

**Zserver**

Версия 4.0  
для Windows 2000/2003

Система защиты корпоративных серверов

**Руководство администратора**

**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 Zserver 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 Zserver и ее документацию принадлежит компании SecurIT, © с 2001 г. по настоящее время. Все права защищены.

SecurIT является 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: (495) 208-9141

Тел./Факс: (495) 208-9784

E-mail: [info@securit.ru](mailto:info@securit.ru)

HTTP: [www.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

<b>ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ.....</b>	<b>3</b>
<b>ВВЕДЕНИЕ.....</b>	<b>8</b>
Краткий обзор глав.....	8
Условные обозначения.....	8
Порядок оказания технической поддержки.....	9
<b>ГЛАВА 1    ОПИСАНИЕ ZSERVER.....</b>	<b>10</b>
1.1    Для чего служит ZSERVER.....	10
1.2    Комплект поставки.....	10
1.2.1    Виды дистрибутивов.....	11
1.2.2    Конфигурация Zserver.....	11
1.3    Требования к программно-аппаратному обеспечению.....	11
1.4    Общая структура системы.....	12
1.5    Сервер защиты данных.....	12
1.6    Консоль управления.....	13
1.6.1    Интерфейс консоли.....	13
1.6.2    Смарт-карта и PIN-код.....	13
1.6.3    Кворум ключей шифрования.....	14
1.7    Средства подачи серверу сигнала тревоги.....	15
<b>ГЛАВА 2    УСТАНОВКА КОМПОНЕНТОВ СИСТЕМЫ.....</b>	<b>16</b>
2.1    Установка аппаратных средств.....	16
2.1.1    Устройство для работы со смарт-картами.....	16
2.1.2    Лицензионный ключ защиты.....	16
2.1.3    «Красная кнопка».....	16
2.2    Установка программного обеспечения ZSERVER.....	16
<b>ГЛАВА 3    НАЧАЛО РАБОТЫ С ZSERVER.....</b>	<b>19</b>
3.1    Консоль управления.....	19
3.2    Соединение с сервером.....	19
3.3    Подготовка ключа шифрования.....	21
3.3.1    Генерация ключа.....	21
3.3.2    Смена PIN-кода смарт-карты.....	22
3.3.3    Загрузка ключа.....	23
3.4    Зашифровывание данных.....	24
3.4.1    Зашифровывание раздела.....	24
3.4.2    Шифрованное форматирование диска.....	26
3.5    Смена паролей по умолчанию пользователей ZSERVER.....	26
3.6    Настройка сигнала тревоги.....	27
<b>ГЛАВА 4    ЭКСПЛУАТАЦИЯ ZSERVER.....</b>	<b>31</b>
4.1    Загрузка ключа и открытие диска.....	31
4.2    Закрытие диска и выгрузка ключа шифрования.....	31
4.3    Подача сигнала тревоги.....	32
4.4    Управление общим доступом.....	33
4.4.1    Добавление общей папки.....	35
4.4.2    Изменение параметров общей папки.....	35
4.4.3    Удаление общей папки.....	36
4.4.4    Назначение прав управления общими ресурсами.....	36
4.5    Настройка параметров работы ZSERVER.....	37
4.5.1    Ведение журнала операций.....	38
4.5.2    Задание нестандартного сетевого порта.....	38
4.5.3    Просмотр конфигурации Zserver.....	39
<b>ГЛАВА 5    ОБСЛУЖИВАНИЕ ZSERVER.....</b>	<b>40</b>
5.1    Управление ключами шифрования.....	40
5.2    Одновременная работа с несколькими серверами.....	40
5.3    Расшифровывание дисков.....	42

5.4	ПЕРЕШИФРОВАНИЕ ДИСКОВ .....	42
5.5	УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ .....	43
5.6	УДАЛЕНИЕ И ОБСЛУЖИВАНИЕ УСТАНОВЛЕННЫХ КОМПОНЕНТОВ .....	45
5.7	ОБНОВЛЕНИЕ ZSERVER .....	45
<b>ПРИЛОЖЕНИЕ А. ДЕМО-ВЕРСИЯ СИСТЕМЫ ZSERVER.....</b>		<b>46</b>
<b>ПРИЛОЖЕНИЕ В. ОСОБЕННОСТИ РАБОТЫ С ДИНАМИЧЕСКИМИ ДИСКАМИ.....</b>		<b>47</b>

## ВВЕДЕНИЕ

Целью данного Руководства является описание всех существующих компонентов программно-аппаратного комплекса Zserver для того чтобы максимально полно и правильно использовать возможности системы.

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

Система Zserver предназначена для защиты информации, хранимой и обрабатываемой на серверах, работающих под управлением операционных систем Windows 2000/2003.

Система Zserver разработана исключительно на базе документированных возможностей, изложенных в соответствующих материалах компании Microsoft. В руководстве не содержится информация по администрированию сетей Microsoft Windows и работе с серверами Microsoft Windows 2000/2003.

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

Система Zserver 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. Описание Zserver** – содержит общие сведения, описывающие принципы работы и архитектуру программно-аппаратного комплекса Zserver, а также возможности системы, требования к оборудованию и программному обеспечению сервера.

**Глава 2. Установка Zserver** – пошаговое описание процесса подключения аппаратных средств и установки системы Zserver.

#### **Глава 3. Начало работы с Zserver**

В этой главе изложена последовательность операций, необходимых для подготовки Zserver к эксплуатации, таких как: генерация ключа, зашифровывание разделов и т.д.

**Глава 4. Эксплуатация Zserver** – содержит сведения о повседневных действиях с Zserver: загрузка ключа, открытие раздела и прочие.

**Глава 5. Обслуживание Zserver** – работа с ключами шифрования и операции с зашифрованными разделами.




**Приложения.** Особенности демонстрационной версии и работа с динамическими дисками.

### **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
• Перечисление	Пункт перечисления
1. Выберите в меню...	Шаг процедуры, выполняемой пользователем
 На заметку	Полезная информация, на которую желательно обратить внимание
 Важная информация	Информация, на которую мы рекомендуем обратить особое внимание
 Внимание!	Предупреждение об опасности потери данных, выхода оборудования из строя и т. п.
«Server»	Названия меню, пунктов меню, окон, их элементов и т. п.

### **Порядок оказания технической поддержки**

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

Телефон: (495) 208-8900

Факс: (495) 208-9784

E-mail: [support@securit.ru](mailto:support@securit.ru)

HTTP: [www.securit.ru](http://www.securit.ru)

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

- 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 Zserver;
- точную последовательность Ваших действий, вызывающих возникновение проблемы.

# Глава 1 Описание Zserver

## 1.1 Для чего служит Zserver

Zserver работает по принципу "прозрачного" шифрования разделов жестких дисков на сервере. Система автоматически, в online режиме, зашифровывает данные при их записи на носитель и расшифровывает при чтении с него. Это обеспечивает хранение данных на носителе в зашифрованном виде и невозможность использования ее без ключа шифрования даже при изъятии сервера или носителя.

Шифрование в режиме online не требует каких-либо изменений в работе пользователей и приложений, а современные стойкие алгоритмы шифрования с ключом от 128 бит надежно защищают данные от посторонних взоров.

Возможность использования кворума ключей шифрования позволяет свести к минимуму человеческий фактор, а сигнал "тревога", посланный с любого компьютера или мобильного устройства из любой точки мира, мгновенно сделает зашифрованные данные недоступными.

Удобное и интуитивно понятное управление комплексом осуществляется с помощью единой консоли, которая может работать на любой рабочей станции в локальной сети или через Интернет.

Благодаря специальной оптимизации алгоритмов и процедур, работа системы оказывает минимальное, обычно не различимое в реальной работе воздействие на производительность системы. Технология защищенных ресурсов общего доступа гарантирует невозможность получения неавторизованного доступа к данным в процессе работы и позволяет вообще отключить сетевой доступ к данным в случае, если они используются только для сервера приложений.

Высокая надежность системы и минимальный риск потери данных даже в случае системных сбоев обеспечиваются за счет таких возможностей, как откат и восстановление шифрования, и обнаружение испорченных секторов на диске.

В зависимости от конфигурации Zserver могут быть доступны дополнительные возможности системы:


- Управление общим доступом – контроль над общими ресурсами, расположенными на зашифрованном разделе файл-сервера;
- Поддержка MS Cluster Services под управлением Windows 2000/2003 Server;
- Модуль Script Pack - вызов сценариев при событиях открытия, закрытия дисков или сигнала тревоги;
- Использование алгоритма шифрования ГОСТ 28147-89.

## 1.2 Комплект поставки

В комплект поставки системы Zserver входит:

- компакт-диск с дистрибутивом системы;
- данная документация;
- лицензионный ключ защиты для LPT или USB порта;
- устройство для работы со смарт-картами ACR ACS-30U;
- 2 микропроцессорные смарт-карты ACOS1;

- устройство "Красная кнопка" для COM-порта;
- рекламно-информационные материалы.

 В отдельные комплекты вместо смарт-карт и устройства для работы с ними могут входить USB-идентификаторы. В таком случае обратитесь к дополнительному документу

### 1.2.1 Виды дистрибутивов

Система Zserver поставляется либо как отдельный продукт, либо в комплекте с системой защиты резервных копий (Zserver + Zbackup).

Таким образом, возможны два варианта установки:


- Установка только Zserver;
- Установка Zserver совместно с Zbackup (Zserver + Zbackup).

В данном руководстве описывается установка и приемы работы в основном с Zserver, хотя многое также относится и к Zbackup. В случае установки дистрибутива **«Zserver + Zbackup»** проконсультируйтесь также с **«Руководством Администратора Zbackup»**.

### 1.2.2 Конфигурация Zserver

В зависимости от варианта приобретенной системы Вам могут быть доступны следующие возможности:

- удаленное администрирование – возможность, позволяющая удаленно управлять сервером по протоколу TCP/IP с других рабочих станций сети;
- работа со стримерами (в случае поставки комплекта Zserver + Zbackup);
- управление общими ресурсами (Sharing);
- поддержка MS Cluster Services;
- поддержка алгоритма шифрования ГОСТ 28147-89;
- поддержка вызова сценариев (с использованием Script Pack);
- демонстрационная версия<sup>1</sup>.

 Конфигурация системы хранится в памяти лицензионного ключа и отображается в консоли управления в настройках сервера, на вкладке **«Лицензия»**. См п. 4.5.3 Просмотр конфигурации Zserver.

## 1.3 Требования к программно-аппаратному обеспечению

Требования к аппаратной части и программному обеспечению различны для каждого компонента Zserver и указаны в таблице 2:

Таблица 2. Минимальные системные требования Zserver

Аппаратные и программные средства	Компоненты системы Zserver		
	Сервер защиты	Консоль управления	Система подачи сигнала тревоги
<b>Процессор</b>	Pentium или выше		
<b>Оперативная память</b>	128 Мб		32 Мб
<b>Порты</b>	LPT (не обязательно)	Свободный USB	Свободный COM

<sup>1</sup> Ограничения демонстрационной версии описываются в Приложении А

	свободный) или USB		
<b>ОС</b>	Windows 2000 SP4 /2003	Windows 2000 SP4/ XP / 2003	Windows 2000 SP4/ XP / 2003
<b>Прочие программные средства</b>	Сетевой протокол TCP/IP		

**И** В файле readme.txt, находящемся в корневом каталоге установочного компакт-диска, содержится наиболее свежая информация о последней версии Zserver. Обязательно прочтите этот файл, чтобы удостовериться в том, что Ваше оборудование и программное обеспечение удовлетворяет требованиям совместимости с системой Zserver.

## 1.4 Общая структура системы

Zserver состоит из трех основных модулей:

1. Сервер защиты данных;
2. Консоль управления сервером;
3. Модуль подачи сигнала тревоги.

Взаимодействие этих компонентов осуществляется по технологии Клиент-Сервер, с использованием протокола TCP/IP. Соединение клиентской части с сервером является защищенным, поскольку для каждой сессии по специальному алгоритму каждой из сторон генерируется уникальный ключ шифрования. Данным ключом шифруется весь обмен данными между модулями системы, что исключает возможность перехвата информации путем анализа сетевого трафика. Такая технология позволяет удаленно управлять системой Zserver через Интернет без каких-либо дополнительных средств защиты трафика.

## 1.5 Сервер защиты данных

Ядро системы – *Сервер защиты данных* – устанавливается на сервер с защищаемой информацией и осуществляет «прозрачное» шифрование данных. После установки ядра системы автоматически запускаются системные драйвера и служба «SecurIT Zkernel», которая непосредственно реализует операции с сервером по инструкциям, передаваемым консолью управления.

Основные компоненты сервера защиты данных:

- драйвер, реализующий перехват обращений к дискам;
- криптоядро, реализующее шифрование данных;
- служба, осуществляющая операции с сервером;
- набор системных библиотек;
- драйвер для работы с ключом защиты.

**И** К компьютеру, где установлен данный компонент, должен быть подсоединен лицензионный ключ. Он предназначен для защиты ПО Zserver от тиражирования и подсоединяется к LPT или USB-порту (в зависимости от комплекта поставки) того компьютера, где установлен сервер защиты. Он также содержит информацию о конфигурации системы. В отсутствие ключа система работать не будет.

## 1.6 Консоль управления

Управление серверным модулем и выполнение необходимых операций с системой Zserver выполняет консоль управления. Этот модуль является основным средством для управления доступом к дискам, операций с ключами и прочими средствами Zserver.

Данный модуль может быть размещен на любом компьютере, связанном с сервером защиты через локальную сеть или через Интернет по протоколу TCP/IP.

- ! Даже в том случае, если оба компонента установлены непосредственно на одном компьютере, наличие протокола TCP/IP обязательно.

