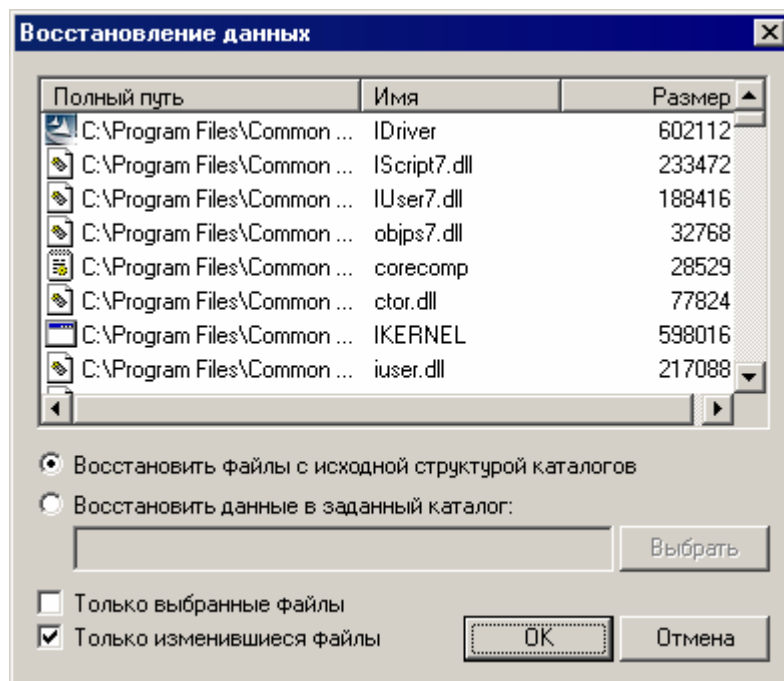
2. В стандартном диалоговом окне **“Открытие файла”** выберите файл архива, из которого Вы хотели бы извлечь файлы.
3. В диалоговом окне **“Восстановление данных”**

§ Если Вы хотите извлечь из архива только некоторые находящиеся в нем файлы, выделите их в списке и установите во включенное состояние переключатель **“Только выделенные файлы”**. О том, как выделить в списке несколько файлов, написано в предыдущем пункте.

§ Если Вы хотите, чтобы находящиеся в архиве файлы были записаны в исходные каталоги (иными словами, туда, откуда они были скопированы в архив), установите во включенное состояние кнопку выбора **“Восстановить файлы с исходной структурой каталогов”**.

§ Если Вы хотите записать файлы в другой каталог, установите во включенное состояние кнопку выбора **“Восстановить данные в заданный каталог”**. Затем наберите в расположенном рядом поле ввода полный путь к тому каталогу, в который Вы хотите поместить файлы из архива. Каталог можно выбрать в диалоговом окне, которое открывается при нажатии на кнопку **“Выбрать”**.

§ Бывает, что при записи файлов в исходные каталоги имеет смысл распаковывать только те файлы, которые со времени помещения в архив их резервных копий изменились. Например, если у Вас “испортилась” база данных, Вы можете заменить “испортившиеся” файлы их резервными копиями. Для того чтобы распаковать только изменившиеся файлы, установите во включенное состояние переключатель **“Только изменившиеся файлы”**.



4. Нажмите на кнопку **“OK”**.

