Aladdin

Secret Disk Server NG 3.2. Краткое руководство

Версия 1.0, май 2006

ВАЖНО:

ПОЖАЛУЙСТА, ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ПРЕЖДЕ ЧЕМ ОТКРЫТЬ ПАКЕТ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ И/ИЛИ ИСПОЛЬЗОВАТЬ ЕГО СОДЕРЖИМОЕ И/ИЛИ ПРЕЖДЕ, ЧЕМ ЗАГРУЖАТЬ ИЛИ УСТАНАВЛИВАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

ВСЕ УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ ПРОДУКТОВ с использованием электронных ключей и смарт-карт eToken (включая без ограничений библиотеки, утилиты, дискеты, CD ROM, ключи и смарт-карты eToken®, Руководства, описания и др. документацию) (далее ”Продукт”), ПРЕДОСТАВЛЯЕМЫЕ КОМПАНИЕЙ ALADDIN (или любым дочерним предприятием – каждое из них упоминаемое как «ALADDIN»), ПОДЧИНЯЮТСЯ И БУДУТ ПОДЧИНЯТЬСЯ УСЛОВИЯМ, ОГОВОРЕННЫМ В ДАННОМ СОГЛАШЕНИИ.

ОТКРЫВАЯ ПАКЕТ, СОДЕРЖАЩИЙ ПРОДУКТ И/ИЛИ ЗАГРУЖАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (как определено далее по тексту) И/ИЛИ УСТАНАВЛИВАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА ВАШ КОМПЬЮТЕР И/ИЛИ ИСПОЛЬЗУЯ ДАННЫЙ ПРОДУКТ, **ВЫ ПРИНИМАЕТЕ ДАННОЕ СОГЛАШЕНИЕ И СОГЛАШАЕТЕСЬ С ЕГО УСЛОВИЯМИ**.

ЕСЛИ ВЫ НЕ СОГЛАСНЫ С ДАННЫМ СОГЛАШЕНИЕМ, НЕ ОТКРЫВАЙТЕ ЭТОТ ПАКЕТ И/ИЛИ НЕ ЗАГРУЖАЙТЕ И/ИЛИ НЕ УСТАНАВЛИВАЙТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И НЕЗАМЕДЛИТЕЛЬНО (не позднее 7 дней с даты получения этого пакета) ВЕРНИТЕ ЭТОТ ПРОДУКТ В ALADDIN, СОТРИТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВСЕ ЕГО ЧАСТИ В СВОЕМ КОМПЬЮТЕРЕ И НЕ ИСПОЛЬЗУЙТЕ ЕГО НИКОИМ ОБРАЗОМ.

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между вами (физическим или юридическим лицом) - конечным пользователем (далее "Пользователь") и компанией Aladdin Software Security R.D. (далее "Aladdin") относительно передачи неисключительного права на использование программного обеспечения (далее "ПО"), работающего с электронными ключами и смарт-картами eToken.

1. Права и Собственность. ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Это программное обеспечение, поддерживающее eToken, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как "Программное обеспечение" (ПО), и связанная с ней документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остается исключительной собственностью компании Aladdin.

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтвержденные или включенные в приложенные/ взаимосвязанные/ имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на Продукт являются и будут являться собственностью исключительно компании Aladdin.

Данное соглашение не передает вам права на ПО, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничего в данном Соглашении не подтверждает отказ компании Aladdin от прав на интеллектуальную собственность по какому бы то ни было законодательству.

2. Лицензия. После уплаты соответствующего вознаграждения Aladdin настоящим предоставляет вам, а вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как описано в прилагаемой к ПО документации и только в соответствии с условиями данного Соглашения:

2.1. Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах вашего предприятия, как описано в соответствующей документации компании Aladdin.

2.2. Вы можете добавить/присоединить ПО к программам вашего компьютера с единственной целью, описанной в данном Руководстве.

3. Требования к использованию. Продукт должен использоваться и обслуживаться строго в соответствии с описаниями и инструкциями компании Aladdin, приведенными в данном и других документах Aladdin. За исключением указанного выше в разделах 1 и 2 вы соглашаетесь:

3.1. Не использовать, не модифицировать, и не выдавать сублицензии на данное ПО и любой другой Продукт компании Aladdin, за исключением явных разрешений в данном Соглашении и в Руководстве по интеграции.

© 2006, Aladdin

3.2. Не продавать, не выдавать лицензий или сублицензий, не сдавать в аренду, не передавать, не переводить на другие языки, не закладывать, не разделять ваши права в рамках данного Соглашения с кем-либо или кому-либо ещё.

3.3. Не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное ПО и не пытаться раскрыть (получить) исходные коды данного ПО.

3.4. Не помещать данное ПО на сервер с возможностью доступа к нему третьих лиц через открытую сеть.

3.5. Не использовать какие бы то ни было резервные или архивные копии данного ПО (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

4. Обслуживание и поддержка. Aladdin не несет обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов данного ПО.

5. Ограниченная гарантия. Aladdin гарантирует, что:

5.1 Данное ПО с момента поставки его вам в течение двенадцати (12) месяцев будет функционировать в полном соответствии с Руководством Пользователя (Администратора), при условии, что оно будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

5.2 Ключ (смарт-карта) eToken в течение двенадцати (12) месяцев с момента поставки будет в достаточной мере свободен от значительных дефектов в материалах, конструктивных характеристиках и качестве.

6. Отказ от гарантии. ALADDIN НЕ ГАРАНТИРУЕТ, ЧТО ЛЮБОЙ ИЗ ЕГО ПРОДУКТОВ БУДЕТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ, ИЛИ ЧТО ЕГО РАБОТА БУДЕТ БЕСПЕРЕБОЙНОЙ ИЛИ БЕЗОШИБОЧНОЙ. В ОБЪЕМЕ, ПРЕДУСМОТРЕННОМ ЗАКОНОДАТЕЛЬСТВОМ РФ, ALADDIN ОТКРЫТО ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ГАРАНТИЙ, НЕ ОГОВОРЕННЫХ ЗДЕСЬ, ОТ ВСЕХ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ ГАРАНТИЮ ТОВАРНОГО ВИДА И ПРИГОДНОСТИ ИСПОЛЬЗОВАНИЯ ДЛЯ ОПРЕДЕЛЁННОЙ ЦЕЛИ.

НИ ОДИН ИЗ ДИЛЕРОВ, ДИСТРИБЬЮТОРОВ, ПРОДАВЦОВ, АГЕНТОВ ИЛИ СОТРУДНИКОВ ALADDIN НЕ УПОЛНОМОЧЕН ПРОИЗВОДИТЬ МОДИФИКАЦИИ, РАСШИРЕНИЯ ИЛИ ДОПОЛНЕНИЯ К ДАННОЙ ГАРАНТИИ.

Если вы произвели какие-либо модификации ПО или любой из частей данного Продукта во время гарантийного периода, если ключ (смарт-карта) eToken подвергся повреждению, неосторожному или неправильному обращению, если вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если Продукт используется на или в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в данном Руководстве, или используется на компьютере с любым установленным нелицензионным программным обеспечением.

7. Ограничение возмещения. В случае нарушения гарантии, оговоренной выше, Aladdin может по собственному усмотрению:

7.1. Заменить или бесплатно отремонтировать Продукт или его составляющие, если это не противоречит вышеупомянутому ограничению гарантии.

7.2. Возместить стоимость, выплаченную вами за Продукт или его компоненты. Любая замененная или отремонтированная компонента будет на гарантии или в течение промежутка времени, оставшегося от начального гарантийного периода, или в течение 30 дней, если срок начального гарантийного периода истекает ранее. Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее семи (7) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Aladdin. Все Продукты должны быть возвращены дистрибьютору, через которого была совершена покупка (если покупка состоялась не непосредственно в Aladdin), и отправлена возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Продукты или их компоненты должны быть отправлены с копией платежных документов и накладных.

8. Исключение косвенных убытков. Стороны признают, что Продукт по сути своей сложный и не может быть полностью лишен ошибок. ALADDIN НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ, ПОБОЧНЫЕ ИЛИ ПОТЕНЦИАЛЬНЫЕ УБЫТКИ), ВКЛЮЧАЯ, БЕЗ ОГРАНИЧЕНИЙ, ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЕННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ КАКОГО-ЛИБО ИСПОЛЬЗОВАНИЯ ДАННОГО ПО И/ИЛИ

ЛЮБОЙ КОМПОЕНТЫ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ ALADDIN ПИСЬМЕННО УВЕДОМЛЁН О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

9. Ограничение ответственности. В СЛУЧАЕ ЕСЛИ, НЕСМОТРЯ НА УСЛОВИЯ ДАННОГО СОГЛАШЕНИЯ, ALADDIN ПРИЗНАН ОТВЕТСТВЕННЫМ ЗА УБЫТКИ НА ОСНОВАНИИ КАКИХ-ЛИБО ДЕФЕКТОВ ИЛИ НЕСООТВЕТСТВИЯ ЕГО ПРОДУКТОВ, ПОЛНАЯ ОТВЕТСТВЕННОСТЬ ЗА КАЖДУЮ ЕДИНИЦУ ДЕФЕКТНЫХ ПРОДУКТОВ НЕ БУДЕТ ПРЕВЫШАТЬ СУММУ, ВЫПЛАЧЕННУЮ КОМПАНИИ ALADDIN ЗА ЭТИ ДЕФЕКТНЫЕ ПРОДУКТЫ.

10. Прекращение действия. В случае невыполнения вами условий данного Соглашения действие вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

(i) Лицензия, предоставленная вам данным Соглашением, прекращает свое действие, и вы после ее прекращения не сможете продолжать дальнейшее использование данного ПО и других лицензионных Продуктов;

(ii) Вы незамедлительно вернёте в компанию Aladdin всё имущество, в котором используются права Aladdin на интеллектуальную собственность и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в них в электронном виде. Разделы 1, 3, 6-11 будут продолжать действовать даже в случае прекращения действия настоящего Соглашения.

11. Применимое законодательство. Данное Соглашение должно быть истолковано и определено в соответствии с законами России (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Применение Конвенции Организации Объединённых Наций о Договорах международной купли-продажи товаров (the United Nations Convention of Contracts for the International Sale of Goods) однозначно исключается. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

12. Государственное регулирование и экспортный контроль. Вы соглашаетесь с тем, что Продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом. Продукт является предметом дополнительного экспортного контроля, относящегося к вам или вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт Продукта ограничения.

13. Программное обеспечение третьих сторон. Если Продукт содержит в себе любое программное обеспечение, предоставленное какой-либо третьей стороной, такое программное обеспечение третьей стороны предоставляется ”как есть” без какой-либо гарантии, и разделы 2, 3, 6, 8, 9-12 настоящего Соглашения применяются ко всем таким поставщикам программного обеспечения и к поставляемому ими программному обеспечению, как если бы это были Aladdin и Продукт соответственно.