Для разграничения полномочий по управлению системой Zserver существуют специальные средства авторизации пользователей (см. п. 5.5 Управление пользователями). Для установления соединения с сервером защиты необходимо предъявить имя пользователя и его пароль.

### 1.6.1 Интерфейс консоли

В верхней части консоли управления находится горизонтальное меню и панель инструментов для выполнения операций с системой.

В левой части Консоли находится древовидный список, состоящий из основных разделов для каждого сервера, а в правой части отображается подробная информация о каждом разделе.

- i Для каждого элемента дерева и списка существует собственное контекстное меню с набором команд, подходящих к этому объекту. Команда, выделенная жирным шрифтом, вызывается при двойном щелчке мышью по объекту.

### 1.6.2 Смарт-карта и PIN-код

Для надежного и безопасного хранения ключей шифрования системой Zserver используются смарт-карты ACOS1. На одной смарт-карте возможно хранить до 16 ключей шифрования. При записи ключей с разными именами они будут сохраняться в различные ячейки памяти смарт-карты. Если при чтении ключа на смарт-карте находится более одного ключа, то система предложит выбрать один из них.

При работе со смарт-картой необходимо ввести PIN-код, состоящий из 8 произвольных символов. Правильность PIN-кода контролируется операционной системой смарт-карты. Производитель смарт-карты гарантирует невозможность получения доступа к информации в ее памяти без корректной PIN-аутентификации.


-  В случае четырехкратного неправильного ввода PIN-кода подряд карта блокируется, что на практике означает невозможность ее дальнейшего использования.

Таким образом, ключи шифрования, находящиеся на этой смарт-карте, будут потеряны без возможности их дальнейшего восстановления.

- ! Смарт-карты, входящие в комплект поставки системы, имеют PIN-код по умолчанию **securent** (буквы нижнего регистра).

При работе со смарт-картами ACOS реализована возможность ввода PIN-кода «под принуждением». Вы можете использовать его, если кто-то, угрожая Вам, потребует назвать (или ввести) PIN-код доступа к смарт-карте с ключами шифрования. PIN-код «под принуждением» представляет собой обратную последовательность символов обыкновенного PIN. К примеру, для PIN по умолчанию – **securent**, PIN-код «под принуждением»: **stneruces**. При смене PIN для смарт-карты соответственным образом изменится и PIN-код «под принуждением».

После ввода PIN-кода **«под принуждением»** система удалит все записанные ключи шифрования из памяти смарт-карты и выведет соответствующую ошибку.


 После таких действий, даже введя правильный PIN, получить доступ к ключам шифрования будет невозможно. Таким образом, информация, зашифрованная этими ключами (при отсутствии резервных копий ключей), будет уничтожена.

! В операционной системе смарт-карты ACOS отсутствует функциональность для входа под принуждением. В связи с этим, данная возможность реализуется программно одним из модулей системы Zserver. Если злоумышленники будут знать PIN-код для входа под принуждением и воспользуются при этом сторонними утилитами для работы со смарт-картами ACOS, то при вводе этого PIN-кода смарт-карта будет возвращать ошибку, а при вводе PIN-кода **«под принуждением»** наоборот, то есть, правильного PIN-кода, злоумышленник получит доступ к памяти карты. Поэтому PIN-код **«под принуждением»** безопасно использовать только в том случае, если у пользователя есть возможность самому ввести его в ответ на соответствующее приглашение системы Zserver. Если PIN-код карты, даже в виде PIN-кода для входа под принуждением, станет известен злоумышленникам, они могут получить доступ к памяти карты.

! Смарт-карта ACOS позволяет пользователю сделать 8 попыток ввода неправильного PIN-кода до того, как смарт-карта будет заблокирована. В связи с описанной выше возможностью ввода PIN-кода под принуждением, при вводе неправильного PIN-кода, он будет проверяться картой два раза. Таким образом, с использованием ПО Zserver пользователь будет иметь всего 4 попытки ввода PIN-кода.



В системе Zserver предусмотрена возможность смены PIN-кода. Смена PIN-кода подробно описана в п. 3.3.2 Смена PIN-кода смарт-карты.

Работа со смарт-картам осуществляется через PC/SC интерфейс, предоставляемый ОС Windows. В комплект данной поставки входит PC/SC-совместимое устройство для работы со смарт-картами ACS ACR30U, подключаемое через USB-интерфейс.

 Возможно осуществлять работу со смарт-картами с помощью любых PC/SC совместимых считывателей смарт-карт.

### 1.6.3 Кворум ключей шифрования

Zserver поддерживает создание и работу со специальными наборами ключей. Во время генерации ключа шифрования (см. п. 3.3.1 Генерация ключа) можно включить опцию **«Использовать кворум ключей»** и указать общее количество ключей и количество ключей для кворума. Кворум – это то число от общего количества ключей, которое необходимо и достаточно для формирования из них ключа шифрования. Например, если Вы выбрали общее число ключей - 4, а кворум - 2, то любые два ключа из этого набора, будучи загруженными в память сервера, сформируют полноценный ключ шифрования. При этом порядок загрузки ключей роли не играет.

В консоли неполные кворумы отображаются значком , и при этом в скобках указано, сколько ключей загружено и сколько является кворумом. Если значок ключа выглядит , это значит, что кворум достигнут, и Zserver может работать со сформированным ключом шифрования.

## 1.7 Средства подачи серверу сигнала тревоги

Для мгновенной блокировки защищаемой информации в системе реализован отдельный модуль подачи сигнала тревоги. После подачи сигнала тревоги защищаемые логические диски становятся полностью недоступными либо происходит перезагрузка сервера.

При этом все ключи шифрования удаляются из оперативной памяти, а доступ к зашифрованным дискам блокируется. Для возобновления нормальной работы с защищенными разделами необходимо перезагрузить систему и повторно ввести ключи шифрования. Кроме этого, по сигналу тревоги могут быть запущены ранее написанные и зарегистрированные сценарии из состава Script Pack.



Реакция системы на сигнал тревоги может вызвать потерю данных в открытых файлах. Не забывайте периодически сохранять данные. Для уменьшения риска порчи информации используйте опцию перезагрузки при получении сигнала тревоги (см п. 3.6 Настройка сигнала тревоги).

Подача сигнала тревоги осуществляется по протоколу TCP/IP, используя механизмы, аналогичные консоли управления. Модуль тревоги может быть установлен на любом компьютере, связанном с сервером защиты через локальную сеть или через Интернет по протоколу TCP/IP.

Подача сигнала тревоги может быть инициирована либо нажатием **«Красной кнопки»**, подключенной к СОМ-порту любой рабочей станции, либо двойным щелчком по значку модуля в системной панели. Также сигнал тревоги можно вызвать, запустив приложение ssagent.exe с параметром -a.

Основные компоненты модуля:

- системная служба, осуществляющая опрос **«Красной кнопки»**;
- приложение для управления службой;
- приложение, осуществляющее настройку модуля;
- набор системных библиотек.

## Глава 2 Установка компонентов системы

### 2.1 Установка аппаратных средств

#### 2.1.1 Устройство для работы со смарт-картами

Устройство необходимо установить на тот компьютер, на котором будет производиться администрирование Zserver посредством консоли управления. Подключение устройства и установка драйвера производится согласно отдельному документу **«Руководство по установке устройства работы со смарт-картами»**.

#### 2.1.2 Лицензионный ключ защиты

Установка ключа производится непосредственно на сервер, где планируется зашифровывать разделы с данными. Поскольку драйвер ключа устанавливаются автоматически в процессе инсталляции Zserver, никаких дополнительных приложений запускать не требуется.

- Если у Вас ключ для LPT порта, подключите его до запуска установки Zserver.
- Если у Вас ключ для USB порта, то подключите его во время установки Zserver в тот момент, когда программа этого потребует. См шаг 6 п. 2.2 Установка программного обеспечения Zserver.

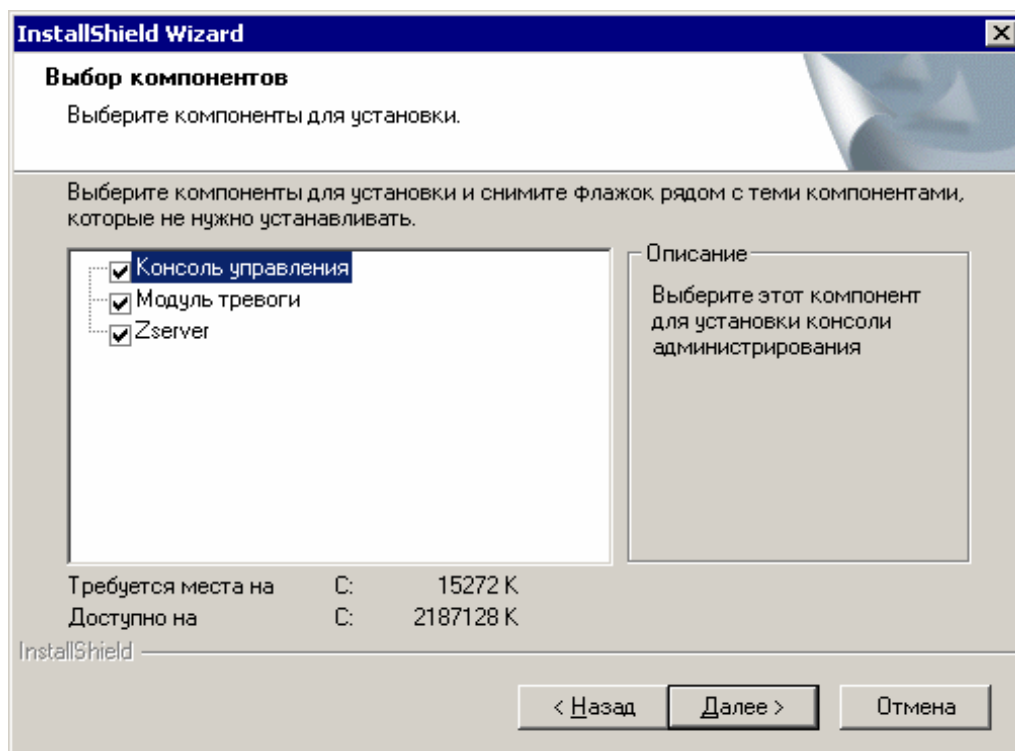
#### 2.1.3 «Красная кнопка»

Установка **«красной кнопки»** заключается в подсоединении ее к свободному 9-штырьковому COM-порту. Специального ПО для работы с ней не требуется.

### 2.2 Установка программного обеспечения Zserver

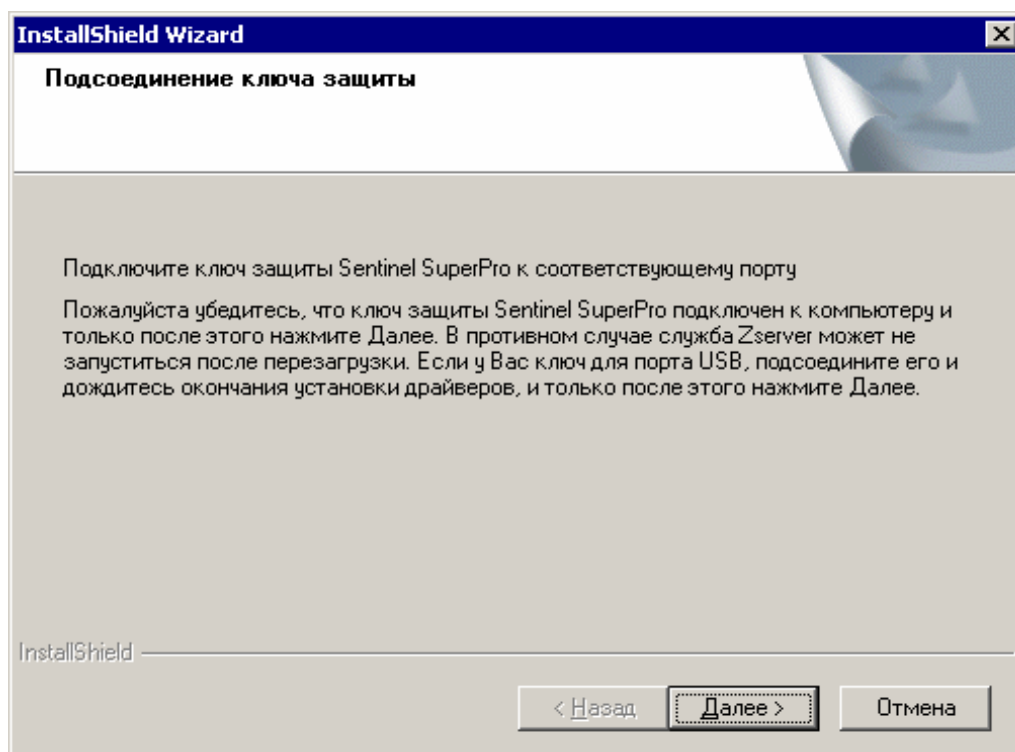
1. Запустите файл **SETUP.EXE** из папки **SETUP** на дистрибутивном диске. Мастер установки проведет необходимые предварительные операции и отобразит приглашающее окно;
2. Нажмите кнопку **«Далее»** и ознакомьтесь с Лицензионным соглашением. Если Вы согласны с предлагаемыми условиями, нажмите **«Да»**;
3. Укажите каталог для установки файлов Zserver или воспользуйтесь папкой по умолчанию. Нажмите **"Далее"**;
4. Выберите те модули системы, которые были запланированы к установке на данном компьютере.





