Aladdin

Secret Disk Server NG 3.1. Руководство по внедрению

Версия 1.1, апрель 2006

Содержание

Обзор Secret Disk Server NG 3.1

Защита от несанкционированного доступа (НСД) информации, хранящейся и обрабатываемой в компьютерных системах, является сегодня весьма актуальной задачей. Для решения этой задачи должен использоваться комплекс, включающий в себя технические, программно-аппаратные средства и административные меры защиты информации.

Secret Disk Server New Generation (Secret Disk Server NG) 3.1 – это современный программно-аппаратный комплекс защиты корпоративной информации (баз данных, файловых архивов, бизнес-приложений и их данных), хранящейся на серверах под управлением операционных систем Microsoft Windows 2000 / XP / Server 2003.

Secret Disk Server NG 3.1 использует проверенную и надёжную технологию защиты данных методом их «прозрачного» шифрования, суть которого заключается в том, что криптографическое преобразование информации выполняется в фоновом режиме при чтении и записи на диск, одновременно с работой пользователя или приложения и абсолютно незаметно для них без снижения производительности.

Secret Disk Server NG 3.1 не имеет встроенных средств шифрования, а использует внешние — входящие в состав операционной системы криптографический драйвер режима ядра и Microsoft Enhanced CSP или/и отдельно устанавливаемые Signal-COM CSP, КриптоПро CSP 2.0, Secret Disk NG Crypto Pack 3.1.

С помощью Secret Disk Server NG 3.1 на сервере могут быть зашифрованы разделы, логические диски, простые и составные динамические тома, RAID-массивы, а также съёмные диски (при необходимости организации безопасной передачи большого объёма данных). Имеется возможность мгновенного блокирования доступа к информации при подаче серверу сигнала «тревога» — например, от обычной «красной кнопки», радиобрелока или при срабатывании датчиков сигнализации.

Secret Disk Server NG 3.1 включает средства безопасного удалённого администрирования (подключение/отключение защищённых дисков, резервное копирование/восстановление ключей шифрования и др.). Для выполнения любой задачи администрирования сервера необходим USB-ключ / смарт-карта eToken с лицензией администратора Secret Disk Server NG.

В зависимости от типа и характера использования данных, которые необходимо защитить на сервере, возможны три основных сценария использования Secret Disk Server NG 3.1:

1. **Secret Disk Server NG 3.1 для файл-серверов** позволяет защищать информацию на доступных по сети дисках сервера. Предлагаются *лицензии файл-сервера* с ограничением на количество одновременных подключений по сети ко всем защищённым дискам сервера (лицензии файл-сервера на 5, 10, 25, 50, 100 пользователей), либо без такого ограничения (лицензия файл-сервера на неограниченное количество пользователей).
2. **Secret Disk Server NG 3.1 для серверов приложений** позволяет защищать от несанкционированного копирования и неавторизованного доступа расположенные на сервере файлы корпоративных баз данных, почтовые хранилища, данные бизнес-приложений. При наличии *лицензии сервера приложений* на сервере можно создавать защищённые диски, доступ к которым будут иметь только приложения, исполняемые на самом сервере (например, MS SQL Server) и пользователи, имеющие право локального входа на сервер. Доступ к этим дискам по сети невозможен (даже для администратора домена Windows через административные сетевые ресурсы).

Файлы баз данных, почтовые хранилища, данные бизнес-приложений, расположенные на таком защищённом диске, недоступны по сети и могут обрабатываться только приложениями, исполняющимися на сервере.
Лицензия сервера приложений не ограничивает число серверных приложений, которые могут работать с данными на защищённом диске, а также число пользователей этих приложений, работающих через приложения с данными на защищённом диске.

3. **Secret Disk Server NG 3.1 для файл-сервера и сервера приложений:** в этом сценарии на сервере можно защищать диски, предоставленные в общий доступ по сети, и создавать защищённые диски, доступные только серверным приложениям.

Поставляемые вместе с продуктом эксплуатационная документация и методические материалы (в том числе и данное руководство по внедрению) позволяют не только быстро установить систему и ввести её в промышленную эксплуатацию, но и внести соответствующие дополнения в должностные инструкции специалистов по информационной безопасности вашей компании.

Даже если в вашей организации пока нет человека, ответственного за информационную безопасность, то с помощью методических материалов и руководств, входящих в комплект поставки Secret Disk Server NG 3.1, вы сможете сделать первый шаг на пути построения защищённой информационной системы для вашего бизнеса.

Назначение Secret Disk Server NG 3.1

Программно-аппартный комплекс Secret Disk Server New Generation 3.1 предназначен **для защиты конфиденциальной информации**, хранящейся и обрабатываемой на корпоративном сервере под управлением операционной системы Microsoft Windows 2000 / Server 2003 / XP.

Secret Disk Server NG 3.1 обеспечивает:

- криптографическую **защиту от несанкционированного доступа** к конфиденциальной информации;
- **двухфакторную аутентификацию** администратора при обращении к инструментам управления;
- **разграничение и контроль доступа** к защищённой информации;
- **сокрытие наличия конфиденциальных данных** на сервере;
- **многопользовательскую и коллективную работу** с защищёнными данными;
- возможность **экстренного предотвращения несанкционированного доступа** к данным.

С помощью Secret Disk Server NG 3.1 вы можете защитить от несанкционированного доступа информацию, хранящуюся и обрабатываемую:

- на файловых серверах;
- в базах данных (БД);
- на почтовых серверах;
- различными бизнес-приложениями, имеющими многоуровневую архитектуру и предоставляющими пользователям услуги прикладного уровня (например, системы документооборота, ERP- и CRM- системы).

Источники угроз

Список лиц, которые могут получить доступ к хранящимся на вашем сервере незащищённым конфиденциальным данным, оказывается, на удивление, весьма обширным.

- **Злоумышленник —** человек, сознательной целью которого является получение доступа к вашим конфиденциальным данным. Злоумышленник действует целенаправленно и может привлекать *значительные технические ресурсы* (например, вычислительные мощности) для получения доступа к интересующей его информации. Злоумышленник может постараться применить целый комплекс мер, включая *социальную инженерию*, *физический доступ* к серверу и дискам с конфиденциальными данными и т. д.
- **Постороннее лицо** — например, сотрудник сервисной организации, куда был сдан сервер на ремонт/профилактику.
- **Любопытный сотрудник** — сотрудник организации, который по роду своей деятельности не должен иметь доступа к конфиденциальным данным, но желающий с ними ознакомиться. Скорее всего, такой человек не станет применять никаких целенаправленных действий по получению доступа к конфиденциальным данным, но не применёт воспользоваться *ошибками администрирования*, например, неожиданно предоставившейся возможностью просмотра содержимого диска с конфиденциальной информацией по сети.
- **Легальный пользователь системы** — сотрудник, обладающий правом доступа к самому серверу, но недостаточными полномочиями для доступа к конфиденциальной информации. Такой человек может попытаться *повысить свой уровень полномочий* в серверной операционной системе до административного, например, с целью скопировать интересующие его файлы (базу данных, хранилище электронных писем) для их последующего просмотра.
- **Обиженный/увольняемый сотрудник** может воспользоваться *периодом времени до отзыва* администратором *его прав доступа* к конфиденциальным данным для копирования или изменения этих данных.
- **Администратор операционной системы** по умолчанию имеет самый высокий уровень прав доступа**.** Системный администратор имеет возможность обратиться по сети к любому диску сервера с помощью так называемых *административных сетевых ресурсов* вида \\server\D$).

Не следует забывать и о роли человеческого фактора. В случае **ошибки администратора** при настройке прав, доступ к конфиденциальным данным может получить любой пользователь.

Также источником угроз являются **компьютерные вирусы, сетевые черви и троянские программы**. Если список программного обеспечения, устанавливаемого на сервере, всегда известен и само программное обеспечение свободно от вирусов, то компьютеры пользователей могут быть заражены вирусами и/или содержать троянские программы.

Используя параметры учётной записи пользователя, работающего в данный момент за заражённым компьютером, вирус может выполнять сканирование сетевых ресурсов и пытаться прочитать хранящиеся на них файлы. Если таким пользователем является администратор, то вирусу становится доступно содержимое дисков сервера через *административные сетевые ресурсы*.

Как Secret Disk Server NG 3.1 обеспечивает конфиденциальность данных

Конфиденциальность данных может быть нарушена в результате:
- хищения данных;
- утраты данных.

Ниже приведён краткий перечень источников угроз конфиденциальности данных, хранящихся и обрабатываемых на серверах и рабочих станциях.

Данный список не является исчерпывающим, но в нём перечислены те основные источники угроз, которые актуальны для большинства предприятий малого и среднего бизнеса.

Источники угроз	**Реализованные в Secret Disk Server NG 3.1 меры противодействия**
Внешние угрозы	
Злоумышленник, получивший физический доступ к серверу и/или дискам с конфиденциальными данными и обладающий возможностью привлечения значительных вычислительных ресурсов для получения доступа к данным. Посторонее лицо, получившее легальный доступ к серверу (например, при сервисном обслуживании).	• Защита данных на жёстких и съёмных дисках методом «прозрачного» шифрования. Данные на защищённых дисках всегда хранятся в зашифрованном виде. Даже в случае изъятия сервера или утери съёмного диска данные невозможно использовать. • Отключенный зашифрованный диск выглядит как неформатированный. • Для криптографической защиты данных могут применяться проверенные временем стойкие алгоритмы шифрования, предоставляемые: - криптографическим драйвером режима ядра, входящим в состав Microsoft Windows (алгоритм TripleDES с длиной ключа 168 бит); - поставщиком службы криптографии Signal-COM CSP (алгоритм ГОСТ 28147-89 с длиной ключа 256 бит); - поставщиком службы криптографии КриптоПро CSP 2.0 (алгоритм ГОСТ 28147-89 с длиной ключа 256 бит); - подключаемым внешним пакетом дополнительных алгоритмов шифрования (AES с длиной ключа 128 и 256 бит, Twofish с длиной ключа 256 бит). • Перешифрование защищённых дисков со сменой ключа и/или алгоритма шифрования. Перешифрование диска выполняется как одна операция. Не надо сначала расшифровывать данные (тем самым временно снимая с них защиту), а затем зашифровывать данные с новым ключом и/или по другому алгоритму. Данные всегда надёжно защищены. • Сетевой трафик сеанса администрирования криптографически защищён, что исключает его прослушивание или подмену злоумышленником. • Сигнал «тревога» может быть подан как внешним устройством (например, «красной кнопкой», радиобрелоком или охранной сигнализацией), так и с по-

Источники угроз	Реализованные в Secret Disk Server NG 3.1 меры противодействия
	мощью обычного пользовательского интерфейса (из командной строки, с использованием мыши). Реакция на сигнал «тревога» определяется для сервера в целом и для каждого защищённого диска в отдельности. Предусмотрены возможности отключения дисков, полного удаления всех конфигурационных данных и ключевой информации. • Для каждого защищённого диска могут быть определены индивидуальные сценарии. Эти сценарии могут выполняться перед подключением диска, после подключения, перед отключением, после отключения. Например, после подключения защищённого диска с файлами базы данных Microsoft SQL Server с помощью сценария может быть запущена сама СУБД.
«Человеческий фактор» и внутренние угрозы	
Социальная инженерия	• Аппаратная двухфакторная аутентификация администраторов Secret Disk Server NG с использованием цифровых сертификатов X.509: для выполнения административных задач надо иметь персональный сертификат открытого ключа с соответствующим закрытым ключом в памяти eToken и знать PIN-код. Таким образом, недостаточно узнать только PIN-код или только завладеть eToken — необходимы оба фактора. Пропажу eToken пользователю легко обнаружить и сообщить о ней для принятия необходимых дополнительных мер по защите информации.
Ошибки администрирования Возможность получения доступа к данным через административные сетевые ресурсы Повышение пользователем уровня своих полномочий на сервере	• Для каждого защищённого диска нужно определить, будет ли он доступен пользователям по сети или только приложениям, выполняющимся непосредственно на сервере. Например, для защиты от копирования файлов корпоративной базы данных целесообразно разместить их на защищённом диске и запретить к нему прямой сетевой доступ пользователей. • Оснастка консоли управления Microsoft является основным интерфейсом администратора Secret Disk Server NG. Эта оснастка встроена в консоль управления компьютером и хорошо знакома администраторам, что значительно уменьшает вероятность случайных ошибок при администрировании.
Наличие периода времени между принятием организационного (кадрового) решения об	• Интеграция с системами PKI. Secret Disk Server NG 3.1 использует сертификаты X.509 и связанные с ними криптографические ключи для защиты мастер-ключей защищённых дисков и аутентификации. Для выполнения административных задач надо

Источники угроз	Реализованные в Secret Disk Server NG 3.1 меры противодействия
отзыве прав доступа пользователя к конфиденциальным данным до реального отзыва его прав администратором	иметь действительный персональный сертификат открытого ключа, установленный в памяти eToken вместе с соответствующим закрытым ключом, и знать PIN-код. Для отзыва прав администратора Secret Disk Server NG достаточно лишь отозвать сертификат.

Как Secret Disk Server NG 3.1 обеспечивает доступность данных

Доступность данных может быть нарушена в результате:
- блокирования данных (невозможность получить доступ к данным) и
- уничтожения данных.

В Secret Disk Server NG 3.1 реализован комплекс мер, позволяющих обеспечить высокую степень доступности защищаемых данных.

Источники угроз	Реализованные в Secret Disk Server NG 3.1 меры противодействия
Поломка/отказ серверного оборудования Сбой электропитания	• Остановка или прерывание процесса зашифрования, перешифрования или расшифрования не приводят к потере данных. Приостановленный вручную или прерванный из-за отключения питания компьютера процесс может быть возобновлён в любой момент. • Форматирование и проверка дисков на наличие ошибок может производиться как стандартными средствами операционной системы, так и встроенными инструментами Secret Disk Server NG 3.1. • Сигнал «тревога» может быть подан датчиком охранной, пожарной или аварийной сигнализации. В этом случае работа с защищёнными дисками может быть корректно завершена, а сервер – подготовлен к отключению электропитания. • Индивидуальные сценарии для каждого защищённого диска могут выполняться перед подключением диска, после подключения, перед отключением, после отключения. Например, перед отключением защищённого диска с базой данных Microsoft SQL Server с помощью сценария может быть корректно остановлена работа СУБД.
Возможность наличия ошибок в программном обеспечении	• Secret Disk Server NG 3.1 не имеет встроенных средств шифрования, а для выполнения криптографических операций используются внешние модули, прошедшие тщательное тестирование и сертификацию в независимых лабораториях. Это гарантирует отсутствие ошибок при шифровании данных.
Ошибки администрирования Поломка/отказ	• Механизмы резервного копирования ключевой информации (как на уровне сервера, так и на уровне каждого защищённого диска в отдельности) позволяют восстановить доступ к защищённым дискам в

Источники угроз	Реализованные в Secret Disk Server NG 3.1 меры противодействия
оборудования	случаях *утраты eToken администратора* (утеря PIN-кода, блокировка, поломка), компрометации или завершения срока действия сертификата, случайного *удаления защищённого хранилища* (например, при переустановке операционной системы на сервере).

Дополнительные меры по обеспечению доступности данных

К дополнительным мерам по обеспечению доступности данных, реализованным в Secret Disk Server NG 3.1, можно отнести следующее:

1. Поддержка всех типов программных и аппаратных RAID-массивов.
2. Расширение защищённых дисков при их заполнении. Защищённые диски могут быть созданы на основе томов динамических жёстких дисков. При этом поддерживается их расширение штатными средствами Microsoft Windows.
3. Поддержка современных операционных систем семейства Windows — Microsoft Windows Server 2003, Windows 2000 Advanced Server, Server и Professional, Windows XP Home Edition и Professional.

Как Secret Disk Server NG 3.1 обеспечивает целостность данных

Целостность данных может быть нарушена в результате:

- модификации данных;
- отрицания подлинности данных;
- навязывания ложной информации.

В Secret Disk Server NG 3.1 реализован комплекс мер, позволяющих обеспечить целостность защищаемых данных.

Источники угроз	Реализованные в Secret Disk Server NG 3.1 меры противодействия
Прямой доступ к данным на неподключенном защищённом диске	• Защита данных на жёстких и съемных дисках методом «прозрачного» шифрования. Данные на защищённых дисках всегда хранятся в зашифрованном виде. Даже в случае изъятия сервера или утери съёмного диска данные невозможно контролируемо модифицировать, в том числе, с целью навязывания ложной информации. • Зашифрованный диск, который не подключен средствами Secret Disk Server NG 3.1, выглядит как неформатированный. • Для форматирования раздела необходимо обладать полномочиями администратора.

Описание архитектуры

Архитектура Secret Disk Server NG 3.1

Программные компоненты

Secret Disk Server NG 3.1 состоит из следующих компонентов:

- *сервер* — компонент, осуществляющий операции с дисками и защищённым хранилищем;
- *интерфейс администратора* — оснастка консоли управления Microsoft, позволяющая администратору управлять серверной частью Secret Disk Server NG 3.1, в том числе с удалённого компьютера;
- *Secret Disk NG Alarm*— инструменты для подачи сигнала «тревога», приводящего к запуску на сервере команд, предназначенных для предотвращения несанкционированного доступа к информации в чрезвычайных ситуациях.

Компьютеры

Компоненты Secret Disk Server NG 3.1 можно устанавливать как на один и тот же компьютер, так и на различные компьютеры в любых сочетаниях. Если вы устанавливаете на один компьютер два или три компонента Secret Disk Server NG 3.1, убедитесь в том, что:

- данный компьютер удовлетворяет требованиям к программному обеспечению каждого из компонентов;
- аппаратное обеспечение данного компьютера готово к поддержке всех устанавливаемых компонентов одновременно.

Именование компьютеров

Компьютер с установленным компонентом «сервер» будем называть *сервером*.

Компьютер с установленным интерфейсом администратора будем называть *рабочей станцией администратора*.

Компьютер с установленными инструментами Secret Disk NG Alarm будем называть *рабочей станцией для подачи сигнала «тревога»*.

Если на компьютере установлены два или три компонента, его именование зависит от компонента, об использовании которого идёт речь.

Схема лицензирования

В Secret Disk Server NG 3.1 имеются три объекта лицензирования:

- количество администраторов Secret Disk Server NG;
- количество одновременных клиентских подключений по сети ко всем защищённым дискам сервера, предоставленным в общий доступ;
- возможность запрещать сетевой доступ к защищённому диску.

Инструментом, обеспечивающим функционирование системы Secret Disk Server NG 3.1 в соответствии с имеющимися лицензиями, являются USB-ключи и/или смарт-карты eToken:

- каждый администратор Secret Disk Server NG является владельцем *eToken администратора*, в памяти которого имеется лицензия администратора. При необходимости увеличения числа администраторов нужно приобрести дополнительные USB-ключи и/или смарт-карты eToken с лицензией администратора Secret Disk Server NG;
- к каждому серверу подключается *eToken сервера*, в памяти которого имеется *лицензия файл-сервера*, содержащая информацию о максимальном количестве клиентских подключений, и/или *лицензия сервера приложений*, позволяющая запрещать сетевой доступ к защищённым дискам.

Таким образом, при работе с сервером USB-ключи и/или смарт-карты eToken используются *только на самом сервере и рабочей станции администратора*. Для рядовых пользователей предоставленный в общий доступ зашифрованный диск является обычным сетевым ресурсом.

Примечания:

- один и тот же *eToken администратора* можно использовать при администрировании различных серверов;
- *лицензия файл-сервера* ограничивает общее количество одновременных подключений по сети ко всем предоставленным в общий доступ защищённым дискам данного сервера;
- *лицензия сервера приложений* не ограничивает число серверных приложений, которые могут работать с данными на защищённом диске, а также число пользователей этих приложений, работающих через приложения с данными на защищённом диске;
- субъектам, осуществляющим клиентские подключения к серверу, лицензий не требуется.

Пример лицензирования

Предположим, что приобретён Secret Disk Server NG 3.1 с *лицензией файл-сервера* на 10 пользователей и *лицензией сервера приложений*. На сервере защищены диск **D:**, предоставленный в общий доступ по сети, и диск **E:**, на котором установлен экземпляр Microsoft SQL Server 2000 и корпоративная база данных. Доступ по сети к защищённому диску **E:** запрещён (это возможно, т.к. приобретена *лицензия сервера приложений*). При покупке ПО Microsoft SQL Server у Microsoft была приобретена процессорная лицензия.

В этом случае:

1. Одновременный доступ по сети к диску **D:** сервера смогут иметь не более 10 пользователей (ограничение *лицензии файл-сервера*).
2. Число пользователей, которые могут работать с корпоративной базой данных через Microsoft SQL Server, неограничено.

USB-ключи и смарт-карты eToken

В базовый комплект поставки Secret Disk Server NG 3.1 входят два eToken — *eToken администратора* и *eToken сервера*.

eToken администратора

eToken администратора применяется на рабочей станции администратора. В его памяти содержится лицензия администратора Secret Disk Server NG. В базовом комплекте поставки

eToken администратора носит имя `Administrator` и имеет наклейку с надписью `Administrator`.

ВНИМАНИЕ!
Никогда не форматируйте eToken администратора и не удаляйте никакие файлы из его памяти! Иначе вы можете удалить лицензию администратора, в результате чего работа Secret Disk Server NG 3.1 с данным eToken станет невозможной!

В процессе эксплуатации Secret Disk Server NG 3.1 для каждого из используемых поставщиков криптографии в памяти eToken администратора должен присутствовать соответствующий сертификат с закрытым ключом. При необходимости сертификат и закрытый ключ могут быть сгенерированы встроенными средствами Secret Disk Server NG 3.1.

В качестве *eToken администратора* может выступать:

- USB-ключ eToken R2;
- USB-ключ eToken PRO;
- смарт-карта eToken PRO.

eToken сервера

eToken сервера должен быть всегда подключен к серверу. В памяти *eToken сервера* хранится, по меньшей мере, одна из серверных лицензий:

- **лицензия файл-сервера**, содержащая информацию о максимально возможном количестве одновременных сетевых подключений ко всем защищённым дискам на данном сервере (3, 5, 10, 25, 50, 100 или неограниченное число подключений);
- **лицензия сервера приложений**, позволяющая запрещать сетевой доступ к защищённым дискам.

В базовом комплекте поставки eToken сервера носит имя `Server` и имеет наклейку с надписью `Server`.

ВНИМАНИЕ!
Никогда не форматируйте eToken сервера и не удаляйте никакие файлы из его памяти! Иначе

вы можете удалить лицензию сервера, и работа вашего экземпляра Secret Disk Server NG 3.1 станет невозможной!

В качестве *eToken сервера* может использоваться USB-ключ или смарт-карта eToken PRO.

Если один и тот же компьютер является как сервером, так и рабочей станцией администратора, то возможно использование одного электронного ключа eToken PRO, совмещающего функции *eToken администратора* и *eToken сервера* — при наличии в памяти данного eToken как лицензии администратора, так и хотя бы одной из серверных лицензий.

«Красная кнопка»

«Красная кнопка» — устройство, подключаемое к порту COM сервера или рабочей станции для подачи серверу сигнала «тревога».

Контакты «красной кнопки» замыкаются при нажатии. Для подачи сигнала «тревога» (замыкания контактов) можно использовать любое другое исполнительное устройство, например датчик охранной или пожарной сигнализации.

При соответствующих настройках на стороне сервера подача сигнала «тревога» (например, нажатие на кнопку или срабатывание охранной сигнализации) приведёт к запуску на сервере команд для блокирования дальнейшего доступа к защищённым данным.

«Красная кнопка», входящая в комплект поставки Secret Disk Server NG 3.1, является аппаратным компонентом Secret Disk NG Alarm. Более подробная информация о ней изложена в документации Secret Disk NG Alarm.

Радиобрелок и радиоприёмник для подачи сигнала «тревога»

Радиоприёмник, подключаемый к порту COM сервера или рабочей станции, обеспечивает возможность дистанционной подачи серверу сигнала «тревога» с помощью радиобрелока.

Радиус действия радиобрелока составляет порядка 50 метров и зависит от особенностей помещения (наличие стен, перегородок из различных материалов). После ввода системы в эксплуатацию рекомендуется опытным путём проверить фактическую дальность действия радиобрелоков.

С одним радиоприёмником может работать до 12 радиобрелоков.

При соответствующих настройках на стороне сервера подача сигнала «тревога» приведёт к запуску на сервере команд, предназначенных для предотвращения несанкционированного доступа к информации в чрезвычайных ситуациях.

Радиобрелоки и радиоприёмники являются дополнительными аппаратными компонентами Secret Disk NG Alarm и приобретаются отдельно.

Как работает Secret Disk Server NG 3.1

Secret Disk Server NG 3.1 обеспечивает защиту данных, хранящихся на:

- основных разделах и логических дисках базовых жёстких дисков;
- томах динамических дисков;
- съёмных дисках.

Защита информации обеспечивается шифрованием данных «на лету» с помощью стойких алгоритмов шифрования. При чтении данных с диска происходит их расшифрование, при записи на диск — зашифрование. Находящиеся на диске данные всегда зашифрованы.

Защищённый диск можно подключать и отключать. Отключенный защищённый диск выглядит как неформатированный. С подключенным защищённым диском вы работаете точно так же, как с обычным диском. Для того чтобы преобразовать обычный диск в защищённый (зашифровать диск), подключить защищённый диск или выполнить другие административные операции, необходимо *обладать* смарт-картой или USB-ключом eToken администратора, *знать* PIN-код и иметь соответствующие полномочия как на уровне сервера в целом, так и по отношению к данному диску.

В памяти eToken администратора должны присутствовать:

- *лицензия администратора*;
- *сертификат открытого ключа* администратора Secret Disk Server NG и соответствующий ему *закрытый ключ*.

Можно использовать уже *имеющиеся сертификаты* (например, сертификат для входа в сеть или ЭЦП и шифрования почты). Если у администратора нет цифрового сертификата, Secret Disk Server NG сгенерирует закрытый ключ и сертификат.

При работе с *КриптоПро CSP 2.0* и *Signal-COM CSP* используются сертификаты открытого ключа, совместимые с этими поставщиками службы криптографии. В остальных случаях в Secret Disk Server NG 3.1 применяются сертификаты на основе ключей RSA. Таким образом, у администратора может быть не один, а два или даже три сертификата — по одному для каждого стандарта.

Примечание: Как правило, если в организации используются сертифицированные российские средства шифрования, то администратору достаточно иметь сертификат с закрытым ключом, созданный с помощью Signal-COM CSP или КриптоПро CSP 2.0. Диски при этом шифруются только по алгоритму, соответствующему ГОСТ-28147-89. Если же использование именно российских криптографических средств является необязательным, то применяется сертификат, связанный с ключевой парой RSA, а диски шифруются по алгоритмам AES, DES, Triple DES или Twofish. Таким образом, в большинстве практических случаев администратор использует единственный сертификат.

При обращении к инструментам управления Secret Disk Server NG 3.1 администратор должен подключить к компьютеру свой eToken, указать свой сертификат и ввести PIN-код. Таким образом реализуется ***двухфакторная аутентификация*** администратора при обращении к элементам управления.

В начале процесса создания защищённого диска администратор Secret Disk Server NG должен выбрать *алгоритм шифрования диска* из списка имеющихся в системе и поддерживаемых Secret Disk Server NG алгоритмов шифрования.

Алгоритмы, реализуемые криптографическим драйвером режима ядра, входящим в состав Windows (DES и Triple DES), всегда доступны для использования. Алгоритм, соответствующий ГОСТ-28147-89, можно использовать при наличии на сервере и рабочей станции администратора поставщика службы криптографии *КриптоПро CSP 2.0* или *Signal-COM CSP*. Кроме того, если на сервере установлен пакет дополнительных криптографических алгоритмов *Secret Disk NG Crypto Pack 3.1*, то вы можете применять для шифрования дисков алгоритмы AES и Twofish.

После выбора *алгоритма шифрования* выполняется генерация уникального *ключа шифрования диска*. Для каждого администратора Secret Disk Server NG сгенерированный *ключ шифрования диска* зашифровывается с применением открытого ключа соответствующего сертификата и сохраняется в зашифрованном виде на системном диске сервера в так называемом *защищённом хранилище*.

Содержимое диска шифруется посекторно с использованием выбранного *алгоритма шифрования* и сгенерированного *ключа шифрования диска*. Процесс шифрования диска может быть *приостановлен* администратором или даже *прерван* (например, из-за перебоев электропитания), однако это не повлечёт за собой потерю данных. Приостановленный или прерванный процесс шифрования может быть *возобновлён* в любой удобный момент. По завершении процесса шифрования всё содержимое диска становится зашифрованным, что обеспечивает **надёжную криптографическую защиту** хранящихся на нём данных.

При прямом просмотре содержимое отключенного защищённого диска выглядит как случайная последовательность битов или, говоря по-другому, «белый шум», поскольку все данные зашифрованы. По содержимому раздела диска невозможно определить, является ли данный раздел просто неформатированным, или же на нём имеется какая-то информация. Так Secret Disk Server NG обеспечивает **защиту конфиденциальной информации от несанкционированного доступа**, а также **сокрытие наличия данных** на компьютере.

Для того чтобы открыть доступ к данным на защищённом диске, администратор Secret Disk Server NG должен *подключить* диск. Для этого хранящийся в памяти eToken *закрытый ключ* (доступ к которому возможен только после ввода PIN-кода) будет использован для расшифрования *ключа шифрования диска*. Расшифрованный таким образом *ключ шифрования диска* загружается в драйвер Secret Disk Server NG 3.1 (при использовании драйверов режима ядра) или передаётся поставщику службы криптографии (CSP).

На сервере может быть зарегистрировано произвольное число администраторов Secret Disk Server NG. Любой администратор может добавить нового администратора или удалить существующего из списка зарегистрированных администраторов Secret Disk Server NG. При добавлении нового администратора указывается сертификат открытого ключа, который добавляемый администратор будет использовать. При этом *ключи шифрования* всех защищённых дисков считываются из *защищённого хранилища*, расшифровываются с применением закрытого ключа добавляющего администратора, зашифровываются с использованием открытого ключа добавляемого администратора и записываются в *защищённое хранилище*. Таким образом, добавляемый администратор будет иметь доступ к тем же дискам, что и добавляющий.

По умолчанию все администраторы равноправны по отношению ко всем защищённым дискам сервера. Вместе с тем в Secret Disk Server NG предусмотрена возможность, **коллективной работы** администраторов с **разграничением доступа**: каждому защищённому диску можно сопоставить свой уникальный список администраторов, имеющих полномочия управлять данным защищённым диском.

Пользователи обращаются к защищённым дискам по сети в зависимости от полномочий, определяемых операционной и файловыми системами. В качестве альтернативы **многопользовательского доступа** к данным на защищённом диске можно использовать запрет сетевого доступа, например, для дисков, на которых хранятся корпоративные базы данных. Непосредственно обращаться к данным на таком диске будут только соответствующие приложения, установленные на сервере. А пользователи смогут работать с данными не напрямую, а только через интерфейс этих приложений. Доступ по сети к содержимому такого подключенного защищённого диска невозможно будет получить никому, даже администратору домена Windows через административные сетевые ресурсы (например, `\\server\D$`). Благодаря этому с помощью Secret Disk Server NG 3.1 можно обеспечить так называемую **«защиту от системного администратора»**.

Таким образом, **разграничение и контроль доступа** к защищённым данным осуществляется средствами операционной системы, файловой системы и приложений, работающих с информацией на защищённых дисках.

В состав Secret Disk Server NG 3.1 входит программно-аппаратный комплекс Secret Disk NG Alarm, состоящий из программного обеспечения и «красной кнопки». Если в результате возникновения нештатной ситуации возникает угроза несанкционированного доступа к данным, хранящимся на защищённых дисках, нажатие «красной кнопки» приводит к выполнению на сервере команд, **экстренно предотвращающих несанкционированный доступ**. В частности, предусмотрены несколько режимов отключения защищённых дисков и полное удаление защищённого хранилища.

Установка и развёртывание Secret Disk Server NG 3.1

Аппаратные и программные требования

Требования к серверу

Требования к программному обеспечению сервера

На сервере должна быть установлена одна из операционных систем:

- Microsoft Windows Server 2003;
- Microsoft Windows 2000 Advanced Server с установленным пакетом обновления 2 или выше;
- Microsoft Windows 2000 Server с установленным пакетом обновления 2 или выше;
- Microsoft Windows 2000 Professional с установленным пакетом обновления 2 или выше;
- Microsoft Windows XP Professional с установленным пакетом обновления 1 или выше;
- Microsoft Windows XP Home Edition с установленным пакетом обновления 1 или выше.

Примечание: для управления сервером через удалённый рабочий стол необходима операционная система Microsoft Windows Server 2003 или Windows XP Professional.

Также должны быть установлены:

- набор драйверов eToken Run Time Environment (eToken RTE) версии 3.51.19 или выше;
- Signal-COM CSP или/и КриптоПро CSP 2.0 (при необходимости использования сертифицированных российских средств криптографической защиты);
- драйвер устройства чтения смарт-карт (если в качестве eToken сервера используется смарт-карта eToken PRO).

При возможности выбора между драйверами, поставляемыми вместе с Windows, и драйверами производителей для контроллеров устройств, на которых будут создаваться защищённые диски, предпочтение следует отдавать драйверам производителей.

Требования к аппаратному обеспечению сервера

Сервер должен удовлетворять требованиям, изложенным в документации операционной системы и используемых поставщиков криптографии.