14. Разное. Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

© 2006, Aladdin

СОДЕРЖАНИЕ

© 2006, Aladdin

ОБЩИЕ СВЕДЕНИЯ

Программно-аппаратный комплекс Secret Disk Server NG 3.2 разработан для обеспечения безопасной работы с конфиденциальной информацией, хранящейся на корпоративном сервере. С помощью Secret Disk Server NG 3.2 вы можете зашифровывать диски, превращая их в *защищённые диски* (*защищённые тома*).

Подключенный защищённый диск используется точно так же, как и обычный диск. *Отключенный защищённый диск* представляется системе как неформатированный.

Для управления защищёнными дисками используется персональный электронный USB-ключ или смарт-карта *eToken*. Шифрование и подключение защищённых дисков, резервное копирование и восстановление мастер-ключей осуществляются лишь после предъявления eToken зарегистрированного администратора и ввода соответствующего PIN-кода. В системе Secret Disk Server NG 3.2 может быть несколько зарегистрированных администраторов.

В Secret Disk Server NG 3.2 имеется инструмент резервного копирования защищённого хранилища, в котором содержатся зашифрованные копии мастер-ключей и информация об администраторах Secret Disk Server NG.

Для чрезвычайных ситуаций предусмотрен инструмент «красная кнопка». Он позволяет удалённо отключать защищённые диски. При определённых настройках нажатие «красной кнопки» приводит также к удалению с сервера ключевой информации. В результате даже если злоумышленники завладеют нужным электронным ключом или смарт-картой eToken, узнают PIN-код и будут обладать полным доступом к серверу, они не смогут прочесть информацию, не располагая резервной копией защищённого хранилища.

Secret Disk Server NG 3.2 не имеет встроенных средств шифрования. В Secret Disk Server NG 3.2 используются установленные в данной операционной системе поставщики криптографии.

Стандартный поставщик криптографии Secret Disk Server NG 3.2 использует:

- криптографический драйвер режима ядра, входящий в состав Microsoft Windows и реализующий алгоритм Triple DES — для шифрования дисков;

  Примечание: Secret Disk Server NG 3.2 поддерживает защищённые диски, созданные с помощью Secret Disk Server NG 3.0—3.1 с использованием алгоритма DES, однако при перешифровании таких дисков с помощью Secret Disk Server NG 3.2 применяются более стойкие алгоритмы.
- Microsoft Enhanced CSP — для генерирования и защиты мастер-ключей защищённых дисков, а также аутентификации.

Кроме того, Secret Disk Server NG 3.2 совместим с Signal-COM CSP и КриптоПро CSP. Использование этих поставщиков службы криптографии позволяет шифровать диски по алгоритму, соответствующему ГОСТ 28147-89 «Система обработки информации. Защита криптографическая», и защищать мастер-ключи защищённых дисков также с использованием сертифицированных российских криптографических средств.

Наконец, вы можете бесплатно загрузить с веб-сайта компании Aladdin пакет Secret Disk NG Crypto Pack, дополняющий стандартный поставщик криптографии Secret Disk Server NG 3.2 алгоритмами AES и Twofish.

© 2006, Aladdin

СЕРТИФИКАТЫ И КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ

В Secret Disk Server NG 3.2 сертификаты открытого ключа и соответствующие закрытые ключи применяются для:

- аутентификации администраторов;
- защиты мастер-ключей защищённых дисков.

В памяти eToken каждого из администраторов для каждого из используемых данным администратором поставщиков криптографии должен содержаться сертификат с соответствующим закрытым ключом.

Сертификат является идентификатором администратора. При регистрации администратора указывается сертификат для каждого из поставщиков криптографии, который администратор будет использовать. Secret Disk Server NG 3.2 сопоставляет администратору только по одному сертификату для каждого поставщика криптографии.

В Secret Disk Server NG 3.2 могут использоваться сертификаты, выданные центром сертификации вашего предприятия. В качестве альтернативы в Secret Disk Server NG 3.2 предусмотрено встроенное средство создания сертификатов.

Двухфакторная аутентификация

При обращении к инструментам управления Secret Disk Server NG 3.2 вы должны подключить к компьютеру свой eToken администратора, указать свой сертификат. Если вы используете несколько поставщиков криптографии, то в процессе аутентификации вы можете применять любой из сертификатов, связанных в системе Secret Disk Server NG 3.2 с вашей учётной записью.

Подключив eToken и указав сертификат, вы вводите PIN-код, подтверждая тем самым владение соответствующим закрытым ключом. Таким образом, аутентификация администратора в Secret Disk Server NG 3.2 основана на двух факторах:

- владение eToken администратора;
- знание PIN-кода.

Защита мастер-ключей защищённых дисков

В начале процесса зашифрования или перешифровани диска администратор Secret Disk Server NG должен выбрать алгоритм шифрования диска. При выборе алгоритма шифрования указывается поставщик криптографии, реализующий этот алгоритм.

После выбора алгоритма шифрования поставщик криптографии генерирует мастер-ключ защищённого диска. Для каждого администратора Secret Disk Server NG сгенерированный мастер-ключ защищённого 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 мастер-ключа защищённого диска.

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) используется для расшифрования находящейся в защищённом хранилище копии мастер-ключа защищённого диска, относящейся к данному администратору. Расшифрованный таким образом мастер-ключ защищённого диска загружается в драйвер Secret Disk Server NG 3.2 или передаётся под управление используемого поставщика службы криптографии (CSP). При чтении данных с защищённого диска происходит их расшифрование с помощью мастер-ключа защищённого диска, а при записи на диск — зашифрование с помощью того же ключа. Находящиеся на защищённом диске данные всегда зашифрованы.

© 2006, Aladdin

НОВОЕ В ВЕРСИИ

Версию 3.2 отличают от предшественников два новшества:

Новые модели eToken

Помимо моделей eToken, использовавшихся с предыдущими версиями, Secret Disk Server NG 3.2 поддерживает eToken NG-OTP и eToken PRO с операционной системой Siemens CardOS V4.20. Для функционирования этих моделей необходимо, чтобы на компьютере был установлен набор драйверов eToken Run Time Environment версии 3.60.116 или выше.

КриптоПро CSP 3.0

Secret Disk Server NG 3.2 поддерживает новую версию поставщика службы криптографии, выпускаемого компанией Крипто-Про — КриптоПро CSP 3.0. При этом сохраняется и поддержка предыдущей версии — КриптоПро CSP 2.0. Переход от использования КриптоПро CSP 2.0 к использованию КриптоПро CSP 3.0 не является обязательным.

При необходимости обновление версии КриптоПро CSP можно осуществлять как до, так и после установки Secret Disk Server NG 3.2. При этом никаких действий, относящихся непосредственно к Secret Disk Server NG 3.2, выполнять не нужно. Для того чтобы использовать при работе с КриптоПро CSP 3.0 ключевые контейнеры, созданные в памяти eToken с помощью КриптоПро CSP 2.0, руководствуйтесь инструкциями, приведёнными в документации «модуля поддержки USB-ключей / смарт-карт eToken для СКЗИ „КриптоПро CSP" версии 3.0».

© 2006, Aladdin

ВНЕДРЕНИЕ SECRET DISK SERVER NG 3.2: ОСНОВНЫЕ ШАГИ

ВНИМАНИЕ! Во избежание ошибок, ведущих к потере данных, перед внедрением Secret Disk Server NG 3.2 на основных серверах вашей организации рекомендуется осуществить аналогичные действия на тестовых компьютерах.

Как правило, для внедрения Secret Disk Server NG 3.2 вам необходимо выполнить следующее.

1. На сервере и на рабочей станции администратора установите eToken Run Time Environment. Подробнее об этом см. в брошюре «Электронные ключи и смарт-карты eToken. Руководство администратора».
2. Установите программное обеспечение сервера и рабочей станции администратора.
3. Подключите к серверу eToken сервера.
4. Зарегистрируйте одного или нескольких администраторов Secret Disk Server NG и выберите для них сертификаты.

   При регистрации первого администратора подключите его eToken к рабочей станции администратора. Подробнее о регистрации администраторов см. в разделе «Добавление администраторов».

   При выборе готовых сертификатов удостоверьтесь в том, что у вас есть резервные копии сертификатов и закрытых ключей. Если у вас нет готовых сертификатов, создайте сертификаты в памяти eToken администраторов средствами Secret Disk Server NG 3.2, при создании сохраняя резервные копии. Подробнее о выборе и создании сертификатов см. в разделе «Сертификаты».
5. При желании загрузите с веб-сайта компании Aladdin бесплатный пакет Secret Disk NG Crypto Pack, дополняющий стандартный поставщик криптографии Secret Disk Server NG 3.2 алгоритмами AES и Twofish, и установите его.
6. Зашифруйте диски.
7. Сохраните резервные копии мастер-ключей защищённых дисков.
8. Сделайте резервную копию защищённого хранилища.
9. Храните все резервные копии в надёжных местах.
10. Осуществите настройки сигнала «тревога» для сервера и для каждого из защищённых дисков.
11. Установите и настройте Secret Disk NG Alarm.
12. Подключите защищённые диски.

© 2006, Aladdin

СХЕМА ЛИЦЕНЗИРОВАНИЯ

В Secret Disk Server NG 3.2 три объекта лицензирования:

- количество администраторов Secret Disk Server NG;
- количество клиентских подключений к данному серверу;
- возможность запрещать сетевой доступ к защищённому диску

Инструментом, обеспечивающим функционирование системы Secret Disk Server NG 3.2 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*;
- 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.

Примечание: лицензия файл-сервера ограничивает общее количество одновременных подключений ко всем защищённым дискам данного сервера.

Один и тот же eToken с лицензией администратора можно использовать при администрировании разных серверов.

Субъектам, осуществляющим клиентские подключения к серверу, лицензий не требуется.

СОСТАВ И АППАРАТНАЯ КОНФИГУРАЦИЯ

Программные компоненты

Secret Disk Server NG 3.2 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 3.2, 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 3.2 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 3.2, убедитесь:

- в том, что данный компьютер удовлетворяет требованиям к программному обеспечению каждого из компонентов;
- в том, что 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.

eToken

eToken администратора применяется на рабочей станции администратора. В его памяти содержится лицензия администратора.

Для каждого из используемых поставщиков криптографии в памяти eToken администратора должен присутствовать соответствующий сертификат с закрытым ключом.

В качестве *eToken администратора* может выступать:

- USB-ключ eToken NG-OTP;
- USB-ключ или смарт-карта eToken PRO;
- USB-ключ eToken R2.

 © 2006, Aladdin

eToken сервера должен быть всегда подключен к серверу. *eToken сервера* содержит лицензию файл-сервера, содержащая информацию о максимальном количестве сетевых подключений, или/и лицензию сервера приложений, позволяющую запрещать сетевой доступ к защищённым дискам.

В качестве *eToken сервера* может использоваться eToken PRO или eToken NG-OTP.