**i** Если Вы запустили установку в среде Windows 9x/Me, Вам будут доступны только компонент «Модуль тревоги».

- Для продолжения нажмите "Далее";
5. Перед началом процесса установки убедитесь, что в поле «Текущие настройки» указана соответствующая информация и нажмите «Далее»;
6. Программа установки скопирует и зарегистрирует все необходимые файлы. После чего, если вы устанавливали какой-либо из компонентов сервера защиты ("Zserver" и/или «Zbackup»), Вам будет предложено подсоединить ключ защиты к порту USB и затем перезагрузить операционную систему;



! Без перезагрузки ОС не запустятся все компоненты сервера защиты. Поэтому перезагрузка после установки является обязательной.

7. После перезагрузки компьютера программа установки завершит все необходимые операции, и система Zserver будет готова к работе.

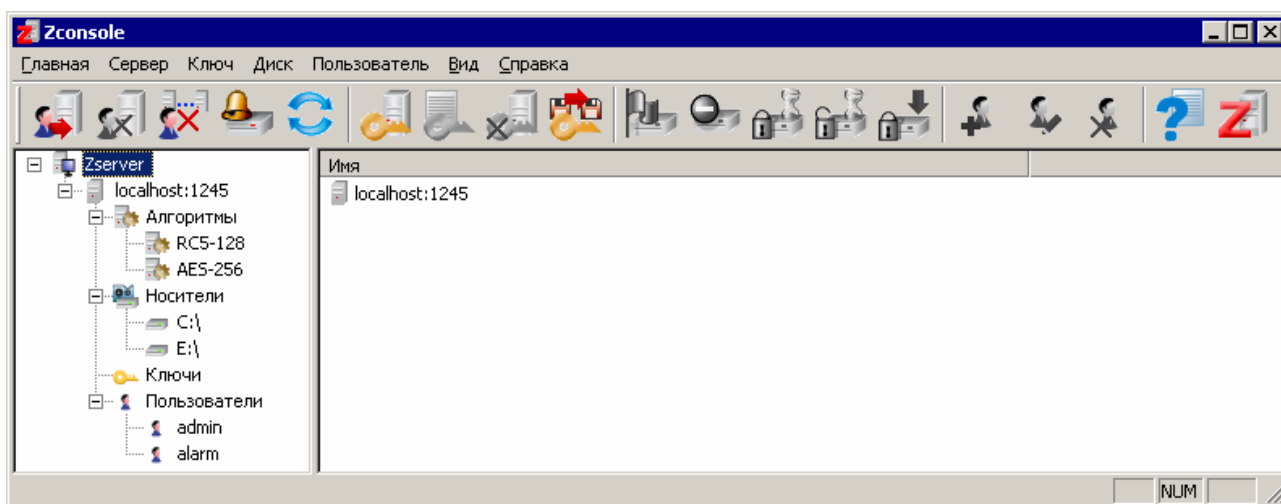
## Глава 3 Начало работы с Zserver

### 3.1 Консоль управления

Для администрирования системы Zserver предназначена *консоль управления*. Данное приложение может использоваться для управления не только Zserver, но и другими продуктами компании SecurIT.



Подробное описание консоли находится в п. 1.6 Консоль управления.

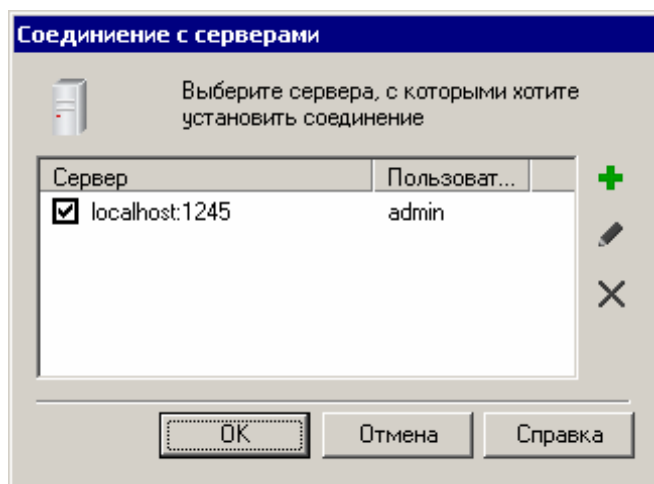



Консоль управления устанавливается в каталог «Program Files\Common Files\SecurIT» и запускается из меню «Пуск» – «Программы» – «SecurIT».

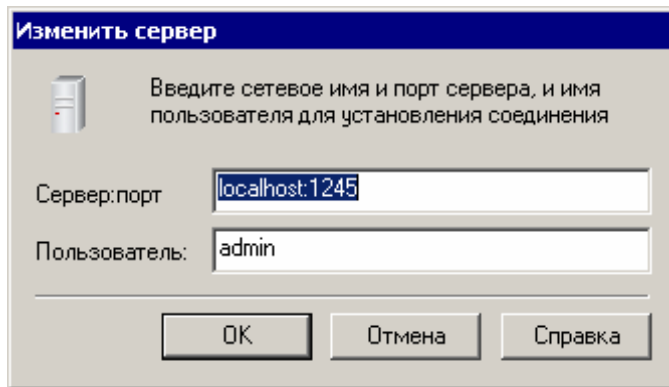
### 3.2 Соединение с сервером

Работа с Zserver начинается с установления соединения. Для этого:

1. Выберите команду «Начать сеанс» в меню «Сервер» или нажмите кнопку .



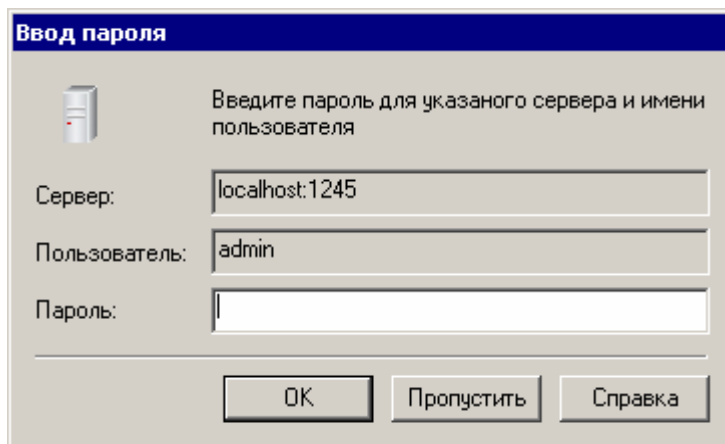
2. В появившемся диалоговом окне отобразится список серверов для установления соединения. Добавьте новый сервер с помощью кнопки  или измените текущую запись, открыв окно редактирования двойным щелчком мыши.



- В поле «**Сервер**» введите сетевое имя (или IP адрес) и через двоеточие номер порта сервера (по умолчанию – 1245), например `srv2:1245`;  
 (i) Если программа администрирования и сам сервер защиты находятся на одном компьютере, вместо имени сервера можно указать `localhost`.
- В поле «**Пользователь**» введите имя пользователя системы Zserver (по умолчанию `admin`) и нажмите «**ОК**».  
 ! В системе Zserver ведется собственная база данных пользователей, не имеющая ничего общего с пользователями ОС Windows.

Нажмите «**ОК**» в окне установки соединения.

3. Введите пароль (по умолчанию `admin`) и нажмите «**ОК**».



! Обязательно смените пароль при начале эксплуатации системы. См п. 3.5 Смена паролей по умолчанию пользователей Zserver

4. Защищенное соединение с сервером установлено.

(i) Если в Вашей сети установлено несколько систем Zserver и/или Zbackup, то консоль управления позволяет одновременно управлять ими всеми. См п. 5.2 Одновременная работа с несколькими серверами.


Для завершения сеанса работы с текущим сервером выберите пункт «**Завершить сеанс**» из меню «**Сервер**» или нажмите кнопку

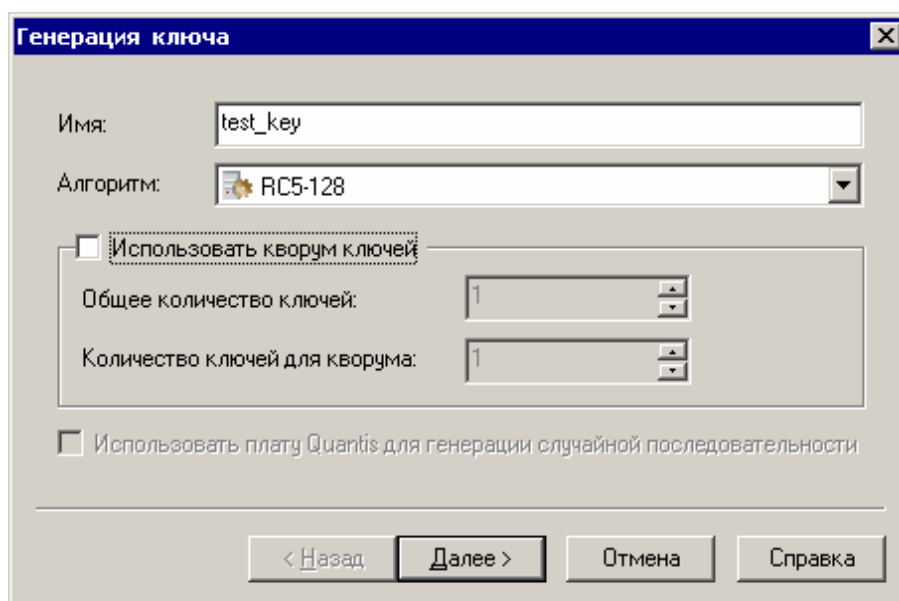
### 3.3 Подготовка ключа шифрования

Генерация ключей шифрования осуществляется непосредственно пользователем, с использованием случайных чисел. В качестве источника случайной информации выступает движение мыши. После завершения процедуры генерации ключа производится его запись на смарт-карту, защищенную PIN-кодом.

#### 3.3.1 Генерация ключа

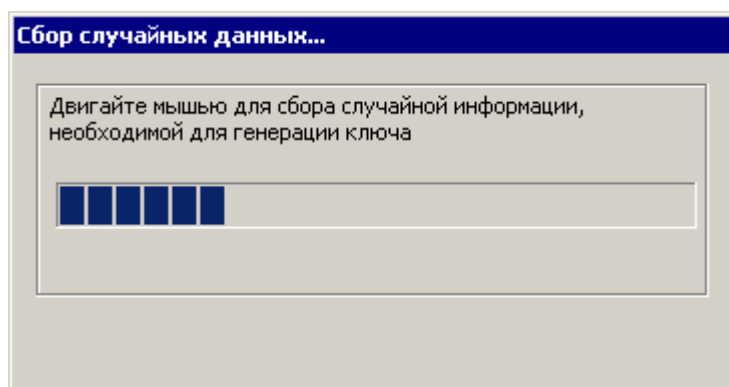
Для того чтобы создать ключ шифрования:


1. Выберите команду **"Сгенерировать ключ"** из меню **"Ключ"** или нажмите кнопку .
2. Введите имя ключа (не менее четырех символов) и выберите алгоритм шифрования, для которого будет создаваться ключ.



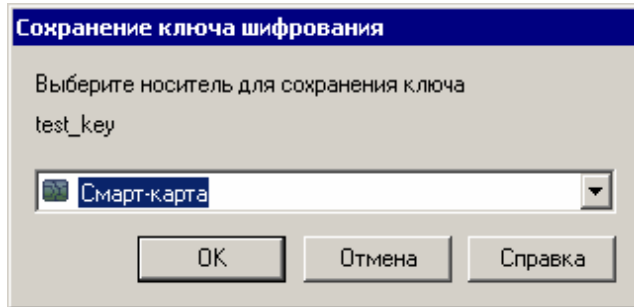
Если Вы планируете использовать кворум ключей (см п. 1.6.3 Кворум ключей шифрования), то отметьте пункт **«Использовать кворум ключей»** и введите общее число ключей и кворум. Нажмите **«Далее»**.

3. Двигайте мышью в пределах окна **«Сбор случайных данных»** для накопления массива случайных чисел.





4. Выберите носитель, на который будет сохранен ключ шифрования и нажмите **«ОК»**.  
 Носитель **«Файл»** не предназначен для хранения ключа, поскольку ключевая информация находится в нем в открытом виде. Используйте только аппаратные носители ключей. При записи ключа шифрования в файл необходимо учитывать, что эта возможность существует лишь для резервного копирования ключа шифрования на случай потери или механического повреждения карты. С этой

целью копию ключа шифрования настоятельно рекомендуется сразу сохранять на съемный носитель: дискету, флэш-диск и т.п. Если Вы сохраните ключ на жесткий диск, затем скопируете на дискету и потом удалите файл, то у заинтересованных лиц будет возможность восстановить его.




5. Введите PIN-код для выбранного носителя и нажмите **«ОК»**. PIN-код для смарт-карт по умолчанию: `securent` (буквы нижнего регистра).

 Четырехкратный ввод подряд неправильного PIN-кода приведет к блокированию смарт-карты и к невозможности получить доступ к ключам, находящимся на ней.