Кроме того, в зависимости от вида eToken сервера, сервер должен иметь:

- свободный порт USB (для USB-ключа eToken PRO);
- устройство чтения смарт-карт, поддерживающее смарт-карты eToken PRO (например, ASEDrive IIIe) — для смарт-карты eToken PRO.

Объём свободного места на жёстком диске для установки компонента «сервер»: 5 МБ.

Требования к рабочей станции администратора

Требования к программному обеспечению рабочей станции администратора

На рабочей станции администратора должна быть установлена одна из операционных систем:

- Microsoft Windows XP Professional с установленным пакетом обновления 1 или выше;
- Microsoft Windows XP Home Edition с установленным пакетом обновления 1 или выше;
- Microsoft Windows 2000 Professional с установленным пакетом обновления 2 или выше;
- Microsoft Windows 2000 Advanced Server с установленным пакетом обновления 2 или выше;
- Microsoft Windows 2000 Server с установленным пакетом обновления 2 или выше;
- Microsoft Windows Server 2003.

Примечание: для управления сервером через удалённый рабочий стол необходима операционная система Microsoft Windows XP Professional или Windows Server 2003.

Также должны быть установлены:

- набор драйверов eToken Run Time Environment (eToken RTE) версии 3.51.19 или выше;
- Signal-COM CSP или/и КриптоПро CSP 2.0 (при необходимости использования сертифицированных российских средств криптографической защиты);
- eToken для КриптоПро CSP 2.0 версии 2.0 (для хранения ключевых контейнеров КриптоПро CSP 2.0 в памяти eToken администратора);
- eToken для Signal-COM CSP (для хранения сертификатов и ключевых контейнеров Signal-COM CSP в памяти eToken администратора);
- драйвер устройства чтения смарт-карт (если в качестве eToken администратора используется смарт-карта eToken PRO).

Требования к аппаратному обеспечению рабочей станции администратора

Рабочая станция администратора должна удовлетворять требованиям, изложенным в документации операционной системы и используемых поставщиков криптографии.

Кроме того, в зависимости от вида eToken администратора, рабочая станция администратора должна иметь:

- свободный порт USB (для USB-ключа eToken);
- устройство чтения смарт-карт, поддерживающее смарт-карты eToken PRO (например, ASEDrive IIIe), — для смарт-карты eToken PRO.

Объём свободного места на жёстком диске для установки интерфейса администратора: 4 МБ.

Выбор аппаратной платформы в зависимости от планируемой нагрузки

О производительности, достигаемой при реализации алгоритмов, можно судить по следующей таблице:

Алгоритм	Длина ключа, бит	Программная реализация	Относительная производительность
AES	128	Secret Disk NG Crypto Pack	46,55
Twofish	256	Secret Disk NG Crypto Pack	42,67
AES	256	Secret Disk NG Crypto Pack	36,57
DES	56	Windows Kernel Mode Crypto Driver	26,95
Triple DES	168	Windows Kernel Mode Crypto Driver	10,67

Замедление процессов чтения/записи данных после зашифрования диска может быть ощутимо, только если скорость выполнения операций ввода/вывода вашей дисковой подсистемой превышает производительность Secret Disk Server NG 3.1 при использовании соответствующего алгоритма шифрования.

На практике только редкие специализированные приложения, работая с данными на защищённом диске, в состоянии постоянно требовать подобный уровень производительности операций ввода/вывода. К таким приложениям можно отнести, в частности, программное обеспечение для работы с потоковыми аудио- и видеоданными. При его использовании для обработки информации, хранящейся на защищённых дисках сервера, рекомендуется обязательно провести предварительное нагрузочное тестирование с реальным объёмом данных.

При размещении на защищённых дисках сервера баз данных, файловых архивов, почтовых баз и использовании современных процессоров (частотой от 1 ГГц) замедление работы после зашифрования диска практически неощутимо.

При использовании поставщиков службы криптографии (Signal-COM CSP и КриптоПро CSP 2.0) производительность существенно зависит от размеров файлов. Чем меньше файлов, тем ниже производительность. В целом, поставщики службы криптографии демонстрируют более низкую производительность, чем драйверы режима ядра (Secret Disk NG Crypto Pack и Windows Kernel Mode Crypto Driver).

Рекомендуемая установка

Для того чтобы максимально полно использовать заложенные в Secret Disk Server NG 3.1 возможности, выполните следующую установку:

- *на сервере* установите компоненты «сервер», интерфейс администратора и Secret Disk NG Alarm,
- *на рабочей станции администратора* (одной или нескольких) — интерфейс администратора,
- *на рабочей станции для подачи сигнала «тревога»* (одной или нескольких) — Secret Disk NG Alarm.

Создайте на сервере защищённые диски и определите права доступа пользователей к каждому из них.

- Если защищённый диск применяется для защиты файлов баз данных, почтовых хранилищ и других данных, обрабатываемых только выполняющимися на сервере приложениями, то запретите прямой доступ пользователей к этому диску.
- Если защищённый диск используется для хранения файлов, обрабатываемых локально на компьютерах пользователей, то его содержимое должно быть предоставлено для общего доступа по сети. Создайте средствами операционной системы одну или несколько групп пользователей и предоставьте право сетевого доступа к этому диску созданным группам.

После создания защищённого диска, а также после каждого перешифрования (смены ключа шифрования) любого из имеющихся в системе защищённых дисков, обязательно **создавайте резервные копии ключей шифрования дисков и защищённого хранилища**. Проведите тестовое восстановление ключей шифрования для каждого диска, а также восстановление всего защищённого хранилища из созданных резервных копий

Настройте реакцию сервера и, при необходимости, каждого из защищённых дисков на **сигнал «тревога»**. Если в помещении установлена **охранная или пожарная сигнализация**, используется СКУД (система контроля и управления доступом в помещения), обязательно используйте их возможности для подачи серверу сигнала «тревога».

1. **Радиоприёмники** для подачи серверу сигнала «тревога» рекомендуется подключать как к самому серверу, так и к рабочей станции для подачи сигнала «тревога». Подключение радиоприёмника к рабочей станции позволяет значительно увеличить зону подачи сигнала «тревога» с радиобрелока.
2. Подключение радиоприёмника к самому серверу позволит подать сигнал «тревога» даже в случае неработоспособности сети (например, при отключении электропитания в здании сервер может продолжать работу от источника бесперебойного питания, принять и обработать сигнал «тревога»).

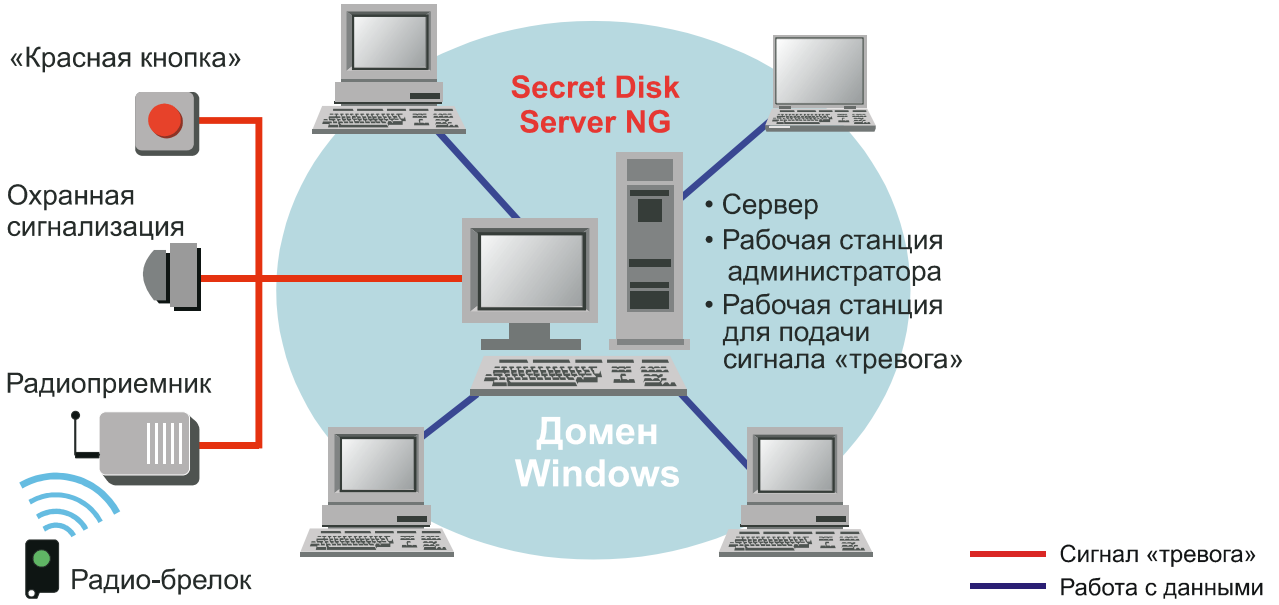
Проведите **тестирование** в различных ситуациях (штатное отключение защищённого диска администратором, отключение по сигналу «тревога», подключение) и убедитесь в том, что все подсистемы настроены и работают корректно.

Всегда имейте как минимум один **запасной (резервный) USB-ключ или смарт-карту eToken с лицензией администратора**. Имея резервную копию хранилища и/или ключей шифрования дисков, даже в случае выхода из строя основного eToken администратора вы сможете оперативно восстановить доступ к защищённым данным и обеспечить возможность продолжения работы сотрудников.

Типовые сценарии использования Secret Disk Server NG 3.1

Один компьютер

Если на вашем сервере имеется возможность подключения двух eToken или в памяти вашего eToken имеется как лицензия администратора, так и лицензия сервера, то вы можете установить все компоненты Secret Disk Server NG 3.1 только на один компьютер.



Преимущества данного сценария:

- нет внешних признаков наличия установленного Secret Disk Server NG 3.1 (подключенные «красные кнопки», ПО для подачи сигнала тревога на компьютерах сотрудников);
- никто из сотрудников организации (за исключением системного администратора и администратора Secret Disk Server NG) не знает об установке и использовании Secret Disk Server NG 3.1.

Недостатки данного сценария:

- отсутствие возможности удалённого управления сервером;
- отсутствие возможности подачи сигнала «тревога» с удалённой рабочей станции;
- ограниченная дальность подачи сигнала «тревога» с помощью радиобрелока (не более 50 метров от самого сервера).

Данный сценарий может рекомендоваться только в исключительных случаях, например при острой нехватке квалифицированного IT-персонала.

Сервер и рабочая станция администратора

Если вы хотите осуществлять управление сервером Secret Disk Server NG через удалённый рабочий стол, вам необходимо установить на сервере как компонент «сервер», так и интерфейс администратора.

Если для управления сервером вы хотите подключаться к нему с помощью консоли управления Microsoft, то интерфейс администратора должен быть установлен на вашей рабочей станции.

Для того чтобы вам были доступны оба способа удалённого управления, установите интерфейс администратора на оба компьютера.

В любом случае, на рабочей станции администратора должен быть установлен eToken Run Time Environment, а для подачи сигнала «тревога» — и Secret Disk NG Alarm. Последний также можно установить как на сервер, так и на рабочую станцию администратора.

Поскольку для регистрации первого администратора Secret Disk Server NG необходимы административные полномочия на сервере, при использовании консоли управления Microsoft рабочая станция администратора и сервер должны входить в один и тот же домен или в домены, между которыми установлены доверительные отношения.

Преимущества данного сценария:

- возможность удалённого управления сервером;
- возможность подачи сигнала «тревога» с удалённой рабочей станции;
- значительно увеличивается дальность подачи сигнала «тревога» с помощью радиобрелока (50 метров от рабочей станции для подачи сигнала «тревога», которая, в свою очередь, может быть удалена от сервера в пределах топологии сети);
- ограничен круг лиц, знающих об установке в организации Secret Disk Server NG (системный администратор и администратор Secret Disk Server NG).

Сервер, рабочая станция администратора, рабочая станция для подачи сигнала «тревога», являющиеся членами доверенных доменов

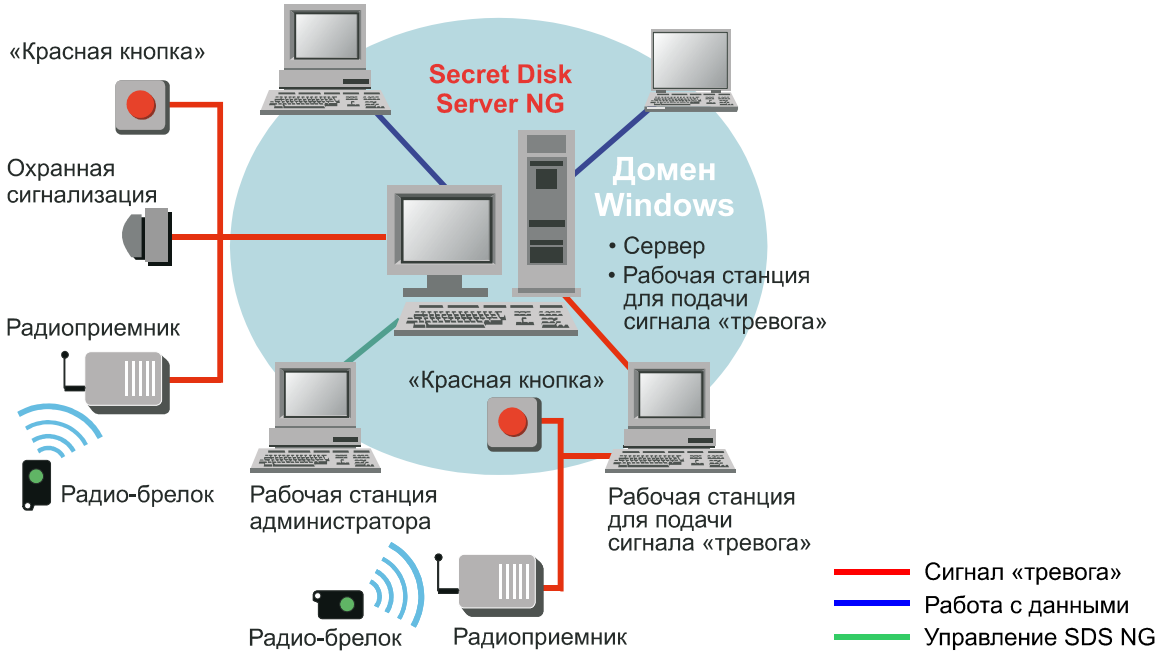
Если вы хотите осуществлять управление сервером Secret Disk Server NG через удалённый рабочий стол, то вам необходимо установить на сервере как компонент «сервер», так и интерфейс администратора.

Если для управления сервером вы хотите подключаться к нему через консоль управления Microsoft, то интерфейс администратора должен быть установлен на вашей рабочей станции.

Для того чтобы вам были доступны оба способа удалённого управления, установите интерфейс администратора на оба компьютера.

В любом случае, на рабочей станции администратора должен быть установлен eToken Run Time Environment.

Secret Disk NG Alarm устанавливается на отдельной рабочей станции. Кроме того, при желании его можно устанвить также и на сервере, и на рабочей станции администратора.



Поскольку для регистрации первого администратора Secret Disk Server NG необходимы административные полномочия на сервере, при использовании консоли управления Microsoft рабочая станция администратора и сервер должны входить в один и тот же домен или в домены, между которыми установлены доверительные отношения.

Преимущества данного сценария:

- возможность удалённого управления сервером;
- возможность подачи сигнала «тревога» с удалённой рабочей станции;
- нет ограничения дальности подачи сигнала «тревога» с помощью радиобрелока (50 метров от рабочей станции для подачи сигнала «тревога», которая, в свою очередь, может быть удалена от сервера в пределах топологии сети).

Недостатки данного сценария:

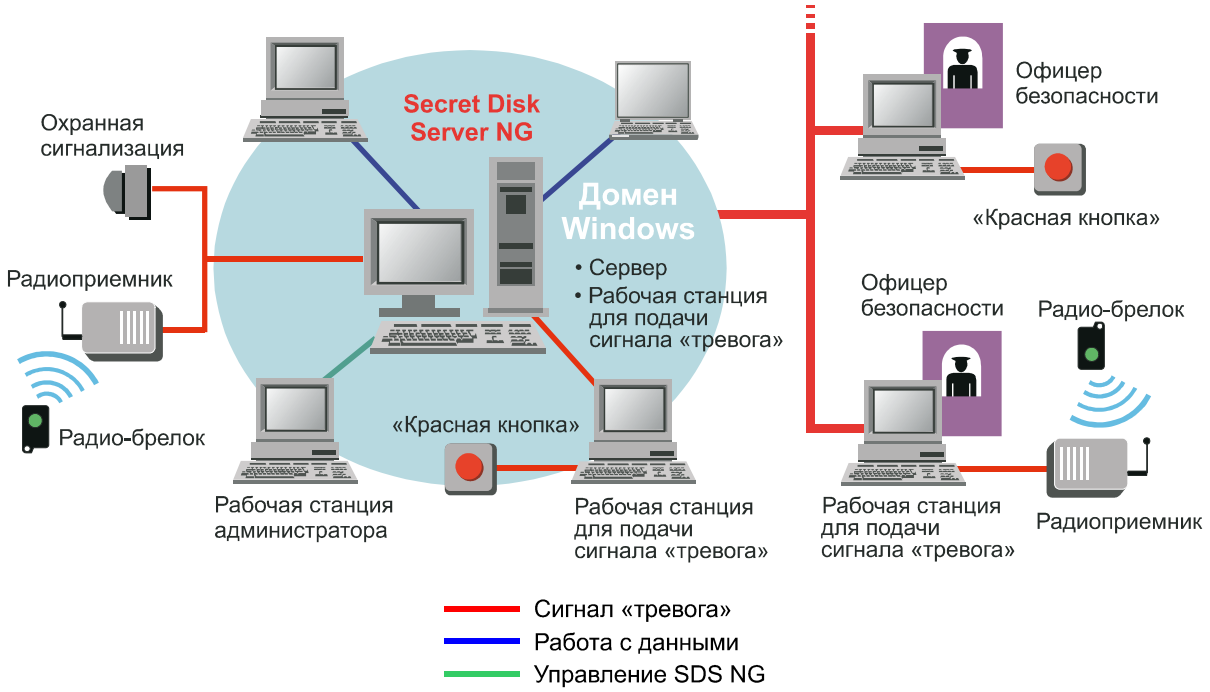
- наличие внешних признаков установленного Secret Disk Server NG (подключенные «красные кнопки», ПО для подачи сигнала «тревога» на компьютерах сотрудников).

Данный сценарий может быть рекомендован в большинстве случаев. Однако при наличии в организации службы охраны рекомендуется использовать следующий сценарий.

Сервер, рабочая станция администратора и внешняя рабочая станция для подачи сигнала «тревога»

В качестве рабочей станции для подачи сигнала «тревога» может выступать, например, компьютер офицера безопасности. Этот компьютер может не быть членом доверенного домена, на нём обычно устанавливается ПО для систем контроля и управления доступом (СКУД).

В данном сценарии компьютер офицера безопасности также используется для подачи сигнала «тревога».



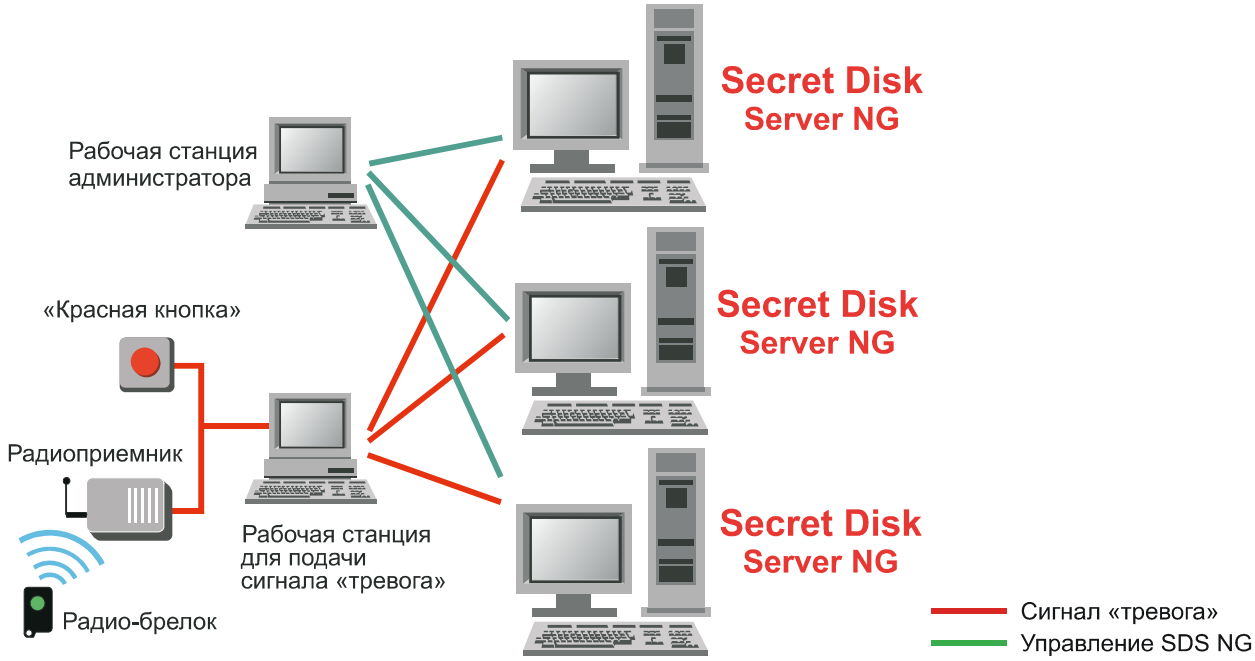
Преимущества данного сценария:

- возможность удалённого управления сервером;
- возможность подачи сигнала «тревога» с удалённой рабочей станции;
- нет ограничения дальности подачи сигнала «тревога» с помощью радио-брелока (50 метров от рабочей станции для подачи сигнала «тревога», которая, в свою очередь, может быть удалена от сервера в пределах топологии сети).

Данный сценарий может быть рекомендован при наличии в организации службы охраны.

Несколько серверов, рабочая станция администратора и рабочая станция для подачи сигнала «тревога»

При необходимости вы можете приобрести дополнительные eToken сервера или лицензии сервера для имеющихся у вас eToken и установить компонент «сервер» на несколько серверов. Управление серверами Secret Disk Server NG можно осуществлять централизованно. Для этого нужно использовать подключение к удалённым рабочим столам или на рабочей станции администратора подготовить консоль управления Microsoft с несколькими оснастками **Управление Secret Disk Server**, подключенными к разным серверам.



В Secret Disk NG Alarm 3.1 предусмотрена возможность подачи сигнала «тревога» одновременно нескольким серверам.

Защита базы данных с помощью Secret Disk Server NG 3.1

Наиболее популярным способом получения несанкционированного доступа к содержимому базы данных (БД) является попытка прочитать файлы БД на уровне ОС (как обычные файлы). Если администратором БД не были предприняты дополнительные меры по шифрованию содержащейся в ней информации (а чаще всего это именно так), то простое копирование файлов БД по сети и последующий прямой просмотр их содержимого позволят злоумышленнику получить доступ к хранящейся в БД информации.

Именно поэтому защищённая система должна быть спроектирована и построена так, чтобы:

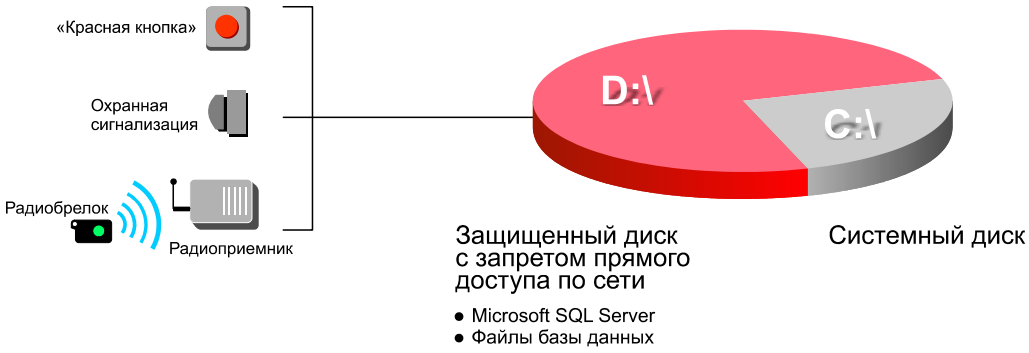
- файлы программного обеспечения СУБД не были доступны по сети;
- к файлам БД на сервере не было доступа по сети — пользователи получают доступ к информации, хранящейся в БД, только посредством СУБД;
- сами файлы БД были зашифрованы. Шифрование файлов БД используется как простой и эффективный способ защиты данных от несанкционированного доступа в случае физического обращения злоумышленника к носителю информации;
- сервер БД не выполнял функции файлового сервера.

Для защиты файлов БД на физическом уровне разместите их на защищённом диске. В настройках защищённого диска запретите прямой доступ пользователей по сети к этому диску.

Выполните следующие действия:

1. Разместите сервер БД в охраняемом помещении. Убедитесь в том, что охранная сигнализация, установленная в серверной комнате, может быть использована для подачи сигнала «тревога» серверу.
2. Создайте средствами Secret Disk Server NG 3.1 защищённый диск достаточного объёма и запретите к нему прямой доступ по сети.
3. Создайте резервную копию ключа шифрования защищённого диска или резервную копию всего защищённого хранилища.
4. Настройте реакцию сервера на сигнал «тревога».
5. Установите ПО СУБД и файлы БД на созданный защищённый диск.
6. Определите сценарии, которые будут выполняться после подключения защищённого диска (запуск СУБД и открытие БД) и перед отключением защищенного диска (закрытие БД и завершение работы СУБД).
7. Проведите тестирование в различных ситуациях (штатное отключение защищённого диска администратором, отключение по сигналу «тревога», подключение) и убедитесь в том, что все подсистемы настроены и работают корректно.

Пример: защита БД Microsoft SQL Server



Защита почтового сервера с помощью Secret Disk Server NG 3.1

При обмене электронными письмами уже давно применяются такие средства обеспечения безопасности данных, как ЭЦП и шифрование электронных писем.

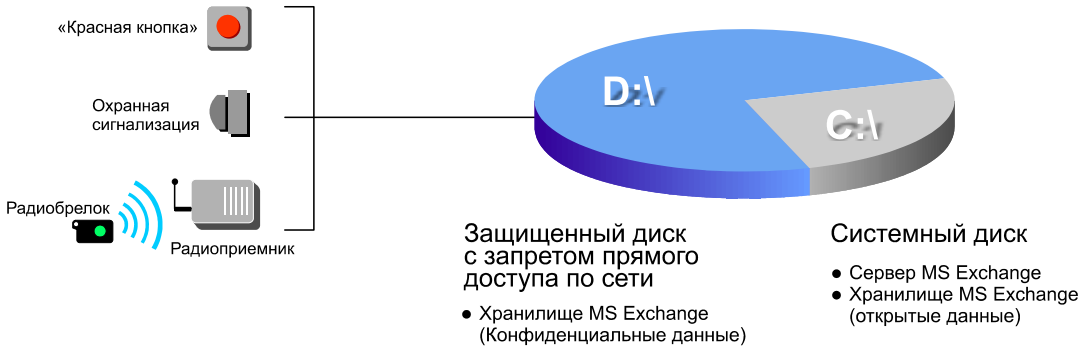
Если отправитель использовал шифрование, то такое письмо, находящееся в хранилище почтового сервера, надёжно защищено от прочтения посторонними. К сожалению, это скорее исключение, чем правило — по данным исследований Gartner Group, более 90% писем, пересылаемых сегодня по сети Интернет, вообще никак не защищены.

Использование почтовых клиентов, обеспечивающих шифрование локального почтового ящика пользователя решает задачу защиты уже полученных писем. Если письмо было отослано в незашифрованном виде, то в процессе доставки оно будет храниться в открытом виде на всех промежуточных почтовых серверах, а на почтовом сервере получателя оно будет храниться в открытом виде вплоть до момента его загрузки почтовым клиентом. В течение всего времени хранения (а это может быть от нескольких минут до нескольких дней или даже недель) злоумышленник, получивший доступ к файлам почтового хранилища на сервере, может прочесть письмо.

По аналогии с защитой базы данных, выполните следующие действия для обеспечения безопасности почтового сервера:

1. Разместите почтовый сервер в охраняемом помещении. Убедитесь в том, что охранная сигнализация, установленная в серверной комнате, может быть использована для подачи сигнала «тревога» серверу.
2. Создайте средствами Secret Disk Server NG 3.1 защищённый диск достаточного объёма и запретите к нему прямой доступ по сети.
3. Создайте резервную копию ключа шифрования защищённого диска или резервную копию всего защищённого хранилища.
4. Настройте реакцию сервера на сигнал «тревога».
5. Установите ПО почтового сервера и сами файлы почтового хранилища на созданный защищённый диск.
6. Определите сценарии, которые будут выполняться после подключения защищённого диска (запуск почтового сервера) и перед отключением защищённого диска (завершение работы почтового сервера).
7. Проведите тестирование в различных ситуациях (штатное отключение защищённого диска администратором, отключение по сигналу «тревога», подключение) и убедитесь в том, что все подсистемы настроены и работают корректно.

Пример: защита почтового сервера Microsoft Exchange Server



Использование Secret Disk Server NG 3.1 на терминальных серверах Windows Server 2003

Преимущества использования Secret Disk Server NG 3.1 для серверов приложений на терминальных серверах Windows Server 2003

В общем случае доступ по сети к дискам сервера может быть получен:

- через сетевые ресурсы (если диск предоставлен в общее пользование или через административные сетевые ресурсы);
- при работе с сервером через удалённый рабочий стол;
- через приложение, выполняющееся на сервере и предоставляющее доступ к данным на диске через собственный интерфейс (например, веб-сервер).

Secret Disk Server NG 3.1 для серверов приложений запрещает доступ к защищённым дискам сервера по сети (как через обычные, так и через административные сетевые ресурсы).

Терминальный сервер на базе Windows Server 2003 может быть настроен таким образом, чтобы при подключении к удалённому рабочему столу пользователи не имели возможности обращаться к локальным дисковым устройствам и копировать данные с дисков сервера на свои диски.

Кроме того, в целях защиты конфиденциальной информации от копирования на терминальном сервере не следует устанавливать приложения, способные передавать данные по сети.

Таким образом, использование Secret Disk Server NG 3.1 для серверов приложений позволяет полностью исключить возможность копирования файлов с терминального сервера.

Переход с предыдущих версий

Новое в версии 3.1

Отличие от Secret Disk Server NG 3.0.x

По сравнению с Secret Disk Server NG 3.0.x в Secret Disk Server NG 3.1 существенно увеличена производительность. Основной вклад в это увеличение внесла применённая в новой версии технология многопоточного шифрования. Эта технология позволяет оптимально использовать имеющиеся на сервере вычислительные мощности.

На многопроцессорных серверах и в однопроцессорных системах с технологией Hyper-Threading происходит значительное увеличение производительности операций чтения и записи при работе с защищёнными дисками за счёт эффективного использования всех доступных вычислительных ресурсов. Применение технологии многопоточного шифрования приводит к заметному увеличению производительности и на обычных однопроцессорных системах.

При повышении производительности на 30—50%, наблюдавшемся на стендовых испытаниях, потери скорости выполнения операций чтения и записи за счёт шифрования данных снижались в несколько раз. Такое снижение привело к тому, что в работе прикладных систем не наблюдалось заметного замедления после перехода к использованию защищённых дисков.

Отличия от Secret Disk Server 1.6

Поддержка современных операционных систем

Secret Disk Server NG 3.1 поддерживает самую современную на сегодняшний день серверную операционную систему семейства Windows — Microsoft Windows Server 2003. Кроме того, Secret Disk Server NG 3.1 может быть установлен на компьютеры, работающие под управлением Microsoft Windows 2000 Advanced Server, Server и Professional, Windows XP Home Edition и Professional.

Интерфейс

Основным интерфейсом администратора Secret Disk Server NG 3.1 является оснастка консоли управления Microsoft. Эта оснастка встроена в консоль управления компьютером. Ее также можно использовать в любых других инструментах, созданных на основе консоли управления Microsoft, в том числе и для удалённого управления.

Удаленное администрирование

В Secret Disk Server NG 3.1 администратор может работать удалённо как через интерфейс консоли управления Microsoft, так и через удалённый рабочий стол. При этом, в отличие от предыдущей версии продукта, eToken администратора при удалённом управлении подключается не к серверу, а к рабочей станции администратора.

Файловые системы

Защищённые диски могут иметь формат любой из файловых систем Windows XP, 2000 и Server 2003:

- FAT (FAT16);

- FAT32;
- NTFS.

После шифрования диски сохраняют исходный формат. Допускается переформатирование защищённых дисков со сменой файловой системы. Форматирование и проверка дисков на наличие ошибок может производиться как стандартными средствами операционной системы, так и встроенными инструментами Secret Disk Server NG 3.1.

Поддержка динамических томов

Защищённые диски могут быть созданы не только на основе основных разделов и логических дисков в дополнительных разделах базовых дисков, но и на основе томов динамических дисков. При этом поддерживается расширение защищённых дисков, созданных на основе простых и составных динамических томов средствами Windows при соблюдении двух условий:

- расширяемый том должен иметь формат NTFS;
- расширяемый том должен быть изначально создан на динамическом диске, а не получен из основного раздела или логического диска в результате преобразования базового диска в динамический.