Если один и тот же компьютер является как сервером, так и рабочей станцией администратора, то возможно использование одного eToken, совмещающего функции *eToken администратора* и *eToken сервера* при наличии необходимых лицензий.

В стандартном комплекте поставки Secret Disk Server NG 3.2 eToken администратора носит имя `Administrator`, а eToken сервера — `Server`. При желании вы можете переименовать любой из них. О переименовании eToken см. в документе *eToken. Руководство администратора*, (файл `eToken_Admin_Guide.pdf` в папке `Doc` компакт-диска Secret Disk Server NG 3.2).

«Красная кнопка»

«Красная кнопка» — устройство, подключаемое к порту COM рабочей станции для подачи сигнала «тревога». Нажатие на кнопку приводит к запуску на сервере команд, предназначенных для предотвращения несанкционированного доступа к информации в чрезвычайных ситуациях. «Красная кнопка» является аппаратным компонентом Secret Disk NG Alarm. Более подробная информация о ней изложена в документации этого комплекса.

СОВМЕСТИМОСТЬ С ДРУГИМИ ПРОГРАММАМИ

Secret Disk Server NG 3.2 может успешно использоваться совместно со многими программами при условии выполнения системных требований каждой из них. Вместе с тем, при использовании Secret Disk Server NG 3.2 необходимо учитывать особенности этой системы:

1. *При подключенных защищённых дисках не рекомендуется* запускать на сервере процессы установки и удаления программ, реализующих функции подключения дисков, аналогичные подключению защищённых дисков. К этой категории относятся, в частности, программы, способные подключать файлы-образы компакт-дисков. Прежде чем устанавливать или удалять такие программы, отключите все защищённые диски.
2. Использование компонентов Secret Disk Server NG 3.x и Secret Disk NG 3.x на одном компьютере невозможно.

© 2006, Aladdin

ОБНОВЛЕНИЕ ВЕРСИИ SECRET DISK SERVER

Переход с Secret Disk Server 1.x

Система Secret Disk Server NG 3.2 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 3.2. При такой схеме система Secret Disk Server 1.x работает только со своими секретными дисками, а система Secret Disk Server NG 3.2 — только со своими защищёнными дисками.

Для того чтобы Secret Disk NG Alarm мог работать с «красной кнопкой», использовавшейся с Secret Disk Server 1.x, необходимо изменить схему подключения кнопки к разъёму порта RS-232. Подробнее см. в документации Secret Disk NG Alarm.

Если вы используете Secret Disk Server 1.x с операционной системой Microsoft Windows 2000 или XP, для корректного перехода к Secret Disk Server NG 3.2 выполните следующие действия.

1. Установите Secret Disk Server NG 3.2 и зарегистрируйте администратора Secret Disk Server NG на данном сервере, выбрав сертификат(ы) для защиты мастер-ключей защищённых дисков и аутентификации.
2. Зашифруйте с помощью Secret Disk Server NG 3.2 один или несколько дисков достаточной ёмкости.
3. Скопируйте все данные с секретных дисков Secret Disk 1.x на созданные с помощью Secret Disk Server NG 3.2 защищённые диски.
4. Расшифруйте все секретные диски Secret Disk Server 1.x.
5. Удалите Secret Disk Server 1.x.

Если вы используете Secret Disk Server 1.x с операционной системой Windows NT 4.0, для корректного перехода к Secret Disk Server NG 3.2 выполните следующие действия.

1. Перенесите все данные с секретных дисков на обычные диски.
2. Расшифруйте все секретные диски.
3. Удалите систему Secret Disk Server 1.x.
4. Установите на компьютер операционную систему Windows 2000, Windows Server 2003 или Windows XP.
5. Для Windows 2000 установите пакет обновления (Service Pack) 2 или выше, или убедитесь в том, что он включён в уже осуществлённую вами установку. Для Windows XP установите пакет обновления (Service Pack) 1 или убедитесь в том, что он включён в уже осуществлённую вами установку.
6. Установите Secret Disk Server NG 3.2 и зарегистрируйте администратора Secret Disk Server NG на данном сервере, выбрав сертификат(ы) для защиты мастер-ключей защищённых дисков и аутентификации.
7. Зашифруйте один или несколько дисков подходящей ёмкости.
8. Перенесите все конфиденциальные данные с обычных дисков на защищённые.

Переход с Secret Disk Server NG 3.0 или 3.0.1

Для перехода от Secret Disk Server NG 3.0 или 3.0.1 к Secret Disk Server NG 3.2 вам не нужно приобретать какие-либо лицензии. Достаточно лишь иметь программу установки сервера и интерфейса администратора Secret Disk Server NG.

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

1. Удалите Secret Disk Server NG 3.0 (3.0.1), сохранив защищённое хранилище.
2. Установите Secret Disk Server NG 3.2.

Переход с Secret Disk Server NG 3.0.2 или 3.1.x

Для перехода от Secret Disk Server NG 3.0.2 или 3.1.x к Secret Disk Server NG 3.2 вам не нужно ни приобретать какие-либо лицензии, ни удалять установленную версию Secret Disk Server. Достаточно лишь иметь программу установки сервера и интерфейса администратора Secret Disk Server NG.

Для того чтобы обновить версию Secret Disk Server NG:

1. В меню компакт-диска Secret Disk Server NG 3.2 нажмите **Установить Secret Disk Server NG**.
2. В диалоговом окне с сообщением о том, что произойдёт обновление установленной версии Secret Disk Server NG, нажмите **Да**/**Yes**.
3. В диалоговом окне с сообщением о продолжении установки Secret Disk Server NG 3.2 что нажмите **Далее**. Установка займёт некоторое время.
4. Убедитесь в том, что процесс установки завершён успешно, и нажмите **Готово**.
5. По завершении 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 Secret Disk Server NG 3.2 будет считаться успешно состоявшейся.

Переход от демонстрационной версии к полнофункциональной

Для перехода от демонстрационной версии Secret Disk Server NG 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 полнофункциональной, выполните следующее.

1. Расшифруйте все защищённые диски.
2. Удалите демонстрационную версию Secret Disk Server NG, включая защищённое хранилище.
3. Установите полнофункциональную версию Secret Disk Server NG 3.2 и зарегистрируйте администратора Secret Disk Server NG на данном сервере,

 © 2006, Aladdin

выбрав сертификат(ы) для защиты мастер-ключей защищённых дисков и аутентификации.

4. Зашифруйте диски, содержащие конфиденциальные данные.

СЕРВЕР И ИНТЕРФЕЙС АДМИНИСТРАТОРА

Системные 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.

Кроме того, на сервере должен быть установлен набор драйверов eToken Run Time Environment (eToken RTE) версии 3.00.116, 3.51.19, 3.60.116 (рекомендуемая версия) или 3.65.26.

Примечания:
1. Для управления сервером через удалённый рабочий стол необходима версия 3.51.19 или выше.
2. Версии ниже 3.60.116 не поддерживают eToken NG-OTP и некоторые модели eToken PRO.

При необходимости использования сертифицированных российских средств криптографической защиты на сервере следует применять Signal-COM CSP или/и КриптоПро CSP версии 2.0 или 3.0.

Если в качестве eToken сервера используется смарт-карта eToken PRO, то на сервере должен быть установлен драйвер соответствующего устройства чтения смарт-карт.

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.

 © 2006, Aladdin

Кроме того, в зависимости от вида eToken сервера, сервер должен иметь:
- для USB-ключа eToken — свободный порт USB;
- для смарт-карты eToken PRO — устройство чтения смарт-карт, поддерживающее смарт-карты eToken PRO, (например, ASEDrive III).

Объём свободного места на жёстком диске для установки сервера: 7 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 Server 2003 или Windows XP Professional.

Кроме того, на рабочей станции администратора должен быть установлен набор драйверов eToken Run Time Environment (eToken RTE) версии 3.00.116, 3.51.19, 3.60.116 (рекомендуемая версия) или 3.65.26.

Примечания:
1. Для управления сервером через удалённый рабочий стол необходима версия 3.51.19 или выше.
2. Версии ниже 3.60.116 не поддерживают eToken NG-OTP и некоторые модели eToken PRO.

При необходимости использования сертифицированных российских средств криптографической защиты на рабочей станции администратора следует применять те же поставщики службы криптографии, что и на сервере — Signal-COM CSP или/и КриптоПро CSP версии 2.0 или 3.0.

Для хранения ключевых контейнеров Signal-COM CSP в памяти eToken на рабочей станции администратора должен быть установлен модуль eToken для Signal-COM CSP.

Если вы используете КриптоПро CSP 2.0, на рабочей станции администратора должен быть установлен eToken для КриптоПро CSP 2.0 версии 2.1.

При использовании КриптоПро CSP 3.0 убедитесь в том, что в число настроенных ключевых носителей входит ваша модель eToken.

Если в качестве eToken администратора используется смарт-карта eToken PRO, то на рабочей станции администратора должен быть установлен драйвер соответствующего устройства чтения смарт-карт.

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:

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

Объём свободного места на жёстком диске для установки интерфейса администратора: 8 МБ.

Установка и удаление

Необходимые полномочия

Для установки и удаления программного обеспечения необходимы полномочия локального администратора.

Меню компакт-диска

После того как вы вставите компакт-диск Secret Disk Server NG 3.2 в устройство чтения компакт-дисков, на экране появится окно меню компакт-диска. Если это окно не появилось, выполните следующее.

1. Из меню **Пуск**/**Start** выберите **Выполнить**/**Run**.
2. Введите путь к файлу `startcd.exe`, расположенному в корневой папке компакт-диска. Если, например, `d` — буква диска, соответствующая устройству для чтения компакт-дисков, введите:

   `d:\startcd.exe`.
3. Нажмите **OK**. На экране появится окно меню компакт-диска.

- Для запуска программы установки eToken Run Time Environment 3.60 нажмите **Установить eToken RTE**.
- Для запуска программы установки сервера и интерфейса администратора нажмите **Установить Secret Disk Server NG**.
- Для запуска программы установки Secret Disk NG Alarm нажмите **Установить утилиту подачи сигнала «тревога»**.
- Для того чтобы просмотреть документацию Secret Disk Server NG 3.2 и рекламно-информационные материалы по другим продуктам компании Aladdin, нажмите **Документация**.
- Если вы хотите открыть в окне браузера домашнюю страницу веб-сайта компании Aladdin, нажмите **Веб-сайт компании ALADDIN**.
- Для выхода из меню компакт-диска нажмите **Выход**.

 © 2006, Aladdin

Установка

Для того чтобы установить сервер и/или интерфейс администратора Secret Disk Server NG 3.2, выполните следующую последовательность действий.

1. Убедитесь в том, что компьютер удовлетворяет системным требованиям.
2. В меню компакт-диска Secret Disk Server NG 3.2 нажмите **Установить Secret Disk Server NG**.
3. В окне приветствия программы установки нажмите **Далее**.
4. 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 не будут установлены.
5. Для того чтобы компоненты Secret Disk Server NG 3.2 были установлены в папку по умолчанию, нажмите **Далее**.