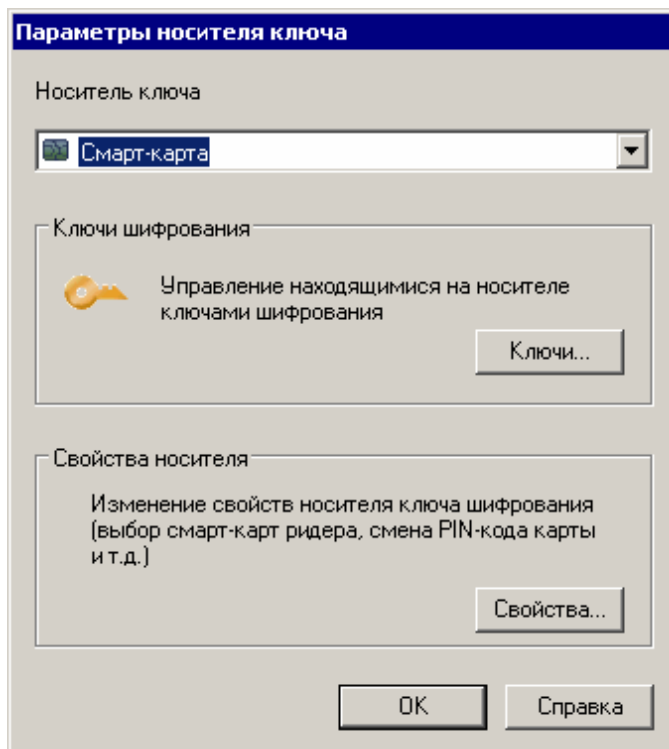
 Если на смарт-карте уже существует ключ с таким именем, система Zserver предложит его перезаписать.

6. Если Вы сгенерировали ключи для кворума, то повторите шаги 4-5 для каждого из набора ключей. Более подробно о кворуме – см п. 1.6.3 Кворум ключей шифрования

### 3.3.2 Смена PIN-кода смарт-карты

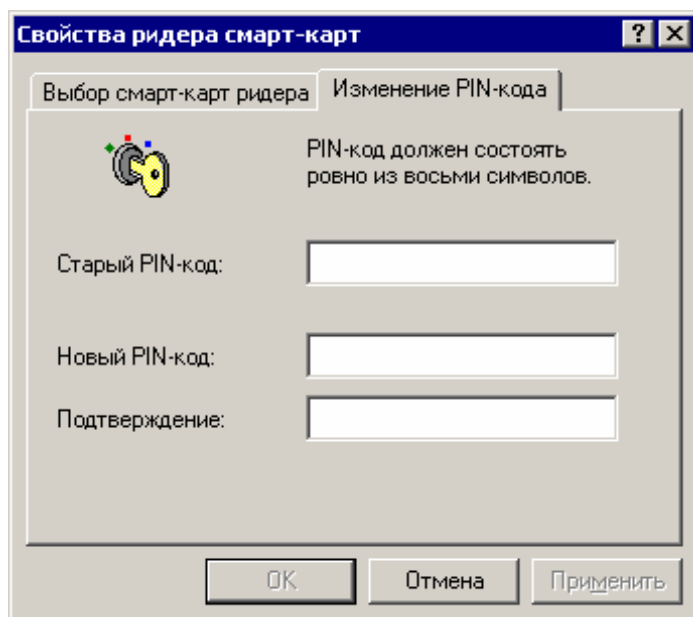
 Сразу после записи ключа на смарт-карту настоятельно рекомендуется сменить PIN-код по умолчанию. Для этого:

1. Вставьте смарт-карту в устройство для работы с ней;
2. Выберите пункт **«Параметры носителя ключа»** из меню **«Ключ»**;




3. В списке носителей ключа выберите **«Смарт-карта»** и нажмите кнопку **«Свойства»**;

Переключитесь на вкладку «Изменение PIN-кода»;




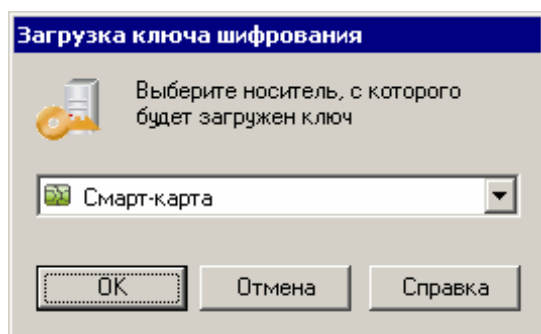
4. Введите в поля соответствующие коды и нажмите «ОК».



 PIN-код должен содержать ровно 8 символов.



### 3.3.3 Загрузка ключа


Для того чтобы загрузить ключ шифрования в память сервера:

1. Вставьте смарт-карту в устройство или подключите иной носитель с ключом шифрования;
2. Выберите команду «Загрузить ключ» из меню «Ключ» или нажмите кнопку .
3. В окне «Загрузка ключа шифрования» выберите нужный тип носителя ключа и нажмите «ОК»;



4. Введите PIN-код для выбранного носителя и нажмите «ОК»;
5.  Четырехкратный ввод подряд неправильного PIN-кода приведет к блокированию смарт-карты и к невозможности получить доступ к ключам, находящимся на ней.
5. Если в памяти смарт-карты находится несколько ключей шифрования, выберите нужное имя ключа и нажмите «ОК»;
6. Загруженный ключ отобразится в консоли управления, в разделе «Ключи» со значком .

 Если загруженный ключ входит в состав кворума ключей, то он будет отображаться в виде контура ключа () и в скобках будет указано, сколько ключей из


данного кворума уже загружено. Как только Вы загрузите необходимое число ключей шифрования, изображение ключа изменится на  и Zserver сможет использовать загруженный ключ для шифрования данных.

Более подробно о кворумах ключей шифрования можно узнать в п. 1.6.3 Кворум ключей шифрования.

### 3.4 Зашифровывание данных


После того, как Вы сгенерировали ключ шифрования и загрузили его в память сервера, можно приступить к зашифровыванию раздела (логического диска). Для этого необходимо выбрать одну из двух функций системы Zserver:

- Зашифровывание существующего раздела с данными - займет много времени, но с файлами можно будет продолжить работу во время зашифровывания;
- Быстрое шифрованное форматирование нового раздела - есть смысл использовать в том случае, если Вы только что установили новый жесткий диск либо у Вас пустой раздел без файлов.




 Не могут быть зашифрованы разделы, содержащие файлы операционной системы (включая файл подкачки и реплики Active Directory), а также загрузочный раздел.


#### 3.4.1 Зашифровывание раздела

Данная операция производит последовательное посекторное зашифровывание всего раздела, включая служебную информацию файловой системы и свободное место.

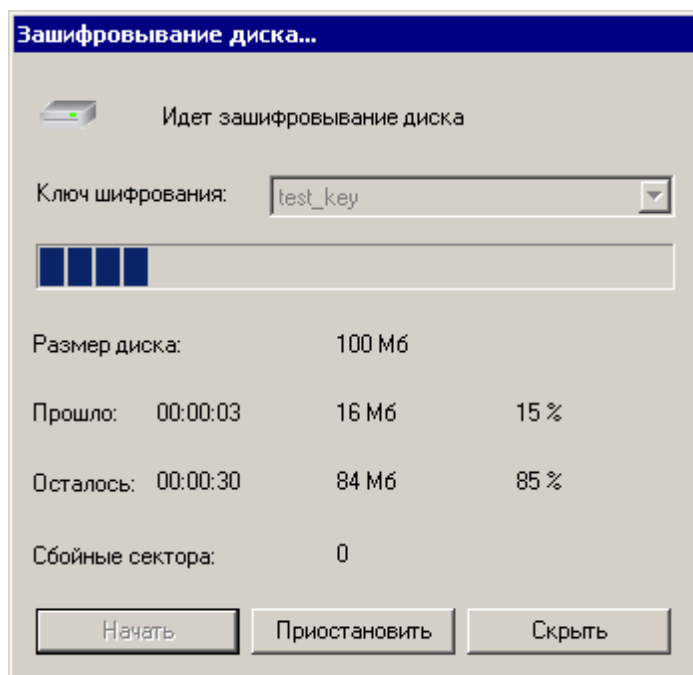
 Зашифровывание раздела производится в фоновом режиме, что означает доступность файлов для пользователей и приложений сервера. Таким образом, можно зашифровывать диски, не блокируя доступ к разделу. Тем не менее, рекомендуется зашифровывать диски во время минимальной загрузки сервера, поскольку операции чтения-записи и шифрования используют значительную часть ресурсов компьютера.

Для того чтобы зашифровать данные на логическом диске:


1. Поставьте курсор на нужный диск и выберите команду **«Открыть»** из меню **«Диск»** или нажмите на кнопку . При этом значок диска изменится на , а состояние диска станет **«Незашифрован»**;
2. Выберите команду **«Зашифровать»** из меню **«Диск»** или нажмите на кнопку . В появившемся окне **«Зашифровывание диска»** выберите загруженный в память сервера ключ шифрования и нажмите кнопку **«Начать»**. Процесс зашифровывания запустится;



 Зашифровывание производится непосредственно сервером, а консоль выполняет лишь функции управления. Во время зашифровывания можно производить другие операции с сервером либо вообще закрыть консоль.






3. Вы можете наблюдать за ходом процесса зашифрования с помощью индикатора прогресса, а также оценить, когда зашифрование завершится с помощью значения «Осталось:»;
4. В любой момент времени можно приостановить процесс зашифрования, нажав кнопку «**Приостановить**». Этим можно воспользоваться при необходимости перезагрузить сервер либо предоставить другим приложениям все ресурсы сервера;
5. При нажатии на кнопку «**Заккрыть**» окно с индикатором закроется, однако, шифрование продолжится, и его статус будет отображаться в поле «**Состояние**».


 Для отображения индикатора процесса зашифрования нужно дважды щелкнуть мышью по значку диска.


	C:\	Несъемный	(неизвестно)		4086		
	E:\	Несъемный	Зашифровывается (28%)	Да	100	test_key	RC5-128

6. Когда зашифрование полностью завершится, значок диска изменится на , а в состоянии диска появится надпись «**Зашифрован**».

Zserver обеспечивает защиту данных от сбоев во время зашифрования раздела, что означает доступность информации и возможность продолжить процесс шифрования после, например, потери питания сервера.

Действия в случае перезагрузки сервера:


1. Загрузите ключ (см п. 3.3.3 Загрузка ключа);
2. Выберите команду «**Открыть**» из меню «**Диск**». При этом значок диска изменится на , а состояние диска станет «**Зашифровывается (...%, приостановлено)**». При этом все файлы на диске станут доступны;
3. Выберите команду «**Продолжить зашифрование**» из меню «**Диск**». Процесс зашифрования продолжится.

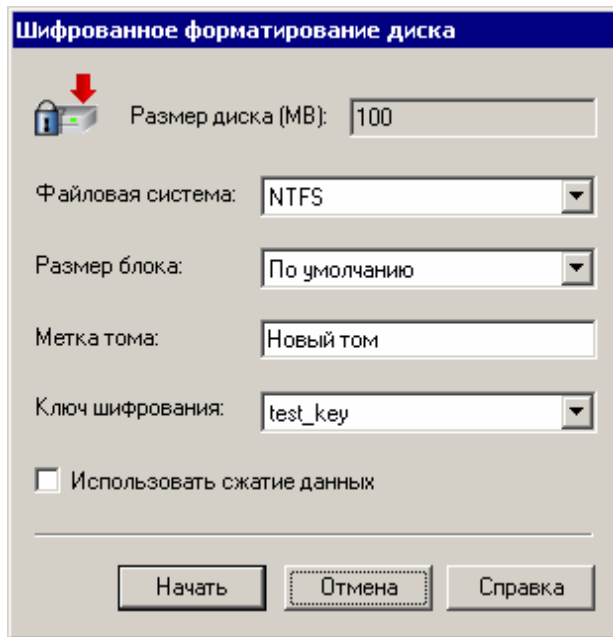
 Если по каким-то причинам Вы не желаете продолжать процесс зашифрования и хотите расшифровать раздел обратно, то этот процесс можно «**откатить**» обратно. Для этого приостановите зашифрование и выберите команду «**Откатить зашифрование**» из меню «**Диск**».


### 3.4.2 Шифрованное форматирование диска


Данная возможность позволяет не зашифровывать целиком только что созданный пустой раздел, что требует достаточно много времени, а сразу включить режим прозрачного шифрования и быстро отформатировать диск. Для этого раздел не должен содержать файловой системы, т.е. операцию «**Форматировать с шифрованием**» нужно проводить на только что созданном разделе.

Для выполнения форматирования с шифрованием:

1. Поставьте курсор на нужный диск и выберите команду «**Форматировать с шифрованием**» из меню «Диск» или нажмите на кнопку .
2. В окне «**Шифрованное форматирование диска**» выберите тип файловой системы, размер блока и задайте метку тома в соответствующих полях;




3. Укажите в поле «**Ключ шифрования диска**» нужный ключ, а также отметьте при необходимости опцию файловой системы NTFS «**Использовать сжатие данных**»;
4. Нажмите на кнопку «**Начать форматирование**». Zserver включит режим прозрачного шифрования и произведет его быстрое форматирование. После этой операции значок диска изменится на , и состояние диска станет «**Зашифрован**».

 Раздел не должен содержать файловую систему, иначе Zserver выдаст ошибку.

### 3.5 Смена паролей по умолчанию пользователей Zserver

После установки в Zserver имеются два пользователя: admin (пароль admin) с правами администратора и alarm (пароль alarm) с правом только подачи сигнала тревоги. В целях безопасности рекомендуется сменить им пароли.

Для того, чтобы изменить пароль пользователя:

1. Поставьте курсор на нужного пользователя и выберите команду «**Изменить**» из меню «Пользователь» или нажмите на кнопку .
2. В окне «**Изменить параметры пользователя**» введите в поля «Пароль» и «Подтверждение» новый пароль данного пользователя, после чего нажмите «ОК».

Более подробно работа с пользователями описывается в п. 5.5 Управление пользователями.