Глава 8 Настройка Zdisk


8.1 Общие параметры системы

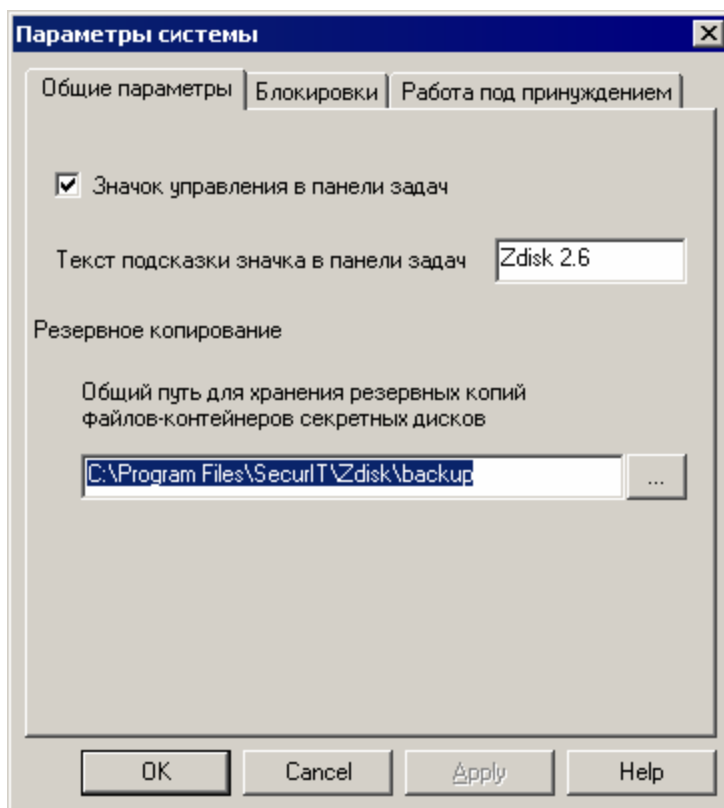
! Изменение параметров системы возможно только при подключенном электронном идентификаторе. При изменении параметров, после нажатия кнопки **“ОК”** или **“Применить”**, поиск идентификатора может занять некоторое время.

2

Для настройки общих параметров системы

1. Выберите в меню **“Диск”** пункт **“Параметры системы”**.
2. Вы увидите закладку **“Общие параметры”**. На ней:

- § Если Вы хотите, чтобы значок  не отображался в правой части панели задач Windows, установите переключатель **“Значок управления в панели задач”** в выключенное состояние. Здесь же в поле ввода **“Текст подсказки значка в панели задач”** Вы можете указать текст, который будет появляться в качестве подсказки при наведении на значок курсора мыши. Это может быть удобно для маскировки использования системы Zdisk от посторонних пользователей.
- § В поле ввода **“Общий путь для хранения резервных копий файлов-контейнеров секретных дисков”** введите путь к каталогу, в котором будут сохраняться резервные копии файлов-контейнеров (подробнее см. п. 7.2).



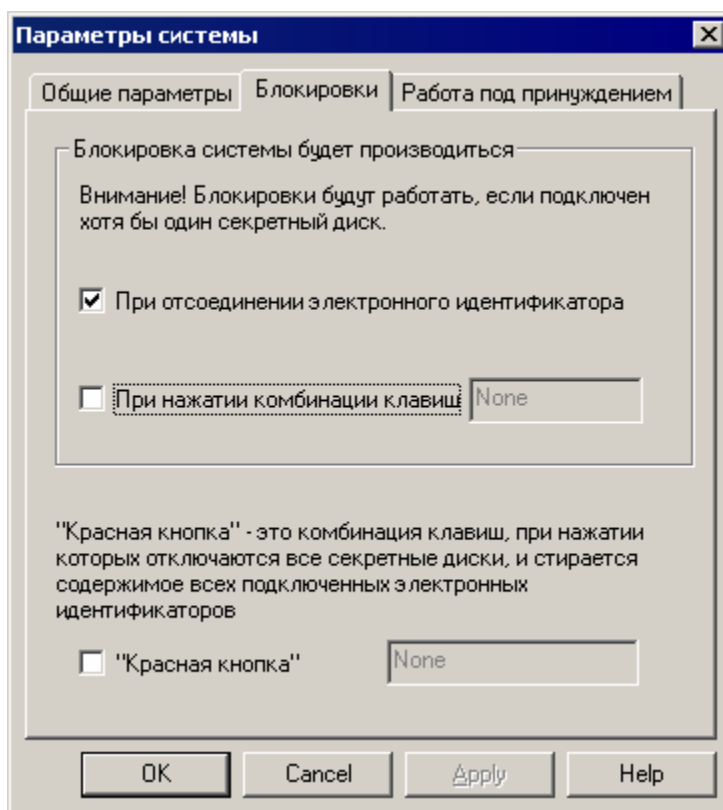
8.2 Настройка блокировки консоли

2

Для ввода параметров блокировки консоли (см. п. 4.5)

1. Выберите в меню **“Диск”** пункт **“Параметры системы”**.