   Если вы хотите, чтобы компоненты Secret Disk Server NG 3.2 были установлены в другую папку, нажмите **Изменить**, выберите папку, нажмите **OK** и нажмите **Далее**.
6. Выберите компонент(ы) Secret Disk Server NG 3.2, которые вы хотите установить на данном компьютере, и нажмите **Далее**.
7. Для начала процесса установки нажмите **Установить**.
8. Процесс установки займёт некоторое время.
9. Убедитесь в том, что процесс установки завершён успешно, и нажмите **Готово**.
10. По завершении 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 Secret Disk Server NG 3.2 будет считаться успешно состоявшейся.

Отказ от установки

Отказаться от установки сервера и/или интерфейса администратора можно в любом диалоговом окне программы установки, кроме последнего. Для этого:

- нажмите **Отмена**;
- в окне подтверждения нажмите **Да**;
- нажмите **Готово**.

Удаление

Для того чтобы удалить сервер и/или интерфейс администратора Secret Disk Server NG из операционной системы, выполните следующее.

1. Щёлкните **Пуск**/**Start** > **Все Программы** / **Программы** > **Secret Disk NG** > **Server** > **Удаление**.
2. В окне подтверждения нажмите **Да**/**Yes**.
3. При необходимости закройте требуемые окна и нажмите **Повторить**.

4. При удалении сервера на экране появится окно **Удаление защищённого хранилища**.

   Если вы не хотите удалять защищённое хранилище, нажмите **Нет**. Если вы хотите удалить защищённое хранилище:
   - убедитесь в том, что вы располагаете резервными копиями мастер-ключей всех остающихся защищённых дисков или всего защищённого хранилища;
   - нажмите **Да**.

5. Нажмите **Да**/**Yes**, чтобы перезагрузить компьютер или **Нет**/**No**, чтобы отложить перезагрузку.

Интерфейс администратора

Основным интерфейсом администратора Secret Disk Server NG является **Управление Secret Disk Server**. Это оснастка, встроенная в консоль управления компьютером. Её также можно использовать в любых других инструментах, созданных на основе консоли управления Microsoft, в том числе для удалённого управления защищёнными дисками.

Все действия, имеющие отношение к доступу к конфиденциальной информации, администратор может осуществлять только при условии, что он при обращении к оснастке **Управление Secret Disk Server**:

- подключил eToken администратора;
- верно указал сертификат для защиты мастер-ключей и аутентификации, хранящийся в памяти eToken;
- подтвердил свою подлинность, введя PIN-код.

Только после успешного выполнения этих действий открывается сеанс управления, при котором можно работать с оснасткой **Управление Secret Disk Server**.

Советы:

Для того чтобы исключить возможность несанкционированного использования полномочий администратора Secret Disk Server NG:

- не открывайте сеанс управления без необходимости;
- не оставляйте сеанс управления открытым, отходя от компьютера;
- выполнив необходимые административные действия, незамедлительно закрывайте сеанс управления.

Открытие сеанса управления

Для того чтобы обратиться к интерфейсу администратора в консоли управления компьютером и открыть сеанс управления:
щёлкните **Пуск**/**Start** > **Все Программы** / **Программы** > **Secret Disk NG** > **Server** > **Управление компьютером**;

- если сервер установлен на удалённом компьютере:
- в дереве консоли щёлкните правой кнопкой мыши **Управление компьютером (локальным)**/**Computer Management (Local)** и выберите **Подключиться к другому компьютеру**/**Connect to another computer**;

© 2006, Aladdin

- в окне **Выбор компьютера**/**Select Computer** введите IP-адрес или имя удалённого компьютера вручную или воспользуйтесь стандартным диалогом выбора объекта, нажав **Обзор**/**Browse**;
- нажмите **OK**.
- подключите eToken администратора;

  Примечания:

  1. В памяти подключенного eToken должен находиться сертификат с закрытым ключом, принадлежащий одному из зарегистрированных на данном сервере администраторов. Этот сертификат должен быть выбран данным администратором для одного из поставщиков криптографии.
  2. В случае если не зарегистрировано ни одного администратора Secret Disk Server NG, то при обращении к оснастке **Управление Secret Disk Server** необходимо пройти процедуру добавления администратора.

- в дереве консоли в узле **Запоминающие устройства** / **Storage** щёлкните **Управление Secret Disk Server**;
- в окне **Secret Disk Server NG: идентификация** укажите один из сертификатов, используемых вами для аутентификации в системе Secret Disk Server NG 3.2 и защиты мастер-ключей защищённых дисков;

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

- нажмите **OK**;
- при необходимости выберите считыватель (eToken) и введите PIN-код (интерфейс зависит от поставщика криптографии).

Список зарегистрированных администраторов

Для того чтобы открыть список администраторов Secret Disk Server NG, зарегистрированных на данном сервере, в дереве консоли щёлкните **Администраторы**.

Имя администратора отображается в ячейке **Имя**. В этой же ячейке располагается значок администратора. Значок может принимать один из двух видов:

- — зарегистрированный на данном компьютере администратор Secret Disk Server NG, открывший текущий сеанс управления;
- — зарегистрированный на данном компьютере администратор Secret Disk Server NG, не открывавший текущий сеанс управления.

Добавление администратора

Только администраторы Secret Disk Server NG, зарегистрированные на данном сервере, могут обращаться к защищённым дискам. Для того чтобы добавить администратора в список зарегистрированных администраторов, щёлкните правой кнопкой мыши по узлу **Администраторы** дерева консоли или по свободному месту в правой панели и выберите **Добавить администратора**.

Редактирование регистрационной информации

Вы можете изменить информацию об администраторе в окне свойств администратора. Кроме того, для администратора, открывшего сеанс управления, вы можете также изменять набор используемых сертификатов. Для того чтобы открыть окно свойств администратора, выделите строку и выполните одно из действий:

- нажмите клавишу ENTER;
- на панели инструментов консоли нажмите кнопку **Отобразить окно свойств** / **Properties** ();
- дважды щёлкните по выделенной строке;
- в меню **Действие**/**Action** выберите **Свойства**/**Properties**;
- щёлкните правой кнопкой мыши и выберите **Свойства**/**Properties**.

Удаление администратора из списка

Для того чтобы удалить администратора из списка, выделите соответствующую строку. Далее выполните любое из следующих действий:

- нажмите клавишу DELETE;
- на панели инструментов консоли нажмите кнопку **Удалить**/**Delete** ();
- щёлкните правой кнопкой мыши и выберите **Удалить**/**Delete**;
- в меню **Действие**/**Action** выберите пункт **Удалить**/**Delete**.

Список дисков

Для того чтобы открыть список защищённых и незашифрованных дисков, в дереве консоли щёлкните **Диски**.

Метка тома и буква диска отображаются в ячейке **Том**. Значок, отражающий состояние диска, также располагается в этой ячейке. Значок диска в списке может принимать один из семи видов:

— незашифрованный том на жёстком диске или том на жёстком диске, находящийся в процессе зашифрования/расшифрования;

— отключенный защищённый том на жёстком диске;

— подключенный защищённый том на жёстком диске;

— диск, процесс зашифрования, перешифрования или расшифрования которого приостановлен;

— незашифрованный съёмный диск или съёмный диск, находящийся в процессе зашифрования/расшифрования;

— отключенный защищённый съёмный диск;

— подключенный защищённый съёмный диск.

© 2006, Aladdin

В ячейке **Статус** отображается состояние диска:

- `Зашифрован` — защищённый диск;
- `Перешифрование` (с указанием процентов готовности) — диск находится в процессе перешифрования;
- `Перешифрование приостановлено` — для возобновления работы с файлами и папками на диске необходимо завершить процесс его перешифрования;
- `Расшифрование` (с указанием процентов готовности) — защищённый том находится в процессе расшифрования;
- `Расшифрование приостановлено` — для возобновления работы с файлами и папками на диске необходимо завершить процесс его расшифрования;
- `Системный` — диск является системным и зашифрован быть не может;
- `Шифрование` (с указанием процентов готовности) — диск находится в процессе зашифрования;
- `Шифрование приостановлено` — для возобновления работы с файлами и папками на диске необходимо завершить процесс его зашифрования.

В строке незашифрованного диска, не являющегося системным, ячейка **Статус** пуста.

В ячейках **Файловая система** и **Размер** указываются, соответственно, файловая система и ёмкость диска.

Зашифрование диска

Диск, не являющийся системным или защищённым, можно зашифровать. Для этого:

- выберите диск из списка;
- щёлкните правой кнопкой мыши и выберите **Зашифровать**, нажмите кнопку **Зашифровать диск** () на панели инструментов консоли или выберите пункт **Зашифровать** в меню **Действие**/**Action** консоли.

Резервное копирование мастер-ключа защищённого тома

Для того чтобы предотвратить потерю данных на защищённых томах в случае повреждения или уничтожения защищённого хранилища или потери eToken администратора, следует создавать резервные копии мастер-ключей. Для создания резервной копии выберите защищённый том, щёлкните правой кнопкой мыши и выберите **Сохранить мастер-ключ** или выберите пункт **Сохранить мастер-ключ** из меню **Действие**/**Action** консоли.

Подключение защищённого диска

Для того чтобы подключить защищённый диск, выполните одно из действий:

- щёлкните правой кнопкой мыши и выберите **Подключить**;
- в меню **Действие**/**Action** выберите **Подключить**.

© 2006, Aladdin

Отключение защищённого диска

Для того чтобы отключить защищённый диск, выполните одно из действий:

- щёлкните правой кнопкой мыши и выберите **Отключить**;
- в меню **Действие**/**Action** выберите **Отключить**.

Восстановление доступа к защищённому диску

Если у вас нет доступа к защищённому тому, присутствующему на данном сервере, вы располагаете файлом резервной копии мастер-ключа и знаете пароль этого файла, то вы можете восстановить доступ к защищённому диску. Для того чтобы осуществить эту операцию, не выделяйте ни одного диска в списке дисков. Вместо этого выполните одно из действий:

- щёлкните правой кнопкой мыши по значку **Диски** в дереве консоли и выберите **Восстановить доступ к защищённому тому**;
- щёлкните правой кнопкой мыши по свободному месту в списке дисков и выберите **Восстановить доступ к защищённому тому**;
- в меню **Действие**/**Action** консоли выберите пункт **Восстановить доступ к защищённому тому**;

Перешифрование защищённого диска

Любой защищённый диск, присутствующий в списке дисков, можно перешифровать. Для этого:

- выберите защищённый диск из списка;
- щёлкните правой кнопкой мыши и выберите **Перешифровать** или выберите пункт **Перешифровать** из меню **Действие**/**Action** консоли.