### 3.6 *Настройка сигнала тревоги*

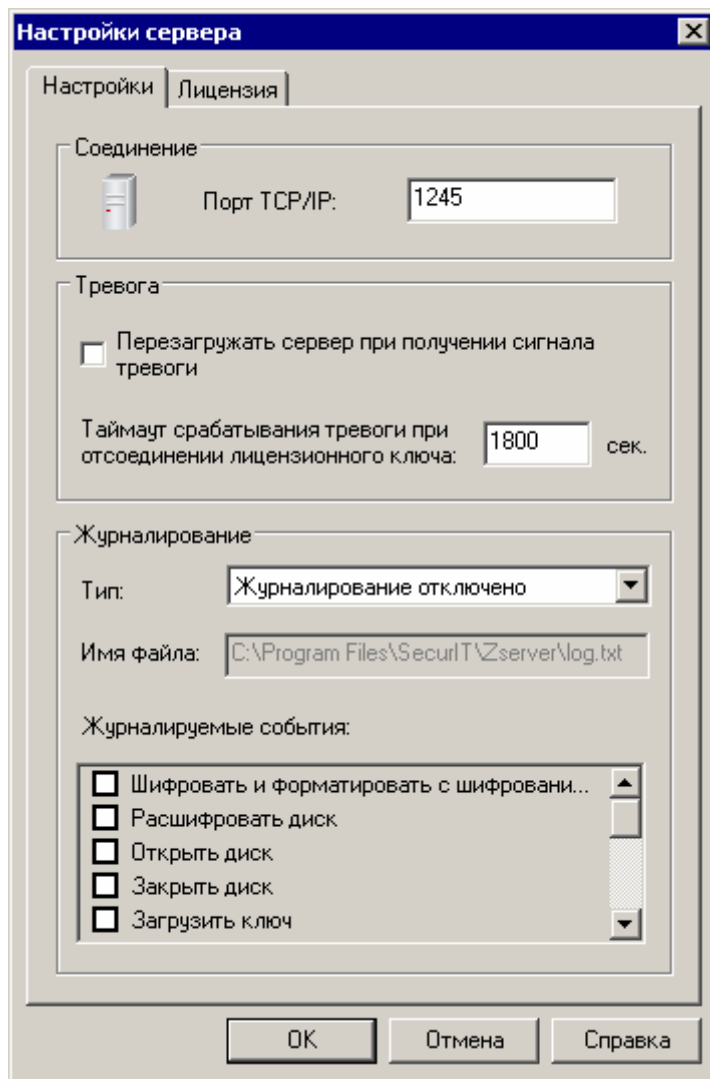
При получении сигнала тревоги серверный модуль может либо заблокировать доступ к зашифрованным данным либо произвести перезагрузку сервера.



Блокирование данных во время работы с ними приложений может привести к порче или утере информации.

По умолчанию сервер настроен на блокировку доступа. Для того чтобы при получении сигнала тревоги производить перезагрузку сервера:


1. Запустите консоль управления и установите соединение с сервером (см.п. 3.2 Соединение с сервером);
2. Поставьте курсор на пункт в дереве со значком , обозначающим сервер, например srv2:1245;
3. Выберите пункт «**Настройки**» из меню «**Сервер**»;

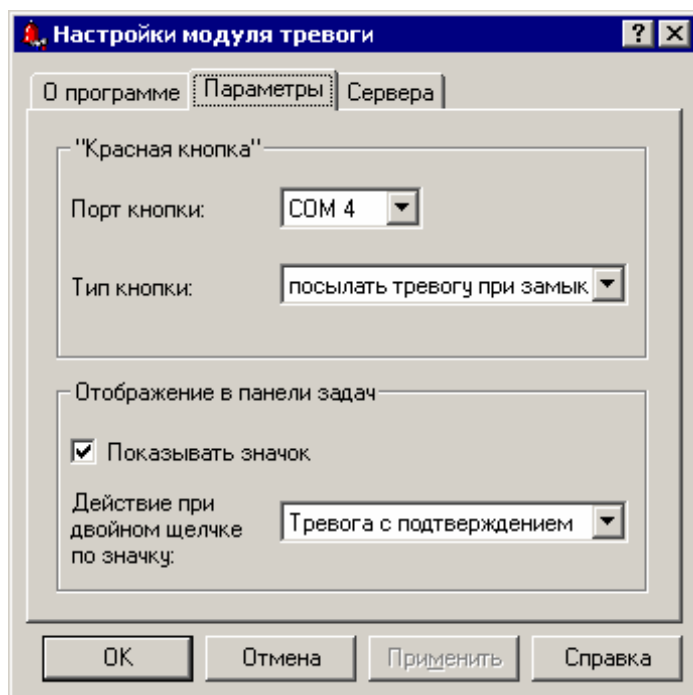


4. Включите опцию «**Перезагружать сервер при получении сигнала тревоги**» и нажмите «**ОК**».

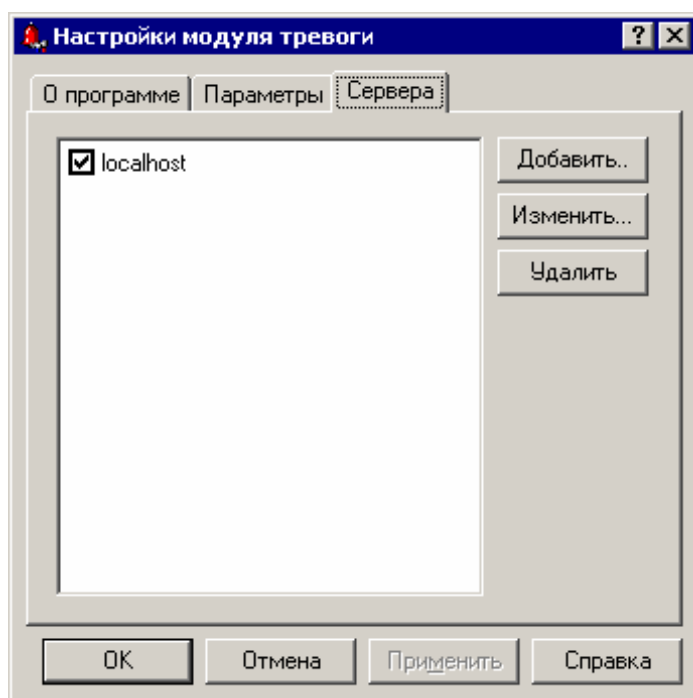
**i** Перезагрузка сервера вместо блокирования дисков обеспечивает более корректное завершение операций с диском и значительно снижает риск повреждения данных.

Для настройки модуля подачи сигнала тревоги:

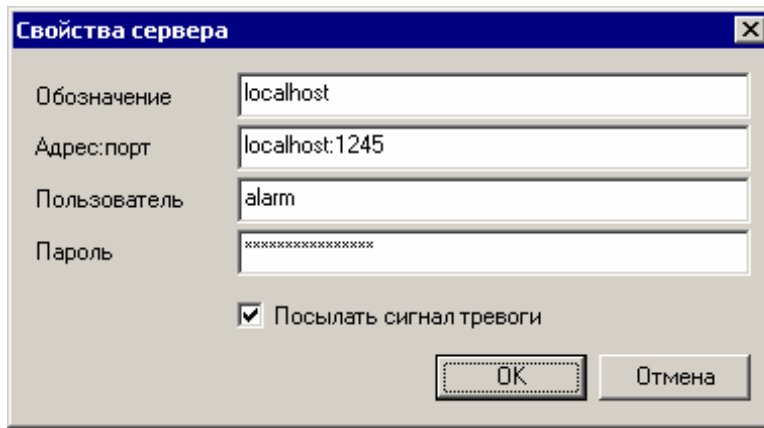
1. Запустите программу «**Настройка модуля тревога**». Ее можно вызвать либо из меню «**Пуск**» – «**Программы**» – «**Zserver**», либо щелкнув правой кнопкой мыши по значку  и выбрав в меню пункт «**Настройки...**».



2. Переключитесь на закладку «**Параметры**», где находятся настройки «**красной кнопки**». Выберите в поле «**Порт кнопки**» – COM-порт, к которому подключена «**красная кнопка**», а в поле «**Тип кнопки**» - «**В нормальном состоянии разомкнута**»;
3. При необходимости настройте параметры отображения значка в панели задач;
4. На закладке «**Сервера**» укажите сервер, на который следует подавать сигнал тревоги. Поставьте курсор на запись в списке и нажмите кнопку «**Изменить**»;



5. Укажите в окне «**Свойства сервера**» в соответствующих полях сетевой адрес и порт, имя и пароль пользователя, имеющий право на подачу сигнала тревоги. Задайте серверу имя в поле «**Обозначение**» и убедитесь, что включена опция «**Посылать сигнал тревоги на сервер**». Нажмите «**ОК**»;



6. Закройте окно настроек модуля, нажав «ОК».

**i** Процедура подачи сигнала тревоги описана в п. 4.3 Подача сигнала тревоги.

При работе модуля тревоги осуществляется журналирование в EventLog (раздел Application) следующих событий:

- Нажатие «**красной кнопки**» или инициирования сигнала тревоги другими способами;
- Удачная передача сигнала тревоги серверу;
- Неудачная передача сигнала тревоги серверу.

**i** В случае неудачной передачи сигнала тревоги модуль ssagent выдает предупреждающее сообщение.

Параметр типа DWORD

HKEY\_LOCAL\_MACHINE\SOFTWARE\SecurIT\SecurIT Server\2.0\Alarm  
\LogEvents

служит для включения (отключения) журналирования сигнала тревоги.



00000000	Журналирование отключено
00000001	Журналирование включено (по умолчанию)

## Глава 4 Эксплуатация Zserver

### 4.1 Загрузка ключа и открытие диска

После загрузки сервера зашифрованные данные недоступны, и раздел с ними выглядит как неотформатированная область.



Для того чтобы открыть зашифрованный раздел:



1. Запустите консоль управления и установите соединение с сервером (см.п. 3.2 Соединение с сервером);
2. Вставьте смарт-карту в устройство или подключите иной носитель с ключом шифрования диска;
3. Выберите команду "Загрузить ключ" из меню "Ключ" или нажмите кнопку ;
4. В окне «Загрузка ключа шифрования» выберите нужный тип носителя ключа и нажмите «ОК»;
5. Введите PIN-код для выбранного носителя и нажмите «ОК»;
6. Если в памяти смарт-карты находится несколько ключей шифрования, выберите нужное имя ключа и нажмите «ОК»;
7. Загруженный ключ отобразится в консоли управления, в разделе «Ключи» со значком .



Четырехкратный ввод подряд неправильного PIN-кода приведет к блокированию смарт-карты и к невозможности получить доступ к ключам, находящимся на ней.




Если загруженный ключ входит в кворум ключей, то он будет выглядеть в виде значка , а в скобках будет отображаться, сколько ключей от данного кворума находится на данный момент в памяти сервера. Для того чтобы ключом можно было открыть диск, необходимо загрузить недостающие ключи кворума. Как только Вы загрузите необходимое число ключей шифрования, изображение ключа изменится на значок  и Zserver сможет использовать загруженный ключ для шифрования данных.


8. Поставьте курсор на нужный диск и выберите команду «Открыть» из меню «Диск» или нажмите на кнопку . При этом значок диска изменится на , а состояние диска станет «Зашифрован»;
9. Если на сервере установлен модуль расширения **Script Pack**, то сразу после открытия диска произойдет выполнение заданных сценариев, например запуск системных служб. Работа со сценариями подробно описана в отдельном руководстве по Script Pack.

### 4.2 Заккрытие диска и выгрузка ключа шифрования

Для прекращения доступа к диску можно воспользоваться как операцией закрытия дисков, так и подачей сигнала тревоги (в экстренных случаях). Заккрытие диска предполагает штатный режим завершения работы с данными, поэтому предварительно необходимо завершить все приложения, работающие с ними, и закрыть открытые файлы.

Для того чтобы закрыть диск:

1. Запустите консоль управления и установите соединение с сервером (см.п. 3.2 Соединение с сервером);
2. Убедитесь, что все файлы на диске никем не используются и закрыты;
3. Поставьте курсор на нужный диск и выберите команду «Заккрыть» из меню «Диск» или нажмите на кнопку .


4. Если на сервере установлен модуль расширения **Script Pack**, то перед непосредственным закрытием диска произойдет выполнение заданных сценариев, например остановка системных служб или отключение всех сетевых пользователей от диска. Работа со сценариями подробно описана в отдельном руководстве по Script Pack.
5. Затем значок диска изменится на , а состояние диска станет «(неизвестно)».

После того, как диск закрыт, желательно выгрузить ключ шифрования из памяти сервера.



Если ключ шифрования останется в памяти сервера, то у злоумышленника останется возможность открыть диск и получить доступ к защищенным данным.



Для выгрузки ключа шифрования:

1. Убедитесь, что ключ шифрования не используется каким-либо диском, т.е. в числе использований ключа должно отображаться «**не используется**»;
2. Поставьте курсор на нужный ключ и выберите команду «**Выгрузить**» из меню «**Ключ**» или нажмите на кнопку . При этом ключ выгрузится из памяти сервера и удалится из списка ключей в консоли управления.

### 4.3 Подача сигнала тревоги

В экстренных случаях единственным возможным способом прекращения доступа к зашифрованной информации остается подача сигнала тревоги. При этом, в зависимости от настроек сервера, все операции чтения-записи на зашифрованном разделе останавливаются и ключ шифрования выгружается из памяти либо производится перезагрузка сервера (см п. 3.6 Настройка сигнала тревоги).

Подача сигнала тревоги может быть инициирована:

- Из модуля тревоги:
  - а. изменением состояния «**красной кнопки**», т.е. она либо замыкается, либо размыкается;
  - б. двойным нажатием левой кнопкой мыши по значку ;
  - с. запуском приложения `ssagent.exe` с параметром `-a`;
-  **Подача сигнала** происходит последовательно по всему списку серверов, указанных в настройках (см п. 3.6 Настройка сигнала тревоги). С каждым сервером устанавливается защищенное соединение и по нему передается специальная команда.
- Из Консоли управления - выбором команды «**Тревога**» в меню «**Сервер**».