2. В диалоговом окне **“Параметры системы”** переключитесь на закладку **“Блокировка”**. На этой закладке выберите ситуации, в которых система должна блокировать консоль рабочей станции.
 - a. Если Вы хотите, чтобы режим блокировки включался при отсоединении электронного идентификатора, установите во включенное состояние переключатель **“При отсоединении электронного идентификатора”**.
 - b. Если Вы хотите, чтобы режим блокировки включался при нажатии некоторой комбинации клавиш, установите во включенное состояние переключатель **“При нажатии комбинации клавиш”**. Затем перейдите (например, щелкнув мышью) в поле ввода и нажмите нужную комбинацию клавиш. Если Вы хотите, чтобы блокировка системы происходила при нажатии клавиш <Ctrl>+<Alt>+<L>, нажмите эту комбинацию клавиш.



3. Нажмите на кнопку **“ОК”**.

8.3 Работа под принуждением

В системе Zdisk предусмотрена возможность задать для каждого секретного диска пароль для входа под принуждением. Вы можете использовать его, если кто-то, угрожая Вам, потребует назвать (или ввести) пароль доступа к диску с конфиденциальными данными. После ввода пароля для входа под принуждением система на некоторое достаточно короткое время подключит диск, а затем сотрет записанный в электронном идентификаторе личный ключ пользователя (если соответствующая опция была включена) и будет симулировать сбой операционной системы. Даже если Ваши противники поймут, что их провели, и заставят Вас назвать настоящий пароль, они не смогут получить доступ к секретным дискам — личный ключ уже будет уничтожен.

i Пароль для входа под принуждением задается при создании секретного диска. Пароль для входа под принуждением возможно изменить в свойствах секретного диска на закладке **“Действия”** (см. п. 5.1).

2 Для ввода параметров работы под принуждением:

1. Выберите в меню **“Диск”** пункт **“Параметры системы”**.
2. В диалоговом окне **“Параметры системы”** переключитесь на закладку **“Работа под принуждением”**. На этой закладке в группе **“Действие при подключении под принуждением”** задайте характер сбоя, который система будет симулировать после ввода пароля для входа под принуждением.

i Для того чтобы при вводе пароля для входа под принуждением содержимое электронного идентификатора действительно уничтожалось, необходимо установить во включенное состояние переключатель **“Уничтожить содержимое электронного идентификатора”**.

3. Нажмите на кнопку **“ОК”**.

8.4 Настройка **“Красной кнопки”**

Функция **“Красная кнопка”** позволяет в критической ситуации моментально отключить все секретные диски и очистить память электронного идентификатора при нажатии заданной комбинации клавиш. При этом могут быть потеряны несохраненные данные, например открытые документы Microsoft Word, что, однако, в иных ситуациях может оказаться меньшим из зол.

! Пользоваться **“Красной кнопкой”** рекомендуется только в случае серьезной опасности, поскольку восстановление возможности доступа к секретным дискам потребует времени.

М Если у Вас нет резервных копий рабочих ключей секретных дисков или Вашего личного ключа (см. гл. 6), использование **“Красной кнопки”** приведет к практически необратимой потере всей информации, хранящейся на секретных дисках.

2 Для включения режима **“Красной кнопки”** и назначения соответствующей комбинации клавиш

1. Выберите в меню **“Диск”** пункт **“Параметры системы”**.
2. В диалоговом окне **“Параметры системы”** переключитесь на закладку **“Блокировка”**.
3. Установите во включенное состояние переключатель **“Красная кнопка”**.
4. Перейдите в поле ввода и нажмите нужную комбинацию клавиш. Например, если Вы хотите, чтобы **“Красная кнопка”** срабатывала при нажатии клавиш **<Ctrl>+<Alt>+<8>**, нажмите эту комбинацию клавиш.

! Заданная в качестве **“Красной кнопки”** комбинация клавиш будет действовать при работе со всеми приложениями, поэтому будьте особенно внимательны при назначении данной комбинации клавиш. Избегайте назначения слишком простых комбинаций клавиш, так как это может привести к случайному нажатию, а, следовательно, к потере доступа ко всей информации, находящейся на подключенных секретных дисках.

! Также не следует назначать в качестве **“Красной кнопки”** комбинации клавиш, используемые по умолчанию операционной системой Windows или другими приложениями. Например, **<Ctrl>+<A>** или **<Ctrl>+<C>**.

Для заметок

Для заметок