Расшифрование защищённого диска

Для того чтобы расшифровать защищённый том:

- выберите защищённый том в списке;
- щёлкните правой кнопкой мыши и выберите **Расшифровать**, нажмите кнопку **Расшифровать диск** () на панели инструментов консоли или выберите пункт **Расшифровать** в меню **Действие**/**Action** консоли.

Свойства защищённого диска

Для того чтобы открыть окно свойств защищённого диска, выполните одно из действий:

- нажмите клавишу ENTER;
- дважды щёлкните;
- на панели инструментов консоли нажмите кнопку **Отобразить окно свойств** / **Properties** ();
- в меню **Действие**/**Action** выберите **Свойства**/**Properties**;
- щёлкните правой кнопкой мыши и выберите **Свойства**/**Properties**.

© 2006, Aladdin

Закрытие сеанса управления

Закрыть сеанс управления можно двумя способами:

Способ 1. Закройте консоль, в которой сеанс управления был открыт, или подключите её к другому компьютеру.

Способ 2. Выполните следующее:

1. Отключите eToken администратора.
2. В дереве консоли выделите **Управление Secret Disk Server**.
3. Выполните одно из действий:
   - нажмите клавишу F5;
   - нажмите кнопку **Обновление**/**Refresh** ();
   - в меню **Действие**/**Action** выберите **Обновить**/**Refresh**;
   - щёлкните правой кнопкой мыши и выберите **Обновить**/**Refresh**.

Окно свойств сервера

Окно свойств сервера содержит информацию об установленной на сервере версии компонента «сервер», а также о серверных лицензиях, расположенных в подключенном к серверу eToken. Кроме того, при открытом сеансе управления и наличии лицензии файл-сервера в этом окне отображается также текущее общее количество сетевых подключений ко всем защищённым дискам.

Для того чтобы открыть окно свойств сервера, в дереве коносоли выберите **Управление Secret Disk Server** и выполните любое из действий:

- на панели инструментов консоли нажмите кнопку **Отобразить окно свойств** / **Properties** ();
- в меню **Действие**/**Action** выберите **Свойства**/**Properties**;
- щёлкните правой кнопкой мыши и выберите **Свойства**/**Properties**.

Зарегистрированные администраторы

Управление защищёнными дисками осуществляют администраторы Secret Disk Server NG, зарегистрированные на данном сервере. Количество администраторов не ограничено.

У каждого администратора Secret Disk Server NG должен быть свой eToken. В памяти этого eToken должны содержаться:

- лицензия администратора;
- сертификат открытого ключа и соответствующий закрытый ключ.

Лицензия администратора позволяет использовать данный eToken в качестве eToken администратора Secret Disk Server NG. eToken без лицензии администратора нельзя использовать в качестве eToken администратора.

Сертификат открытого ключа и соответствующий закрытый ключ служат для:

- аутентификации администратора;
- защиты мастер-ключей защищённых дисков.

© 2006, Aladdin

Если при шифровании дисков вы используете или планируете использовать не один, а несколько поставщиков криптографии, то и сертификатов у администратора должно быть несколько — по одному для каждого поставщика криптографии. При аутентификации в системе Secret Disk Server NG 3.2 можно применять любой из этих сертификатов.

Сертификат является идентификатором администратора Secret Disk Server NG. Сертификаты зарегистрированных на данном сервере администраторов хранятся в защищённом хранилище. Именно по сертификатам сервер отличает одного администратора от другого.

Когда администратор Secret Disk Server NG обращается к серверу, он указывает свой сертификат, находящийся в памяти eToken, а затем вводит PIN-код, подтвержая тем самым владение закрытым ключом, соответствующим указанному сертификату и хранящимся в защищённой области памяти eToken. По сертификату сервер идентифицирует администратора, а на основании закрытого ключа администратор подтверждает свою подлинность.

Добавление администраторов

При добавлении администратора вы вводите имя и комментарий, а также указываете сертификат нового администратора. Если используются несколько поставщиков криптографии, то выбираются несколько сертификатов. Каждый из указанных сертификатов помещается в защищённое хранилище вместе с именем и комментарием.

Регистрация первого администратора

Добавление первого администратора имеет две особенности:

1. Его eToken обязательно должен быть подключен к рабочей стации администратора.
2. Необходимы полномочия локального администратора на сервере.

Если на данном сервере не зарегистрировано ни одного администратора Secret Disk Server NG, то при обращении к оснастке **Управление Secret Disk Server** на экране появляется окно **Secret Disk Server NG: новый администратор**.

Добавление дополнительного администратора

Если один зарегистрированный администратор регистрирует другого, предъявлять eToken добавляемого администратора необязательно. Достаточно лишь выбрать сертификаты без закрытых ключей, которые добавляемый администратор будет использовать. Указываемые сертификаты должны находиться в хранилище **Личные**/**Personal**. Новый администратор сможет получать доступ к системе только при условии, что у него есть eToken с лицензией администратора, в памяти которого хранятся указанные при добавлении администратора сертификаты вместе с соответствующими закрытыми ключами.

Если у добавляемого администратора нет сертификата, Secret Disk Server NG 3.2 может сгенерировать для него сертификат с закрытым ключом. В этом случае eToken добавляемого администратора обязательно должен быть подключен к рабочей станции администратора.

 © 2006, Aladdin

Примечания:

1. При создании сертификата вам потребуется вводить PIN-код. Убедитесь в том, что вы знаете PIN-код eToken добавляемого администратора.
2. Для того чтобы отличать один eToken от другого, назначайте им разные имена. О переименовании eToken см. в документе *eToken. Руководство администратора*, (файл `eToken_Admin_Guide.pdf` в папке `Doc` компакт-диска Secret Disk Server NG 3.2).

Если при добавлении дополнительного администратора в системе имеются защищённые диски, то сервер попытается поместить в защищённое хранилище копии мастер-ключей для нового администратора. Для выполнения этой операции ваш eToken (т.е. eToken добавляющего администратора) должен быть подключен к компьютеру, и может потребоваться ввод PIN-кода один или несколько раз. После успешного добавления новый администратор будет иметь доступ к тем же защищённым дискам, что и вы, при условии, что вы выберете для него все необходимые сертификаты. К дискам, к которым у вас нет доступа, новый администратор также не будет иметь доступа.

Если вы являетесь зарегистрированным администратором Secret Disk Server NG и хотите зарегистрировать ещё одного администратора, то для открытия окна **Secret Disk Server NG: новый администратор** выполните следующее:

1. В дереве консоли выберите **Администраторы**.
2. Выполните любое из действий:

• щёлкните правой кнопкой мыши по узлу **Администраторы** или по свободному месту в списке администраторов Secret Disk Server NG и выберите **Добавить администратора**;
• в меню **Действие**/**Action** выберите **Добавить администратора**.

Последовательность действий

Для того чтобы зарегистрировать администратора, выполните следующее.

1. В окне **Secret Disk Server NG: новый администратор** внесите информацию об администраторе Secret Disk Server NG в графы **Имя** и **Комментарий**.
2. Убедитесь в том, что ваш eToken (eToken добавляющего администратора) подключен к компьютеру.

   Примечания:

   - eToken каждого из администраторов должен содержать лицензию администратора.
   - При регистрации первого администратора вы в одном лице являетесь и добавляющим, и добавляемым администратором.

   Если вы регистрируете дополнительного администратора, убедитесь в том, что у вас есть или сертификаты, которые добавляемый администратор будет использовать, или eToken добавляемого администратора.
3. Выберите для добавляемого администратора Secret Disk Server NG сертификат(ы) для защиты мастер-ключей защищённых дисков и аутентификации. Если подходящего сертификата нет, сгенерируйте сертификат с закрытым ключом.
4. Нажмите **Добавить**.

5. При необходимости введите PIN-код своего eToken (eToken добавляющего администратора) один или несколько раз.
6. 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.`

7. Нажмите **OK**.

Редактирование регистрационной информации

Любой администратор Secret Disk Server NG, зарегистрированный на данном компьютере, может вносить изменения в регистрационную информацию о себе и о других администраторах.

Для того чтобы отредактировать регистрационную информацию, выполните следующую последовательность действий.

1. Откройте Список зарегистрированных администраторов.
2. Выберите администратора, нажмите правую кнопку мыши и выберите пункт **Свойства**/**Properties**.
3. Убедитесь в том, что в появившемся окне открыта вкладка **Общие**.
4. Внесите необходимые изменения и нажмите **OK**.

Удаление администратора из списка

Любой администратор Secret Disk Server NG, зарегистрированный на данном компьютере, может удалить регистрационную информацию о других администраторах.

Для того чтобы удалить администратора из списка, выполните следующее.

1. Откройте Список зарегистрированных администраторов.
2. Выберите администратора Secret Disk Server NG, которого вы хотите удалить из списка, щёлкните правой кнопкой мыши и выберите **Удалить**/**Delete**.
3. В окне подтверждения нажмите **Да**/**Yes**.

Сертификаты

При обращении к интерфейсу администратора у вас должен быть выбран хотя бы один сертификат, чтобы использовать связанные с ним криптографические ключи для аутентификации и защиты мастер-ключей защищённых дисков. Сертификат и соответствующие криптографические ключи должны храниться в памяти eToken администратора.

Вы должны выбрать сертификат для каждого из используемых поставщиков криптографии в любом из случаев:

- если сертификат для данного поставщика криптографии ещё не указан;
- если текущий сертификат недействителен.

Если вы не располагаете сертификатом, вы можете воспользоваться встроенным средством создания сертификатов Secret Disk Server NG 3.2.

 © 2006, Aladdin

Требования к сертификатам

Для защиты мастер-ключей дисков, зашифрованных с помощью стандартного поставщика криптографии Secret Disk Server NG 3.2, может использоваться любой сертификат со следующими параметрами:

- открытый ключ: RSA;
- использование ключа: шифрование ключей.

Для защиты мастер-ключей дисков, зашифрованных с помощью алгоритма ГОСТ 28147-89 (поставщик — Signal-COM CSP или КриптоПро CSP), может использоваться любой сертификат, созданный с помощью соответствующего поставщика службы криптографии со следующими параметрами:

- открытый ключ: ГОСТ Р 34.10-94 (1024 бит) или ГОСТ Р 34.10-2001 (512 бит);
- использование ключа: шифрование ключей.

Кроме того, на сервере и на рабочей станции должно быть настроено доверие центрам сертификации, присутствующим в пути сертификации данного сертификата. Сертификаты этих центров сертификации должны размещаться в соответствующих хранилищах:

- на сервере:
  - сертификат корневого центра сертификации — в хранилище **Доверенные корневые центры сертификации** / **Trusted Root Certification Authorities** локального компьютера;
  - сертификаты всех промежуточных центров сертификации — в хранилище **Промежуточные центры сертификации** / **Intermediate Certification Authorities** локального компьютера;
- на рабочей станции администратора:
  - сертификат корневого центра сертификации — в хранилище **Доверенные корневые центры сертификации** / **Trusted Root Certification Authorities** текущего пользователя;
  - сертификаты всех промежуточных центров сертификации — в хранилище **Промежуточные центры сертификации** / **Intermediate Certification Authorities** текущего пользователя.