При получении сигнала тревоги на сервере происходят следующие события:

1. Если на сервере установлен модуль расширения **Script Pack**, то произойдет выполнение заданных сценариев, например остановка системных служб или рассылка сообщений по сети. Работа со сценариями подробно описана в отдельном руководстве по Script Pack;
2. При включенном параметре «**Перезагружать сервер при получении сигнала тревоги**» (см. п. 3.6 Настройка сигнала тревоги) сервер перезагружается, в противном случае:
  - Все открытые диски закрываются независимо от наличия открытых файлов и работающих с ним приложений, а данные становятся полностью недоступными;



Блокирование данных во время работы с ними приложений может привести к порче или утере информации.



- Ключи шифрования выгружаются из памяти сервера;
  - Все дальнейшие операции с дисками и ключами становятся невозможными вплоть до перезагрузки сервера.
- i** Для восстановления доступа к данным после сигнала тревоги необходимо перезагрузить сервер.

Настройка модуля тревоги описывается в п. 3.6 Настройка сигнала тревоги.

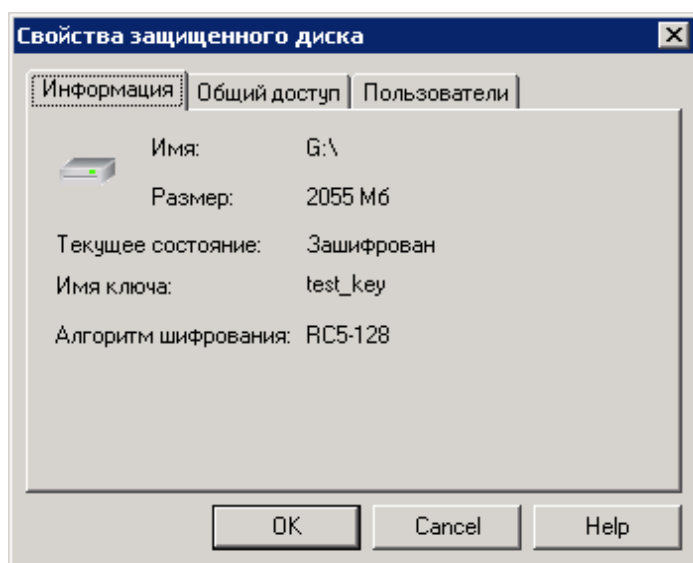
#### 4.4 Управление общим доступом

Система Zserver имеет возможность контролировать назначение общего доступа (Sharing) к файлам и каталогам на зашифрованном разделе.

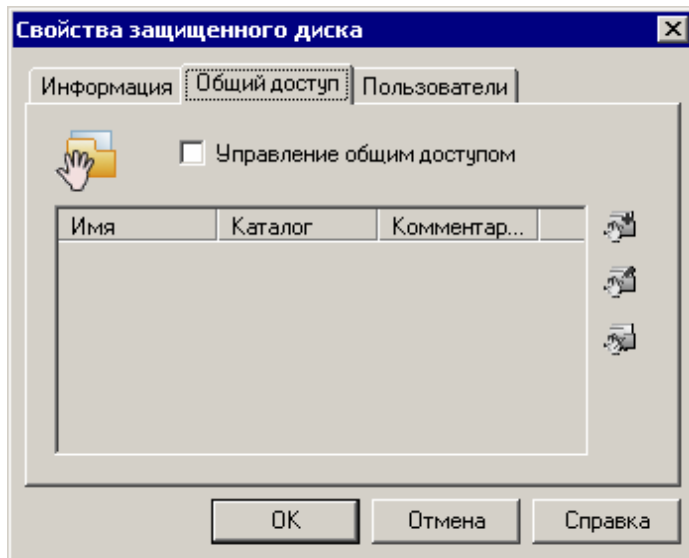
- i** Для использования данной возможности в конфигурации Zserver должен иметься модуль управления общими ресурсами (см п. 1.2.2 Конфигурация Zserver).

Для того чтобы включить контроль над назначением общего доступа на зашифрованном разделе:

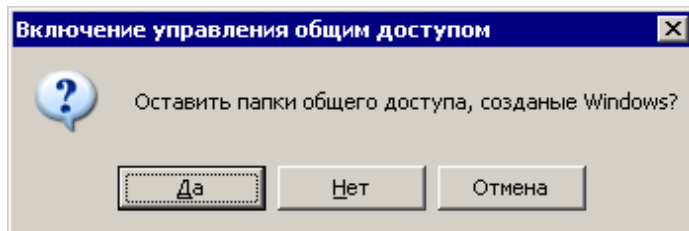
1. Запустите консоль управления и установите соединение с сервером (см.п. 3.2 Соединение с сервером);
2. Убедитесь, что нужный диск зашифрован и открыт;
3. Поставьте курсор на диск и выберите в меню «Диск» пункт «Свойства защищенного диска»;



4. Переключитесь на вкладку «Общий доступ» и включите опцию «Управление общим доступом»;

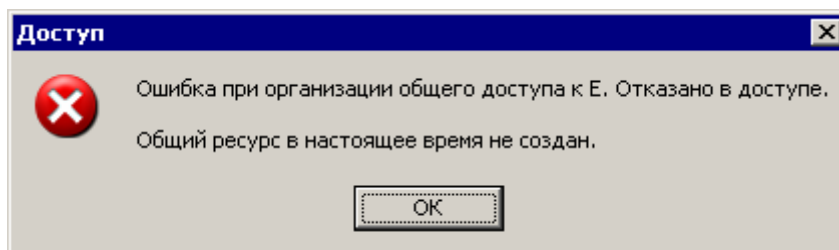


5. Если на диске уже имеются папки с общим доступом, Zserver предложит либо их оставить, либо удалить. Ответьте «Да» или «Нет» в окне «**Включение управления общим доступом**».



6. На вкладке «**Общий доступ**» отобразится список папок с общим доступом.

**i** Теперь все действия с папками общего доступа можно производить только через консоль управления, попытки что-либо сделать с помощью стандартного интерфейса Windows будут заблокированы.




Вся информация о ресурсах хранится на зашифрованном диске в специальном защищенном хранилище, и работать с ней имеют право только администраторы данного диска. Текущий пользователь Zserver автоматически становится администратором данного раздела. Более подробно распределение прав управления общими ресурсами описано в п. 4.4.4 Назначение прав управления общими ресурсами.

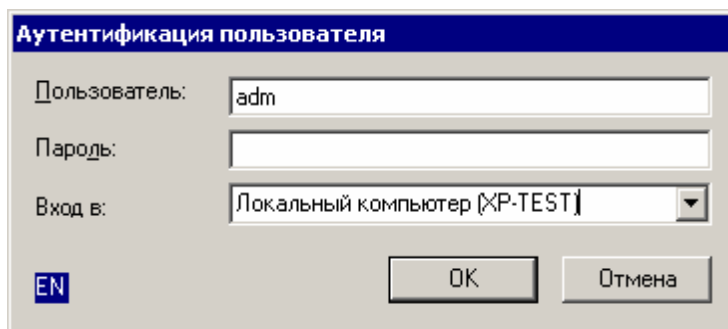
Если у Вас на сервере имеется несколько зашифрованных разделов, то включение управления общим доступом надо провести на каждом разделе.


Zserver позволяет через консоль управления добавлять новые общие ресурсы, изменять и удалять имеющиеся.

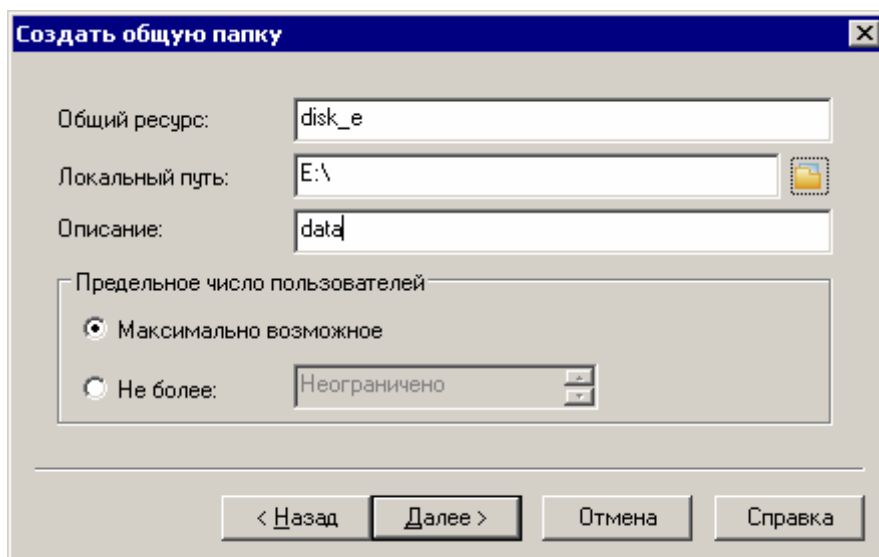
#### 4.4.1 Добавление общей папки


Для того чтобы добавить общую папку:

1. Откройте «Свойства защищенного диска» (см. п. 4.4 Управление общим доступом);
2. Переключитесь на вкладку «Общий доступ»;
3. Нажмите на кнопку ;
4. Введите имя и пароль учетной записи Windows. Это необходимо для загрузки списка пользователей;



5. Укажите в появившемся окне путь к папке с помощью кнопки , а затем введите в соответствующие поля имя общего ресурса и его описание;

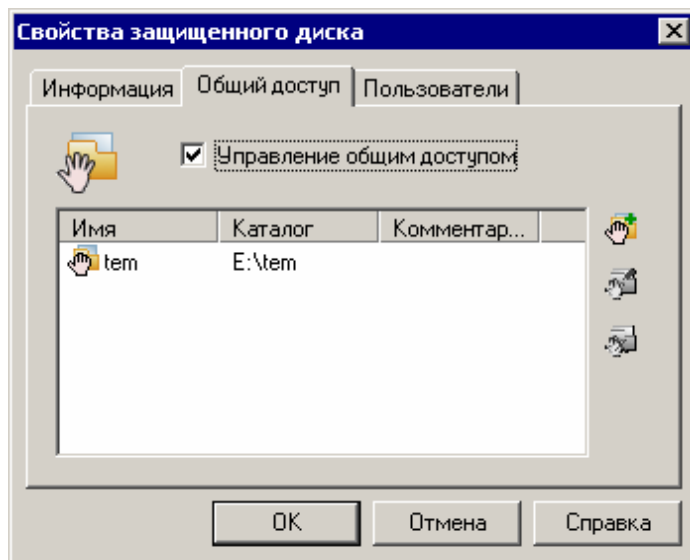


6. Введите число пользователей данного ресурса и нажмите «Далее»;  
 Максимальное число пользователей ограничено конфигурацией Zserver.
7. На следующем шаге выберите нужный тип распределения прав доступа к ресурсу либо составьте свой список контроля доступа, выбрав пункт «Настройка разрешений доступа» и нажав кнопку «Настройки»;
8. Нажмите «Далее», убедитесь, что общая папка была успешно создана, и нажмите «Готово».

#### 4.4.2 Изменение параметров общей папки

Для того чтобы изменить параметры общего ресурса:

1. Откройте «Свойства защищенного диска» (см. п. 4.4 Управление общим доступом);
2. Переключитесь на вкладку «Общий доступ»;

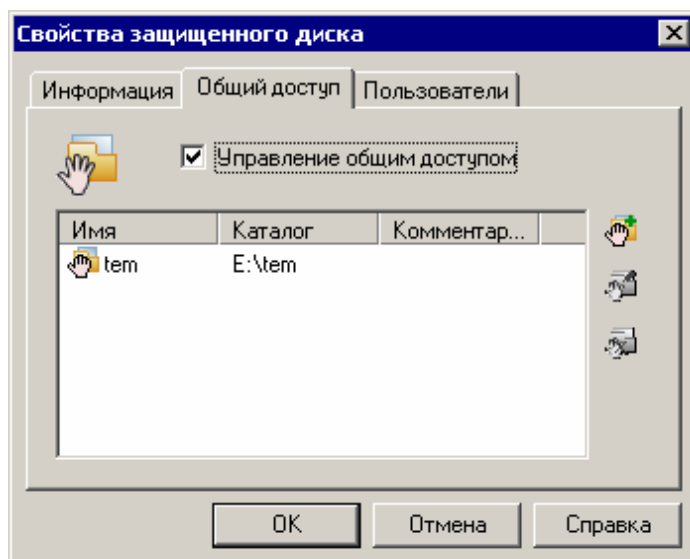


3. Поставьте курсор на нужную папку и нажмите кнопку
4. Отредактируйте необходимые параметры в свойствах папки и нажмите «ОК».

#### 4.4.3 Удаление общей папки

Для того чтобы удалить общий ресурс:

1. Откройте «Свойства защищенного диска» (см. п. 4.4 Управление общим доступом);
2. Переключитесь на вкладку «Общий доступ»;

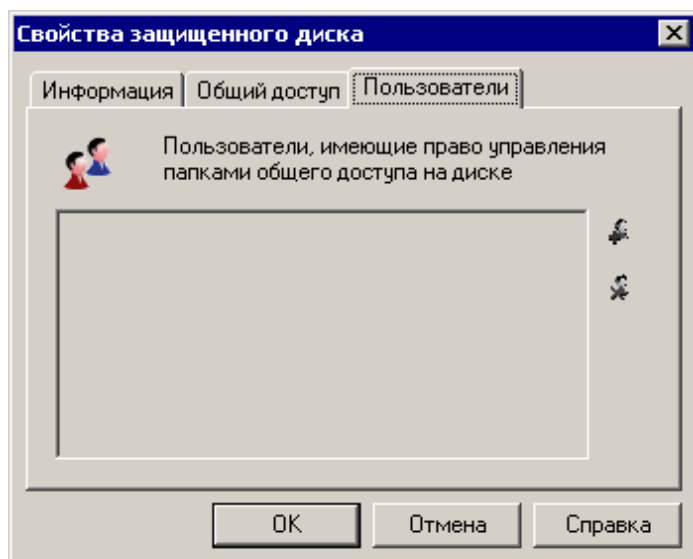




3. Поставьте курсор на нужную папку и нажмите кнопку
4. Подтвердите удаление папки, ответив «Да».