Отсутствие встроенных криптографических средств

Secret Disk Server NG 3.1 не имеет встроенных средств шифрования, но позволяет подключать внешние. Это даёт администраторам системы больше возможностей выбора алгоритма шифрования, максимально удовлетворяющего их требованиям. Для осуществления криптографических преобразований могут применяться:

- криптографический драйвер режима ядра и Microsoft Enhanced CSP, входящие в состав Microsoft Windows;
- Signal-COM CSP;
- КриптоПро CSP 2.0;
- пакет дополнительных алгоритмов шифрования Secret Disk NG Crypto Pack 3.1, бесплатно загружаемый с веб-сайта компании Aladdin.

Запрет сетевого доступа

Доступ к защищённому диску по сети можно запретить, например, для защиты корпоративных баз данных.

Сертификаты открытого ключа

В Secret Disk Server NG 3.1 каждый администратор использует сертификат и связанные с ним криптографические ключи для защиты мастер-ключей защищённых дисков и аутентификации. Закрытый ключ, соответствующий сертификату, служит для расшифрования мастер-ключей при осуществлении операций с защищёнными дисками, а также применяется в процедуре аутентификации администратора при получении доступа к инструментам управления Secret Disk Server NG 3.1.

Для каждого поставщика криптографии, использующегося при шифровании дисков, вы выбираете свой, совместимый с этим поставщиком сертификат. Например, если часть ваших защищённых дисков зашифрована с использованием алгоритма TripleDES

криптографическим драйвером режима ядра, входящим в состав Windows, а другая часть дисков — с использованием алгоритма ГОСТ 28147-89, поставляемого КриптоПро CSP 2.0, то у вас должно быть два сертификата для защиты мастер-ключей защищённых дисков. При аутентификации в системе Secret Disk Server NG 3.1 вы можете применять любой из них.

Сертификат и связанный с ним закрытый ключ должны храниться в памяти eToken.

Использование при работе с Secret Disk Server NG 3.1 сертификатов, выданных в соответствии с правилами, принятыми в вашей организации, способствует тесной интеграции Secret Disk Server NG 3.1 с инфраструктурой открытого ключа Windows 2000 и 2003, RSA Keon, Entrust Authority, Baltimore UniCERT и т. п.

Создание сертификата

Если вы не располагаете сертификатом, Secret Disk Server NG 3.1 сгенерирует его для вас.

Защищенное хранилище

В отличие от Secret Disk Server 1.6, Secret Disk Server NG 3.1 хранит мастер-ключи защищённых дисков не в памяти eToken, а в защищённом хранилище на системном диске. Благодаря этому у вас появилась возможность полностью уничтожать ключевую информацию нажатием «красной кнопки»: при соответствующих настройках, даже если злоумышленники завладеют электронным ключом или смарт-картой eToken, узнают PIN-код и будут обладать полным доступом к серверу, после поступления на сервер сигнала «тревога» они не смогут прочесть информацию, не располагая резервной копией защищенного хранилища.

Сертифицированные российские средства криптографической защиты

1. Совместимость с Signal-COM CSP и КриптоПро CSP 2.0

Secret Disk Server NG 3.1 совместим с поставщиками службы криптографии Signal-COM CSP и КриптоПро CSP 2.0. Теперь вы можете использовать сертифицированные российские криптографические средства для шифрования дисков, защиты мастер-ключей защищённых дисков и аутентификации в системе Secret Disk Server NG 3.1.

2. Алгоритм шифрования дисков

При шифровании дисков с помощью Signal-COM CSP и КриптоПро CSP 2.0 используется алгоритм, соответствующий ГОСТ 28147-89 «Система обработки информации. Защита криптографическая».

Перешифрование дисков

Теперь, если вы хотите сменить алгоритм шифрования диска или мастер-ключ защищённого диска, вам не надо расшифровывать диск, тем самым временно снимая защиту с данных. В Secret Disk Server NG 3.1 предусмотрен удобный механизм перешифрования.

Приостановка процессов шифрования

В Secret Disk Server NG 3.1 остановка или прерывание процесса зашифрования, перешифрования или расшифрования не приводит к потере данных. Приостановленный вручную или прерванный из-за отключения питания компьютера процесс может быть возобновлён в любой удобный для вас момент.

Сценарии

Secret Disk Server NG 3.1 позволяет автоматически запускать сценарии не только после подключения защищённых дисков, но и перед их подключением, а также перед отключением и после него.

Обзор возможных путей перехода

Система Secret Disk Server NG 3.1 не позволяет работать с секретными дисками, созданными с помощью Secret Disk Server 1.x. При этом в операционных системах Microsoft Windows 2000 и XP возможна одновременная работа Secret Disk Server 1.x и Secret Disk Server NG 3.1. При такой схеме система Secret Disk Server 1.x работает только со своими секретными дисками, а Secret Disk Server NG 3.1 — только со своими защищёнными дисками.

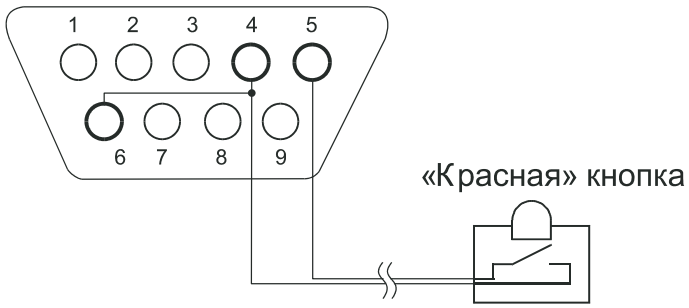
Вы можете установить систему Secret Disk Server NG 3.1, зашифровать с её помощью диски достаточной ёмкости, перенести данные со старых секретных дисков на новые, а затем расшифровать старые секретные диски и удалить Secret Disk Server 1.x.

Если на вашем сервере установлена операционная система Microsoft Windows NT, то перед приведением сервера в соответствие системным требованиям Secret Disk Server NG 3.1 рекомендуется перенести все данные с секретных дисков на обычные диски, расшифровать все секретные диски и удалить Secret Disk Server 1.x.

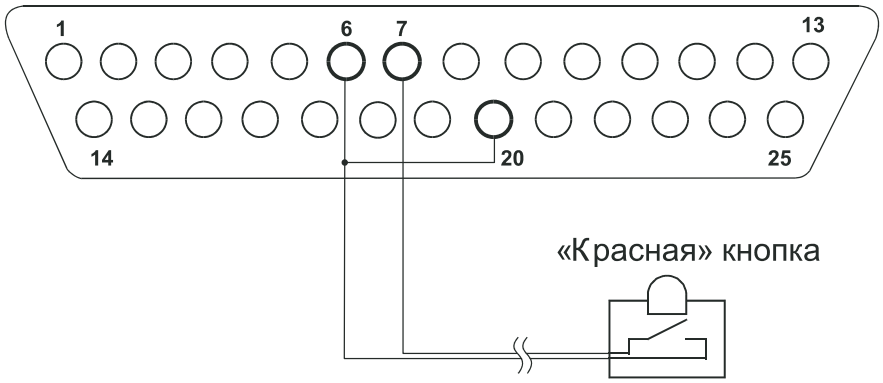
В «красной кнопке», использовавшейся с Secret Disk Server 1.x, замыкались контакты 2 и 3 штекера DB-9 (контакты 3 и 2 штекера DB-25). В «красной кнопке» Secret Disk NG Alarm 3.0 замыкались контакты 4 и 6 штекера DB-9 (контакты 20 и 6 штекера DB-25). Если вы хотите использовать устаревшую кнопку в комплексе Secret Disk NG Alarm 3.1, подключите жилы, замыкаемые кнопкой, к другим контактам:

- для штекера DB-9 — к замкнутым накоротко контактам 4 и 6 с одной стороны и контакту 5 с другой стороны;
- для штекера DB-25 — к замкнутым накоротко контактам 6 и 20 с одной стороны и контакту 7 с другой стороны.

Штекер DB-9, вид со стороны пайки



Штекер DB-25, вид со стороны пайки



Системные требования и принципы работы версий Secret Disk Server NG 3.0.x и 3.1 одинаковы. Для обновления программного обеспечения нового поколения Secret Disk Server не требуются операции шифрования.

Примечание:

При переходе от демонстрационной версии Secret Disk Server NG 3.x к полнофункциональной версии необходимо предварительно расшифровать все защищённые диски.

Пошаговый переход для наиболее типичных случаев

Демонстрационная версия Secret Disk Server NG 3.1

Для перехода от демонстрационной версии Secret Disk Server NG 3.1 к полнофункциональной вам потребуются:

- программа установки полнофункциональной версии;
- eToken сервера с лицензией сервера приложений или/и лицензией файл-сервера;
- eToken администратора с лицензией администратора Secret Disk Server NG.

Для того чтобы заменить демонстрационную версию Secret Disk Server NG 3.1 полнофункциональной, выполните следующее.

1. Расшифруйте все защищённые диски.
2. Удалите демонстрационную версию Secret Disk Server NG 3.1, включая защищённое хранилище.

3. Установите полнофункциональную версию Secret Disk Server NG 3.1 и зарегистрируйте администратора Secret Disk Server NG на данном сервере, выбрав сертификат(ы) для защиты мастер-ключей защищённых дисков и аутентификации.
4. Зашифруйте диски, содержащие конфиденциальные данные.

Secret Disk Server NG 3.0.x

Для того чтобы обновить версию Secret Disk Server NG, выполните следующее.

1. Удалите компоненты Secret Disk Server NG 3.0.x, сохранив на сервере защищённое хранилище.
2. Установите компоненты Secret Disk Server NG 3.1.

Secret Disk Server 1.6 и Windows 2000 Server

1. Убедитесь в том, что в операционной системе установлен пакет обновления 2 или выше. Если это не так, установите необходимый пакет обновления. Для этого можно загрузить программу установки с веб-сайта Microsoft или воспользоваться программой Windows Update или Microsoft Update.
2. Установите Secret Disk Server NG 3.1 и зарегистрируйте администратора Secret Disk Server NG на данном сервере, выбрав сертификат(ы) для защиты мастер-ключей защищённых дисков и аутентификации.
3. Зашифруйте с помощью Secret Disk Server NG 3.1 один или несколько дисков достаточной ёмкости.
4. Скопируйте все данные с секретных дисков Secret Disk Server 1.6 на созданные с помощью Secret Disk Server NG 3.1 защищённые диски.
5. Расшифруйте все секретные диски Secret Disk Server 1.6.
6. Удалите Secret Disk Server 1.6.

Secret Disk Server 1.31 и Windows NT 4.0 Server

1. При наличии достаточного дискового пространства перенесите все данные с секретных дисков на обычные диски.
2. Расшифруйте все секретные диски.
3. Удалите Secret Disk Server 1.31.
4. Установите на сервер операционную систему Windows 2000, Windows Server 2003 или Windows XP.
5. Для Windows 2000 установите пакет обновления 2 или выше или убедитесь в том, что он входит в уже осуществлённую вами установку. Для Windows XP установите пакет обновления 1 или выше или убедитесь в том, что он входит в уже осуществлённую вами установку.
6. Установите eToken Run Time Environment 3.65.
7. Установите Secret Disk Server NG 3.1 и зарегистрируйте администратора Secret Disk Server NG на данном сервере, выбрав сертификат(ы) для защиты мастер-ключей защищённых дисков и аутентификации.
8. Зашифруйте один или несколько дисков подходящей ёмкости.
9. При необходимости перенесите все конфиденциальные данные с обычных дисков на защищённые.

Альтернативные пути перехода

Рекомендуемый способ перехода от Secret Disk Server 1.x на платформе Windows 2000/XP предполагает установку Secret Disk Server NG 3.1 до удаления Secret Disk Server 1.x и перенос данных со старых секретных дисков на новые. Недостаток этого способа: требуется хотя бы один незащищённый диск, объём свободного места на котором позволяет вместить информацию, расположенную на секретных дисках.

Если у вас нет такого количества свободного дискового пространства, то сначала расшифруйте все секретные диски, удалите Secret Disk Server 1.x, а затем установите Secret Disk Server NG 3.1 и зашифруйте диски. Однако этот альтернативный способ тоже имеет недостатки:

- конфиденциальные данные в течение некоторого времени оказываются незащищёнными;
- в случае если операция расшифрования секретных дисков прервется (например, при отключении питания), данные будут потеряны.

Настройка Secret Disk Server NG 3.1 и операционной системы

Имеющиеся возможности по настройке

Вы можете управлять списком администраторов, имеющих полномочия для работы с защищёнными дисками. Каждый администратор может выбирать сертификат, который он использует для аутентификации и защиты ключей шифрования дисков. Отзывом данного сертификата или исключением центра сертификации из числа доверенных можно запретить администратору работу с Secret Disk Server NG 3.1.

Вы можете изменять свойства защищённого диска, в том числе:

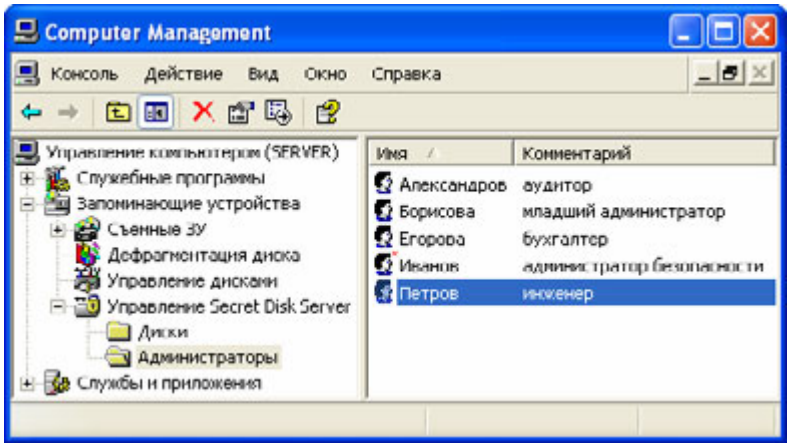
- предоставлять другим администраторам доступ к нему или отказывать в доступе;
- осуществлять настройки, связанные с правилами подключения и отключения.

Реакция сервера на поступление сигнала «тревога», а также время ожидания результата выполнения сценариев при подключении и отключении дисков также подлежат настройке.

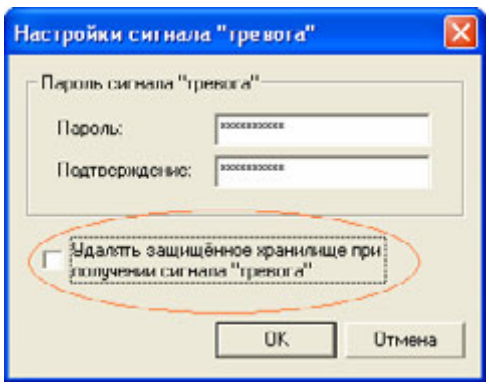
Параметры настройки Secret Disk Server NG 3.1

Вы можете изменять значения следующих параметров:

- свойства сервера:
  - список администраторов Secret Disk Server NG;

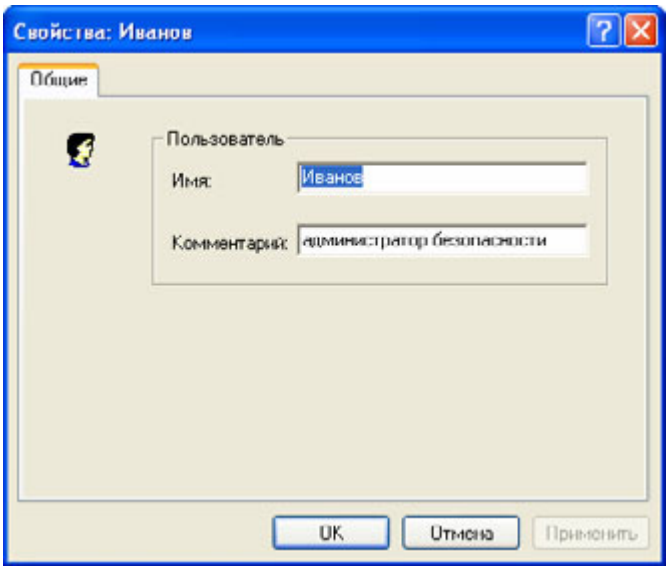


  - удаление защищённого хранилища при получении сигнала «тревога»;



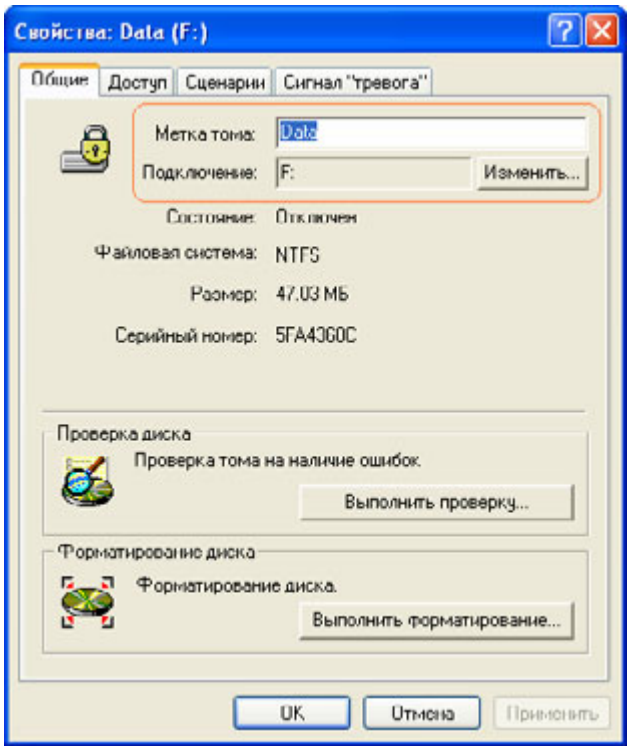
- время ожидания результата выполнения сценариев в миллисекундах (параметр `ActionExecWaitTimeout` типа `DWORD` в разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Secret Disk NG\Server`);

- свойства учётной записи администратора Secret Disk Server NG:



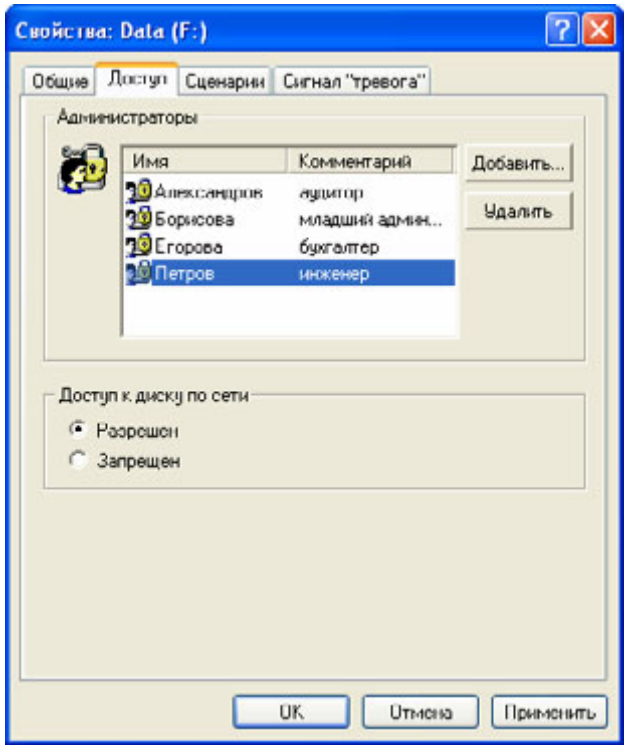
  - имя;
  - комментарий;

- свойства защищённого диска (настраиваются в окне свойств защищённого диска):

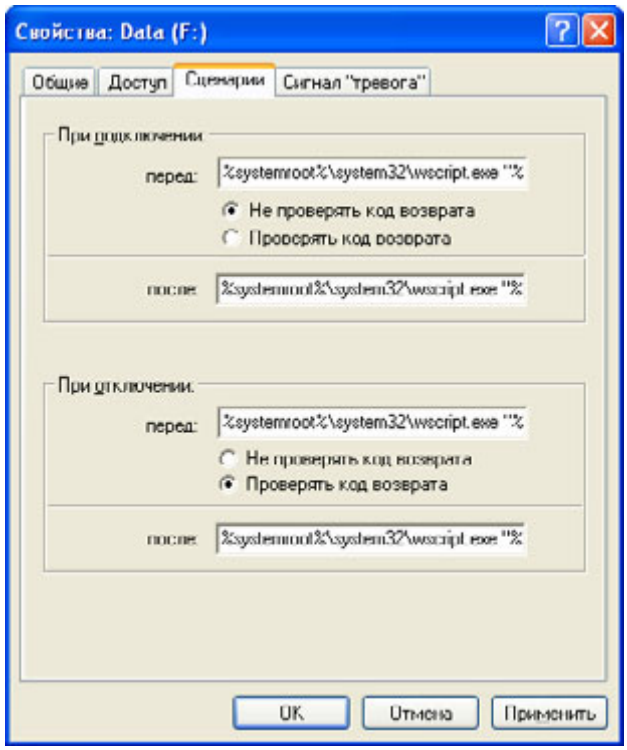


  - метка тома (во вкладке **Общие**);
  - буква диска (во вкладке **Общие**);

- настройки доступа (во вкладке **Доступ**):

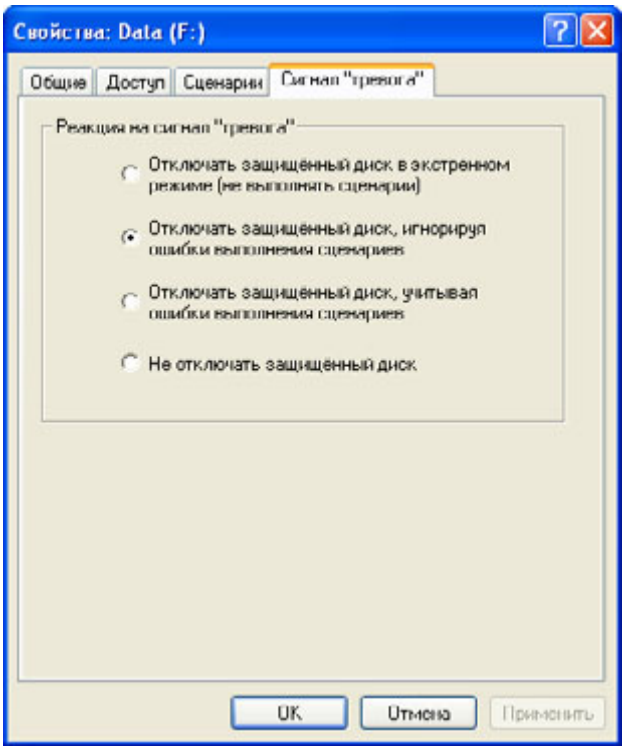


  - список администраторов защищённого диска;
  - запрет доступа к защищённому диску по сети;
- настройки сценариев (во вкладке **Сценарии**):



  - строковая команда для запуска сценария перед подключением защищённого диска;

  - игнорирование кода возврата сценария, запускаемого перед подключением защищённого диска;
  - строковая команда для запуска сценария после подключения защищённого диска;
  - строковая команда для запуска сценария перед отключением защищённого диска;
  - игнорирование кода возврата сценария, запускаемого перед отключением защищённого диска;
  - строковая команда для запуска сценария после отключения защищённого диска;
- реакция защищённого диска на сигнал «тревога» (во вкладке **Сигнал «тревога»**).



Параметры настройки операционной системы

Настройка ОС может потребоваться для разрешения или запрета использования того или иного сертификата для аутентификации в Secret Disk Server NG 3.1. Настройке подлежат следующие параметры:

- на сервере:
  - список **Доверенные корневые центры сертификации** / **Trusted Root Certification Authorities** локального компьютера;
  - список **Промежуточные центры сертификации** / **Intermediate Certification Authorities** локального компьютера;
  - список **Сертификаты, к которым нет доверия** / **Untrusted Certificates** локального компьютера;

- на рабочей станции администратора:
  - список **Доверенные корневые центры сертификации** / **Trusted Root Certification Authorities** текущего пользователя;
  - список **Промежуточные центры сертификации** / **Intermediate Certification Authorities** текущего пользователя;
  - список **Сертификаты, к которым нет доверия** / **Untrusted Certificates** текущего пользователя.

Администрирование и сопровождение

Роли

Для лиц, работающих с Secret Disk Server NG 3.1, предусмотрены следующие роли:

- *системный администратор*;
- *администратор Secret Disk Server NG*;
- *администратор приложения*;
- *пользователь*;
- *офицер безопасности*.

Системный администратор:

- устанавливает и удаляет программное и аппаратное обеспечение;
- регистрирует первого *администратора Secret Disk Server NG*;
- предоставляет *пользователям* права доступа к защищённым дискам.

Администратор Secret Disk Server NG:

- является владельцем eToken администратора;
- добавляет и удаляет других администраторов *Secret Disk Server NG*;
- шифрует диски:
  - зашифрование;
  - перешифрование;
  - расшифрование;
- настраивает параметры сервера и защищённых дисков:
  - пароль сигнала «тревога»;
  - реакцию сервера и защищённых дисков на сигнал «тревога»;
  - настройки доступа к защищённым дискам;
  - настройка сценариев, выполняемых при подключении и отключении защищённых дисков;
- подключает защищённые диски и отключает их в штатном режиме;
- выполняет резервное копирование и восстановление ключевой информации:
  - ключей шифрования дисков;
  - защищённого хранилища.

Администратор приложения:

- составляет сценарии, включающие команды для приложения, выполняемые при подключении и отключении защищённых дисков, к которым обращается приложение;
- устанавливает права доступа *пользователей* к приложению.

Пользователь:

- работает с данными на защищённых дисках на основании прав, предоставленных *системным администратором*;
- работает с серверными приложениями, обрабатывающими данные на защищённых дисках, на основании прав, предоставленных *администратором приложения*. Сетевой доступ к таким защищённым дискам может быть запрещён *администратором Secret Disk Server NG*.

Офицер безопасности:

- подаёт сигнал «тревога»:
  - нажатием «красной кнопки»;
  - с помощью радио-брелока;
  - через интерфейс пользователя утилит Secret Disk NG Alarm 3.1.
- хранит резервные копии:
  - ключей шифрования защищённых дисков;
  - защищённого хранилища.

При необходимости один и тот же человек может совмещать несколько ролей.

Обзор средств администрирования и сопровождения

Основным инструментом администратора Secret Disk Server NG является оснастка **Управление Secret Disk Server** консоли управления Microsoft. Для удалённого управления её можно подключать к другому компьютеру. Возможно также управление через удалённый рабочий стол.

Инструментами, доступными из оснастки **Управление Secret Disk Server**, вы можете осуществлять настройки сервера, добавлять и удалять администраторов, выбирать сертификаты, шифровать диски, осуществлять резервное копирование и восстановление ключей шифрования, подключать и отключать защищённые диски, менять их свойства, а также форматировать и проверять на наличие ошибок.

Для создания сертификатов, используемых при аутентификации и защите мастер-ключей защищённых дисков, вам потребуется соответствующий центр сертификации. В качестве альтернативы вы можете использовать встроенное средство создания сертификатов Secret Disk Server NG 3.1.

Для предотвращения несанкционированного доступа к информации в чрезвычайных ситуациях предназначены инструменты Secret Disk NG Alarm 3.1, позволяющие подавать серверу сигнал «тревога» как с помощью аппаратной «красной кнопки», так и с помощью программных утилит.

Рекомендации по резервному копированию / восстановлению данных

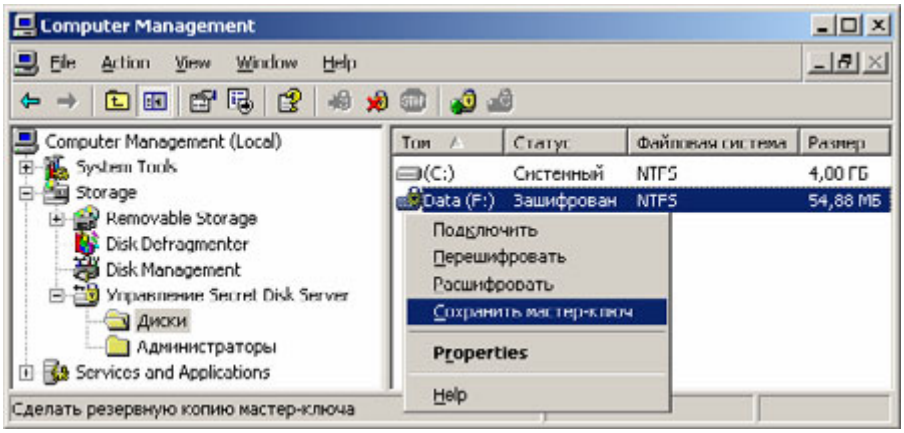
Резервное копирование и восстановление мастер-ключа защищенного диска

Мастер-ключи защищённых дисков хранятся в защищённом хранилище. Для каждого администратора защищённого диска хранится отдельная защищённая копия мастер-ключа.

Если защищённое хранилище будет повреждено или утрачено, или если защищённый диск будет перенесён на другой компьютер, доступ к данным на защищённом диске станет

невозможным. Если вы потеряете eToken администратора, вы не сможете управлять защищёнными дисками.

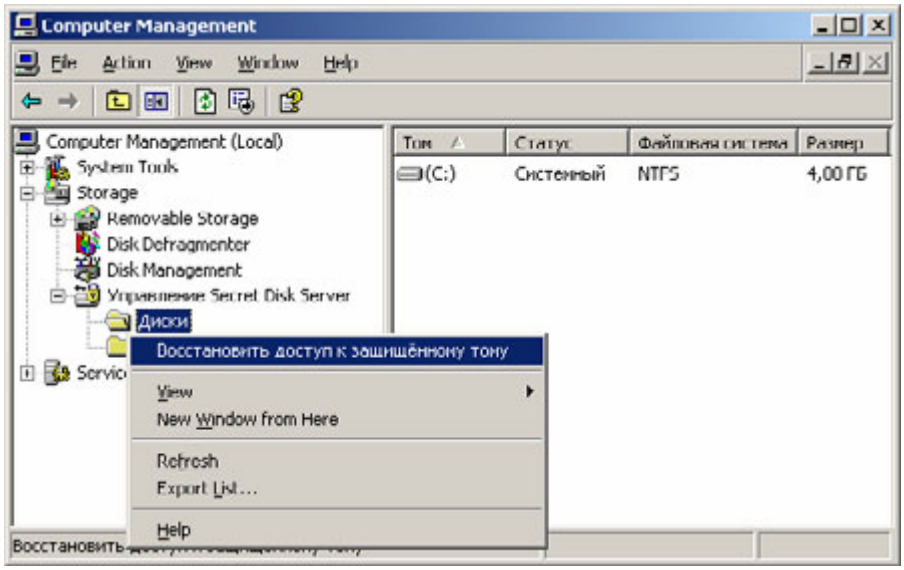
Для того чтобы предотвратить потерю данных, создавайте резервные копии мастер-ключей всех защищённых дисков. Для этого служит пункт **Сохранить мастер-ключ** контекстного меню диска в списке дисков.



Для восстановления доступа к защищённому диску потребуется владение архивным файлом мастер-ключа и знание пароля, заданного при резервном копировании. Храните файл в надёжном месте. Запомните заданный пароль или запишите его и сохраните в надёжном месте, недоступном для посторонних.

Кроме того, при восстановлении доступа у вас должен быть выбран сертификат для использования с соответствующим поставщиком криптографии. Поэтому перед восстановлением убедитесь в том, что такой сертификат у вас выбран, и что он является действительным.

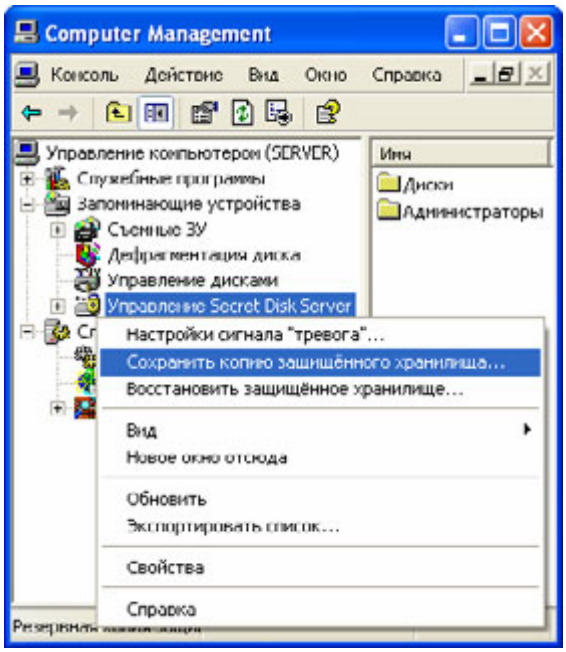
Для восстановления доступа к защищённому диску с помощью резервной копии мастер-ключа служит пункт **Восстановить доступ к защищённому тому** контекстного меню узла **Диски**.