Ни один из сертификатов не должен быть отозван или недействителен.

При использовании сертификатов, созданных с помощью Secret Disk Server NG 3.0.x, все требования, кроме последнего, выполняются автоматически.

Выбор сертификата

Первичный выбор сертификата осуществляется при регистрации нового администратора на данном сервере. Для этого в окне **Secret Disk Server NG: новый администратор** присутствует список **Сертификаты данного администратора** с кнопками **Просмотр** и **Выбрать**.

Для уже зарегистрированного администратора, открывшего сеанс управления:

- в списке зарегистрированных администраторов дважды щёлкните по значку , чтобы открыть окно свойств администратора;
- в окне свойств администратора откройте вкладку **Сертификаты**.

Для того чтобы выбрать сертификат, выполните следующие действия:

1. Выберите поставщик криптографии, который будет использоваться данным администратором.

   Примечание: В поле **Поставщик криптографии** отображается компонент поставщика криптографии, отвечающий за аутентификацию, генерацию и защиту мастер-ключей защищённых дисков.

2. Если вы выбираете сертификат для себя, убедитесь в том, что eToken администратора подключен к компьютеру.

   Примечание: Если вы являетесь зарегистрированным администратором и выбираете сертификат при регистрации другого администратора, то вы необязательно должны иметь eToken, принадлежащий новому администратору, и знать PIN-код. Достаточно того, чтобы копия сертификата размещалась на рабочей станции администратора в хранилище **Личные**/**Personal**.

3. Нажмите **Выбрать**.

4. В окне **Secret Disk Server NG: выбор сертификата** выберите сертификат.

   Примечания:

   - Если вы выбираете сертификат для себя, то сертификат и связанный с ним закрытый ключ должны храниться в памяти eToken администратора.
   - Сертификат, созданный с помощью КриптоПро CSP на другом компьютере, присутствует в списке только в случае, если он установлен на данном компьютере (его копия хранится в реестре операционной системы).
   - При необходимости Secret Disk Server NG 3.2 может сгенерировать сертификат с закрытым ключом. В этом случае eToken администратора, для которого создаётся сертификат, обязательно должен быть подключен к рабочей станции администратора.

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

6. Нажмите **OK**.

7. При необходимости введите PIN-код.

Создание сертификата

Встроенное средство создания сертификатов Secret Disk Server NG 3.2 позволяет создавать сертификаты с закрытыми ключами для аутентификации и защиты мастер-ключей защищённых дисков и сохранять их в памяти eToken. Для того чтобы воспользоваться этим средством в процессе выбора сертификата, выполните следующую последовательность действий:

1. В окне **Secret Disk Server NG: выбор сертификата** нажмите **Создать**.

2. Введите название сертификата и ваш адрес электронной почты (обязательные параметры).

3. Если вы хотите, чтобы в сертификате присутствовали названия вашей организации и/или отдела, а также город и страна, в которых вы находитесь, заполните соответствующие необязательные поля. При этом в поле **Страна** вводите только буквы латинского алфавита.

 © 2006, Aladdin

4. Выберите длину ключа из списка допустимых длин ключа для данного поставщика криптографии.
   - Для Signal-COM CSP допустима только длина ключа 1024 бит (ГОСТ Р 34.10-94 «Система обработки информации. Защита криптографическая. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма»).
   - Для КриптоПро CSP допустимы длины ключа 1024 бит (ГОСТ Р 34.10-94) и 512 бит (ГОСТ Р 34.10-2001 «Система обработки информации. Защита криптографическая. Процессы формирования и проверки электронной цифровой подписи»).
   - Для стандартного поставщика криптографии Secret Disk Server NG 3.2, при использовании eToken PRO рекомендуется выбирать длину ключа 1024 бит (RSA).
5. Если вы хотите создать резервную копию сертификата, убедитесь в том, что флажок **Создать резервную копию сертификата** установлен.

   Примечание: эта возможность недоступна для сертификатов, создаваемых с помощью Signal-COM CSP и КриптоПро CSP.
6. Нажмите **OK**.
7. При необходимости в окне **Сохранение резервной копии сертификата** задайте пароль резервной копии сертификата, укажите путь к создаваемому файлу резервной копии и нажмите **OK**.
8. При необходимости выбирайте считыватель/ключевой носитель (eToken), следуйте указаниям датчика случайных чисел, вводите PIN-код, и т.д. (интерфейс зависит от поставщика криптографии).

   Примечание: Возможно, вам потребуется выбрать eToken не один раз. Обязательно указывайте eToken администратора, для которого создаётся сертификат. Для исключения ошибок:
   - отключите посторонние eToken от компьютера;
   - присваивайте каждому eToken уникальное имя.

   В стандартном комплекте поставки Secret Disk Server NG 3.2 eToken администратора носит имя `Administrator`, а eToken сервера — `Server`. При совместной работе нескольких администраторов Secret Disk Server NG убедитесь в том, что имена их eToken отличаются. О переименовании eToken см. в документе *eToken. Руководство администратора*, (файл `eToken_Admin_Guide.pdf` в папке `Doc` компакт-диска Secret Disk Server NG 3.2).
9. В случае успешного создания сертификата на экране появится окно с сообщением:

   `Сертификат создан успешно.`
10. Нажмите **OK**.

Защищённые диски

Зашифрование диска

Для того чтобы зашифровать диск, выполните следующую последовательность действий.

1. Убедитесь в том, что eToken администратора подключен к компьютеру.
2. В консоли **Управление Secret Disk Server** откройте список дисков.
3. Выберите диск, не являющийся ни системным, ни защищённым.
4. Щёлкните правой кнопкой мыши и выберите **Зашифровать**.
5. В окне **Параметры защищённого диска** назначьте метку тома и выберите букву диска, если вы хотите изменить текущие значения этих параметров.
6. 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.
7. Нажмите **OK**.
8. При необходимости следуйте инструкциям датчика случайных чисел, выбирайте считыватель и вводите PIN-код (интерфейс зависит от поставщика криптографии).
9. Система сгенерирует мастер-ключ защищённого тома, а затем предложит сохранить резервные копии этого мастер-ключа. Резервное копирование мастер-ключа защищённого тома можно осуществлять не только при зашифровании диска, но и в любой другой момент.
10. В окне **Secret Disk Server NG** убедитесь в том, что вы верно выбрали диск для зашифрования, и нажмите **Да**. Чтобы отказаться от зашифрования, нажмите **Нет**.
11. О том, что процесс зашифрования активен, свидетельствует слово `Шифрование` в ячейке **Статус**.
12. 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 зашифрования.
13. Если вы хотите приостановить процесс:
    - нажмите кнопку **Остановить процесс** () на панели инструментов консоли или выберите пункт **Остановить** из меню меню **Действие**/**Action** консоли;
    - если вы действительно хотите приостановить зашифрование, в окне подтверждения нажмите **Да**; в этом случае данные на диске станут недоступными; для возобновления доступа к ним вы должны будете завершить процесс зашифрования позднее, выбрав пункт **Продолжить** в меню **Действие**/**Action** или в контекстном меню.
14. Убедитесь в том, что диск зашифрован: в списке дисков в ячейке **Статус** соответствующей строки появилась запись **Зашифрован**.

© 2006, Aladdin

Подключение защищённого диска

Для того чтобы подключить защищённый диск, выполните следующую последовательность действий:

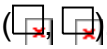
1. Убедитесь в том, что eToken администратора подключен к компьютеру.
2. В узле **Управление Secret Disk Server** щёлкните **Диски**.
3. Выберите отключенный защищённый диск ().
4. Щёлкните правой кнопкой мыши и щёлкните **Подключить**.
5. При необходимости выберите считыватель и (или) введите PIN-код (интерфейс зависит от поставщика криптографии).
6. Убедитесь в том, что значок диска изменился ().
7. Если прошлое отключение защищённого диска было осуществлено принудительно, на экране появится окно **Secret Disk Server NG** с соответствующим сообщением и предложением выполнить проверку диска.

   Для того чтобы выполнить проверку диска на наличие ошибок средствами Secret Disk Server NG 3.2, нажмите **Да**. Если вы используете другие средства проверки дисков, нажмите **Нет** и воспользуйтесь ими.

Отключение защищённых дисков

Отключение защищённого диска в штатном режиме

Для того чтобы отключить защищённый диск, выполните следующую последовательность действий:

1. В узле **Управление Secret Disk Server** щёлкните **Диски**.
2. Выберите подключенный защищённый диск ().
3. Щёлкните правой кнопкой мыши и выберите **Отключить**.
4. Если отключаемый диск занят, на экране появится окно подтверждения. Закройте все приложения, работающие с диском, и нажмите **Да**. Если вы не хотите в данный момент отключать диск, нажмите **Нет**.
5. Убедитесь в том, что значок диска изменился ().

Отключение защищённых дисков по сигналу «тревога»

Все или некоторые подключенные защищённые диски могут отключаться в экстренном режиме по сигналу «тревога».

Для того чтобы настроить отключение защищённых дисков по сигналу «тревога»:

- задайте пароль сигнала «тревога» для данного сервера;
- для каждого из защищённых дисков задайте способ реакции на сигнал «тревога».

Для подачи сигнала «тревога» используйте компонент Secret Disk NG Alarm. Подробная информация содержится в документации Secret Disk NG Alarm.

© 2006, Aladdin

Изменение свойств защищённого диска

Окно свойств защищённого диска

Для того чтобы открыть окно свойств защищённого диска, выполните следующее.

1. В узле **Управление Secret Disk Server** щёлкните **Диски**.
2. Выберите защищённый диск.
3. Нажмите клавишу ENTER.

В каждой из вкладок окна свойств защищённого диска присутствуют три кнопки:

- **OK** — сохраняет изменения и закрывает окно;
- **Отмена**/**Cancel** — закрывает окно без сохранения изменений;
- **Применить**/**Apply** — сохраняет изменения и оставляет окно открытым.

Во вкладке **Общие** представлена следующая информация:

- метка тома;
- буква диска;
- состояние (отключен защищённый диск или подключен);
- файловая система;
- ёмкость;
- серийный номер.

Кроме того, в этой вкладке доступны инструменты форматирования защищённого диска и проверки на наличие ошибок.

Во вкладке **Доступ** вы можете управлять доступом к защищённому диску.

Во вкладке Сценарии вы можете выбрать сценарии для запуска перед подключением и отключением дисков и после этих событий. Кроме того, здесь вы можете управлять правилами подключения и отключения дисков в зависимости от результатов выполнения сценариев.

Правило отключения защищённого диска при поступлении на сервер сигнала «тревога» вы можете выбрать во вкладке **Сигнал "тревога"**.

Изменение метки тома и буквы диска

Метка тома и буква диска — свойства защищённого диска, которые нельзя изменить средствами операционной системы. При подключении защищённого диска используются только метка тома и буква диска, указанные во вкладке **Общие** окна свойств защищённого диска.