#### 4.4.4 Назначение прав управления общими ресурсами

Сразу после включения управления общими ресурсами система заносит текущего пользователя в специальный список администраторов данного раздела. Этот список можно просмотреть и изменить, для этого:

1. Откройте «Свойства защищенного диска» (см. п. 4.4 Управление общим доступом);
2. Переключитесь на вкладку «Пользователи»;




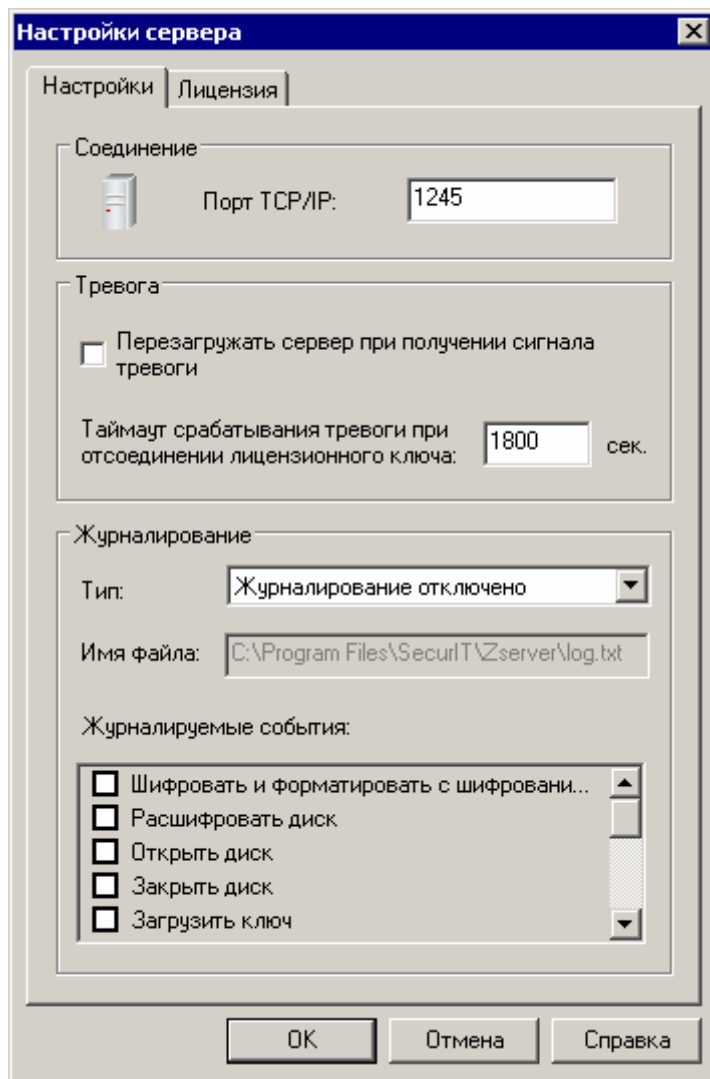
3. Пользователей можно добавлять с помощью кнопки , а также удалять нажатием на .

 В целях безопасности система Zserver запоминает некую производную от пароля администратора диска в специальном хранилище на зашифрованном диске. Поэтому, во время смены пароля зашифрованный диск должен быть открыт. В противном случае пользователь не сможет управлять общим доступом до тех пор, пока не сменит пароль обратно на старый.

## 4.5 Настройка параметров работы Zserver


Изменения параметров Zserver производится в окне «**Настройки сервера**». Для того чтобы его вызвать:

1. Запустите консоль управления и установите соединение с сервером (см.п. 3.2 Соединение с сервером);
2. Поставьте курсор на пункт в дереве со значком , обозначающим сервер, например srv2:1245;
3. Выберите пункт «**Настройки**» из меню «**Сервер**».




#### 4.5.1 Ведение журнала операций

Zserver позволяет журналировать производимые с ним операции в EventLog (раздел Application) или в файл на сервере.

1. Откройте окно «**Настройки сервера**» (см. п. 4.5 Настройка параметров работы Zserver);
2. Выберите тип журналирования в выпадающем списке «**Тип**»;
3. Если Вы выбрали «**В файл**», то укажите в поле «**Имя файла**» путь и имя текстового файла, куда будут заноситься записи о произведенных операциях с Zserver;  
 Путь к файлу должен быть указан относительно сервера.
4. В поле «**Журналируемые события**» отметьте те операции, произведение которых должно отображаться в журнале событий;
5. Нажмите «**ОК**».

#### 4.5.2 Задание нестандартного сетевого порта

 Перед сменой номера сетевого порта убедитесь, что новый порт никем не занят. Список используемых портов можно вызвать с помощью команды `netstat -a`, выполненной на сервере.

Для того чтобы сменить порт по умолчанию 1245 на другой:

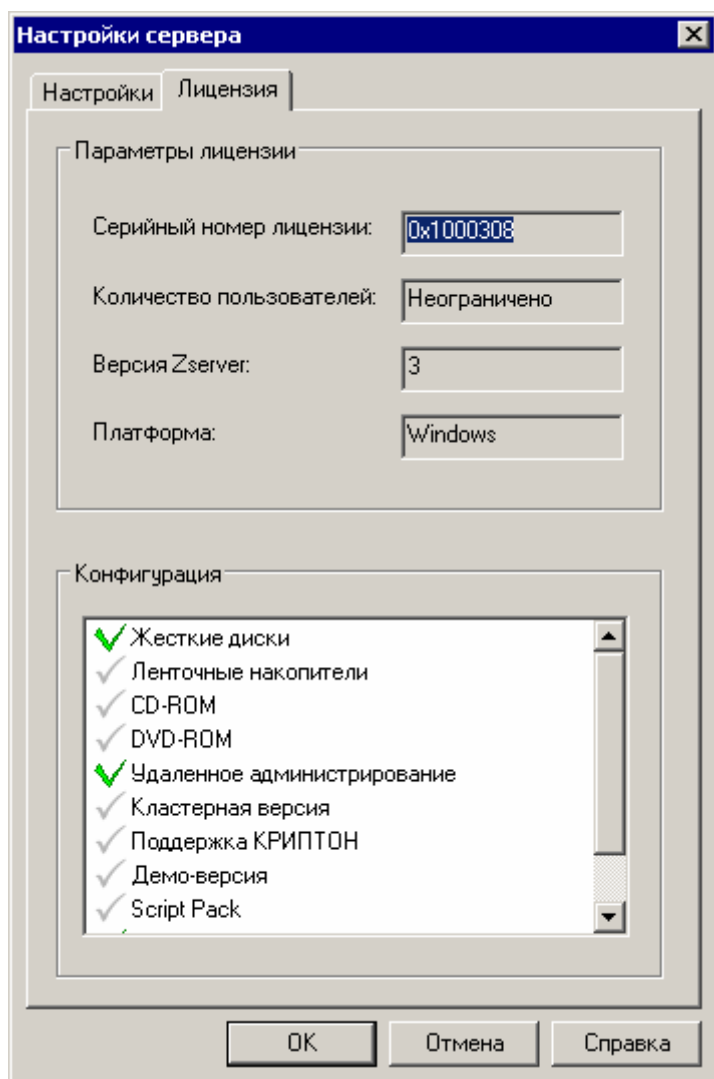
1. Откройте окно **«Настройки сервера»** (см. п. 4.5 Настройка параметров работы Zserver);
2. Введите в поле **«Порт TCP/IP»** номер нового порта и нажмите **«ОК»**;

**!** Не забудьте соответственно поменять номер порта в консоли управления, а также в настройках всех установленных модулей подачи сигнала тревоги.

### 4.5.3 Просмотр конфигурации Zserver

Для того чтобы получить информацию о конфигурации системы:

1. Откройте окно **«Настройки сервера»** (см. п. 4.5 Настройка параметров работы Zserver);
2. Переключитесь на вкладку **«Лицензия»**.




Возможные варианты конфигурации подробно описаны в п. 1.2.2 Конфигурация Zserver.

## Глава 5 Обслуживание Zserver

### 5.1 Управление ключами шифрования

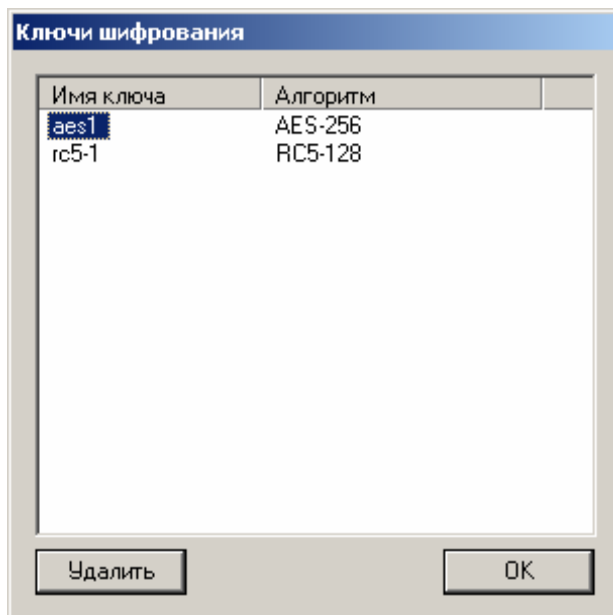
После того, как ключ шифрования был сгенерирован и записан на смарт-карту, возможно, его понадобится скопировать на другой носитель или удалить.

Для того чтобы скопировать ключ:

1. Выберите в консоли управления пункт **«Копировать ключ»** из меню **«Ключ»** или нажмите на кнопку ;
2. Выберите источник ключа, нажмите **«Далее»** и введите, если необходимо, PIN-код;
3. Просмотрите информацию о прочитанном ключе и нажмите **«Далее»**;
4. Выберите носитель, на который необходимо сохранить считанный ключ и введите, если необходимо, PIN-код;
5. Убедитесь в том, что ключ был успешно скопирован, и нажмите **«Готово»**.

Для того чтобы просмотреть список ключей и удалить ключ со смарт-карты либо другого носителя:

1. Выберите в консоли управления пункт **«Параметры носителя ключа»** из меню **«Ключ»**;
2. Выберите устройство хранения ключа и нажмите кнопку **«Ключи...»**;
3. Введите PIN-код;




4. Откроется окно **«Ключи шифрования»**, в котором можно просмотреть информацию о находящихся на носителе ключах и удалить выбранные ключи.


### 5.2 Одновременная работа с несколькими серверами


Консоль управления Zserver поддерживает одновременное управление двумя и более серверами.

Для того чтобы произвести соединение сразу с несколькими серверами:



1. Выберите команду **«Начать сеанс»** в меню **«Сервер»** или нажмите кнопку ;

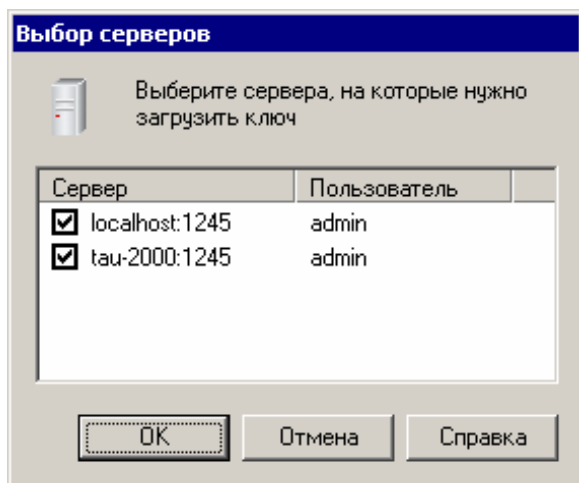


2. Добавьте в список серверов их необходимое число с помощью кнопки , отметьте нужные сервера и нажмите «ОК»;
3. Введите пароль для первого сервера. Если пароли для остальных серверов не отличаются от первого, то консоль их запрашивать не будет;
4. Все сервера отобразятся в древовидном списке в левой части консоли.

 Одновременное соединение с серверами возможно только в том случае, если на них установлена одна и та же версия Zserver.

Для того чтобы загрузить один ключ на несколько серверов:

1. Произведите соединение с несколькими серверами;
2. Вставьте смарт-карту в устройство или подключите иной носитель с ключом шифрования диска;
3. Выберите команду "Загрузить ключ" из меню "Ключ" или нажмите кнопку ;
4. В окне «Загрузка ключа шифрования» выберите нужный тип носителя ключа и нажмите «ОК»;
5. Введите PIN-код для выбранного носителя и нажмите «ОК»;
-  Четырехкратный ввод подряд неправильного PIN-кода приведет к блокированию смарт-карты и к невозможности получить доступ к ключам, находящимся на ней.
6. Если в памяти смарт-карты находится несколько ключей шифрования, выберите нужное имя ключа и нажмите «ОК»;




7. В появившемся списке серверов отметьте те, на которые необходимо загрузить ключ шифрования и нажмите «ОК».

Для того чтобы отправить сигнал тревоги из консоли управления не несколько серверов:

1. Установите соединение с несколькими серверами;
2. Поставьте курсор на корневой узел дерева - «Zserver», и выберите из меню «Сервер» пункт «Тревога».