Резервное копирование и восстановление защищённого хранилища

Поскольку защищённое хранилище содержит информацию об администраторах Secret Disk Server NG и зашифрованные копии мастер-ключей защищённых дисков для всех администраторов Secret Disk Server NG, потеря этого объекта может привести к потере

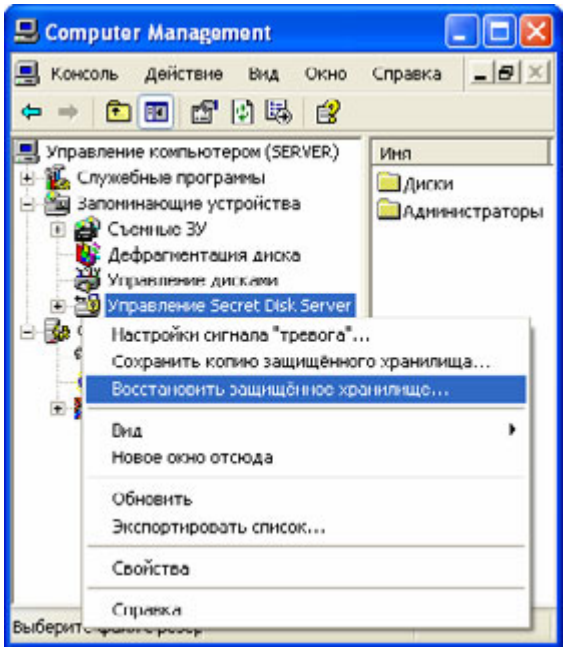
данных или к необходимости по отдельности восстанавливать доступ к защищённым дискам для всех администраторов с помощью архивов мастер-ключей защищённых дисков. Для предотвращения подобных ситуаций сделайте резервную копию всего защищённого хранилища. Для этого воспользуйтесь пунктом **Сохранить копию защищённого хранилища** контекстного меню узла **Управление Secret Disk Server**.



Необходимость восстановления защищённого хранилища может возникнуть в случаях:

- удаления защищённого хранилища по сигналу «тревога»;
- повреждения или случайного удаления файлов защищённого хранилища на системном диске;
- удаления Secret Disk Server NG 3.1 и повторной установки;
- переноса защищённых дисков на другой сервер.

Имея резервную копию, вы сможете легко восстановить работоспособность Secret Disk Server NG 3.1 в случае повреждения или утраты защищённого хранилища. Для этого в контекстном меню узла **Управление Secret Disk Server** служит пункт **Восстановить защищённое хранилище**.



Резервное копирование и восстановление кофиденциальных данных

Для резервного копирования и восстановления конфиденциальных данных вы можете использовать как средства, встроенные в операционную систему, так и программы сторонних разработчиков.

Использование программы архивации Windows

При использовании программы архивации Windows сохраняйте резервные копии на защищённых дисках, которые при необходимости можно подключить на другом сервере. Убедитесь в том, что вы имеете возможность такого подключения:

- создайте на отдельном переносном носителе резервную копию мастер-ключа защищённого диска, на котором хранится или будет храниться архив конфиденциальных данных;
- подключите устройство защищённого диска с архивом к другому серверу;
- с помощью резервной копии мастер-ключа восстановите доступ к защищённому тому;
- убедитесь в том, что вы можете подключить защищённый диск.

Процессы резервного копирования и восстановления данных на защищённых дисках при помощи программы архивации Windows ничем не отличаются от аналогичных процедур на обычных дисках.

Использование Acronis True Image 8.0

Acronis True Image 8.0 позволяет сохранять образы защищённых дисков в виде файлов. При этом, поскольку данные на защищённом диске всегда зашифрованы, данные в архиве также оказываются зашифрованными, и вы можете сохранять файлы образов защищённых дисков на обычных, незащищённых носителях.

Для восстановления данных из файла-образа вам потребуется сначала восстановить диск, а затем (при необходимости) восстановить доступ к защищённому тому или защищённое хранилище. Поэтому, сохраняя образ защищённого диска, убедитесь в том, что вы располагаете резервной копией мастер-ключа этого защищённого диска или/и резервной копией защищённого хранилища.

Интеграция с другими подсистемами

Интеграция с подсистемой безопасности ОС

Для регистрации первого администратора Secret Disk Server NG необходимо иметь полномочия администратора на сервере. Управление полномочиями лучше всего осуществлять посредством групп пользователей.

Аутентификация администраторов Secret Disk Server NG осуществляется на основе сертификатов, интегрированных в инфраструктуру открытых ключей. Для успешной аутентификации необходимо, чтобы сертификат был действительным как в контексте локального компьютера на сервере, так и в контексте текущего пользователя на рабочей станции администратора.

Интеграция с подсистемами безопасности других приложений

Для аутентификации администраторов и защиты мастер-ключей защищённых дисков могут использоваться сертификаты, применяемые в других приложениях.

Типовая модель интеграции

В частности, Secret Disk Server NG 3.1 совместим с сертификатами пользователя со смарт-картой, которые применяются в доменах Windows 2000/2003. Эти же сертификаты могут быть использованы для электронной подписи и шифрования электронных писем.

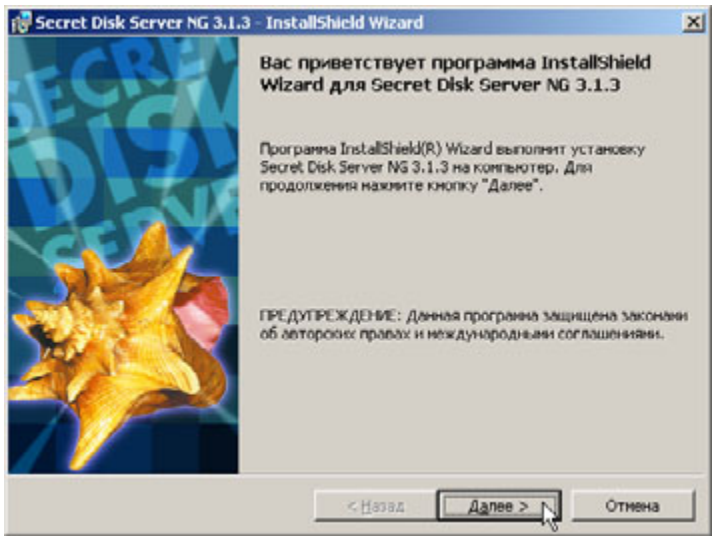
Пошаговые инструкции выполнения типовых задач по администрированию Secret Disk Server NG 3.1

Установка сервера и интерфейса администратора Secret Disk Server NG

Шаг 1

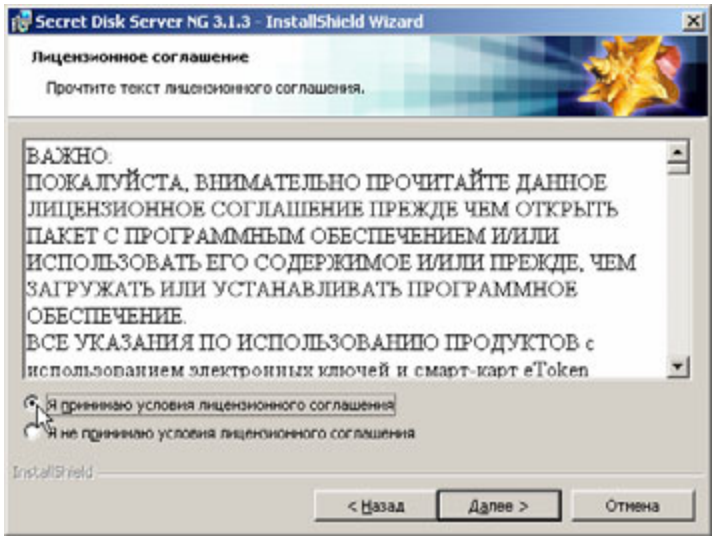
Вставьте компакт-диск Secret Disk Server NG 3.1 в устройство чтения компакт-дисков. На экране появится меню компакт-диска. Нажмите **Установить Secret Disk Server NG**.

Шаг 2



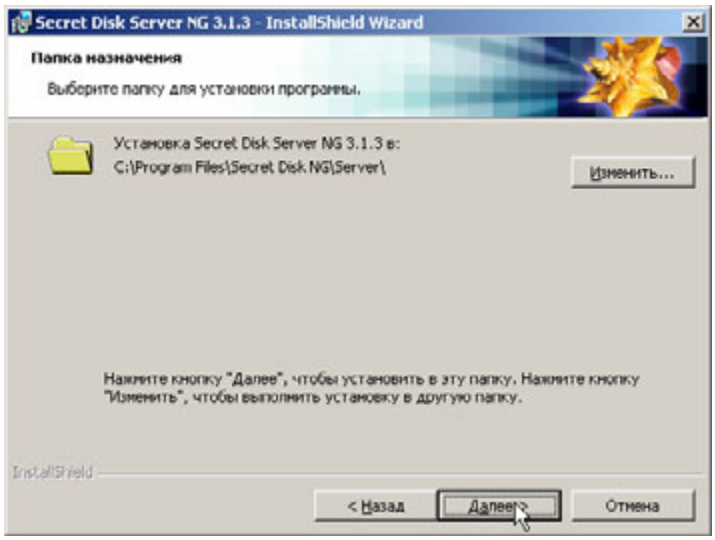
В окне приветствия программы установки нажмите **Далее**.

Шаг 3



Ознакомьтесь с лицензионным соглашением. Если вы согласны с его условиями, выберите **Я принимаю условия Лицензионного соглашения** и нажмите **Далее**. Если не согласны, нажмите **Отмена**, и в появившемся окне нажмите **Да**. В этом случае ни сервер, ни интерфейс администратора Secret Disk Server NG не будут установлены.

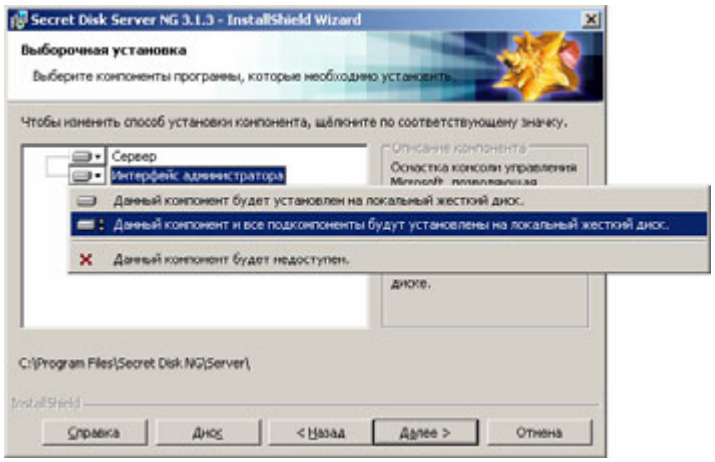
Шаг 4



Для того чтобы компоненты Secret Disk Server NG были установлены в папку по умолчанию, нажмите **Далее**.

Если вы хотите, чтобы компоненты Secret Disk Server NG были установлены в другую папку, нажмите **Изменить**, выберите папку, нажмите **OK** и нажмите **Далее**.

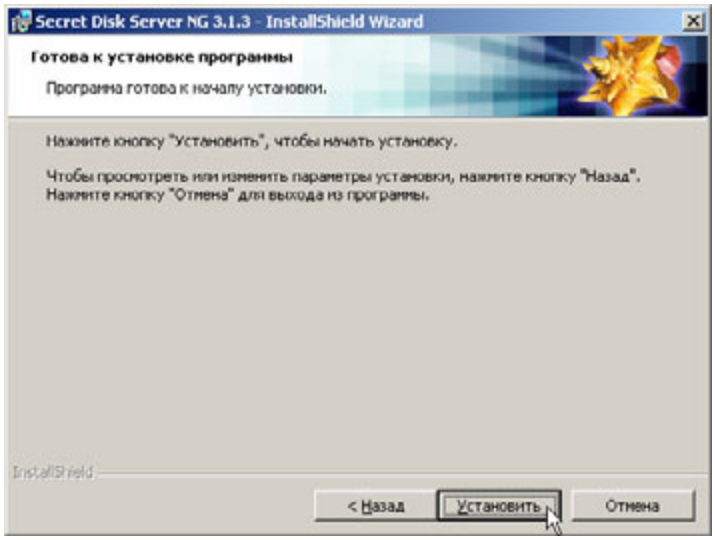
Шаг 5



Убедитесь в том, что компоненты **Сервер** и **Интерфейс администратора** выбраны, и нажмите **Далее**.

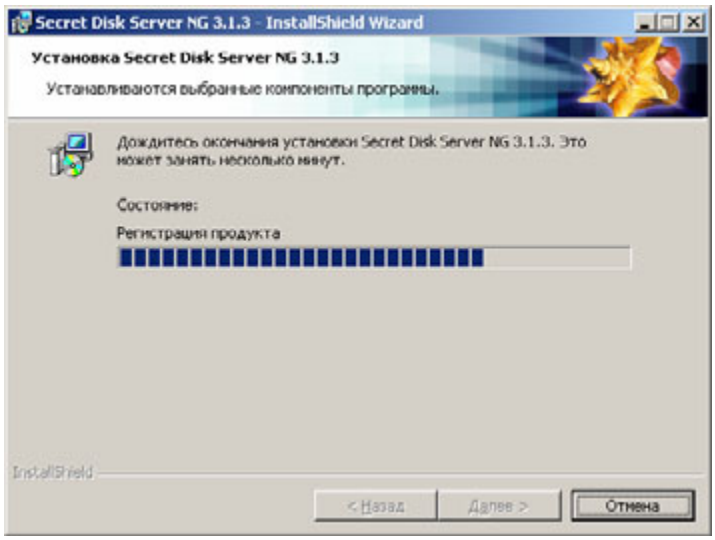
Примечание:
На сервере рекомендуется устанавливать оба компонента, а на рабочей станции администратора — только интерфейс администратора.

Шаг 6



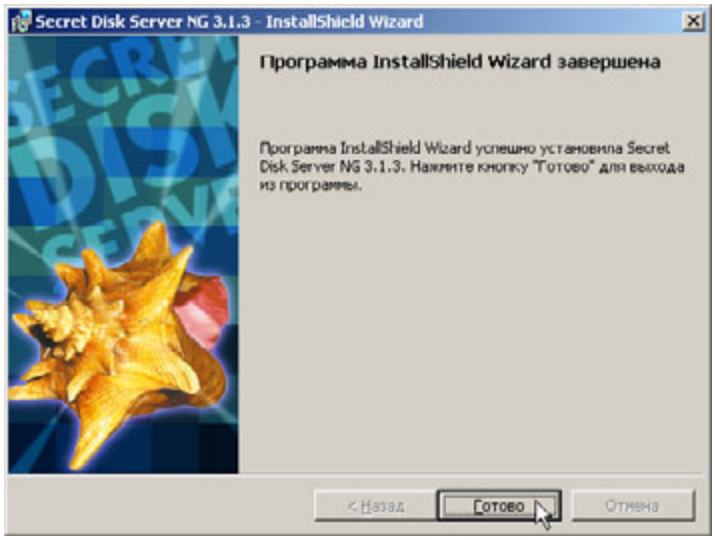
Для начала процесса установки нажмите **Установить**.

Шаг 7



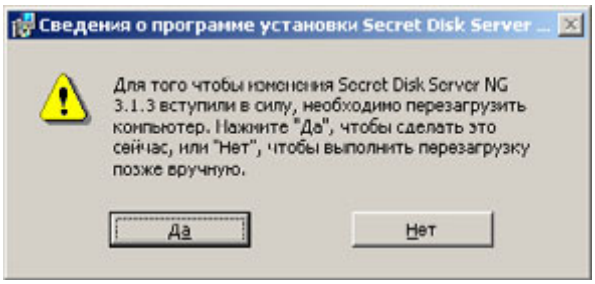
Процесс установки займёт некоторое время. Дождитесь его окончания.

Шаг 8



Убедитесь в том, что процесс установки завершён успешно, и нажмите **Готово**.

Шаг 9



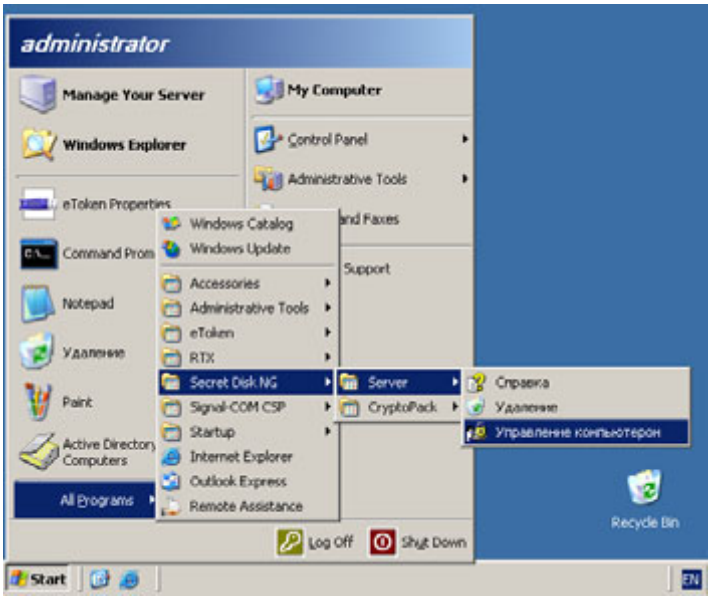
Для завершения процесса установки может потребоваться перезагрузка компьютера. В этом случае нажмите **Да** для немедленной перезагрузки или **Нет**, если вы хотите осуществить перезагрузку позднее. После перезагрузки установка программных компонентов будет считаться успешно состоявшейся. Дальнейшие шаги относятся только к серверу.

Шаг 10

Подключение eToken сервера

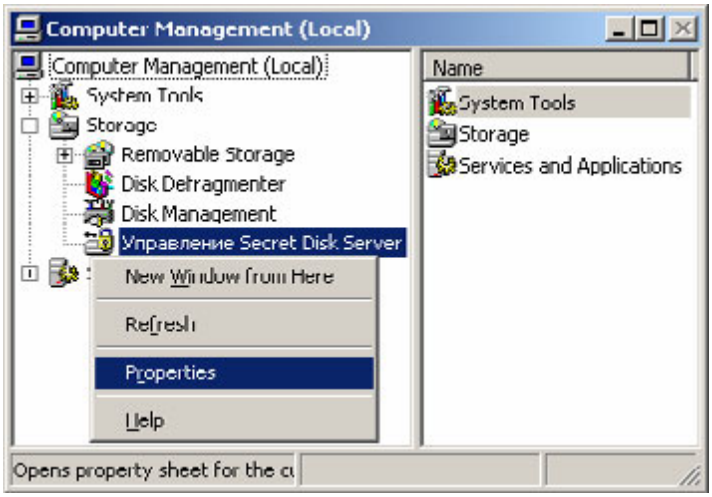
Сервер Secret Disk Server NG будет работоспособен только при подключенном eToken с лицензией сервера. Подключите eToken сервера к порту USB (если это USB-ключ eToken) или вставьте в устройство чтения смарт-карт (если это смарт-карта eToken PRO).

Шаг 11



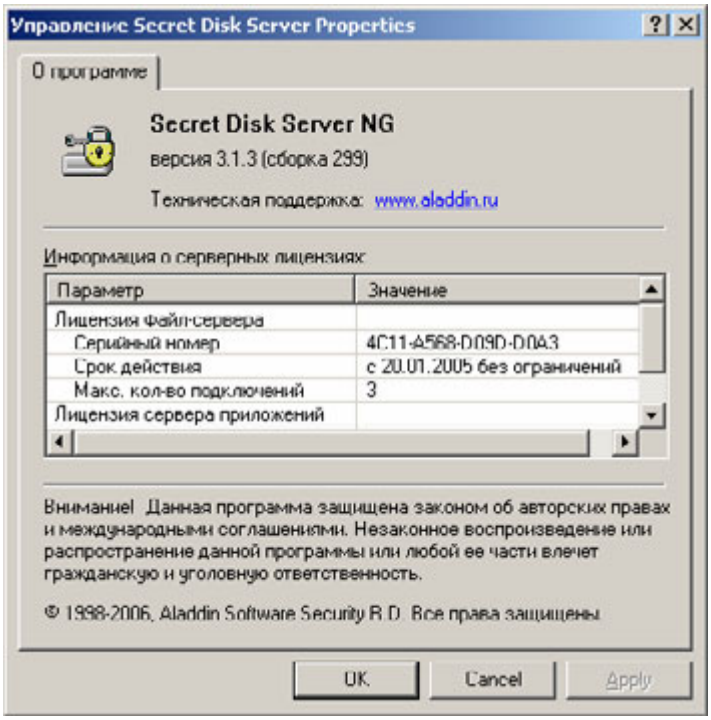
После перезагрузки откройте консоль управления компьютером. Для этого щелкните **Пуск/Start** > **(Все) программы / (All) Programs** > **Secret Disk NG** > **Server** > **Управление компьютером**.

Шаг 12



В дереве консоли щелкните правой кнопкой мыши **Управление Secret Disk Server** и выберите **Свойства/Properties**.

Шаг 13

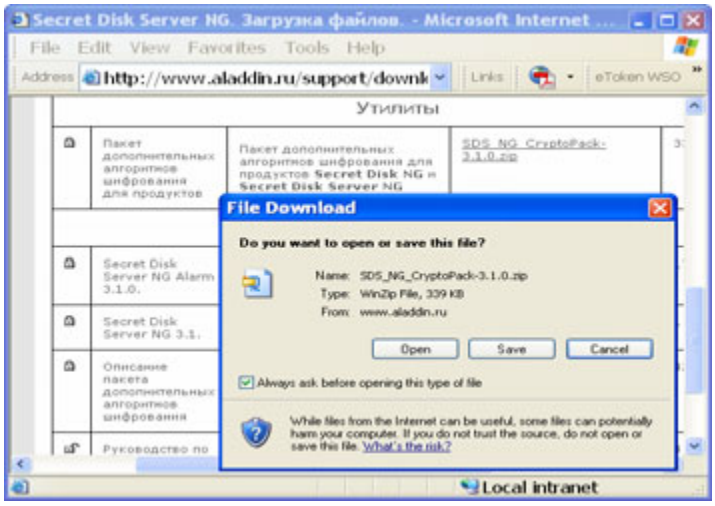


В окне (**Свойства:**) **Управление Secret Disk Server** (**Properties**) вы можете уточнить версию Secret Disk Server, а так же получить информацию о серверных лицензиях.

Установка Secret Disk NG Crypto Pack 3.1

По умолчанию вы можете выбирать для шифрования дисков алгоритмы DES и Triple DES. При этом шифрование осуществляется криптографическим драйвером режима ядра, входящим в состав Microsoft Windows. Установив Secret Disk NG Crypto Pack 3.1 на сервере, вы сможете использовать для шифрования дисков также алгоритмы AES и Twofish. Для того чтобы установить Secret Disk NG Crypto Pack 3.1, выполните следующие шаги.

Шаг 1

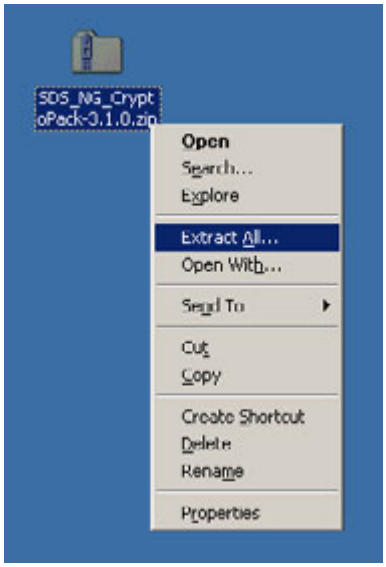


Загрузите архив с программой установки Secret Disk NG Crypto Pack 3.0 с сайта компании Aladdin: http://www.aladdin.ru/support/download/

или

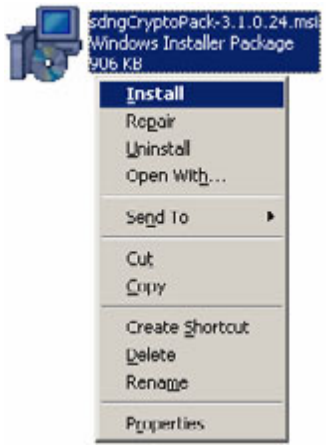
ftp://ftp.aladdin.ru/pub/SecretDisk-ServerNG/utilities/SDS_NG_CryptoPack-3.1.0.zip

Шаг 2



Распакуйте загруженный архив. Если на сервере установлена операционная система Windows 2000, для этого вам потребуется дополнительное программное обеспечение, например, WinZip или WinRAR.

Шаг 3

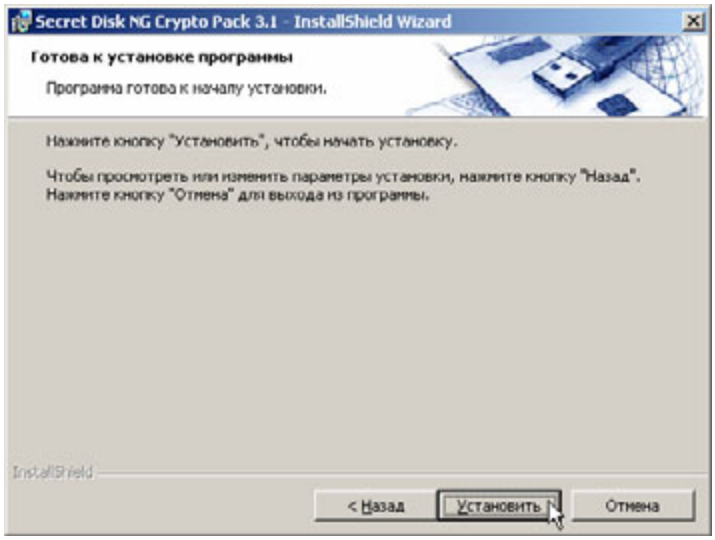


Запустите загруженную программу установки Secret Disk NG Crypto Pack 3.1.

Шаг 4

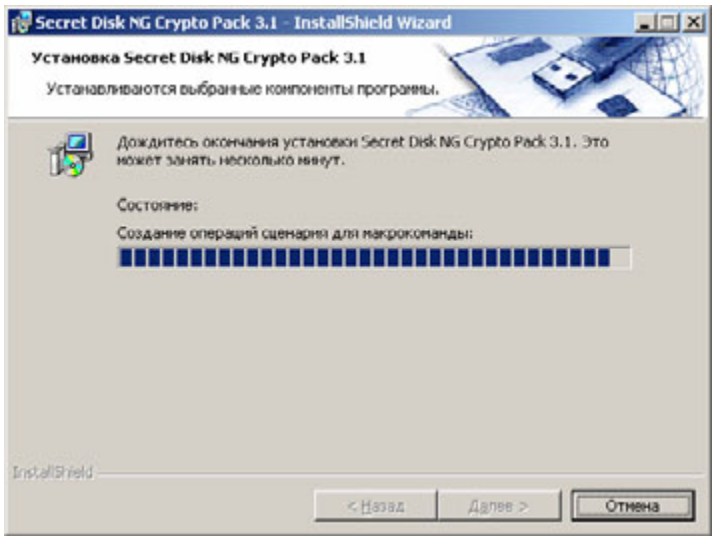
В окне приветствия программы установки нажмите **Далее**.

Шаг 5



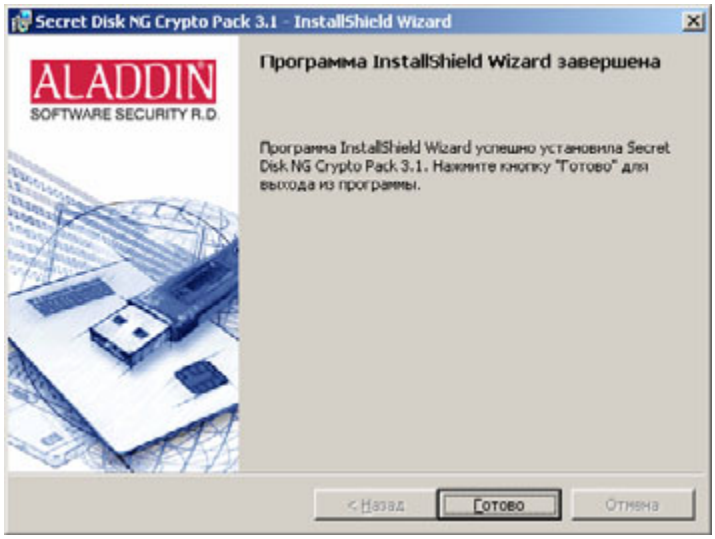
Для начала процесса установки нажмите **Установить**.

Шаг 6



Процесс установки займёт некоторое время. Дождитесь его завершения.

Шаг 7

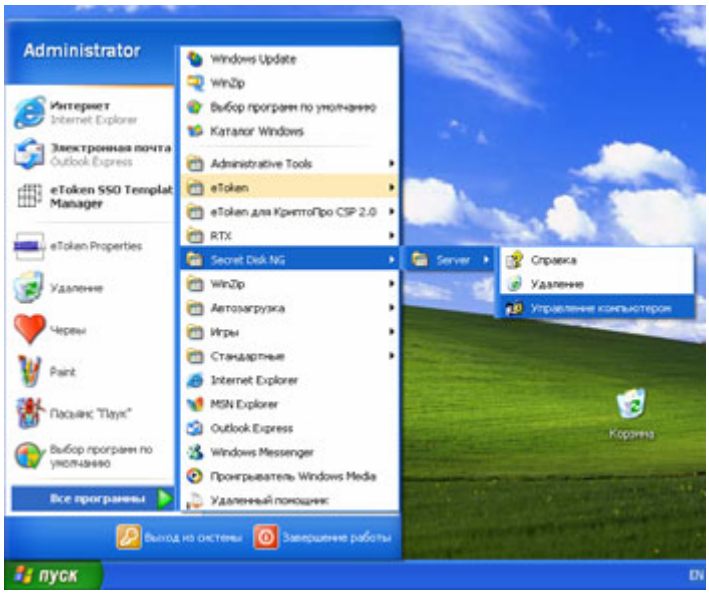


Убедитесь в том, что процесс установки завершён успешно, и нажмите **Готово**.

Удалённое управление с помощью консоли управления Microsoft

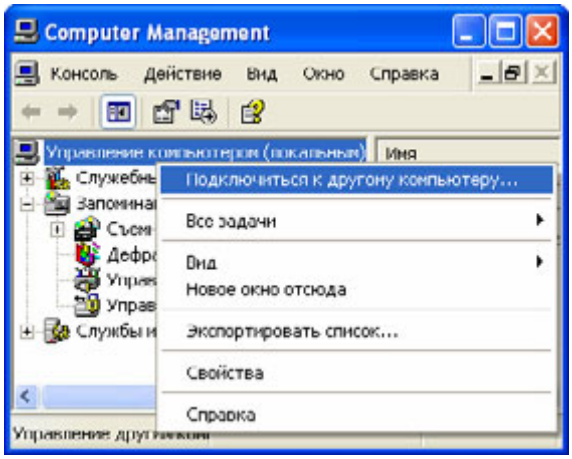
Для того чтобы начать удалённое управление сервером, выполните на рабочей станции пользователя следующие шаги.

Шаг 1



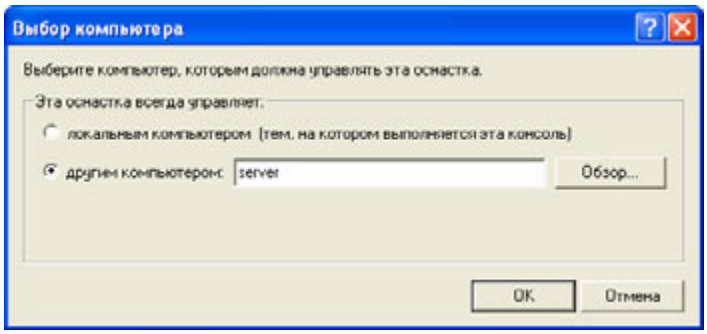
Для того чтобы открыть консоль управления компьютером, щёлкните: **Пуск/Start > (Все) Программы / (All) Programs > Secret Disk NG > Server > Управление компьютером**.

Шаг 2



По умолчанию консоль управления компьютером подключена к локальному компьютеру. Для того чтобы начать её подключение к удалённому серверу, в дереве консоли щёлкните правой кнопкой мыши **Управление компьютером (локальным)/Computer Management (Local)** и выберите **Подключиться к другому компьютеру / Connect to another computer**.

Шаг 3



В окне **Выбор компьютера/Select Computer** введите IP-адрес или имя удаленного компьютера вручную или воспользуйтесь стандартным диалогом выбора объекта, нажав **Обзор/Browse**. Затем нажмите **OK**.

Шаг 4

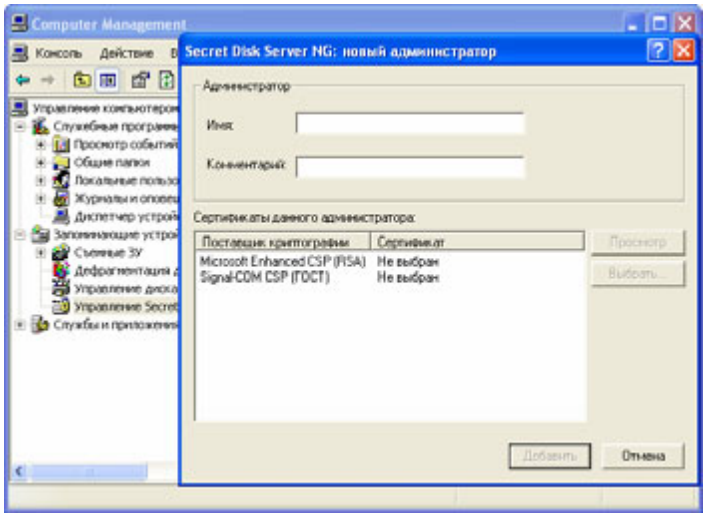
Подключение eToken администратора

Подключите eToken администратора Secret Disk Server NG к рабочей станции администратора.

Регистрация первого администратора Secret Disk Server NG

Для того чтобы начать удалённое управление сервером, выполните на рабочей станции пользователя следующие шаги.