Если метка тома и буква диска подключенного защищённого диска изменяются средствами операционной системы, эти изменения действуют до тех пор, пока данный защищённый диск не отключен. При повторном подключении будут снова использованы метка тома и буква диска, указанные во вкладке **Общие** окна свойств защищённого диска.

Изменить букву можно только у отключенного защищённого диска. При изменении метки тома защищённый диск может быть как подключен, так и отключен.

 © 2006, Aladdin

Для того чтобы изменить метку тома и букву диска средствами Secret Disk Server NG 3.2, выполните следующую последовательность действий.

1. В окне свойств защищённого диска откройте вкладку **Общие**.
2. При необходимости внесите изменения в поле **Метка тома**.
3. Если вы хотите изменить букву диска:
   - убедитесь в том, что параметр **Состояние** принимает значение **Отключен**;
   - нажмите **Изменить**;
   - в окне **Назначение буквы диска** выберите букву из списка **Буква (A - Z)**;
   - нажмите **OK**.
4. Сохраните сделанные изменения.

Управление доступом к защищённому диску

Доступ к защищённому диску по сети

В некоторых случаях для повышения безопасности вы можете полностью запретить доступ к защищённому диску по сети. Например, такой запрет целесообразен для защищённых дисков, на которых расположены базы данных.

Запрещать сетевой доступ к защищённому диску позволяет лицензия сервера приложений, а разрешать такой доступ — лицензия файл-сервера. Если в памяти eToken сервера отсутствует одна из этих лицензий, то вы не сможете осуществить соответствующую настройку доступа.

Для того чтобы установить или отменить запрет на доступ к защищённому диску по сети, выполните следующее.

1. В окне свойств защищённого диска откройте вкладку **Доступ**.
2. В области **Доступ к диску по сети** выберите **Запрещен** для установления запрета или **Разрешен** для отмены запрета.
3. Сохраните сделанные изменения.

Доступ администраторов к защищённому диску

Любой администратор защищённого диска может предоставлять другим администраторам доступ к защищённому диску, а также лишать администраторов доступа.

Для того чтобы другому администратору мог быть предоставлен доступ к защищённому диску, необходимо, чтобы этого администратора был выбран сертификат для поставщика криптографии, обслуживающего данный диск.

Для того чтобы предоставить другому администратору Secret Disk Server NG доступ к защищённому диску или отказать администратору в доступе, выполните следующее.

1. В окне свойств защищённого диска откройте вкладку **Доступ**.
2. Просмотрите список **Администраторы**, в котором перечислены все администраторы Secret Disk Server NG, которые вместе с вами имеют доступ к данному защищённому диску. Для того чтобы лишить администратора права доступа к защищённому диску, выделите соответствующую строку и нажмите

Удалить. Если вы хотите предоставить зарегистрированному администратору Secret Disk Server NG право управлять данным защищённым диском:

- нажмите **Добавить**, чтобы открыть окно **Выбор администратора** со списком всех зарегистрированных администраторов Secret Disk Server NG данного сервера, не имеющих доступа к данному защищённому диску;
- в окне **Выбор администратора** выберите администратора;

  Примечание: в списке **Администраторы** в этом окне перечислены только те администраторы, у которых выбран необходимый сертификат для защиты мастер-ключей и отсутствует доступ к данному защищённому диску.
- убедитесь в том, что ваш eToken администратора подключен к компьютеру, при необходимости подключите его;
- нажмите **Выбрать**;
- при необходимости укажите ваш eToken и введите PIN-код (интерфейс зависит от поставщика криптографии).

Настройки сценариев

Для автоматизации работы с данными на защищённых дисках вам может потребоваться настроить сценарии, выполняемые до и после подключения и отключения защищённых дисков. Например, с помощью сценариев можно запускать службу, работающую с базой данных, сразу после подключения защищённого диска и останавливать её перед отключением. Сценарии запускаются на сервере с той же учётной записью, что и служба Secret Disk Server NG.

Для того чтобы осуществить настройки сценариев, выполните следующую последовательность действий.

1. В окне свойств защищённого диска откройте вкладку **Сценарии**.
2. В области **При подключении**:
   - при **необходимости** введите строковую команду для запуска сценария, который должен выполняться перед подключением защищённого диска, в поле **перед**;

     Примечание: При указании локальных путей во вкладке **Сценарии** соответствующие файлы сценариев должны быть расположены на сервере.
   - 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**;

     Примечание: Время ожидания результата выполнения сценариев по умолчанию — 30 секунд. Этот параметр является общим для всех защищённых дисков. При желании вы можете изменить его значение.
   - при необходимости введите строковую команду для запуска сценария, который должен выполняться после подключения защищённого диска, в поле **после**.

 © 2006, Aladdin

3. 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**.
4. Сохраните сделанные изменения.

При составлении сценариев вам может потребоваться использование буквы подключаемого защищённого диска. Для этого вы можете использовать переменную окружения `SECRETDISK_MOUNTPOINT`, значение которой будет иметь формат `<буква в верхнем регистре>:`, например, `D:`.

Настройка сигнала «тревога» для защищённого диска

По вашему выбору разные защищённые диски могут по-разному реагировать на сигнал «тревога». Для того чтобы осуществить соответствующую настройку для защищённого диска, выполните следующее.

1. В окне свойств защищённого диска откройте вкладку **Сигнал "тревога"**.
2. Выберите реакцию защищённого диска на поступление сигнала «тревога»:
   - **Отключать защищённый диск в экстренном режиме (не выполнять сценарии)** — при отключении диска по сигналу «тревога» не будут выполняться сценарии, указанные во вкладке **Сценарии** окна свойств защищённого диска;
   - **Отключать защищённый диск, игнорируя ошибки выполнения сценариев** — при отключении защищённого диска по сигналу «тревога» сценарии, указанные во вкладке **Сценарии** окна свойств защищённого диска, будут выполняться, но при этом диск будет отключен независимо от результата выполнения сценария, предваряющего отключение;
   - **Отключать защищённый диск, учитывая ошибки выполнения сценариев** — при отключении защищённого диска по сигналу «тревога» сценарии, указанные во вкладке **Сценарии** окна свойств защищённого диска, будут выполняться с учётом настроек, сделанных в этой вкладке;
   - **Не отключать защищённый диск** — поступление на сервер сигнала «тревога» не будет приводить к отключению данного защищённого диска.
3. Сохраните сделанные изменения.

Форматирование защищённого диска

Подключенные защищённые диски можно форматировать теми же способами, что и обычные диски. Кроме того, Secret Disk Server NG 3.2 содержит встроенное средство форматирования. Если вы хотите отформатировать защищённый диск с помощью Secret Disk Server NG 3.2, выполните следующие действия.

1. В окне свойств защищённого диска откройте вкладку **Общие**.
2. Убедитесь в том, что диск подключен (параметр **Состояние** принимает значение `Подключен`).
3. Нажмите **Выполнить форматирование**.
4. В появившемся окне введите параметры форматирования и нажмите **Старт**.
5. Если вы уверены, что хотите отформатировать диск, в окне предупреждения нажмите **OK**, чтобы начать форматирование.

   В противном случае нажмите **Отмена**.
6. По окончании процесса форматирования в окне с сообщением

   `Форматирование завершено`

   нажмите **OK**.

Проверка защищённого диска на наличие ошибок

Подключенные защищённые диски можно проверять на наличие ошибок теми же способами, что и обычные диски. Кроме того, Secret Disk Server NG 3.2 содержит встроенное средство проверки целостности дисков. Во время проверки все файлы на диске должны быть закрыты. Чтобы проверить защищённый диск на наличие ошибок с помощью Secret Disk Server NG 3.2, выполните следующие действия.

1. В окне свойств защищённого диска откройте вкладку **Общие**.
2. Убедитесь в том что диск подключен (параметр **Состояние** принимает значение `Подключен`).
3. Нажмите **Выполнить проверку**.
4. В появившемся окне введите параметры проверки и исправления ошибок:
   - **Автоматически исправлять ошибки**: *при установленном флажке* Secret Disk Server NG 3.2 автоматически исправляет при проверке все ошибки файловой системы. *При снятом флажке* ошибки не исправляются, но регистрируются в **Журнале проверки**.
   - **Отображать полный путь ко всем файлам**: *при установленном флажке* в **Журнале проверки** регистрируются все файлы, в которых обнаружены ошибки, с указанием полного пути. *При снятом флажке* полные пути к файлам, в которых обнаружены ошибки, не записываются в **Журнал проверки**.
   - **Определять место дефектных секторов и восстанавливать на них информацию**: *при установленном флажке* Secret Disk Server NG 3.2 автоматически исправляет ошибки файловой системы, а также восстанавливает содержимое повреждённых секторов. Выбрав этот параметр, вы можете не устанавливать флажок **Автоматически исправлять ошибки**, т.к. при проверке будут исправляться ошибки всех типов. *При снятом флажке* Secret Disk Server NG 3.2 при проверке не осуществляет поиск повреждённых секторов.
   - **Проверять диск, только если он испорченный**: *при установленном флажке* проверка диска на наличие ошибок осуществляется по минимальному набору

 © 2006, Aladdin

критериев. *При снятом флажке* возможны стандартная проверка файловой системы и поиск повреждённых секторов.

5. Для того чтобы начать проверку, нажмите **Старт**. Если вы хотите отказаться от проверки, нажмите **Отмена**.
6. В процессе проверки диска заполняется **Журнал проверки**. Внизу окна отображается информация о том, какая часть операции проверки диска выполнена. По окончании проверки появится сообщение:

   ```
   Проверка диска завершена.
   ```

7. Ознакомьтесь с **Журналом проверки**. Для повторной проверки нажмите **Старт**. Для того чтобы закрыть окно, нажмите **Отмена**.

Особенности защищённых динамических томов

Расширение защищённого тома

Защищённый том динамического жёсткого диска можно расширить средствами Windows при двух условиях:

- исходный том, зашифрованный с помощью Secret Disk Server NG 3.2, был изначально создан на динамическом диске, а не преобразован из раздела или логического диска базового жёсткого диска;
- защищённый диск имеет формат NTFS.

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

1. Убедитесь в том, что том, который вы собираетесь расширить, расположен 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 зеракльные тома

Защищённые диски, созданные на основе зеракльных 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.

Перешифрование защищённого диска

Если вы хотите сменить алгоритм шифрования защищённого диска или сменить мастер-ключ, перешифруйте данный защищённый диск. Для этого выполните следующую последовательность действий.