Для того чтобы завершить все соединения с серверами:

1. При установленном соединении с несколькими серверами выберите из меню «Сервер» пункт «Завершить все сеансы» или нажмите на кнопку .

### 5.3 Расшифровывание дисков

Расшифровывание диска – это операция, обратная зашифровыванию. Данная операция производит последовательное посекторное расшифровывание всего раздела, включая служебную информацию файловой системы и свободное место.

Для того чтобы расшифровать диск:

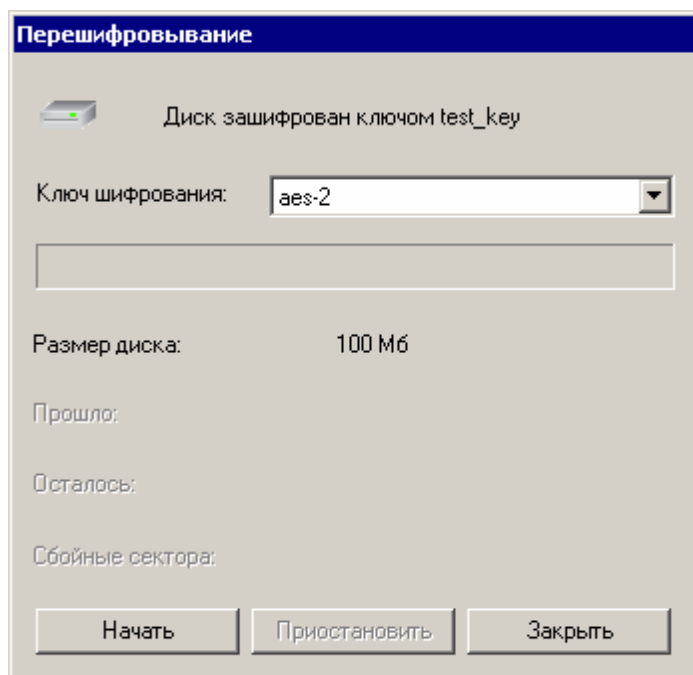
1. Запустите консоль управления и установите соединение с сервером;
2. Убедитесь, что диск открыт и имеет статус **«Зашифрован»**;
3. Выберите из меню **«Диск»** пункт **«Расшифровать»** или нажмите на кнопку ;
4. Нажмите кнопку **«Начать»** в появившемся окне **«Расшифровывание диска...»**. Процесс расшифровывания запустится;  
 ⓘ Расшифровывание производится непосредственно сервером, а консоль выполняет лишь функции управления. Во время расшифровывания можно производить другие операции с сервером либо вообще закрыть консоль.
5. Вы можете наблюдать за ходом процесса расшифровывания с помощью индикатора прогресса, а также оценить, когда расшифровывание завершится с помощью значения **«Осталось:»**;
6. При нажатии на кнопку **«Закрыть»** окно с индикатором закроется, однако, шифрование продолжится, и его статус будет отображаться в поле **«Состояние»**.  
 ⓘ Для отображения индикатора процесса расшифровывания нужно дважды щелкнуть мышью по значку диска.
7. Когда расшифровывание полностью завершится, значок диска изменится на , а в состоянии диска появится надпись **«Незашифрован»**.

### 5.4 Перешифровывание дисков


Перешифровывание диска выполняется в случаях, когда необходимо сменить ключ и/или алгоритм шифрования. Данная операция производит последовательное посекторное расшифровывание старым ключом и зашифровывание новым всего раздела, включая служебную информацию файловой системы и свободное место.


Для того чтобы перешифровать диск:

1. Запустите консоль управления и установите соединение с сервером;
2. Убедитесь, что диск открыт и имеет статус **«Зашифрован»**;
3. Загрузите в память сервера новый ключ шифрования;
4. Выберите из меню **«Диск»** пункт **«Перешифровать»**;
5. В открывшемся окне **«Перешифровывание диска...»** выберите новый ключ шифрования. Процесс перешифровывания запустится;  
 ⓘ Перешифровывание производится непосредственно сервером, а консоль выполняет лишь функции управления. Во время перешифровывания можно производить другие операции с сервером либо вообще закрыть консоль.





6. Вы можете наблюдать за ходом процесса перешифровывания с помощью индикатора прогресса, а также оценить, когда перешифровывание завершится с помощью значения «Осталось»;
7. При нажатии на кнопку «Закреть» окно с индикатором закроется, однако, перешифровывание продолжится, и его статус будет отображаться в поле «Состояние».

 Для отображения индикатора процесса перешифровывания снова нужно дважды щелкнуть мышью по значку диска.

8. Когда перешифровывание полностью завершится, значок диска изменится на , в состоянии диска появится надпись «Зашифрован», а в поле «Имя ключа» будет отображаться новый ключ шифрования.

Операции расшифровывания и перешифровывания производятся в фоновом режиме, при котором все данные доступны для операционной системы и пользователей. В любой момент расшифровывание и перешифровывание можно приостановить, нажав кнопку «Приостановить». Кроме того, при возникновении сбоев (например, отключение питания сервера) все данные остаются в безопасности.

 Для продолжения расшифровывания (перешифровывания) необходимо загрузить ключ (ключи), открыть диск и выбрать пункт «Продолжить ...» из меню «Диск».

 Если по каким-то причинам Вы не желаете продолжать процесс расшифровывания (перешифровывания) и хотите вернуть раздел в первоначальный вид, то эти процессы можно «откатить» обратно. Для этого приостановите расшифровывание (перешифровывание) и выберите команду «Откатить ...» из меню «Диск».


## 5.5 Управление пользователями

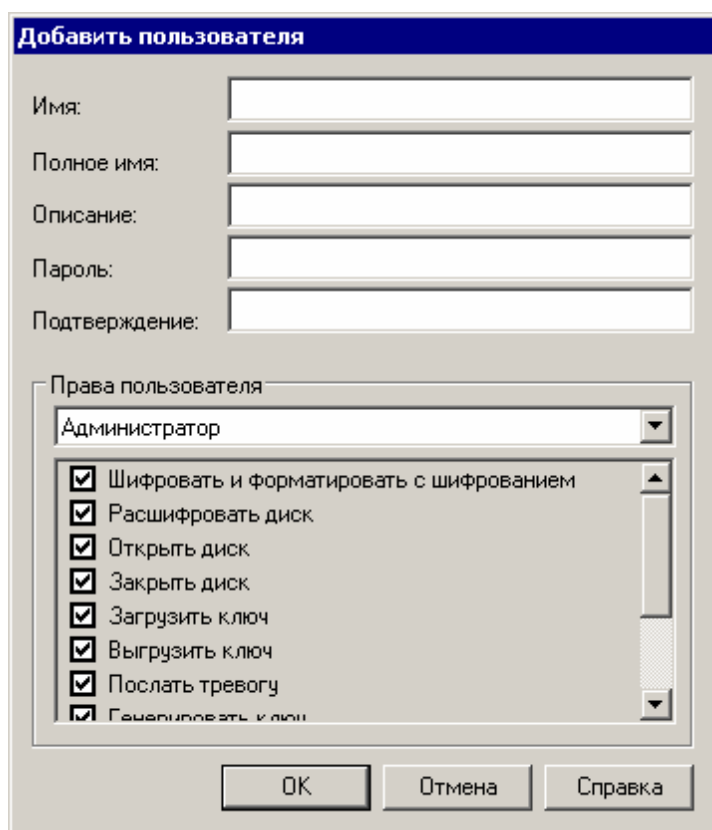
Система Zserver предоставляет возможность разграничивать права доступа по управлению сервером защиты между несколькими пользователями.



- ! Система Zserver не заменяет систему разграничения доступа Windows на основе паролей, а лишь дополняет ее.

После установки в системе Zserver имеются два пользователя: **«admin»** с паролем **«admin»**, наделенный администраторскими полномочиями, и **«alarm»** с паролем **«alarm»**, имеющий возможность только отправлять сигнал тревоги на сервер. Обязательно смените имена и пароли этих пользователей, иначе управление системой Zserver может оказаться в чужих руках.

Для того чтобы добавить пользователя:

1. Запустите консоль управления и установите соединение с сервером;
2. Выберите команду **«Добавить пользователя»** из меню **«Пользователь»** или нажмите на кнопку ;
3. Введите имя пользователя, его полное имя и описание в первые три поля, а в поле **«Пароль»** и **«Подтверждение»** укажите пароль для создаваемого пользователя;




4. Назначьте необходимые права пользователю в поле **«Права пользователя»**. Существует возможность задать следующие права:
  - **«Администратор»** - доступ ко всем операциям;
  - **«Тревога»** - пользователь, имеющий право только отправить сигнал тревоги;
  -  Пользователи с правами **«Тревога»** и **«Выборочные»** не смогут изменить свой пароль, эта операция доступна только администратору.
  - **«Выборочно»** - возможно назначить доступ к каждой операции с Zserver. Отметьте в списке те операции, которые разрешается производить данному пользователю.
  -  У пользователя с выборочными правами специально отключены операции по работе с пользователями, иначе он сможет легко обойти все ограничения.
5. Нажмите **«ОК»** для сохранения учетной записи пользователя в системе Zserver.

**!** Если Вы забыли пароль единственного пользователя с правами администратора, Вам придется переустановить систему Zserver.

Изменение пароля пользователя описано в п. 3.5 Смена паролей по умолчанию пользователей Zserver.

- ! Если Вы используете функции управления общим доступом системы Zserver, то смена пароля пользователю, который является администратором раздела, должна производиться при открытом разделе.

Для того чтобы удалить учетную запись пользователя в системе Zserver:

1. Запустите консоль управления и установите соединение с сервером;
2. Поставьте курсор на необходимого пользователя;
3. Выберите команду «Удалить» из меню «Пользователь» или нажмите на кнопку .

## 5.6 Удаление и обслуживание установленных компонентов

Программа установки позволяет изменять состав установленных компонентов (выборочное удаление и/или добавление) системы без полного удаления Zserver. Кроме того, предусмотрена возможность провести восстановление уже установленных модулей в случае их повреждения. Для запуска режима обслуживания откройте «Установка и удаление программ» из панели управления, поставьте курсор на «Zserver» и нажмите кнопку «Заменить/удалить».

В данном диалоговом окне предлагается выбрать дальнейшие действия:

«Изменить» – добавление или выборочное удаление компонентов системы;

«Исправить» – восстановление уже установленных компонентов;

«Удалить» – полное удаление системы Zserver.



Перед удалением компонента «Zserver» необходимо расшифровать все защищенные разделы, иначе информация на них станет недоступной.

## 5.7 Обновление Zserver

Для того чтобы произвести обновление Zserver:

1. Удалите установленную версию Zserver и перезагрузите компьютер;
2. Установить новую версию Zserver и перезагрузите компьютер;
3. Новая версия Zserver готова к работе, пользовательская база Zserver находится в состоянии «по умолчанию».

После обновления версии все зашифрованные данные снова станут доступны при загрузке соответствующего ключа шифрования.

## Приложение А. Демо-версия системы Zserver

Демо-версия Zserver предназначена для демонстрации возможностей системы. Демонстрационная версия является полнофункциональной рабочей версией системы, за исключением того, что в ней используются только первые восемь бит ключа шифрования. Таким образом, с помощью демо-версии можно изучить работу системы, но защищать ей важную информацию нельзя, так как демо-версия не обеспечивает должного уровня стойкости.

**!** Не используйте демо-версию системы для защиты конфиденциальной информации

При переходе с демо-версии на рабочую необходимо:

1. Расшифровать все диски, зашифрованные с использованием демо-версии Zserver;
2. Сменить электронный ключ защиты;
4. Перезагрузить сервер;
5. Сгенерировать новые ключи шифрования;
6. Зашифровать диски.

## Приложение В. Особенности работы с динамическими дисками

Динамический диск — это новый инструмент, появившийся в Windows 2000 и позволяющий создавать динамические тома. Преимущество нового механизма состоит в том, что для изменения конфигурации и управления динамическими томами не требуется перезагружать компьютер.

На динамических дисках могут располагаться следующие тома:

1. **простые (simple)** — обычные разделы;
2. **составные (spanned)** — физически состоят из нескольких дисков, однако приложениям доступны как одно логическое устройство. Данные записываются последовательно.
3. **тома с чередованием (stripped)** — физически представляют собой несколько одинаковых дисков, представленный одним логическим устройством. Поскольку данные читаются и записываются одновременно на несколько устройств, скорость дисковых операций существенно возрастает.
4. **зеркальные (mirrored)**. Данные записываются одновременно на два физических диска, что позволяет при сбое одного из них снять информацию с другого.
5. **RAID-5** - представляет собой striped volume с коррекцией ошибок. Используется для обеспечения сохранности ценных данных.

Начиная с версии 2.1 система Zserver поддерживает работу с динамическими дисками. После создания того или иного типа тома достаточно произвести стандартные операции с диском - загрузить ключ шифрования, открыть диск и зашифровать его.

Зашифрованные **простые (simple)** и **составные (spanned)** тома можно расширять, используя стандартные средства Windows 2000/2003, но перед этим их необходимо открыть системой Zserver. После такой операции все данные, записывающиеся в дополнительный том, будут "на лету" зашифровываться.

Зашифрованные **простые (simple)** тома допускается зеркалировать, при этом неважно, открыт диск или нет. В случае разделения зеркала (**Break mirror**) оба тома останутся зашифрованными и будут доступны после открытия их по очереди системой Zserver.

Зашифрованные тома **RAID-5** при возникновении сбоев регенерируются в закрытом виде, после чего они открываются стандартным способом.

## Для заметок