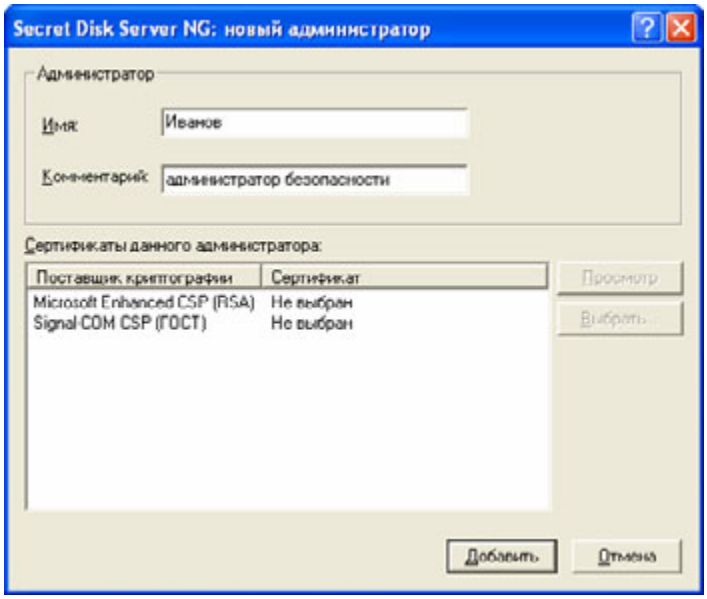
Шаг 1



Убедитесь в том, что eToken администратора подключен, и в дереве консоли нажмите **Управление Secret Disk Server**.

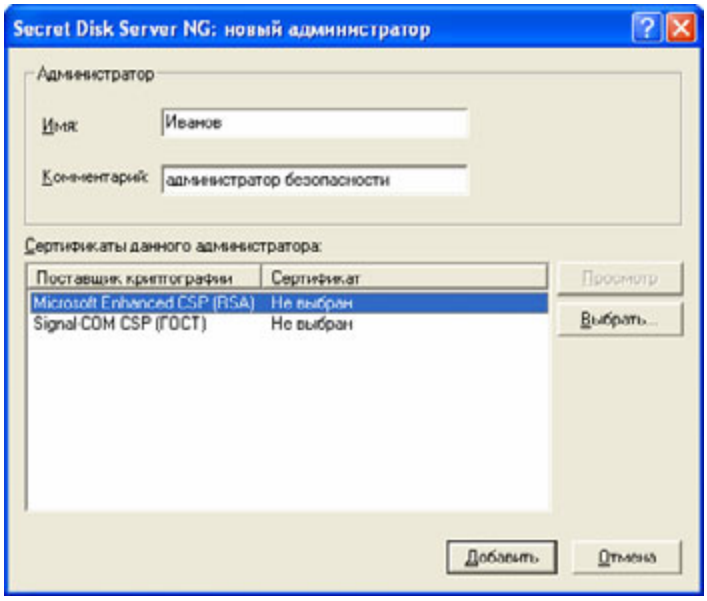
На экране появится окно **Secret Disk Server NG: новый администратор**.

Шаг 2



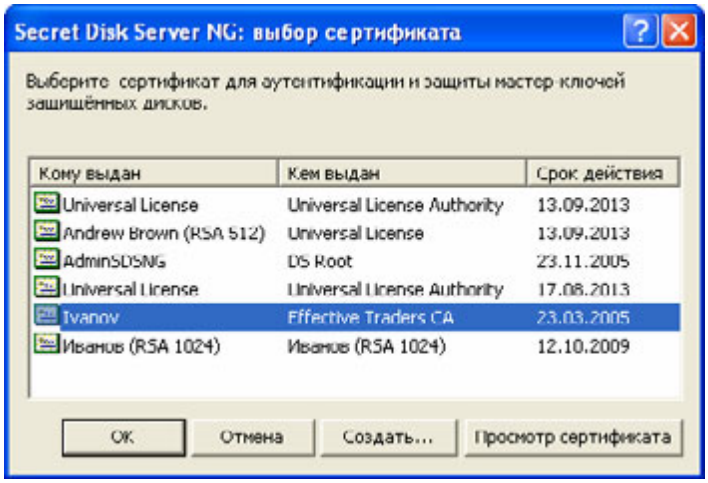
В окне **Secret Disk Server NG: новый администратор** внесите информацию об администраторе Secret Disk Server NG в графы **Имя** и **Комментарий**.

Шаг 3



В списке **Сертификаты данного администратора** выделите поставщик криптографии, который вы будете использовать для шифрования дисков, и нажмите **Выбрать**.

Шаг 4



В окне **Secret Disk Server NG: выбор сертификата** выберите сертификат, расположенный в памяти вашего eToken вместе с соответствующим закрытым ключом, и нажмите **OK**.

Примечания:

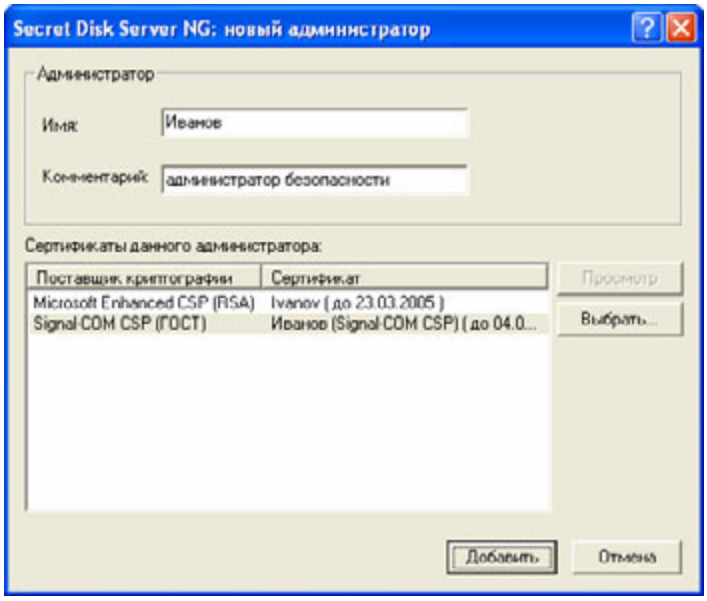
1. Если у вас нет сертификата, нажмите **Создать** и создайте его.
2. При необходимости, для того чтобы уточнить свой выбор, вы можете просмотреть параметры сертификата, нажав **Просмотр сертификата**.

Шаг 5

Введите PIN-код и нажмите **OK**. (Интерфейс зависит от поставщика криптографии.)

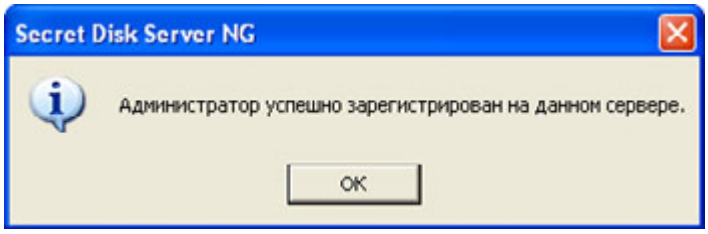
Если для шифрования дисков вы планируете использовать несколько поставщиков криптографии, выполните шаги 3—5 для каждого из них.

Шаг 6



В окне **Secret Disk NG: новый администратор** нажмите **Добавить**.

Шаг 7



В случае успешной регистрации нового администратора Secret Disk Server NG на данном компьютере на экране появится окно с сообщением: `Администратор успешно зарегистрирован на данном сервере`. Нажмите **OK**.

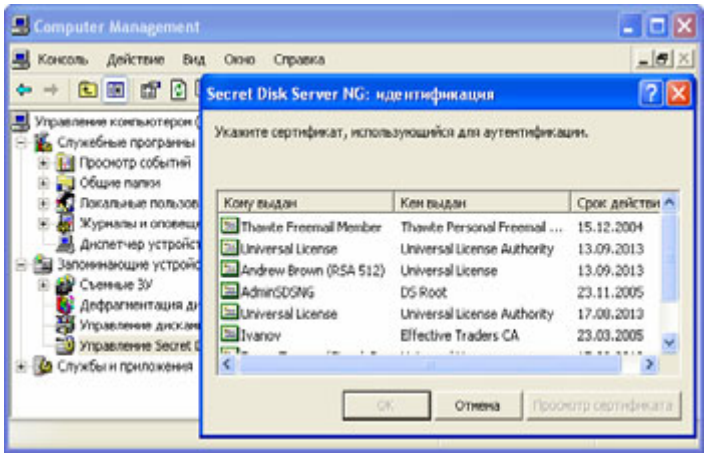
Сразу после регистрации первого администратора автоматически начинается процесс открытия сеанса управления. Для этого вам потребуется вновь указать один из выбранных сертификатов.

Открытие сеанса управления

Для успешного открытия сеанса управления к рабочей станции администратора должен быть подключен eToken администратора, в памяти которого содержатся:

- лицензия администратора;
- сертификат с закрытым ключом, использующийся для аутентификации и защиты мастер-ключей защищённых дисков.

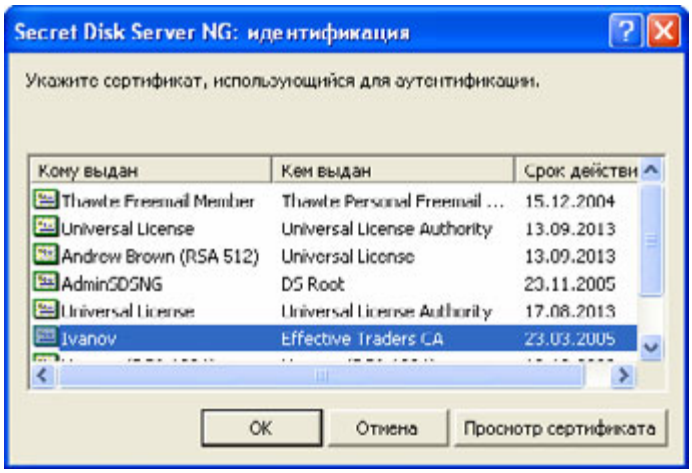
Шаг 1



Для того чтобы начать процесс открытия сеанса управления, убедитесь в том, что eToken администратора подключен к рабочей станции администратора, и в дереве консоли щелкните **Управление Secret Disk Server**. На экране появится окно **Secret Disk Server NG: идентификация**.

Примечание: Сразу после регистрации первого администратора это окно появляется на экране автоматически.

Шаг 2



В окне **Secret Disk Server NG: идентификация** укажите ваш сертификат для защиты мастер-ключей защищённых дисков и аутентификации и нажмите **OK**.

Примечания:

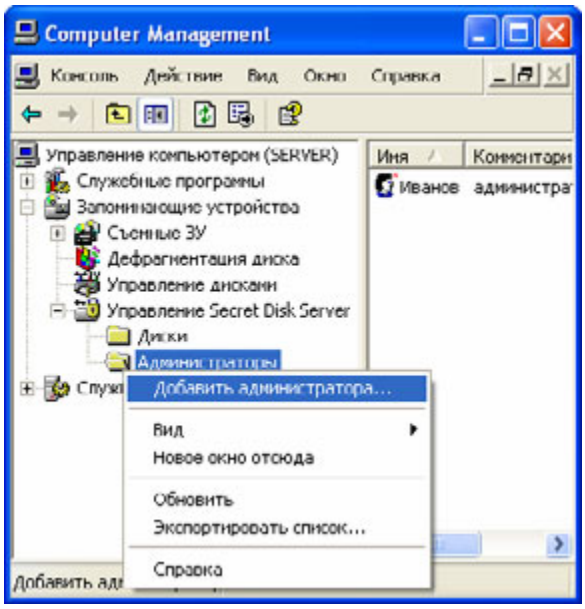
1. При необходимости, для того чтобы уточнить свой выбор, вы можете просмотреть параметры сертификата, нажав **Просмотр сертификата**.
2. Если у вас выбраны сертификаты для нескольких поставщиков криптографии, укажите любой из этих сертификатов.

Шаг 3

При необходимости введите PIN-код (интерфейс зависит от поставщика криптографии).

Регистрация дополнительного администратора Secret Disk Server NG

Шаг 1

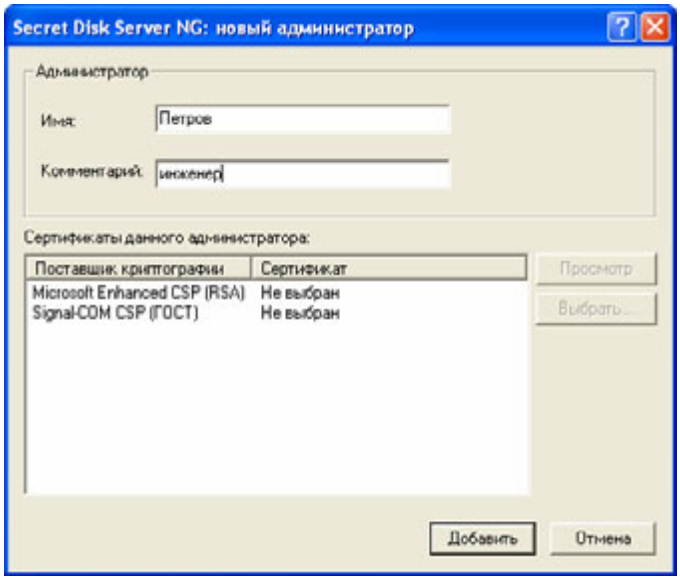


Убедитесь в том, что ваш eToken администратора подключен.

В дереве консоли щёлкните правой кнопкой мыши **Администраторы** и выберите **Добавить администратора**.

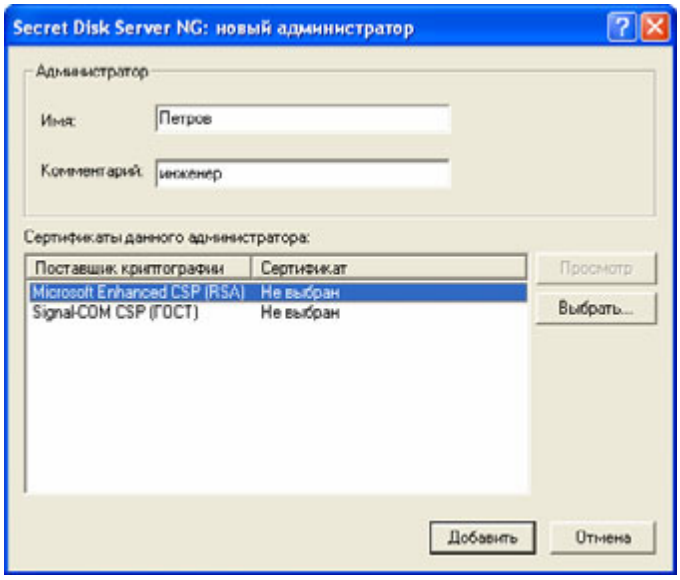
На экране появится окно **Secret Disk Server NG: новый администратор**.

Шаг 2



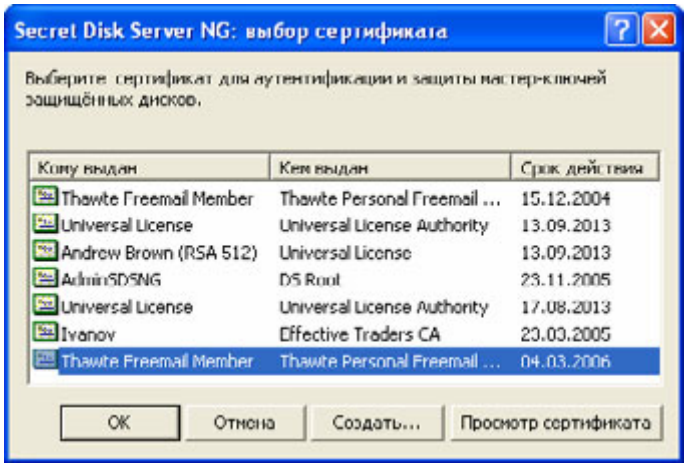
В окне **Secret Disk Server NG: новый администратор** внесите информацию о новом администраторе Secret Disk Server NG в графы **Имя** и **Комментарий**.

Шаг 3



В списке **Сертификаты данного администратора** выделите поставщик криптографии, который добавляемый администратор будет использовать для шифрования дисков, и нажмите **Выбрать**.

Шаг 4

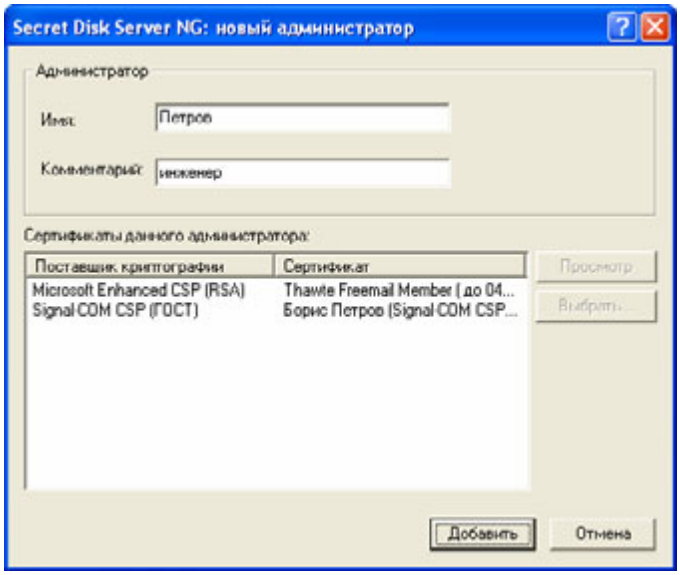


В окне **Secret Disk Server NG: выбор сертификата** выберите сертификат, который добавляемый администратор будет использовать для защиты мастер-ключей защищённых дисков и аутентификации.

Примечания:

1. Сертификат должен находиться вместе с соответствующим закрытым ключом в памяти eToken добавляемого администратора. Если этот eToken не подключен к компьютеру, вы указываете копию сертификата, расположенную в хранилище **Личные**/**Personal**.
2. При необходимости, для того чтобы уточнить свой выбор, вы можете просмотреть параметры сертификата, нажав **Просмотр сертификата**.
3. Если у добавляемого администратора нет сертификата, подключите его eToken, нажмите **Создать** и создайте сертификат с закрытым ключом.
4. Если для шифрования дисков добавляемый администратор будет использовать несколько поставщиков криптографии, выполните шаги 3—5 для каждого из них.

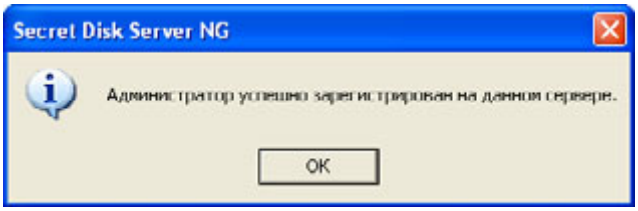
Шаг 5



В окне **Secret Disk NG: новый администратор** нажмите **Добавить**.

При необходимости введите PIN-код своего eToken (eToken добавляющего администратора) один или несколько раз. Это может потребоваться для того, чтобы новый администратор имел доступ к тем же защищенным дискам, что и вы.

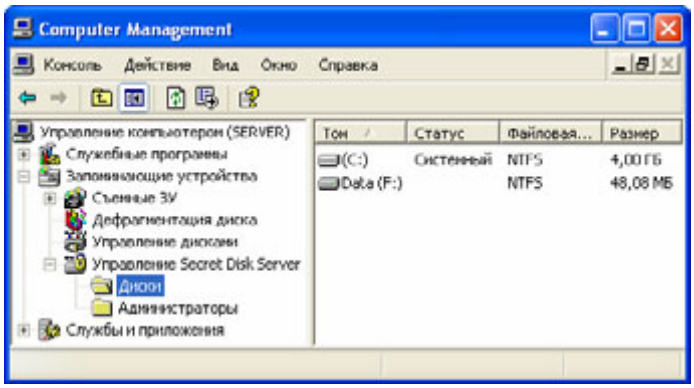
Шаг 6



В случае успешной регистрации нового администратора Secret Disk Server NG на данном сервере на экране появится окно с сообщением: **Администратор успешно зарегистрирован на данном сервере**. Нажмите **OK**.

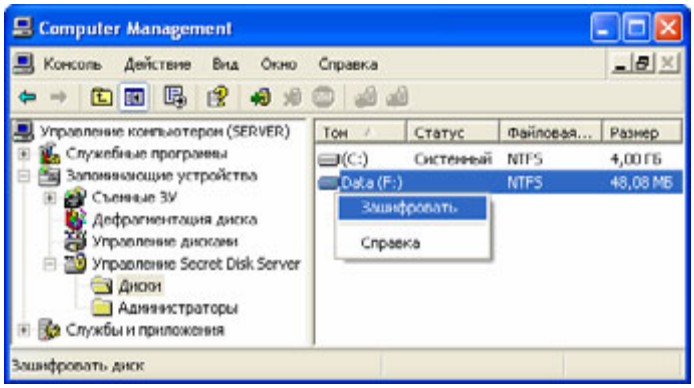
Зашифрование диска

Шаг 1



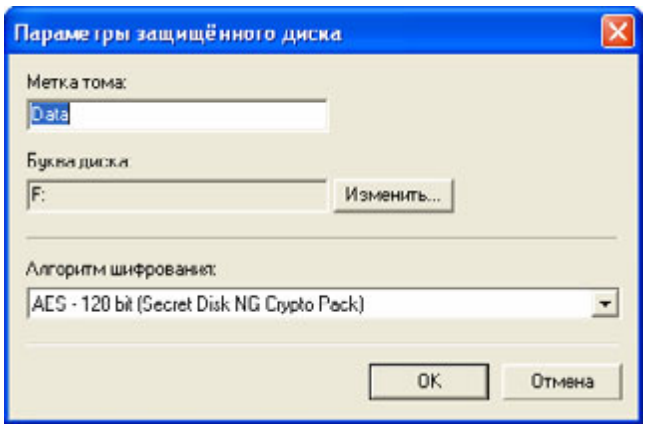
Убедившись в том, что eToken администратора подключен к рабочей станции администратора, в дереве консоли щелкните **Диски**.

Шаг 2



Выберите диск, не являющийся ни системным, ни защищённым. Щёлкните правой кнопкой мыши и выберите **Зашифровать**.

Шаг 3



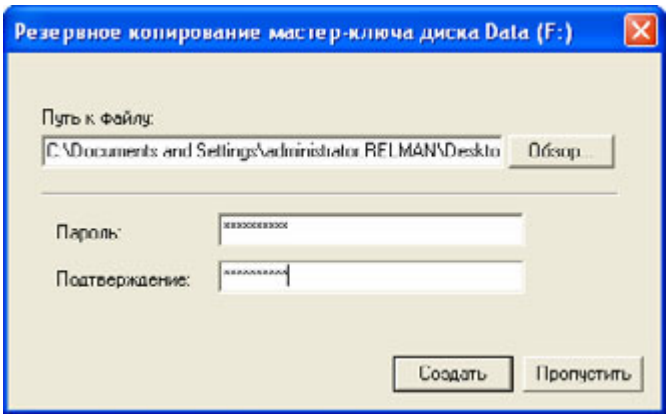
В окне **Параметры защищённого диска** назначьте метку тома и выберите букву диска, если вы хотите изменить текущие значения этих параметров.

Выберите алгоритм шифрования. В списке **Алгоритм шифрования** в скобках указывается поставщик криптографии или его компонент, отвечающий за шифрование дисков. Для успешного создания защищённого тома у вас должен быть выбран сертификат для защиты мастер-ключей дисков, шифруемых с помощью данного поставщика криптографии.

Выбрав параметры защищённого диска, нажмите **OK**.

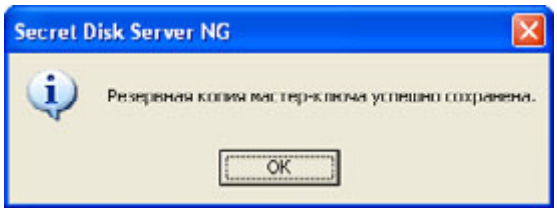
Система сгенерирует мастер-ключ защищённого тома, а затем предложит сохранить резервную копию этого мастер-ключа.

Шаг 4



Укажите путь к файлу резервной копии и введите пароль дважды — в графу **Пароль** и в графу **Подтверждение**. Нажмите **Создать** для завершения операции.

Шаг 5

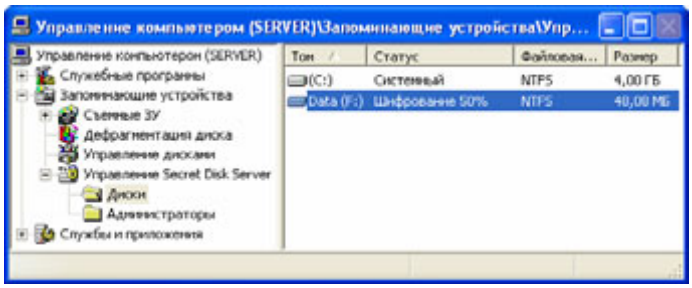


В случае успешного сохранения резервной копии мастер-ключа на экране появляется окно с сообщением: **Резервная копия мастер-ключа успешно сохранена**. Нажмите **OK**.

Шаг 6

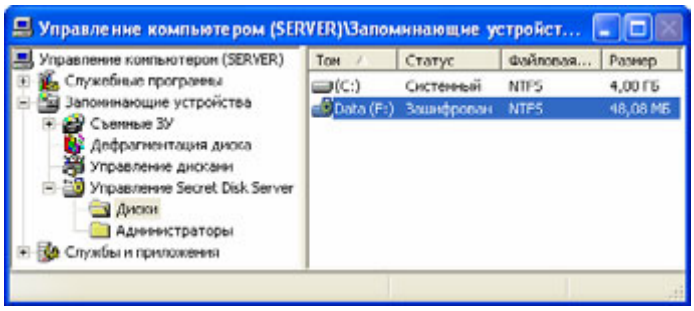
В окне **Secret Disk Server NG** убедитесь в том, что вы верно выбрали диск для зашифрования, и нажмите **Да**.

Шаг 7



О том, что процесс зашифрования активен, свидетельствует слово `Шифрование` в ячейке **Статус**. Дождитесь завершения процесса шифрования диска.

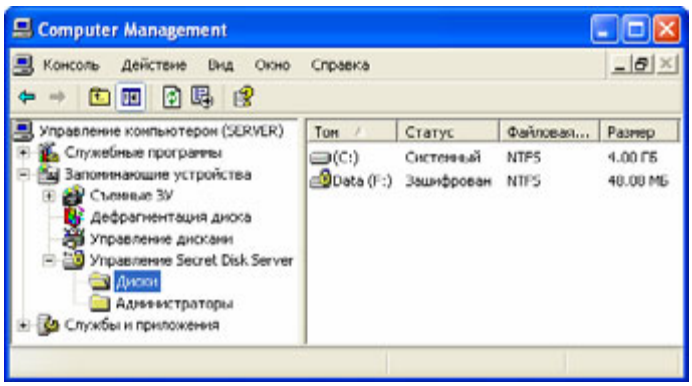
Шаг 8



Убедитесь в том, что диск зашифрован: в списке дисков в ячейке **Статус** соответствующей строки появилась запись **Зашифрован**.

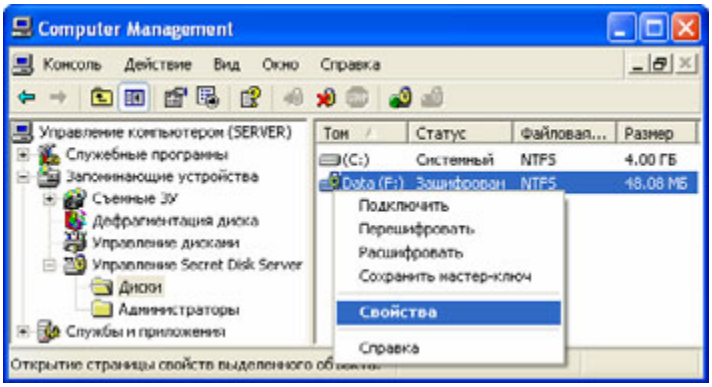
Настройка свойств защищённого диска

Шаг 1



Убедившись в том, что eToken администратора подключен к рабочей станции администратора, в дереве консоли щёлкните **Диски**.

Шаг 2

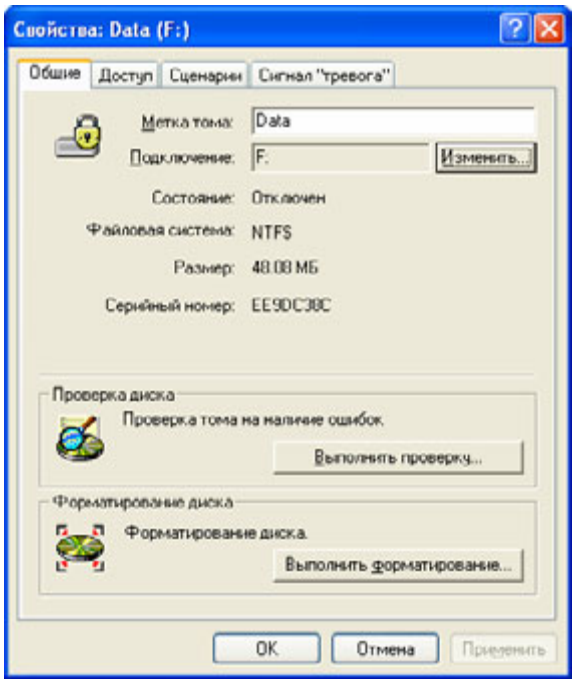


Убедитесь в том, что диск отключен. При необходимости отключите его.

Щёлкните правой кнопкой мыши и выберите **Свойства**/**Properties**.

На экране появится окно свойств защищённого диска.

Шаг 3

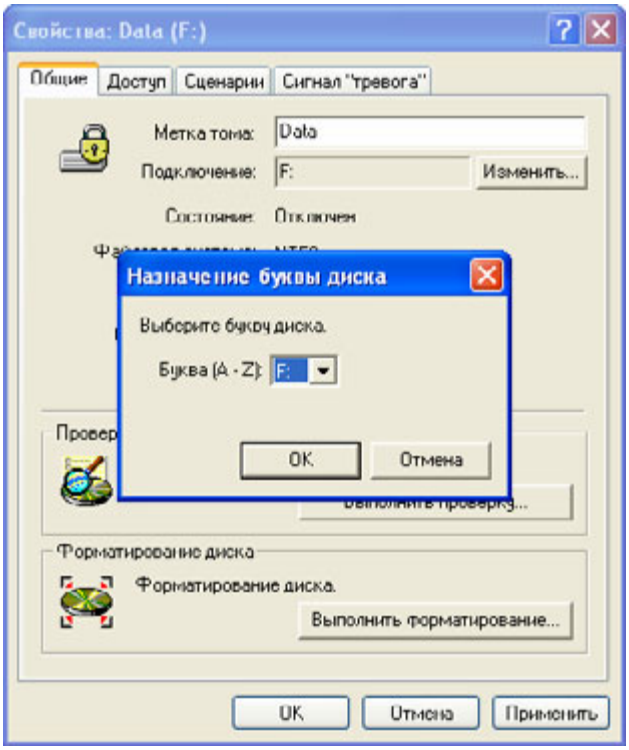


В окне свойств защищённого диска убедитесь в том, что открыта вкладка **Общие**.

При необходимости внесите изменения в поле **Метка тома**.

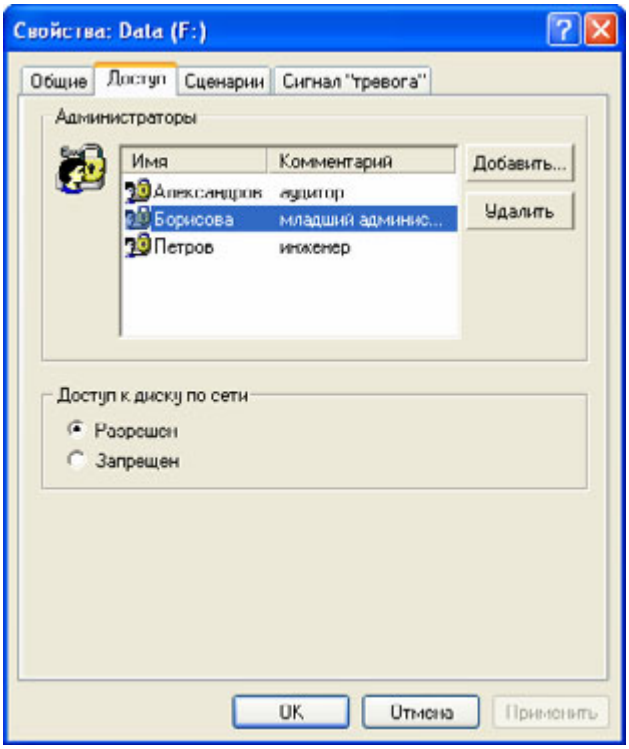
Если вы хотите изменить букву диска, нажмите **Изменить** и перейдите к следующему шагу. В противном случае пропустите следующий шаг.

Шаг 4



В окне **Назначение буквы диска** выберите букву из списка **Буква (A - Z)** и нажмите **OK**.

Шаг 5



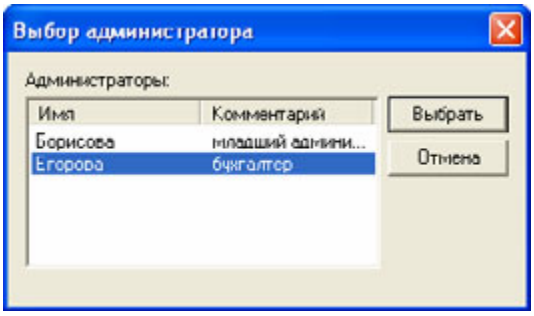
Откройте вкладку **Доступ**.

Для того чтобы отказать одному из администраторов в возможности управления данным диском, выберите этого администратора и нажмите **Удалить**.

Если в списке **Администраторы** отсутствует администратор, то у него нет права управления данным защищённым диском.

Если вы хотите предоставить кому-либо из таких администраторов это право, перейдите к следующему шагу. В противном случае пропустите следующий шаг.

Шаг 6

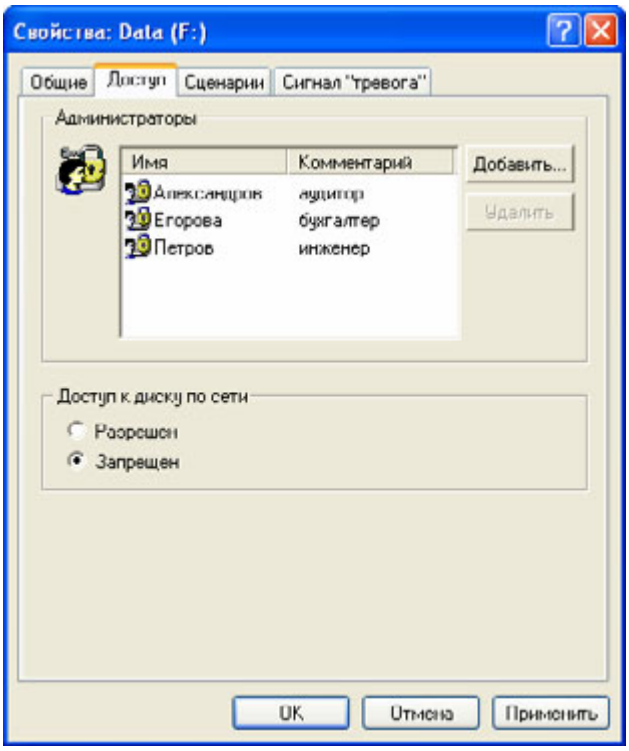


Убедитесь в том, что ваш eToken администратора подключен к компьютеру. При необходимости подключите его.

В окне **Выбор администратора** выберите администратора и нажмите **Выбрать**.

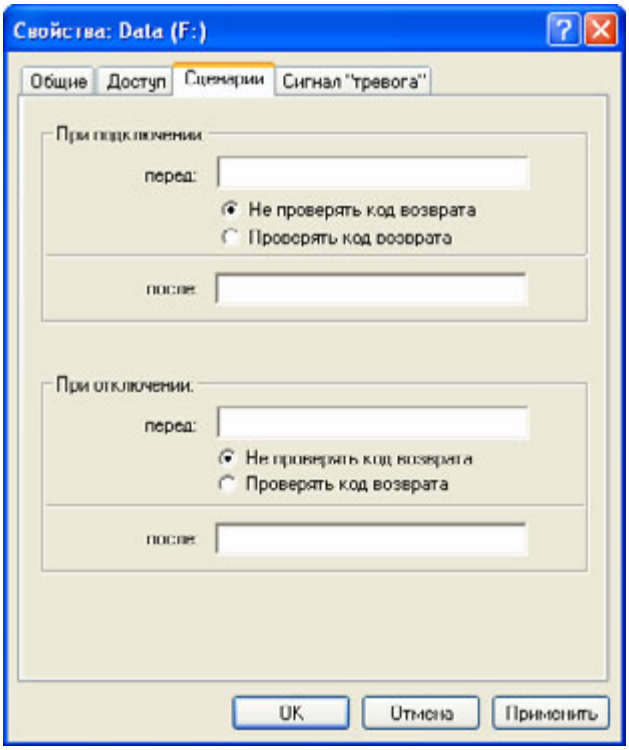
При необходимости укажите ваш eToken и введите PIN-код (интерфейс зависит от поставщика криптографии).

Шаг 7



Для того чтобы установить или отменить запрет на доступ к защищённому диску по сети, в области **Доступ к диску по сети** выберите **Запрещён** или **Разрешён** соответственно.

Шаг 8

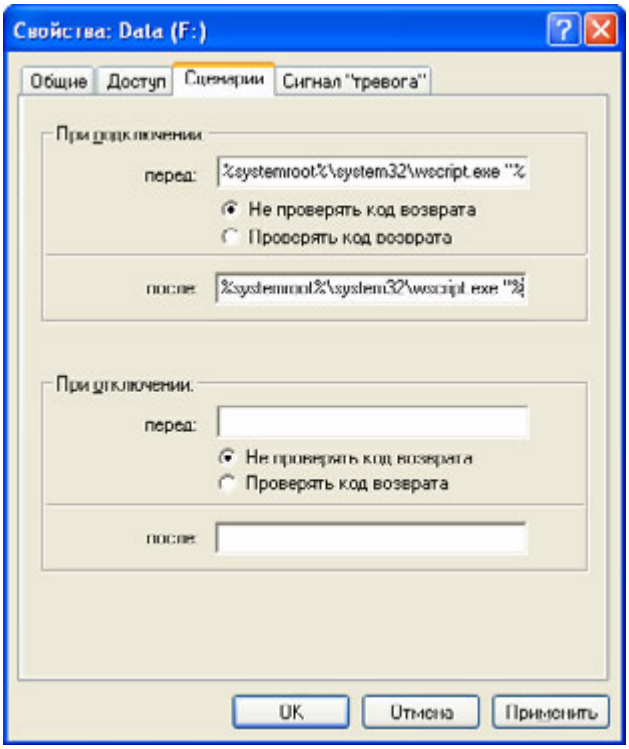


Откройте вкладку **Сценарии**.

Примечание:

При указании локальных путей в этой вкладке соответствующие файлы сценариев должны быть расположены на сервере.

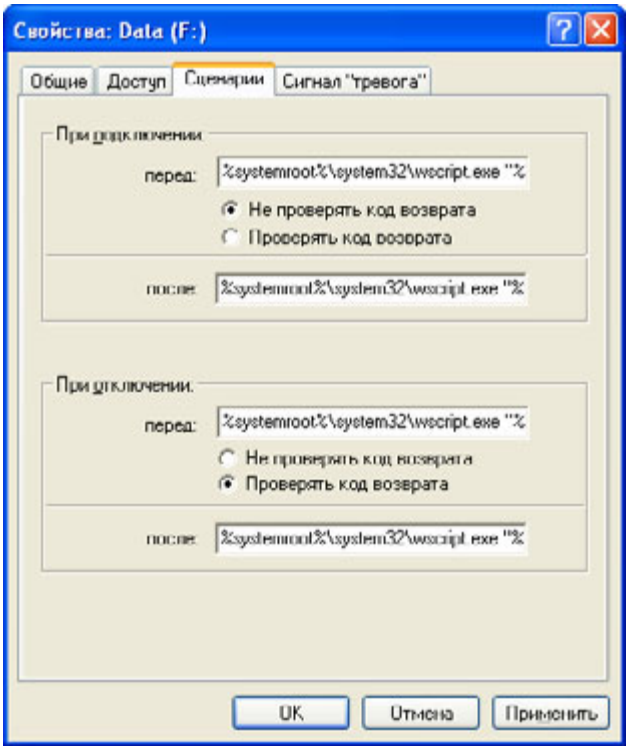
Шаг 9



В области **При подключении**:

- при необходимости введите строковую команду для запуска сценария, который должен выполняться перед подключением защищённого диска, в поле **перед**;
- если вы хотите, чтобы защищённый диск подключался независимо от результата выполнения сценария, выберите **Не проверять код возврата**, а если вы хотите, чтобы защищённый диск подключался лишь в случае успешного выполнения сценария, выберите **Проверять код возврата**;
- при необходимости введите строковую команду для запуска сценария, который должен выполняться после подключения защищённого диска, в поле **после**.

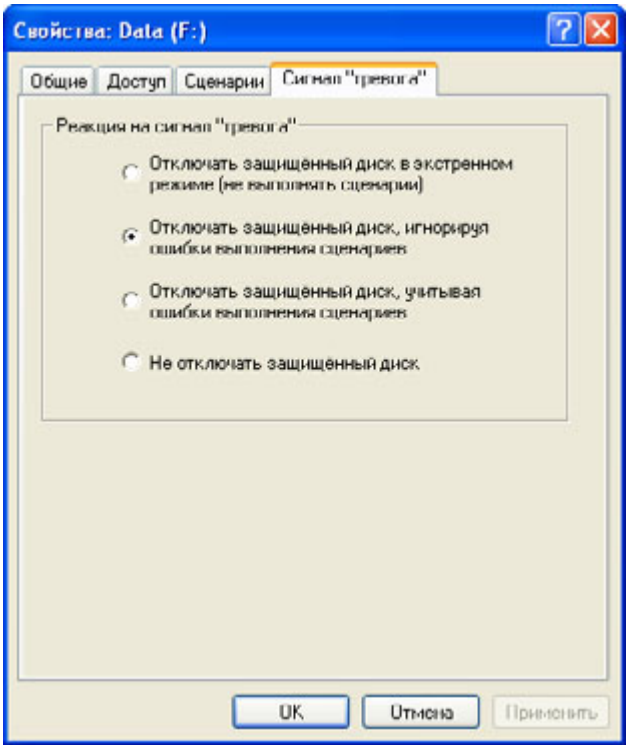
Шаг 10



В области **При отключении**:

- при необходимости введите строковую команду для запуска сценария, который должен выполняться перед отключением защищённого диска, в поле **перед**;
- если вы хотите, чтобы защищённый диск отключался независимо от результата выполнения сценария, выберите **Не проверять код возврата**, а если вы хотите, чтобы защищённый диск отключался лишь в случае успешного выполнения сценария, выберите **Проверять код возврата**;
- при необходимости введите строковую команду для запуска сценария, который должен выполняться после отключения защищённого диска, в поле **после**.

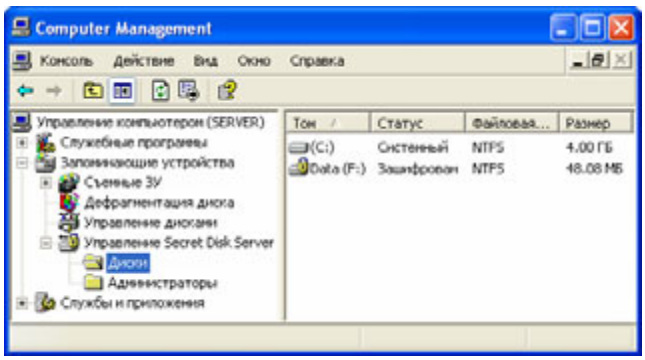
Шаг 11



Во вкладке **Сигнал «тревога»** выберите реакцию защищённого диска на сигал «тревога» и нажмите **Применить** или **OK**.

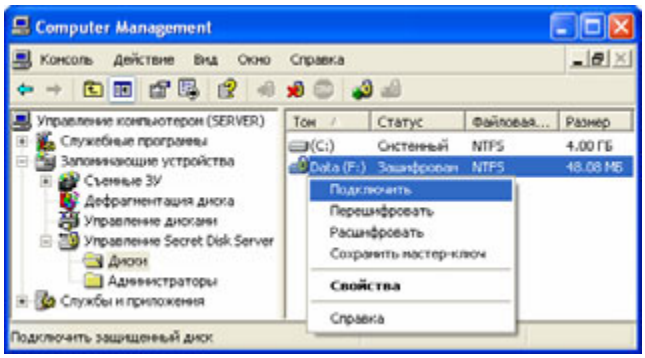
Подключение защищённого диска

Шаг 1



Убедившись в том, что eToken администратора подключен к рабочей станции администратора, в дереве консоли щёлкните **Диски**.

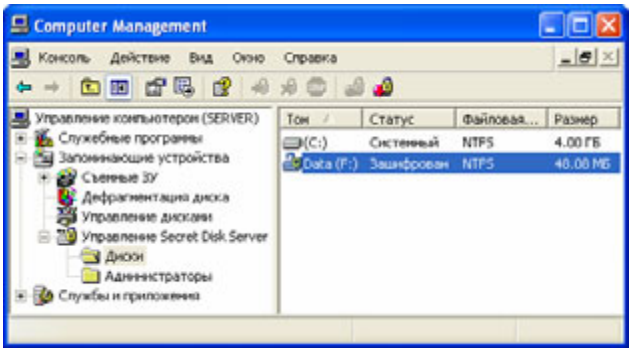
Шаг 2



Выберите отключенный защищённый диск. Щёлкните правой кнопкой мыши и выберите **Подключить**.

При необходимости укажите свой eToken и введите PIN-код (интерфейс зависит от поставщика криптографии).

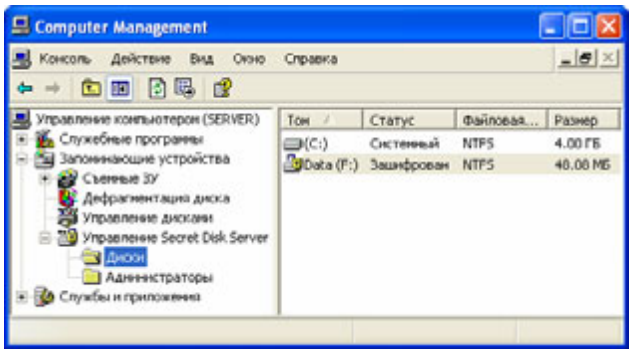
Шаг 3



Убедитесь в том, что защищённый диск успешно подключен (значок диска изменился).

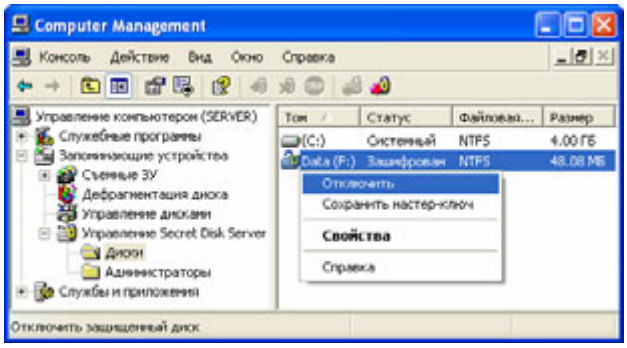
Отключение защищённого диска

Шаг 1



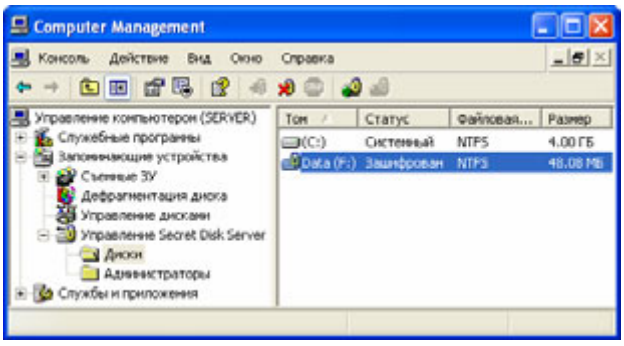
В дереве консоли щёлкните **Диски**.

Шаг 2



Выберите подключенный защищённый диск. Щёлкните правой кнопкой мыши и выберите **Отключить**.

Шаг 3

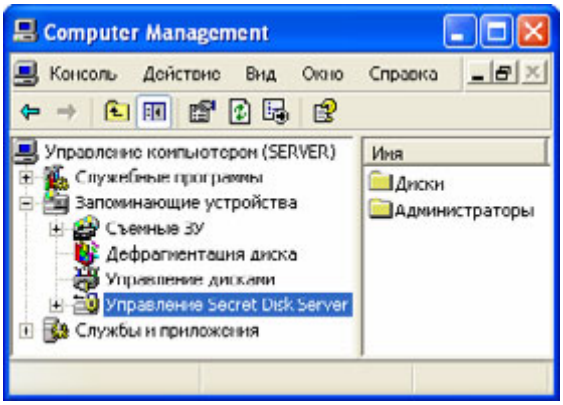


Убедитесь в том, что защищённый диск успешно отключен (значок диска изменился).

Настройка сервера

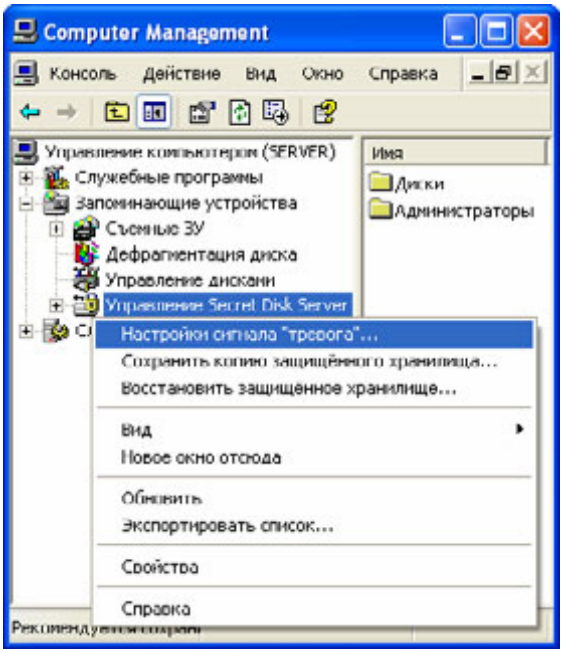
Настройка сигнала «тревога»

Шаг 1



Откройте сеанс управления.

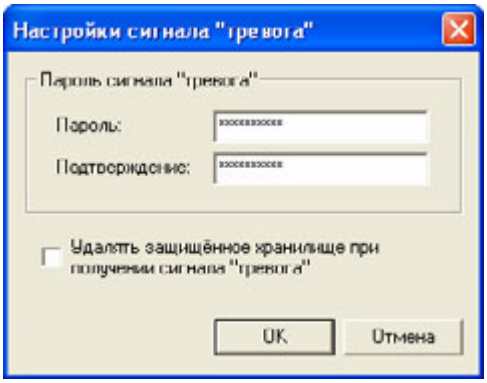
Шаг 2



В дереве консоли щёлкните правой кнопкой мыши **Управление Secret Disk Server**.

На экране появится окно **Настройки сигнала «тревога»**.

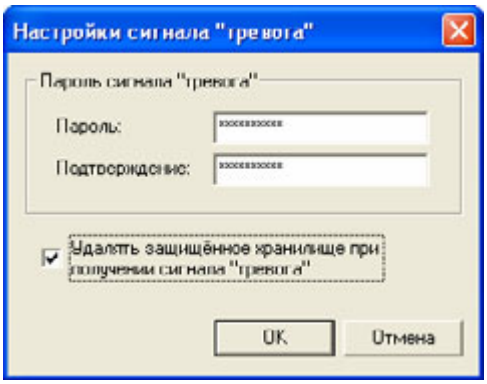
Шаг 3



Задайте пароль сигнала «тревога». Для этого введите желаемую последовательность символов в графы **Пароль** и **Подтверждение**.

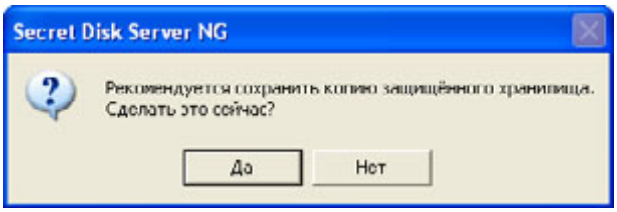
Если вы хотите, чтобы при поступлении сигнала «тревога» удалялось защищённое хранилище, выполните следующие четыре шага. В противном случае пропустите эти шаги.

Шаг 4



Установите флажок. На экране немедленно появится диалоговое окно, предлагающее сохранить копию защищённого хранилища.

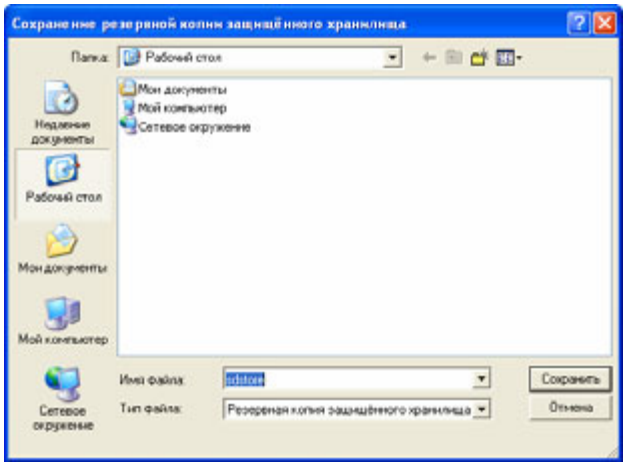
Шаг 5



Нажмите **Да**.

На экране появится окно **Сохранение резервной копии защищённого хранилища**.

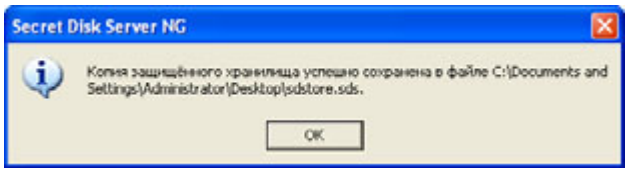
Шаг 6



Выберите папку и введите имя файла, в котором вы хотите сохранить резервную копию защищённого хранилища.

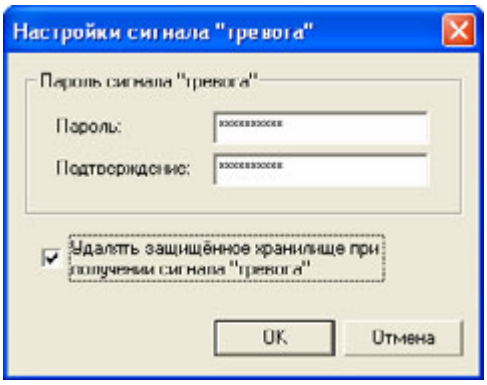
Нажмите **Сохранить**.

Шаг 7



Убедитесь в том, что копия защищённого хранилища успешно сохранена, и нажмите **OK**.

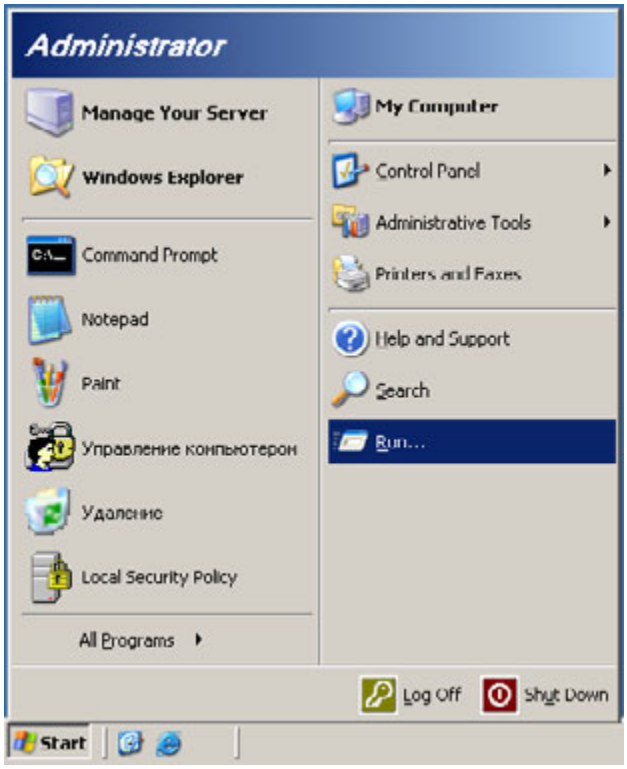
Шаг 8



В окне **Настройки сигнала «тревога»** нажмите **OK**.

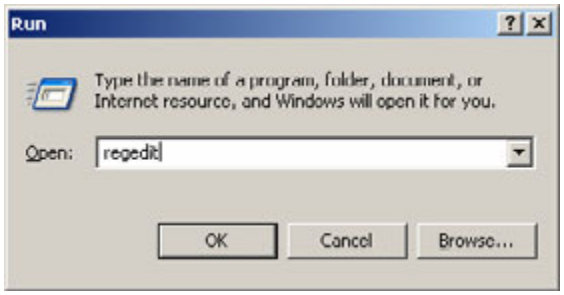
Настройка времени ожидания результатов выполнения сценариев

Шаг 1



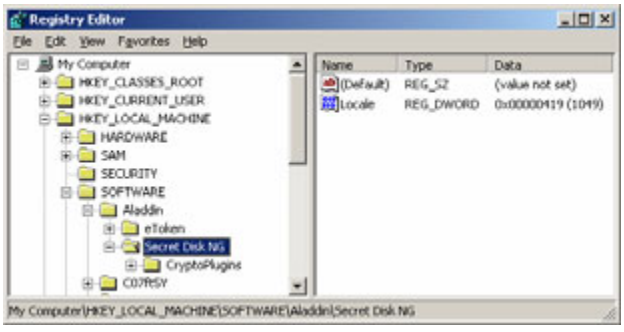
На сервере в меню **Пуск/Start** выберите **Выполнить/Run**.

Шаг 2



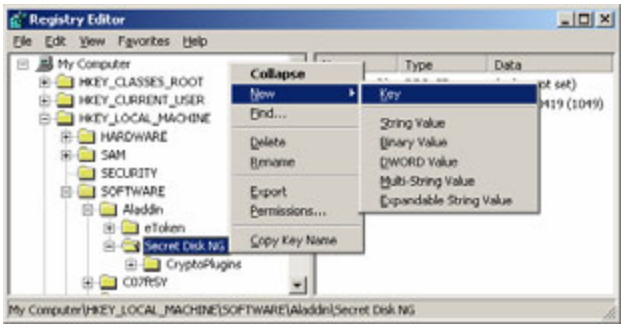
В окне **Запуск программы** / **Run** введите `regedit` и нажмите **OK**.

Шаг 3



В дереве консоли **Редактор реестра** / **Registry Editor** разверните узел `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Secret Disk NG`. Если в этом узле отсутствует раздел `Server`, выполните следующие четыре шага. Если раздел `Server` существует, но в нем отсутствует параметр `ActionExecWaitTimeout`, то пропустите следующие два шага. Если параметр `ActionExecWaitTimeout` существует, то пропустите следующие четыре шага.

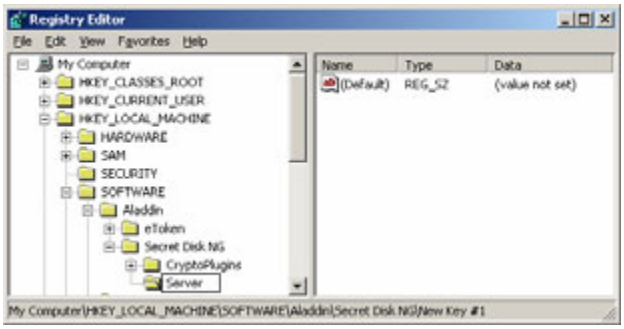
Шаг 4



Для того чтобы начать создание нового раздела, в дереве консоли щелкните правой кнопкой мыши Secret Disk NG, а затем выберите **Создать**/**New** > **Раздел**/**Key**.

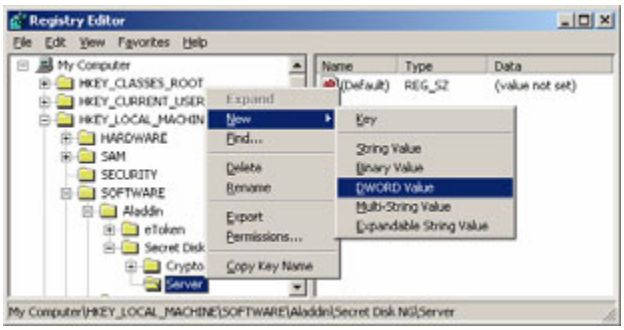
В дереве консоли появится узел `Новый раздел #1` / `New key #1`.

Шаг 5



Замените имя `Новый раздел #1` / `New key #1` именем `Server`.

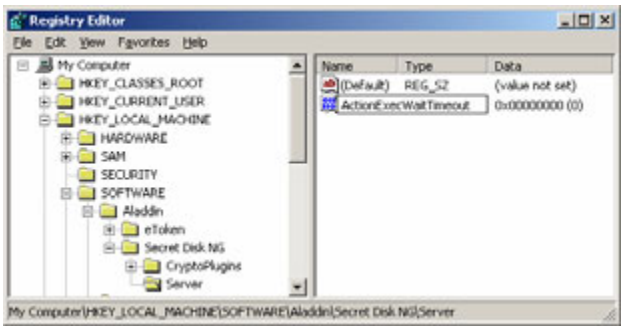
Шаг 6



В дереве консоли щёлкните правой кнопкой мыши по узлу `Server` и выберите **Создать**/**New** > **Параметр DWORD** / **DWORD Value**.

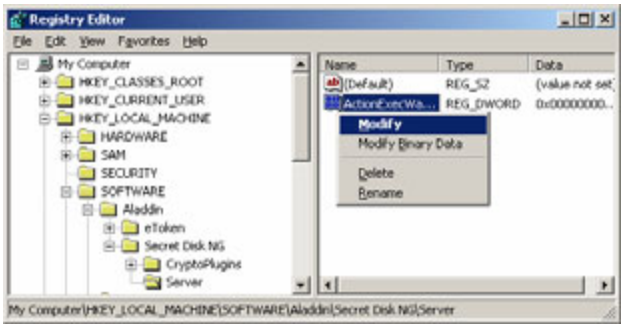
В разделе **Server** появится параметр `Новый параметр #1` / `New value #1`.

Шаг 7



Замените имя `Новый параметр #1` / `New value #1` именем `ActionExecWaitTimeout`.

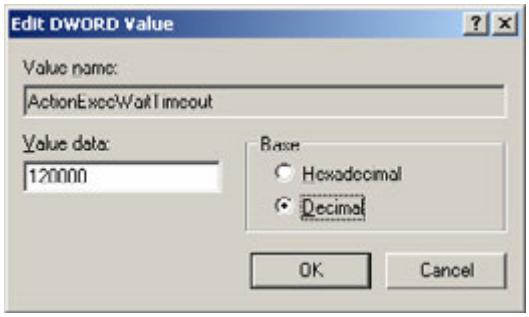
Шаг 8



На строке с параметром `ActionExecWaitTimeout` щёлкните правой кнопкой мыши и выберите **Изменить**/**Modify**.

На экране появится окно **Изменение параметра DWORD** / **Edit DWORD Value**.

Шаг 9



В окне **Изменение параметра DWORD** / **Edit DWORD Value** в поле **Значение** / **Value data** введите желаемую величину в миллисекундах, лежащую в диапазоне от 5000 до 120000 (десятичные числа). Вы можете использовать как десятичную, так и шестнадцатеричную системы счисления. В частности, при вводе десятичного числа в области **Система исчисления** / **Base** переключатель должен быть установлен в положение **Десятичная**/**Decimal**.

Введя желаемое значение, нажмите **OK**.

Настройка завершена. Вы можете закрыть окно **Редактор реестра** / **Registry Editor**.

Установка и настройка Secret Disk NG Alarm 3.1

Для выполнения инструкций по установке и настройке Secret Disk NG Alarm 3.1 требуются полномочия администратора рабочей станции для подачи сигнала «тревога».

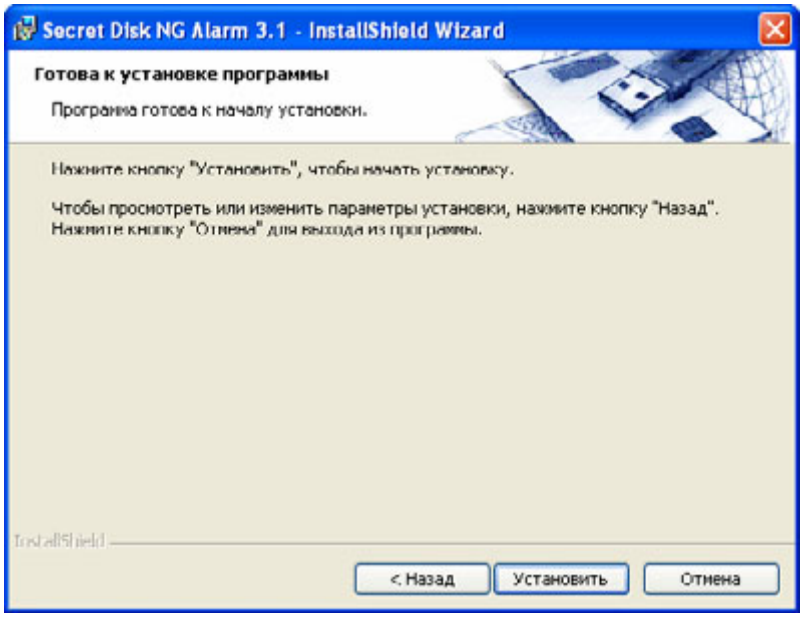
Шаг 1

Вставьте компакт-диск Secret Disk Server NG 3.1 в устройство чтения компакт-дисков. На экране появится окно меню компакт-диска. В меню компакт-диска Secret Disk Server NG 3.1 нажмите **Установить утилиту подачи сигнала «тревога»**.

Шаг 2

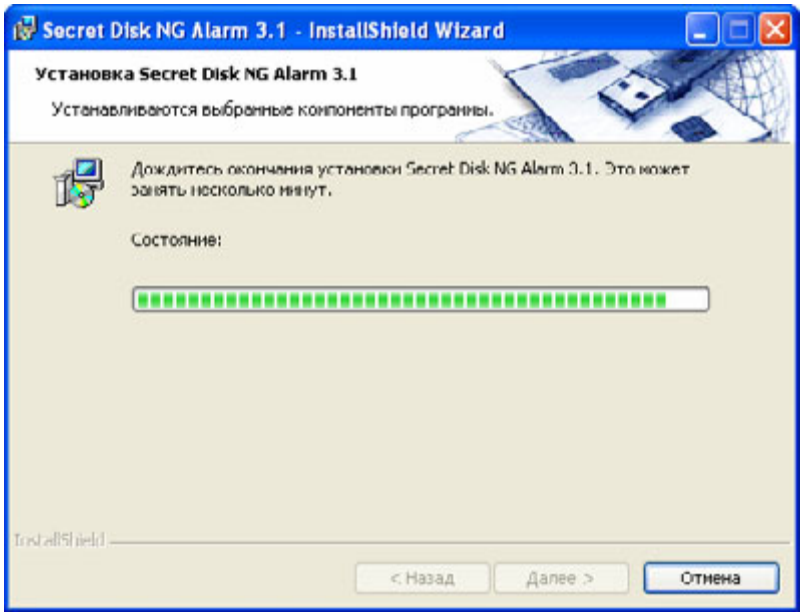
В окне приветствия программы установки нажмите **Далее**.

Шаг 3



Для начала процесса установки нажмите **Установить**.

Шаг 4

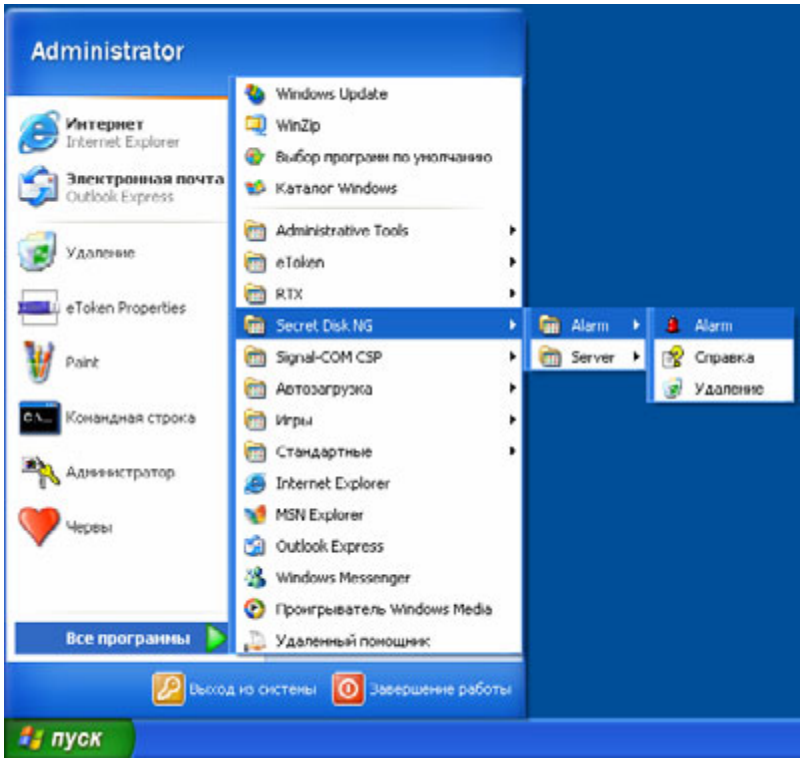


Процесс установки займёт некоторое время. Дождитесь его окончания.

Шаг 5

Убедитесь в том, что процесс установки завершён успешно, и нажмите **Готово**.

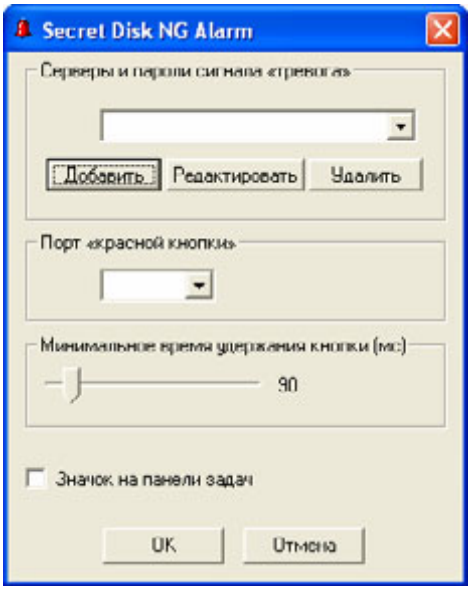
Шаг 6



Для того чтобы начать настройку **Secret Disk NG Alarm 3.1**, щёлкните **Пуск/Start > Все программы (All Programs) / Программы (Programs) > Secret Disk NG > Alarm > Alarm**.

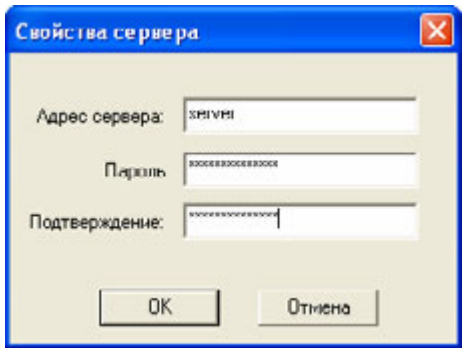
На экране появится окно **Secret Disk NG Alarm**.

Шаг 7



Secret Disk NG Alarm 3.1 может отправлять сигналы «тревога» нескольким серверам. При настройке вы должны будете указать серверы и соответствующие пароли сигнала «тревога». Для добавления нового сервера нажмите **Добавить**.

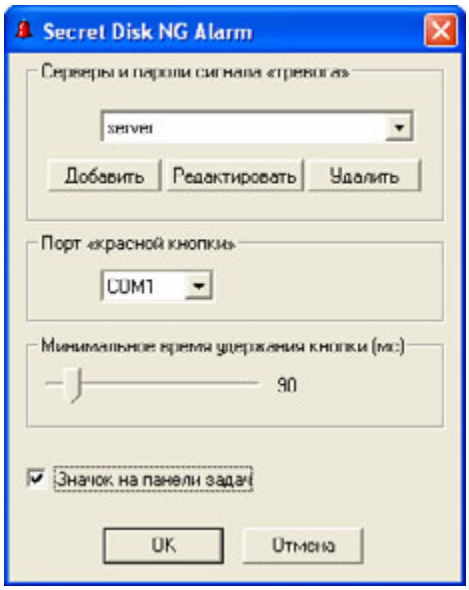
Шаг 8



В окне **Свойства сервера** введите имя или IP-адрес сервера, введите пароль сигнала «тревога» в поля **Пароль** и **Подтверждение** и нажмите **OK**.

При необходимости повторите шаги 7—8 для других серверов.

Шаг 9



Подключите «красную кнопку» к одному из портов COM и укажите этот порт в области Порт «красной кнопки» окна **Secret Disk NG Alarm**.

Если при текущих настройках наблюдается самопроизвольная подача сигнала «тревога», переместите ползунок вправо, а если при текущих настройках кратковременное нажатие «красной кнопки» не приводит к подаче сигнала «тревога» — влево. Если для подачи сигнала «тревога» вы используете датчик пожарной или охранной сигнализации и т. п., установите ползунок в крайнее левое положение.

Для подачи сигнала «тревога» с помощью мыши установите флажок **Значок на панели задач**. Нажмите **OK**.

Подача сигнала «тревога»

Способы подачи сигнала «тревога»

Можно выделить три способа подачи сигнала «тревога»:

- нажатие «красной кнопки»;
- подача сигнала «тревога» с помощью мыши;
- использование утилиты `sdsalrm.exe`.

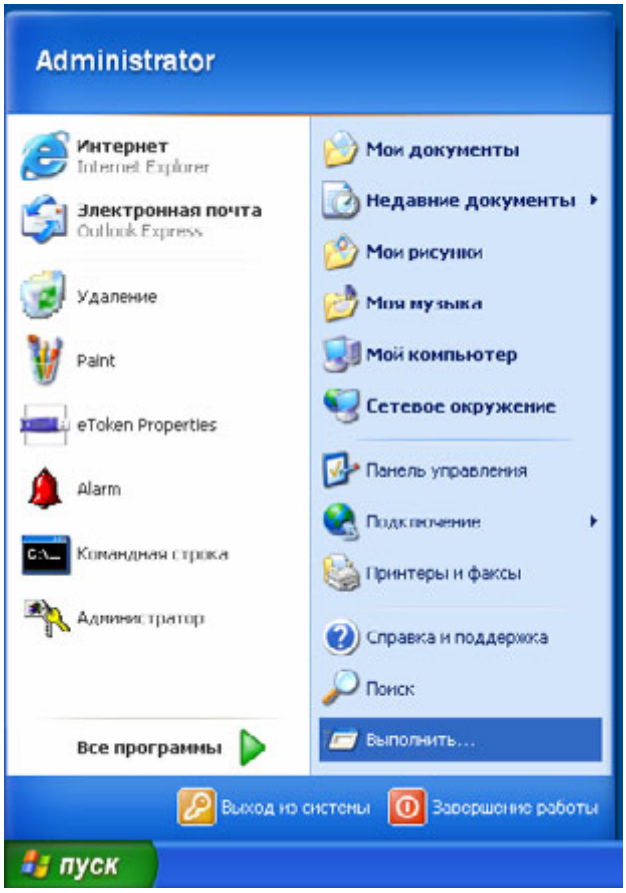
В любом случае на рабочей станции для подачи сигнала «тревога» должен быть установлен Secret Disk NG Alarm 3.0. Кроме того, первые два способа требуют предварительной настройки Secret Disk NG Alarm 3.0.

Для использования «красной кнопки» не требуется пошаговых инструкций: просто нажмите кнопку.

Для того чтобы подать сигнал тревога с помощью мыши, на панели задач щелкните правой кнопкой мыши значок **сигнал «тревога»** () и выберите **Подать сигнал «тревога»**.

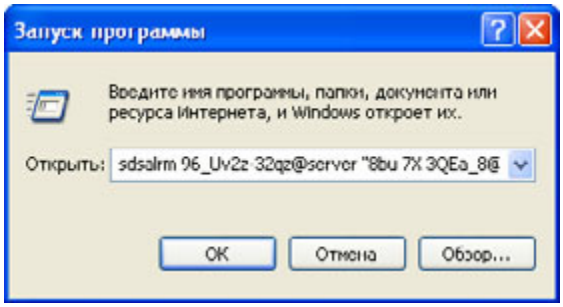
Подача сигнала «тревога» из командной строки

Шаг 1



На рабочей станции для подачи сигнала «тревога» в меню **Пуск**/**Start** выберите **Выполнить**/**Run**.

Шаг 2



В окне **Запуск программы** / **Run** введите:

```
sdsalrm "<пароль1>@<сервер1>"
["<пароль2>@<сервер2>" ...],
```

где:

- `<парольN>` — пароль сигнала «тревога» для сервера N;
- `<серверN>` — имя или IP-адрес сервера N.

Примечания:

1. При отправке сигнала «тревога» нескольким серверам имя/адрес и пароль для каждого сервера указываются в командной строке через пробел.
2. Если пароль сигнала «тревога» для какого-либо сервера (например, сервера 1) не содержит символов пробела, соответствующий параметр команды sdsalrm можно вводить без кавычек:

   ```
   sdsalrm <пароль1>@<сервер1>
   ["<пароль2>@<сервер2>" ...].
   ```

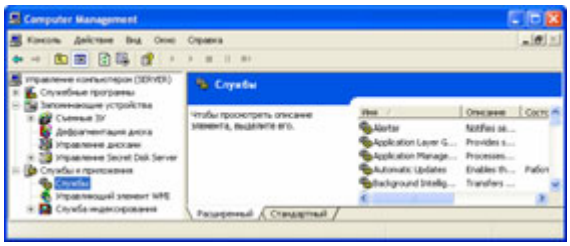
Введя команду в поле **Открыть**/**Open**, нажмите **OK**.

Восстановление сервера после сигнала «тревога»

Если сервер был настроен на удаление защищённого хранилища при поступлении сигнала «тревога», то для восстановления вам потребуется:

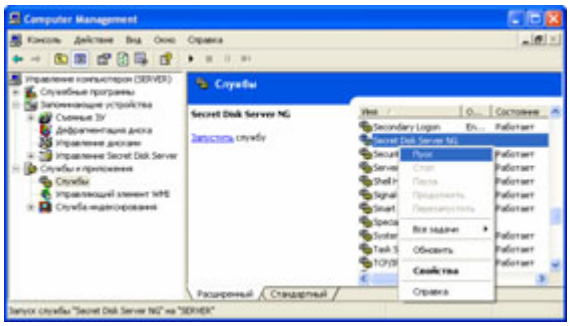
- иметь полномочия администратора на сервере;
- обладать файлом резервной копии защищённого хранилища.

Шаг 1



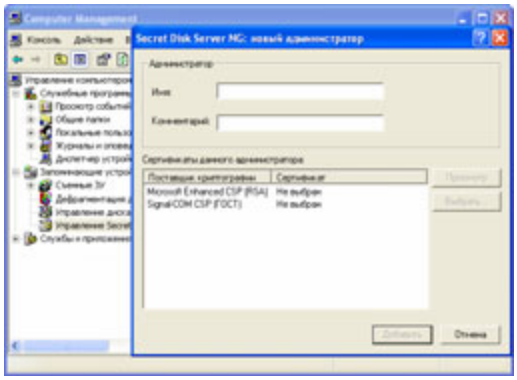
В консоли управления сервером в узле **Службы и приложения** / **Services an Applications** выберите **Службы**/**Services**.

Шаг 2



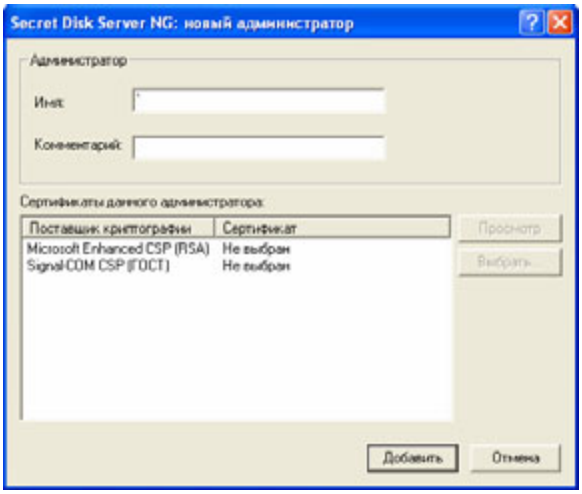
Выделите в списке службу **Secret Disk Server NG**. Если в ячейке **Состояние**/**Status** отсутствует слово **Работает**/**Started**, щелкните правой кнопкой мыши и выберите **Пуск**/**Start**.

Шаг 3



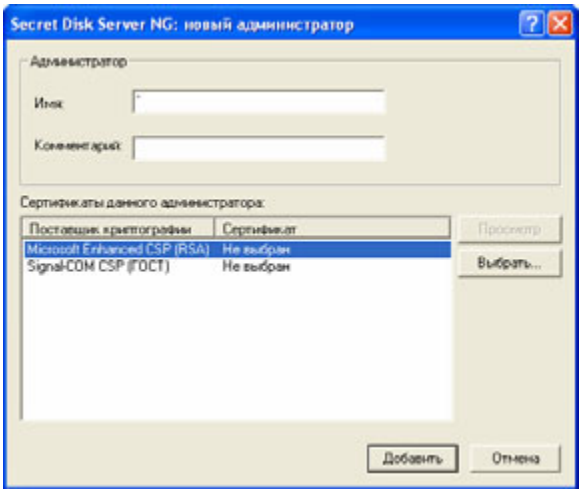
Убедитесь в том, что eToken администратора подключен и в дереве консоли нажмите **Управление Secret Disk Server**. На экране появится окно **Secret Disk Server NG: новый администратор**. Если это окно не появляется, щёлкните правой кнопкой мыши и выберите **Обновить**/**Refresh**.

Шаг 4



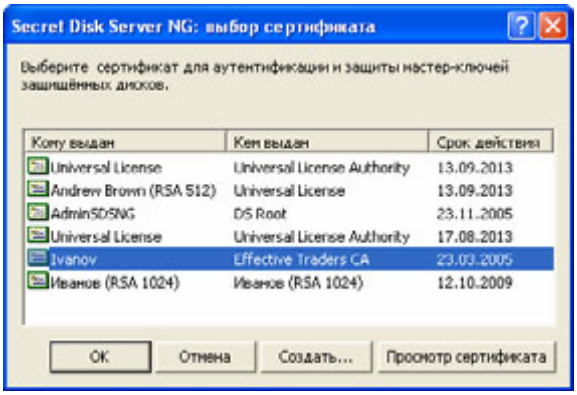
В окне **Secret Disk Server NG: новый администратор** введите один или несколько произвольных символов в графу **Имя**.

Шаг 5



В списке **Сертификаты данного администратора** выделите любой поставщик криптографии и нажмите **Выбрать**.

Шаг 6



В окне **Secret Disk Server NG: выбор сертификата** выберите сертификат, расположенный в памяти вашего eToken вместе с соответствующим закрытым ключом, и нажмите **OK**.

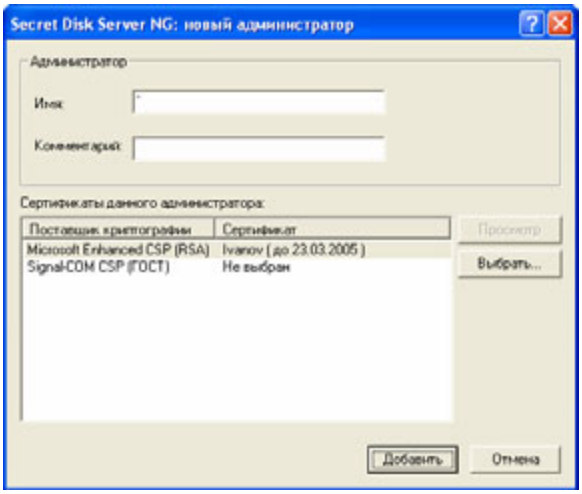
Примечания:

1. Если у вас нет сертификата, нажмите **Создать** и создайте его.
2. При необходимости, для того чтобы уточнить свой выбор, вы можете просмотреть параметры сертификата, нажав **Просмотр сертификата**.

Шаг 7

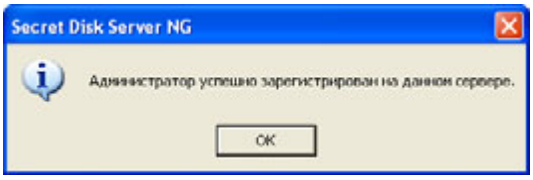
Введите PIN-код и нажмите OK. (Интерфейс зависит от поставщика криптографии.).

Шаг 8



В окне **Secret Disk NG: новый администратор** нажмите **Добавить**.

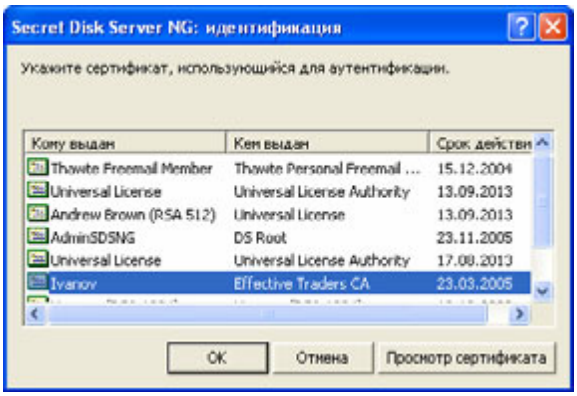
Шаг 9



В окне **Администратор успешно зарегистрирован на данном сервере** нажмите **OK**.

Сразу после регистрации первого администратора автоматически начинается процесс открытия сеанса управления. Для этого вам потребуется вновь указать один из выбранных сертификатов.

Шаг 10



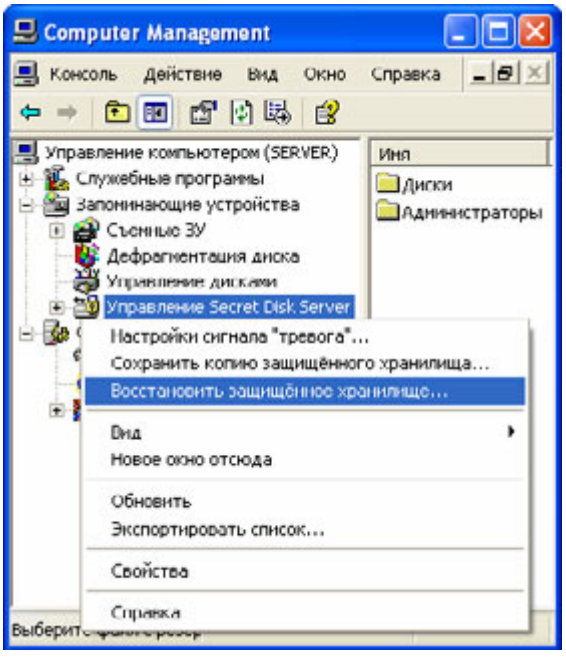
В окне **Secret Disk Server NG: идентификация** укажите выбранный сертификат и нажмите **OK**.

Примечание:

При необходимости, для того чтобы уточнить свой выбор, вы можете просмотреть параметры сертификата, нажав **Просмотр сертификата**.

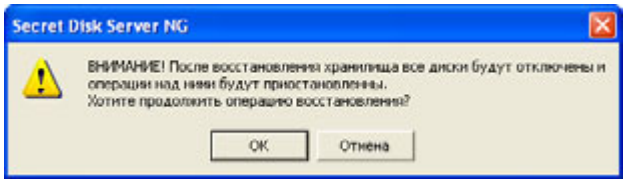
При необходимости введите PIN-код (интерфейс зависит от поставщика криптографии).

Шаг 11



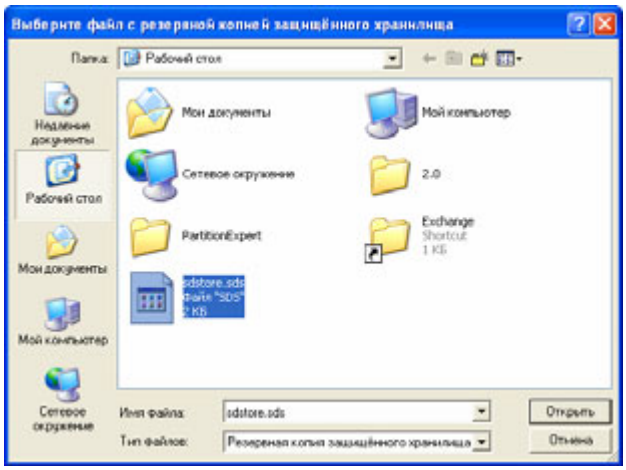
В дереве консоли щёлкните правой кнопкой мыши **Управление Secret Disk Server** и выберите **Восстановить защищённое хранилище**.

Шаг 12



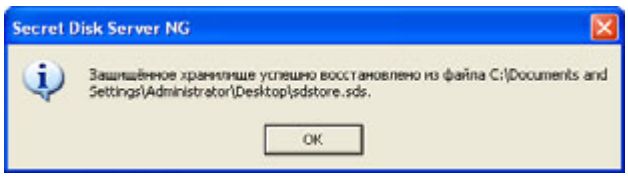
В окне подтверждения нажмите **OK**.

Шаг 13



Выберите файл с резервной копией защищённого хранилища и нажмите **Открыть**.

Шаг 14

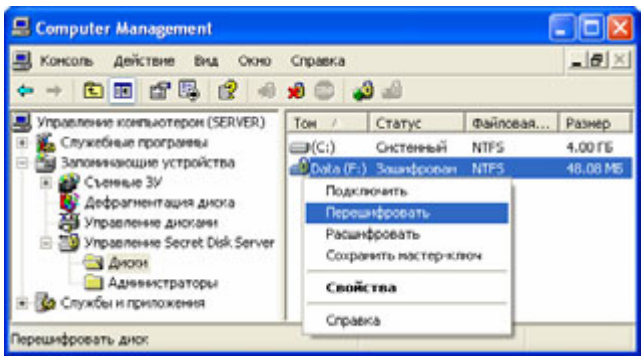


Убедитесь в том, что защищённое хранилище успешно восстановлено, и нажмите **OK**.

При необходимости откройте сеанс управления и подключите защищенные диски.

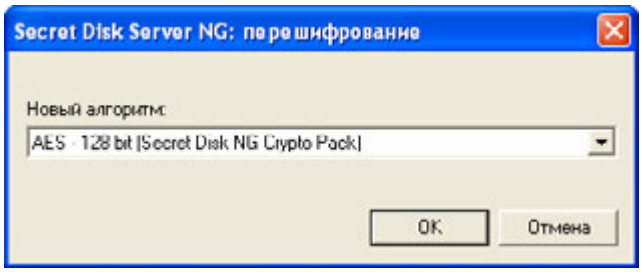
Перешифрование защищённого диска

Шаг 1



Выберите защищённый диск для перешифрования. Убедитесь в том, что выбранный защищённый диск отключен: значок в графе **Том** содержит изображение закрытого замка. Если это не так, отключите защищённый диск. Щелкните правой кнопкой мыши и выберите **Перешифровать**.

Шаг 2



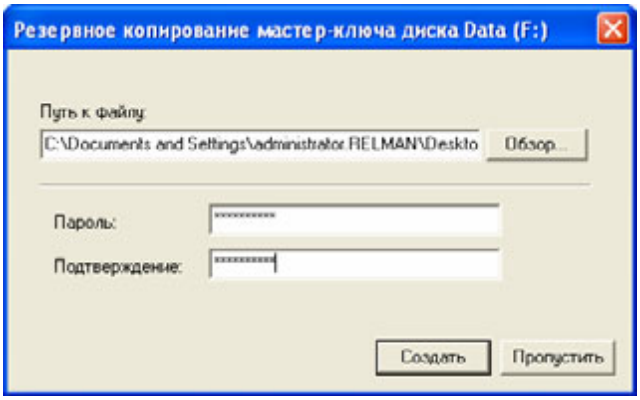
В окне **Secret Disk Server NG: перешифрование** выберите алгоритм шифрования, с помощью которого диск будет зашифрован в результате перешифрования.

В списке **Новый алгоритм** в скобках указывается поставщик криптографии или его компонент, отвечающий за шифрование дисков. Для успешного перешифрования у вас должен быть выбран сертификат для использования с данным поставщиком криптографии. Нажмите **OK**.

Шаг 3

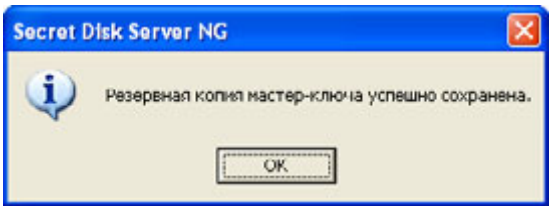
При необходимости подключите eToken, следуйте инструкциям датчика случайных чисел, выбирайте считыватель (eToken) и вводите PIN-код (интерфейс зависит от поставщика криптографии).

Шаг 4



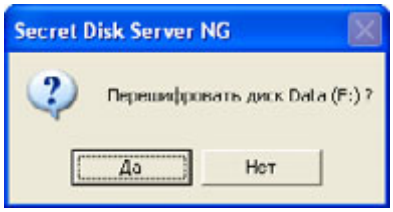
Система сгенерирует мастер-ключ защищённого диска. Для того чтобы сохранить резервную копию этого криптографического ключа, укажите путь к файлу резервной копии и введите пароль дважды — в графу **Пароль** и в графу **Подтверждение**. Нажмите **Создать**.

Шаг 5



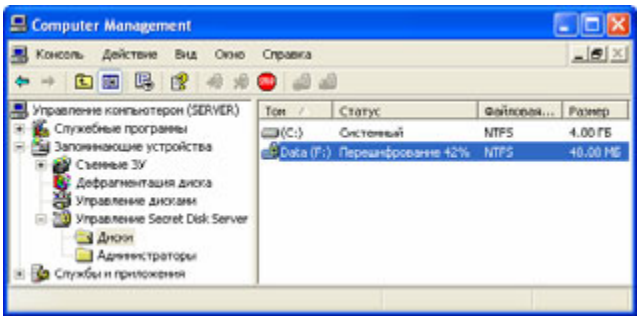
В случае успешного сохранения резервной копии мастер-ключа на экране появляется окно с сообщением: `Резервная копия мастер-ключа успешно сохранена`. Нажмите **OK**.

Шаг 6



В окне подтверждения нажмите **Да**.

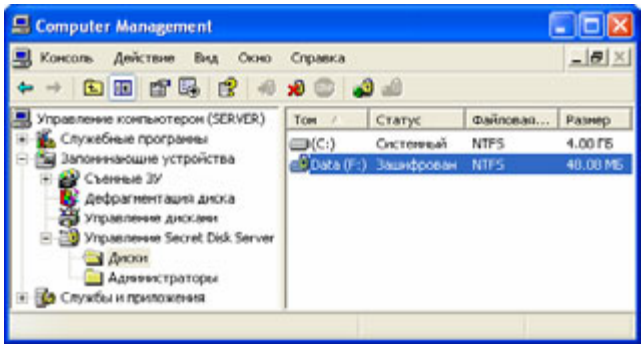
Шаг 7



О том, что процесс перешифрования активен, свидетельствует слово **Перешифрование** с указанием количества процентов готовности в ячейке **Статус**.

Теперь вы можете закрыть сеанс управления, закрыть консоль, закрыть сеанс пользователя Windows. Если вы управляете сервером удалённо, вы можете даже выключить свой компьютер. Эти действия не повлияют на процесс перешифрования.

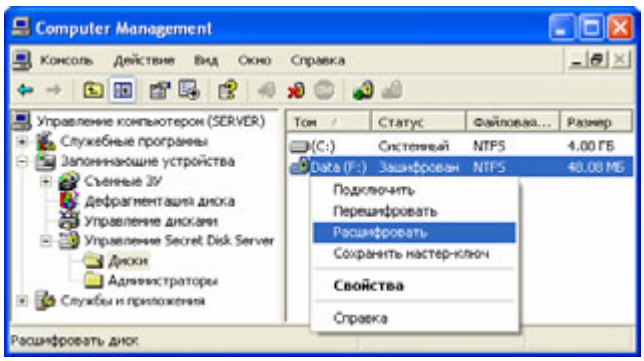
Шаг 8



Когда процесс перешифрования будет завершён, в ячейке **Статус** вновь появится слово `Зашифрован`.

Расшифрование защищённого диска

Шаг 1



Выберите защищённый диск для расшифрования. Убедитесь в том, что выбранный защищенный диск отключен: значок в графе **Том** содержит изображение закрытого замка. Если это не так, отключите защищённый диск. Щёлкните правой кнопкой мыши и выберите **Расшифровать**.

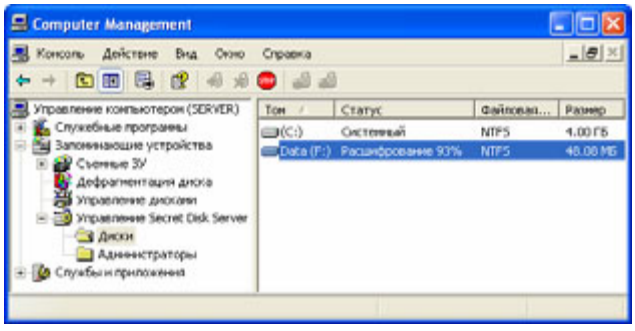
Шаг 2

В окне подтверждения убедитесь в том, что вы верно выбрали защищённый диск для расшифрования, и нажмите **Да**. Чтобы отказаться от расшифрования, нажмите **Нет**.

Шаг 3

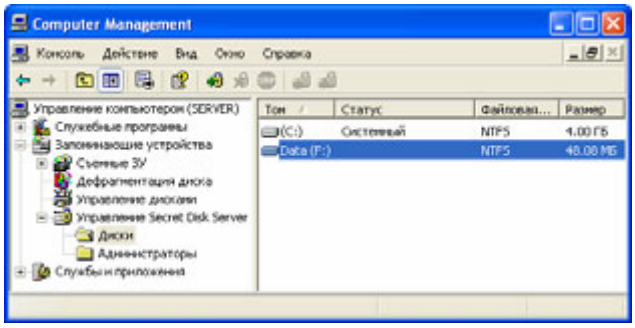
При необходимости выберите считыватель и (или) введите PIN-код (интерфейс зависит от поставщика криптографии).

Шаг 4



О том, что процесс расшифрования активен, свидетельствует слово **Расшифрование** в ячейке **Статус**. Теперь вы можете закрыть сеанс управления, закрыть консоль, закрыть сеанс пользователя Windows. Если вы управляете сервером удаленно, вы можете даже выключить свой компьютер. Эти действия не повлияют на процесс расшифрования.

Шаг 5



Убедитесь в том, что диск расшифрован: в списке дисков ячейка **Статус** соответствующей строки пуста.

Дополнительная информация

Особенности защищённых динамических томов

Расширение защищённого тома

Защищённый простой или составной динамический том можно расширить средствами Windows при двух условиях:

- исходный том, зашифрованный с помощью Secret Disk Server NG 3.0.2, был изначально создан на динамическом диске, а не преобразован из раздела или логического диска базового жесткого диска;
- защищённый диск имеет формат NTFS.

Перед тем как расширять защищённый том средствами операционной системы, выполните следующее.

1. Проверьте, расположен ли том, который вы собираетесь расширить, на динамическом диске.
2. Убедитесь в том, что данный защищённый диск имеет формат NTFS.
3. Убедитесь в том, что защищённый диск подключен. Если это не так, подключите его.

Защищённые зеркальные тома

Защищённые диски, созданные на основе зеркальных томов или преобразованные из простых томов, имеют следующую особенность.

После разделения зеркального тома на два простых тома один из томов становится защищённым простым томом, а другой операционная система воспринимает как неформатированный. Если вы удалите защищённый простой том, то доступ к оставшемуся тому, который воспринимается операционной системой как неформатированный, может быть восстановлен с помощью резервной копии мастер-ключа.

Защищённые тома RAID-5

Защищённые тома RAID-5 имеют следующую особенность.

Если один из динамических дисков, на которых расположен том RAID-5, выйдет из строя, соответствующий защищённый диск исчезнет. Для того чтобы восстановить его, реактивизируйте том RAID-5.

Типичные ошибки

Проблема:

На экране появилось окно **Windows Installer** с сообщением:

```
Данная установка запрещена политикой, выбранной системным
администратором. /

The system administrator has set policies to prevent this
installation.
```

Возможная причина:

Вы не имеете полномочий администратора на данном компьютере.

Решение:

1. Нажмите **OK**.
2. Обратитесь к администратору.

Проблема:

На экране появилось окно **Не найден eToken Run Time Environment**.

Возможная причина:

Ваш компьютер не соответствует системным требованиям.

Решение:

1. Нажмите **OK**.
2. Нажмите **Готово**.
3. Установите eToken Run Time Environment с компакт-диска Secret Disk Server NG 3.1.
4. Запустите программу установки компонентов Secret Disk Server NG 3.1 снова.

Проблема:

На экране появилось окно **Найден Secret Disk NG 3.x**.

Возможная причина:

На вашем компьютере установлен продукт семейства Secret Disk NG.

Решение:

1. Нажмите **OK**.
2. Нажмите **Готово**.
3. Расшифруйте все защищённые тома.
4. Перенесите все данные с защищённых виртуальных дисков на обычные диски.
5. Удалите все файлы виртуальных дисков.
6. Удалите Secret Disk NG 3.x
7. Перезагрузите компьютер.
8. Запустите программу установки компонентов Secret Disk Server NG 3.1 снова.

Проблема:

На экране появилось окно **Обнаружены драйверы Secret Disk NG или Secret Disk Server NG**.

Возможная причина:

На вашем компьютере остались драйверы одного из продуктов семейства Secret Disk NG или Secret Disk Server NG.

Решение:

1. Нажмите **OK**.
2. Нажмите **Готово**.
3. Перезагрузите компьютер.
4. Запустите программу установки компонентов Secret Disk Server NG 3.1 снова.

Проблема:

При попытке обращения к оснастке **Управление Secret Disk Server** вы получили сообщение:

```
Ошибка при открытии сеанса управления...
```

Возможные причины:

1. На сервере не установлен компонент «сервер».
2. На сервере остановлена служба `Secret Disk Server NG`.
3. Вы прервали процедуру открытия сеанса управления.
4. Аутентификация пользователя Windows на удалённом сервере не удалась.

Решение:

1. Убедитесь в том, что на сервере установлен компонент «сервер». Если это не так, установите данный компонент.
2. Убедитесь в том, что на сервере запущена служба Secret Disk Server NG. Если это не так, запустите службу и назначьте ей автоматический тип запуска.
3. Убедитесь в том, что сервер и рабочая станция администратора являются членами доменов, между которыми установлены доверительные отношения. При необходимости обеспечьте выполнение этого требования.
4. Нажмите F5.

Проблема:

При попытке обращения к оснастке **Управление Secret Disk Server** вы получили сообщение об ошибке:

```
eToken сервера не подключен.
```

Возможная причина:

eToken сервера не подключен к серверу.

Решение:

1. Подключите к серверу eToken сервера.
2. Нажмите F5.

Проблема:

На экране появилось окно **Secret Disk Server NG** с сообщением:

`Пожалуйста, подключите eToken`

Возможные причины:

1. Выполняемая операция требует наличие eToken администратора. Появление данного окна при выборе сертификата может быть обусловлено тем, что вы выбрали сертификат, хранящийся вне eToken.
2. Нет доступа к закрытому ключу, соответствующему выбранному сертификату.

Решение:

Если eToken администратора отключен, подключите его и введите PIN-код.

Если в памяти eToken администратора сертификат присутствует без соответствующего закрытого ключа, восстановите сертификат с закрытым ключом из резервной копии (при наличии таковой) и повторите попытку.

Если окно появилось в результате неверного выбора сертификата, выберите сертификат, хранящийся в памяти eToken администратора.

Проблема:

В окне **Secret Disk Server NG: Ошибка** или в консоли появилось сообщение:

`Выбранный сертификат хранится в eToken, который не содержит лицензии администратора.`

Возможная причина:

Вы выбрали сертификат, хранящийся в eToken, который не содержит лицензии администратора, или вне eToken.

Решение:

1. Нажмите **OK**.
2. Выберите сертификат, хранящийся в памяти eToken администратора, или приобретите лицензию администратора для данного eToken.

Проблема:

На экране появилось окно **Secret Disk Server NG** с сообщением:

`Требуются полномочия администратора на сервере.`

Возможная причина:

Выполняемая операция требует наличие у вас полномочий администратора на сервере.

Решение:

1. Нажмите **OK**.
2. Обратитесь к администратору.

Проблема:

При попытке обращения к оснастке **Управление Secret Disk Server** вы получили сообщение:

`Администратор Secret Disk Server NG не определён. ...`

Возможная причина:

Вы неверно указали сертификат для аутентификации.

Решение:

1. Подключите eToken администратора.
2. Нажмите F5.

Проблема:

При создания сертификата на экране появилось окно с сообщением:

`Маркер безопасности не имеет доступного места для хранения дополнительного контейнера.`

Возможная причина:

В памяти eToken администратора недостаточно свободного места.

Решение:

1. Нажмите **OK**.
2. Удалите ненужные данные из памяти eToken администратора или перейдите к использованию другого eToken администратора.
3. Повторите попытку.

Проблема:

При создания сертификата на экране появилось окно с сообщением:

`Недостаточно доступной памяти для выполнения операции.`

Возможная причина:

В памяти eToken администратора недостаточно свободного места.

Решение:

1. Нажмите **OK**.
2. Удалите ненужные данные из памяти eToken администратора или перейдите к использованию другого eToken администратора.
3. Повторите попытку.

Проблема:

При выборе сертификата на экране появилось окно **Secret Disk Server NG: Ошибка** с сообщением:

`Выбранный сертификат недействителен.`

Возможные причины:

1. В пути сертификации сертификата, который вы пытались выбрать:
   - корневой центр сертификации не входит в число доверенных корневых центров сертификации на рабочей станции администратора;

     или
   - по меньшей мере один из сертификатов промежуточных центров сертификации отсутствует в хранилище сертификатов промежуточных центров сертификации на рабочей станции администратора.
2. Срок действия сертификата не начался или истёк.
3. Сертификат отозван.

Решение:

1. Нажмите **OK**.
2. Сверьте срок действия сертификата с текущими датой и временем.
3. Проверьте, не является ли сертификат отозванным.
4. При необходимости добавьте необходимые сертификаты центров сертификации в соответствующие хранилища на рабочей станции администратора или выберите другой сертификат.
5. Устранив причины недействительности сертификата, повторите попытку или выберите другой сертификат.

Проблема:

При выборе сертификата на экране появилось окно **Ошибка при смене сертификата** с сообщением:

`Невозможно проверить действительность сертификата в контексте сервера.`

Возможные причины:

В пути сертификации сертификата, который вы пытались выбрать:

- корневой центр сертификации не входит в число доверенных корневых центров сертификации сервера;

  или
- по меньшей мере один из сертификатов промежуточных центров сертификации отсутствует в хранилище сертификатов промежуточных центров сертификации сервера.

Решение:

1. Нажмите **OK**.
2. Добавьте необходимые сертификаты центров сертификации в соответствующие хранилища сервера или выберите другой сертификат.

Проблема:

При попытке восстановить доступ к защищённому диску на экране появилось окно **Secret Disk Server NG: Ошибка** с сообщением:

```
Ошибка при восстановлении мастер-ключа защищённого диска.

Возможно, вы ввели неверный пароль или выбрали неверную копию
мастер-ключа.
```

Возможные причины:

Вы ввели неверный пароль файла резервной копии.

Решение:

1. Нажмите **OK**.
2. Повторите попытку ввода пароля.

Проблема:

Сертификат, созданный с помощью КриптоПро CSP 2.0 на другом компьютере, не отображается в окне **Выбор сертификата для защиты мастер-ключей**.

Возможная причина:

Сертификат не установлен на данном компьютере (его копия не хранится в реестре операционной системы).

Решение:

Для того чтобы установить на данном компьютере сертификат, созданный с помощью КриптоПро CSP 2.0 на другом компьютере и хранящийся в памяти eToken, выполните следующую последовательность действий.

1. Из **Панели Управления**/**Control Panel** откройте **КриптоПро CSP**/**CryptoPro CSP**.
2. В окне **Свойства: КриптоПро CSP** / **Properties: CryptoPro CSP** нажмите **Просмотреть сертификаты в контейнере** / **View certificates in container**.
3. В окне **Сертификаты в контейнере секретного ключа** / **Контейнер секретного ключа** (**Certificates in private key container** / **Private key container**) нажмтие **Обзор**/**Browse**.
4. В окне **Выбор ключевого контейнера** / **Select key container** выберите ключевой контейнер, в котором хранится нужный сертификат, и нажмите **OK**.
5. В окне **Сертификаты в контейнере секретного ключа** / **Контейнер секретного ключа** (**Certificates in private key container** / **Private key container**) нажмите **Далее**/**Next**.
6. Введите PIN-код вашего eToken.
7. В окне **Сертификаты в контейнере секретного ключа** / **Сертификат для просмотра** (**Certificates in private key container** / **Certificate to view**) нажмите **Свойства**/**Properties**.
8. В окне **Property Page Select Cert** во вкладке **Общие**/**General** нажмите **Установить сертификат / Install Certificate**, чтобы запустить мастер импорта сертификатов.
9. В окне приветствия мастера импорта сертификатов нажмите **Далее/Next**.
10. В окне **Мастер импорта сертификатов** / **Хранилище сертификатов** (**Certificate Import Wizard** / **Certificate Store**) выберите **Поместить все сертификаты в следующее хранилище / Place all certificates in the following store**.
11. Нажмите **Обзор**/**Browse**.

12. В окне **Выбор хранилища сертификата** / **Select Certificate Store** установите флажок **Показать физические хранилища** / **Show physical stores**.
13. Выберите **Личные**/**Реестр** (**Personal**/**Registry**).
14. Нажмите **OK**.
15. В окне **Мастер импорта сертификатов** / **Хранилище сертификатов** (**Certificate Import Wizard** / **Certificate Store**) нажмите **Далее/Next**.
16. В окне **Мастер импорта сертификатов** / **Завершение работы мастера импорта сертификатов** (**Certificate Import Wizard** / **Completing the Certificate Import Wizard**) нажмите **Готово/Finish**.
17. В случае успешной установки сертификата на экране появится окно с сообщением:

    `Импорт успешно выполнен. / The import was successful.`
18. Нажмите **OK**.
19. В окне **Property Page Select Cert** нажмите **OK**.
20. В окне **Сертификаты в контейнере секретного ключа** / **Сертификат для просмотра** (**Certificates in private key container** / **Certificate to view**) нажмите **Готово**/**Finish**.
21. Закройте окно **Свойства: КриптоПро CSP** / **Properties: CryptoPro CSP**.

Проблема:

На экране появилось окно **Secret Disk Server NG** с сообщением:

`Введён неверный PIN-код.`

Возможные причины:

Вы ввели неверный PIN-код.

Решение:

1. Нажмите **OK**.
2. Повторите попытку ввода PIN-кода.

Проблема:

На экране появилось окно **Secret Disk Server NG** с сообщением:

`Администратор с указанным сертификатом уже зарегистрирован на данном сервере.`

Возможная причина:

При добавлении нового администратора вы выбрали сертификат, принадлежащий другому администратору.

Решение:

1. Нажмите **OK**.
2. Выберите другой сертификат.

Проблема:

На экране появилось окно **Создание сертификата** с сообщением:

`Операция прервана.`

Возможная причина:

В окне **Выберите eToken** вы нажали **Отмена**.

Решение:

Нажмите **OK**.

Проблема:

На экране появилось окно **Создание сертификата** с сообщением:

`Создание резервной копии отменено`

Возможная причина:

В окне **Сохранение резервной копии сертификата** вы нажали **Отмена**.

Решение:

1. Нажмите **OK**.
2. В окне **Выберите eToken** нажмите **Отмена**.
3. На экране появится окно **Создание сертификата** с сообщением:

   `Операция прервана.`
4. Нажмите **OK**.
5. В окне параметров создаваемого сертификата снова нажмите **OK**.

Проблема:

На экране появилось окно **Secret Disk Server NG: Ошибка** с сообщением:

`Пароль и подтверждение должны совпадать.`

Возможная причина:

В графы **Пароль** и **Подтверждение** вы ввели разные последовательности символов.

Решение:

1. Нажмите **OK**.
2. Повторите попытку задания пароля.

Проблема:

На экране появилось окно **Диск используется другими приложениями** с сообщением:

`Нельзя перешифровать/расшифровать подключенный защищённый диск.`

Возможная причина:

Защищённый диск, который вы пытаетесь перешифровать/расшифровать, подключен.

Решение:

1. Нажмите **OK**.
2. Отключите защищённый диск.
3. Повторите попытку.

Проблема:

Не удаётся получить доступ к защищённому диску по сети.

Возможные причины:

1. Защищённый диск отключен.
2. Доступ к защищённому диску по сети запрещён.
3. Превышено количество одновременных подключений, определяемое лицензией файл-сервера.
4. eToken сервера отключен.
5. На сервере не запущена служба Secret Disk Server NG.

Решение:

1. Нажмите **OK**.
2. При необходимости подключите защищённый диск.
3. При необходимости разрешите доступ к защищённому диску по сети.
4. При необходимости приобретите лицензию файл-сервера, позволяющую осуществлять больше одновременных подключений.

   Примечание: лицензия файл-сервера ограничивает общее количество одновременных подключений ко всем защищённым дискам данного сервера.
5. Если eToken сервера отключен, подключите его.
6. Убедитесь в том, что на сервере запущена служба Secret Disk Server NG. Если это не так, запустите её.
7. Повторите попытку.

Проблема:

Подача сигнала «тревога» не приводит ни к отключению защищённых дисков, ни к удалению защищённого хранилища.

Возможные причины:

1. Сервер не настроен на удаление защищённого хранилища при поступлении сигнала «тревога».
2. Защищённые диски не настроены на отключение при поступлении сигнала «тревога».
3. Пароль сигнала «тревога», настроенный на сервере, не соответствует паролю сигнала «тревога» для данного сервера, хранящемуся на рабочей станции для подачи сигнала «тревога».
4. Сервер недоступен по сети с рабочей станции для подачи сигнала «тревога».

Решение:

1. Проверьте настройки сигнала «тревога» для сервера. При необходимости внесите изменения.
2. Проверьте настройки сигнала «тревога» для каждого защищённого диска. При необходимости внесите изменения.
3. Выберите новый пароль сигнала «тревога» и внесите его в настройки сервера и Secret Disk NG Alarm 3.0.
4. Проверьте сетевые настройки сервера и рабочей станции для подачи сигнала «тревога», а также физическую целостность сети. При необходимости устраните неполадки.

Проблема:

В окне свойств сервера нет информации о серверных лицензиях.

Возможные причины:

1. На сервере не работает служба `Secret Disk Server NG`.
2. eToken сервера не подключен.

Решение:

1. Нажмите **OK**.
2. Убедитесь в том, что на сервере работает служба `Secret Disk Server NG`. Если это не так, запустите её.
3. Убедитесь в том, что к серверу подключен eToken сервера. Если это не так, подключите его.
4. Откройте окно свойств сервера снова.

Поиск и устранение неисправностей

Если вам не удаётся решить возникшую проблему самостоятельно, обратитесь в службу технической поддержки компании Aladdin по электронной почте: techsup@aladdin.ru. Ваше электронное письмо должно содержать следующие сведения:

- версия операционной системы сервера, установленный пакет обновлений;
- версия операционной системы рабочей станции администратора, установленный пакет обновлений;
- версия eToken Run Time Environment на сервере;
- версия eToken Run Time Environment на рабочей станции администратора;
- аппаратная конфигурация дисковой подсистемы;
- типы дисков — базовые диски или динамические, простые или RAID-массивы, съёмные диски;
- какие тома, разделы, логические диски зашифрованы с помощью Secret Disk Server NG 3.0.2;
- используемые поставщики криптографии;
- используемые алгоритмы шифрования;
- версия встроенного программного обеспечения (FW version) eToken (можно узнать с помощью eToken Properties);
- на каком компьютере установлен Secret Disk NG Alarm 3.0;
- какие лицензии содержатся в памяти eToken сервера;
- запрещён ли доступ к защищённому диску по сети;
- описание проблемы.

Часто задаваемые вопросы

Какие операционные системы поддерживает Secret Disk Server NG 3.1?

Сервер, интерфейс администратора и Secret Disk NG Alarm 3.1 можно устанавливать на компьютеры с операционными системами Microsoft Windows 2000, Windows XP и Windows Server 2003.

Могу ли я переименовать eToken администратора и eToken сервера? Не повлияет ли это на их функциональность?

При желании вы можете переименовать как eToken администратора, так и eToken сервера. Это не повлияет на функциональность. О том, как произвести переименование eToken, см. в документе *eToken. Руководство администратора* (файл `eToken_Admin_Guide.pdf` в папке `Doc` компакт-диска Secret Disk Server NG 3.1).

Нужно ли делать резервные копии мастер-ключей, если есть копия защищённого хранилища, в котором они и так содержатся?

В защищённом хранилище содержатся копии мастер-ключей, зашифрованные с использованием открытых ключей администраторов. Перед использованием мастер-ключи считываются из защищённого хранилища и расшифровываются с помощью закрытых ключей, хранящихся в памяти eToken администратора. Если закрытые ключи, например, будут потеряны (при утрате eToken администратора), то использовать копии мастер-ключей, хранящиеся в защищённом хранилище, будет нельзя.

В отличие от защищённого хранилища, архивы мастер-ключей содержат копии этих ключей, зашифрованные с использованием пароля. Они не зависят от сертификатов и закрытых ключей, а следовательно, от eToken администратора. Резервные копии мастер-ключей защищённых дисков могут пригодиться, например, в следующих случаях:

- повреждение или утрата eToken администратора;
- истечение срока действия сертификата;
- перенос защищённого диска с одного сервера на другой сервер, на которм присутствуют и другие защищённые диски.

Во всех перечисленных случаях резервная копия защищённого хранилища непригодна. Поэтому для предотвращения возможности потери доступа к данным сохраняйте резервные копии мастер-ключей всех защищённых дисков.

Можно ли сделать резервную копию содержимого eToken сервера?

eToken сервера предназначен для предотвращения нелегального использования Secret Disk Server NG 3.1. В памяти eToken сервера хранится лицензия файл-сервера, содержащая информацию о предельном количестве одновременных сетевых подключений, или/и лицензия сервера приложений, позволяющая запрещать сетевой доступ к защищённым дискам. Эти лицензии уникальны для данного eToken. Нельзя использовать другой USB-ключ или смарт-карту eToken PRO в качестве eToken сервера, скопировав в него лицензии из вашего eToken сервера. Поэтому резервное копирование содержимого eToken сервера не предусмотрено.

Где в процессе работы с защищённым диском находится мастер-ключ?

Если в качестве поставщика криптографии используется драйвер режима ядра (Windows Kernel Mode Cyrpto Driver или Secret Disk NG Crypto Pack 3.0), то ключ загружен в драйвер Secret Disk Server NG 3.1. При использовании поставщиков службы криптографии (Signal-COM CSP или КриптоПро CSP 2.0) мастер-ключ находится под управлением соответствующего поставщика. Кроме того, в зашифрованном виде ключ всегда размещён в защищённом хранилище.

Как восстановить администраторский доступ к защищённым дискам при утрате eToken администратора?

Для этого вам потребуются новый eToken с лицензией администратора. Если вы располагаете резервными копиями сертификатов и соответствующих закрытых ключей, которые вы использовали для аутентификации и защиты мастер ключей защищённых дисков, то вам потребуется лишь импортировать эти сертификаты в память нового eToken. Если у вас нет резервных копий сертификатов, то для восстановления доступа необходимо выполнение хотя бы одного из двух условий:

- на сервере помимо администратора, который потерял eToken, зарегистрирован хотя бы ещё один администратор;
- вы располагаете резервными копиями мастер-ключей защищённых дисков и знаете соответствующие пароли.

При первом условии другой администратор сможет добавить вас в качестве нового администратора, и таким образом у вас появится администраторский доступ к защищённым дискам. Во втором случае вам необходимо:

- удалить Secret Disk Server NG 3.1 вместе с защищённым хранилищем;
- установить Secret Disk Server NG 3.1 снова;
- зарегистрировать нового администратора Secret Disk Server NG;
- восстановить доступ ко всем защищённым дискам с помощью резервных копий мастер-ключей.

Какие меры необходимо предпринять для предотвращения негативных последствий утраты eToken администратора?

- Наличие резервных копий сертификатов с закрытыми ключами.
- Коллективная работа нескольких администраторов.
- Резервное копирование мастер-ключей всех защищённых дисков.

Поддерживает ли Secret Disk Server NG 3.1 динамические тома?

Да, поддерживает. Вы можете создавать простые, составные, чередующиеся и отказоустойчивые защищённые динамические тома.

После перезагрузки сервера система осуществляет ресинхронизацию/resynching защищенного тома RAID-5. Нужно ли дожидаться окончания ресинхронизации?

Дожидаться окончания ресинхронизации необязательно. Вы можете подключать и использовать защищенный том RAID-5 сразу после перезагрузки.

Глоссарий

eToken — персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП. eToken выпускается в форм-факторах USB-ключа или смарт-карты.

eToken администратора — eToken, в памяти которого содержится лицензия администратора. Для каждого из используемых поставщиков криптографии в памяти eToken администратора должен присутствовать сертификат с закрытым ключом для защиты мастер-ключей защищённых дисков, шифруемых с помощью данного поставщика криптографии, и аутентификации.

См. также: eToken, лицензия администратора.

eToken сервера — eToken с лицензией файл-сервера и/или лицензией сервера приложений. Наличие подключенного eToken сервера позволяет использовать данный компьютер в качестве сервера Secret Disk Server NG 3.1.

См. также: eToken, лицензия сервера приложений, лицензия файл-сервера.

FAT — FAT16, файловая система, совместимая со всеми версиями Windows.

FAT32 — файловая система, совместимая с Windows 95 OSR2, Windows 98, Windows Me, Windows 2000, Windows XP и Windows Server 2003, но несовместимая с Windows 95, Windows NT и более ранними версиями Windows.

Microsoft Enhanced CSP — поставщик службы криптографии (CSP), входящий в состав операционных систем Windows 2000 (с установленным пакетом обновления 2 или выше), XP и Server 2003.

См. также: Поставщик службы криптографии (CSP).

NTFS — файловая система, совместимая с операционными системами Windows NT, Windows 2000, Windows XP и Windows Server 2003.

Signal-COM CSP — сертифицированный российский поставщик службы криптографии (CSP), реализующий алгоритмы, соответствующие ГОСТ 28147-89 «Система обработки информации. Защита криптографическая», ГОСТ Р 34.10-94 «Система обработки информации. Защита криптографическая. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма», и ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

См. также: Поставщик службы криптографии (CSP).

Закрытие сеанса управления — закрытие или подключение к другому компьютеру консоли с оснасткой **Управление Secret Disk Server** или обновление этой оснастки.

См. также: сеанс управления, открытие сеанса управления.

Зашифрование диска — подготовка диска для использования в качестве защищённого диска.

См. также: защищённый том, подключение защищённого диска.

Защищённое хранилище — объект, хранящийся на системном диске и содержащий информацию об администраторах Secret Disk Server NG, а также зашифрованные копии мастер-ключей защищённых дисков для всех администраторов Secret Disk Server NG.

Защищённый диск — диск, использующийся для безопасного хранения конфиденциальной информации в зашифрованном виде. В Secret Disk Server NG 3.1 в качестве защищённых дисков используются защищённые тома.

См. также: защищённый том, отключенный защищённый диск, подключенный защищённый диск.

Защищённый съёмный диск — защищённый диск, созданный на базе съёмного диска, такого как USB-диск, ZIP и др.

См. также: защищённый диск.

Защищённый том — защищённый диск, созданный на базе основного раздела базового жёсткого диска, логического диска в дополнительном разделе базового жёсткого диска, тома динамического жёсткого диска или съёмного диска, такого как USB-диск, ZIP и др.

См. также: защищённый диск, защищённый съёмный диск.

Крипто-Про — российская компания-разработчик средств защиты информации.

КриптоПро CSP 2.0 — сертифицированный российский поставщик службы криптографии (CSP), реализующий алгоритмы, соответствующие ГОСТ 28147-89 «Система обработки информации. Защита криптографическая», ГОСТ Р 34.10-94 «Система обработки информации. Защита криптографическая. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма», ГОСТ Р 34.10-2001 «Система обработки информации. Защита криптографическая. Процессы формирования и проверки электронной цифровой подписи» и ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

См. также: Поставщик службы криптографии (CSP).

Лицензия администратора — объект, хранящийся в памяти eToken администратора. Наличие лицензии позволяет использовать данный eToken для управления Secret Disk Server.

Лицензия сервера приложений — объект, хранящийся в памяти eToken сервера и позволяющий запрещать сетевой доступ к защищённым дискам.

См. также: eToken сервера, лицензия файл-сервера.

Лицензия файл-сервера — объект, хранящийся в памяти eToken сервера и содержащий информацию о максимальном количестве клиентских подключений.

См. также: eToken сервера, лицензия сервера приложений.

Мастер-ключ защищённого диска — уникальный секретный параметр алгоритма шифрования диска.

Отключение защищённого диска — событие, при котором все операции с файлами и папками на защищённом диске становятся недоступными.

См. также: защищённый диск, подключенный защищённый диск.

Отключенный защищённый диск — защищённый диск, операции с файлами и папками на котором невозможны в данный момент. Для получения доступа к файлам и папкам на таком диске требуется подключить его.

См. также: защищённый диск, *подключение защищённого диска.*

Открытие сеанса управления — успешное прохождение процедуры аутентификации администратора Secret Disk Server NG при обращении к оснастке **Управление Secret Disk Server**.

См. также: сеанс управления, закрытие сеанса управления.

Перешифрование защищённого диска — смена мастер-ключа защищённого диска и (необязательно) алгоритма шифрования.

См также: мастер-ключ защищённого диска.

Подключение защищённого диска — событие, при котором становятся доступными все операции с файлами и папками на защищённом диске, а также его форматирование и проверка на наличие ошибок.

См. также: защищённый диск, отключенный защищённый диск.

Подключенный защищённый диск — защищённый диск, операции с файлами и папками на котором, а также его форматирование и проверку на наличие ошибок можно проводить в данный момент.

См. также: защищённый диск, отключение защищённого диска.

Поставщик криптографии — программное обеспечение, применяемое при генерировании и резервном копировании криптографических ключей, шифровании электронной информации и аутентификации. Стандартный поставщик криптографии Secret Disk Server NG 3.1 по умолчанию состоит из следующих компонентов:

- криптографический драйвер режима ядра, входящий в состав Microsoft Windows — для шифрования дисков;
- Microsoft Enhanced CSP — для генерирования и защиты мастер-ключей защищённых дисков, а также аутентификации.

Кроме того, в качестве поставщиков криптографии Secret Disk Server NG 3.1 может использовать Signal-COM CSP и КриптоПро CSP 2.0.

См. также: Signal-COM CSP, КриптоПро CSP 2.0, Поставщик службы криптографии (CSP).

Поставщик службы криптографии (CSP) — программный код, выполняющий операции проверки подлинности и шифрования, доступные приложениям Windows через интерфейс CryptoAPI. CSP отвечает за создание, уничтожение и использование ключей в различных криптографических операциях. Одни поставщики предоставляют криптографические алгоритмы повышенной надежности, другие содержат аппаратные компоненты, такие как смарт-карты.

См. также: Поставщик криптографии.

Расшифрование защищённого тома — процесс, в результате которого доступ к данным на защищённом томе ограничивается только файловой и операционной системами, а сам диск или том перестаёт существовать в качестве защищённого диска.

Сеанс управления — состояние рабочей станции администратора, при котором к компьютеру подключен eToken администратора и осуществляется работа с оснасткой **Управление Secret Disk Server**.

См. также: открытие сеанса управления, закрытие сеанса управления.

Сигнал-КОМ — российская компания-разработчик программно-аппаратных и инструментальных средств для создания защищённых информационных систем и виртуальных частных сетей.

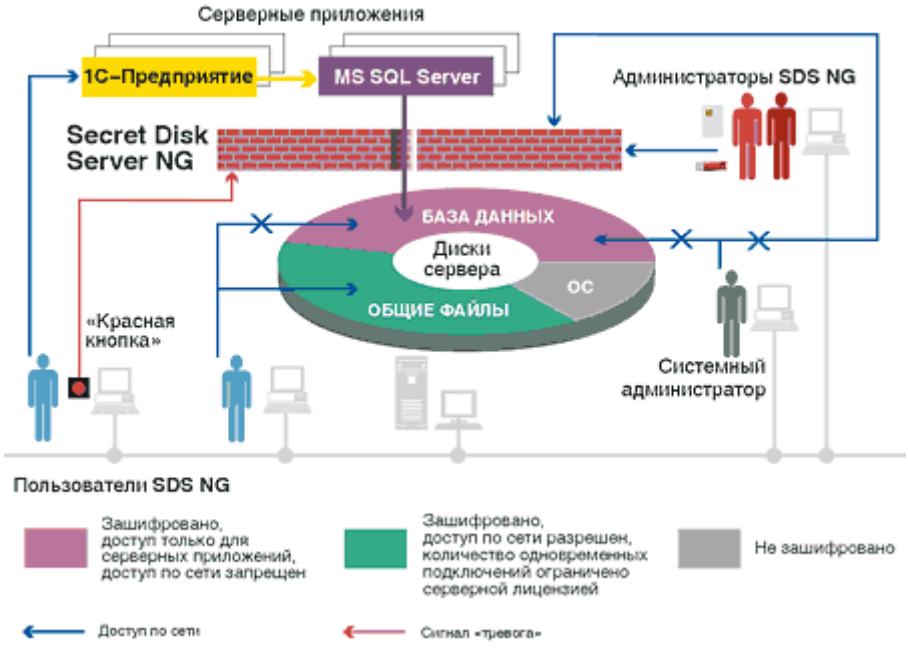
Приложение 1. Пример сценария для отключения хранилища Microsoft Exchange Server перед отключением защищённого диска

```
Dim strMDBName
Dim strSGName
Dim strComputerName
Dim strAdmGrpName
Dim OrgName
Dim LdapDc
strMDBName ="Private Mailbox Store"
strSGName = "PrivateMail"
strComputerName = "Server"
strAdmGrpName = "First Administrative Group"
OrgName = "Effective Traders"
LdapDc = "DC=etraders,DC=com"
Dim iMDB
Dim iServer
Dim strTemp
Dim strMDBUrl
Dim arrStGroup()
set iServer = CreateObject ("CDOEXM.ExchangeServer")
set iMDB = CreateObject ("CDOEXM.MailboxStoreDB")
iServer.DataSource.Open strComputerName
    WScript.echo iServer.DirectoryServer
' Build the URL to the MailboxStoreDB
    strMDBUrl                                                    =
"LDAP://"&iServer.DirectoryServer&"/"&"cn="&strMDBName&",cn="&strS
GName&",cn=InformationStore,cn="&strComputerName&",CN=Servers,CN="
&strAdmGrpName&",CN=Administrative
Groups,CN="&OrgName&",CN=Microsoft
Exchange,CN=Services,CN=Configuration,"& LdapDc
    WScript.echo  "the url is  " & strMDBUrl
'Bind to the MailboxStoreDB
    iMDB.DataSource.Open strMDBUrl
'Dismount the MailboxStoreDB
    iMDB.Dismount(30)
```



```
    WScript.echo "The database "& strMDBName & " was successfuly
dismounted"
'Cleanup
    Set iServer = Nothing
    Set iMDB = Nothing
```

Приложение 2. Пример внедрения Secret Disk Server NG 3.1 на одном сервере



На одном и том же сервере расположены электронные документы для совместной работы и база данных 1С:Предприятие. Дисковая подсистема сервера включает три тома:

- системный;
- защищённый диск с общими файлами;
- защищённый диск с базой данных.

Администраторы Secret Disk Server NG осуществляют удалённое управление сервером Secret Disk Server NG 3.1 через интерфейс администратора. Системный администратор не имеет такой возможности.

Никто, включая системного администратора, не имеет доступа к файлам базы данных по сети, поскольку доступ к соответствующему защищённому диску по сети запрещён.

Пользователи обращаются к общим файлам по сети, а к данным, хранящимся в базе 1С-Предприятие — только через интерфейс этого приложения.

Офицер безопасности имеет возможность одним нажатием «красной кнопки», подключенной к его рабочей станции, отключить защищённые диски и удалить защищённое хранилище.

Предметный указатель