1. Убедитесь в том, что eToken администратора подключен к рабочей станции администратора.
2. Откройте список дисков.
3. Выберите защищённый диск для перешифрования.
4. Убедитесь в том, что выбранный защищённый диск отключен: значок в графе **Том** содержит изображение закрытого замка. Если это не так, отключите защищённый диск.
5. Щёлкните правой кнопкой мыши и выберите **Перешифровать**.
6. 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.
7. Нажмите **OK**.
8. При необходимости следуйте инструкциям датчика случайных чисел, выбирайте считыватель и вводите PIN-код (интерфейс зависит от поставщика криптографии).
9. Система сгенерирует мастер-ключ защищённого диска, а затем предложит сохранить резервные копии мастер-ключа. Резервное копирование мастер-ключа защищённого диска можно осуществлять не только при перешифровании диска, но и в любой другой момент.
10. В окне подтверждения нажмите **Да**.
11. О том, что процесс перешифрования активен, свидетельствует слово `Перешифрование` с указанием количества процентов готовности в ячейке **Статус**.
12. 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.
13. Если вы хотите приостановить процесс:
    - нажмите кнопку **Остановить процесс** () на панели инструментов консоли или выберите пункт Остановить из контекстного меню или меню Действие/Action консоли;

© 2006, Aladdin

- если вы действительно хотите приостановить перешифрование, в окне подтверждения нажмите Да; в этом случае данные на диске станут недоступными; для возобновления доступа к ним вы должны будете завершить процесс перешифрования позднее, выбрав Продолжить из контекстного меню или меню Действие/Action консоли.

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

Расшифрование защищённого тома

Для того чтобы превратить защищённый диск в обычный, выполните следующую последовательность действий.

1. Убедитесь в том, что eToken администратора подключен к рабочей станции администратора.
2. Откройте список дисков.
3. Выберите защищённый диск для расшифрования.
4. Убедитесь в том, что выбранный защищённый диск отключен: значок в графе **Том** содержит изображение закрытого замка. Если это не так, отключите защищённый диск.
5. Щёлкните правой кнопкой мыши и выберите **Расшифровать**.
6. В окне подтверждения убедитесь в том, что вы верно выбрали защищённый диск для расшифрования, и нажмите **Да**. Чтобы отказаться от расшифрования, нажмите **Нет**.
7. При необходимости выберите считыватель и (или) введите PIN-код (интерфейс зависит от поставщика криптографии).
8. О том, что процесс расшифрования активен, свидетельствует слово **Расшифрование** в ячейке **Статус**.
9. 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 расшифрования.
10. Если вы хотите приостановить процесс:
    - нажмите кнопку Остановить процесс () на панели инструментов консоли или выберите пункт Остановить из контекстного меню или меню Действие/Action консоли;
    - если вы действительно хотите приостановить расшифрование, в окне подтверждения нажмите Да; в этом случае данные на диске станут недоступными; для возобновления доступа к ним вы должны будете завершить процесс расшифрования позднее, выбрав Продолжить из контекстного меню или меню Действие/Action консоли.
11. Убедитесь в том, что диск расшифрован: в списке дисков ячейка **Статус** соответствующей строки пуста.

© 2006, Aladdin

Настройки сервера

Настройки сигнала «тревога» для сервера

Для того чтобы осуществить настройки сигнала «тревога», выполните следующее.

1. При открытом сеансе управления в дереве консоли выделите **Управление Secret Disk Server**.
2. Выполните одно из действий:
   - в меню **Действие**/**Action** щёлкните **Настройки сигнала «тревога»**;
   - щёлкните правой кнопкой мыши и выберите **Настройки сигнала «тревога»**.
3. На экране появится окно **Настройки сигнала «тревога»**.
4. Задайте пароль сигнала «тревога». Для этого введите желаемую последовательность символов в графы **Пароль** и **Подтверждение**.
5. Если вы хотите, чтобы при поступлении сигнала «тревога» удалялось защищённое хранилище:
   - установите флажок;
   - на экране появится окно с предложением сохранить копию защищённого хранилища;
   - если вы располагаете актуальной резервной копией защищённого хранилища, нажмите **Нет**;
   - если у вас нет резервной копии защищённого хранилища, нажмите **Да** и перейдите к процедуре сохранения резервной копии защищённого хранилища.

   Важно: для того чтобы после удаления защищённого хранилища вы легко могли восстановить доступ к данным, сделайте резервную копию защищённого хранилища и храните её в надёжном месте.

   Если вы не хотите, чтобы защищённое хранилище удалялось при поступлении сигнала «тревога», снимите флажок.
6. В окне **Настройки сигнала «тревога»** нажмите **OK**.

Время ожидания результатов выполнения сценариев

Время ожидания результата выполнения сценариев — параметр, общий для всех защищённых дисков. По умолчанию его значение составляет 30 секунд. При желании вы можете изменить значение параметра в диапазоне 5000—120000 миллисекунд. Для этого выполните следующее:

1. На сервере в меню **Пуск**/**Start** выберите **Выполнить**/**Run**.
2. В окне **Запуск программы** / **Run** введите `regedit` и нажмите **OK**.
3. В дереве консоли **Редактор реестра** / **Registry Editor** разверните узел `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Secret Disk NG`.
4. Если в узле `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Secret Disk NG` отсутствует раздел `Server`, создайте новый раздел с таким именем.
5. В дереве консоли разверните узел `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Secret Disk NG\Server`.

© 2006, Aladdin

6. Если в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Secret Disk NG\Server` отсутствует параметр `ActionExecWaitTimeout`, создайте новый параметр типа DWORD с таким именем.
7. На строке с параметром `ActionExecWaitTimeout` щёлкните правой кнопкой мыши и выберите **Изменить**/**Modify**.

   На экране появится окно **Изменение параметра DWORD** / **Edit DWORD Value**.
8. 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**.
9. Введя желаемое значение, нажмите **OK** и при необходимости закройте окно **Редактор реестра** / **Registry Editor**.

Примечания:

1. Если параметр `ActionExecWaitTimeout` или весь раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Secret Disk NG\Server` отсутствует, то используется значение по умолчанию (30 секунд).
2. Если вы укажете значение менее 5000, то Secret Disk Server NG 3.2 будет ожидать результаты выполнения сценариев 5 секунд.
3. Если вы укажете значение выше 120000, то время ожидания результатов выполнения сценариев будет составлять 120 секунд.

Резервное копирование и восстановление

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. Имея такую копию, вы сможете легко восстановить работоспособность Secret Disk Server NG 3.2 в случае повреждения или утраты защищённого хранилища.

Резервное копирование защищённого хранилища

Окно **Сохранение резервной копии защищённого хранилища** можно вызвать при открытом сеансе управления, выделив в дереве консоли **Управление Secret Disk Server** и выполнив одно из действий:

- в меню **Действие**/**Action** щёлкнув **Сохранить копию защищённого хранилища**;
- щёлкнув правой кнопкой мыши и выбрав **Сохранить копию защищённого хранилища**.

Это окно также может появляться при настройке удаления защищённого хранилаща в случае полученииия сигнала «тревога».

При появлении на экране окна **Сохранение резервной копии защищённого хранилища** выполните следующее.

1. Укажите путь к файлу резервной копии.
2. Нажмите **Сохранить**.
3. Если вы указали путь к уже существующему файлу, на экране появится окно, предупреждающее вас об этом. Нажмите **Да**, чтобы заменить файл или **Нет**, чтобы ввести путь к новому файлу.
4. Убедитесь в том, что копия защищённого хранилища создана успешно, и нажмите **OK**.

Восстановление защищённого хранилища

Для того чтобы восстановить защищённое хранилище из архива, выполните следующее.

1. При открытом сеансе управления в дереве консоли выделите **Управление Secret Disk Server**.
2. Отключите все защищённые диски.
3. Выполните одно из действий:
   - в меню Действие/Action щёлкните Восстановить защищённое хранилище;
   - щёлкните правой кнопкой мыши и выберите **Восстановить защищённое хранилище**.
4. В окне подтверждения нажмите **OK**. Сеанс управления будет закрыт.
5. В окне **Выберите файл с резервной копией защищённого хранилища** выберите файл и нажмите **Открыть**.
6. Убедитесь в том, что защищённое хранилище успешно восстановлено, и нажмите **OK**.
7. При необходимости восстановите сеанс управления:
   - в окне **Secret Disk Server NG: идентификация** укажите один из сертификатов, используемых вами для аутентификации в системе Secret Disk Server NG 3.2 и защиты мастер-ключей защищённых дисков;

     Примечание: При необходимости, для того чтобы уточнить свой выбор, вы можете просмотреть параметры сертификата, нажав **Просмотр сертификата**.
   - нажмите **OK**;
   - при необходимости выберите считыватель (eToken) и введите PIN-код (интерфейс зависит от поставщика криптографии).

Резервное копирование и восстановление мастер-ключа защищённого диска

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

 © 2006, Aladdin

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, вы можете создать резервные копии мастер-ключей защищённых дисков. Мастер-ключ будет в зашифрованном виде сохранён в файле, защищённом паролем.

Сделать резервную копию мастер-ключа защищённого диска вы можете лишь при условии, что вы являетесь одним из администраторов данного защищённого диска.

Восстановить доступ к защищённому диску из такого файла сможет любой администратор Secret Disk Server NG, если:

- он знает пароль;
- у него выбран сертификат для использования с соответствующим поставщиком криптографии.

Резервное копирование мастер-ключа защищённого диска

Окно для создания резервной копии мастер-ключа защищённого диска можно вызвать, щёлкнув правой кнопкой мыши на соответствующей строке в списке дисков и выбрав пункт **Сохранить мастер-ключ**. Аналогичное окно также автоматически появляется при зашифровании и перешифровании диска.

Мастер-ключ в зашифрованном виде сохраняется в файле с паролем. Для того чтобы сделать резервную копию мастер-ключа защищённого тома, выполните следующее.

1. Укажите путь к файлу резервной копии и введите пароль дважды — в графу **Пароль** и в графу **Подтверждение**.
2. Нажмите **Создать** для завершения операции. Если вы в данный момент не хотите создавать резервных копий мастер-ключа, нажмите **Отмена** или **Пропустить**.
3. Если в поле **Путь к файлу** вы указали путь к уже существующему файлу, на экране появится окно **Secret Disk Server NG: Ошибка** с сообщением:

   ```
   Выбранный файл уже существует.

   Заменить существующий файл?
   ```

   Нажмите **Да**, чтобы заменить файл или **Нет**, чтобы ввести путь к новому файлу.
4. В случае успешного сохранения резервной копии мастер-ключа на экране появляется окно с сообщением:

   ```
   Резервная копия мастер-ключа успешно сохранена.
   ```
5. Нажмите **OK**.

Восстановление доступа к защищённому диску

Для восстановления доступа к защищённому диску вам потребуется:

- иметь
  - файл резервной копии мастер-ключа;

  - eToken администратора, зарегистрированного на данном компьютере;
- знать
  - пароль файла резервной копии мастер-ключа;
  - PIN-код eToken.

Кроме того, должен быть выбран сертификат для использования с соответствующим поставщиком криптографии.

Для восстановления доступа к защищённому диску с помощью файла резервной копии мастер-ключа выполните следующее.

1. Откройте консоль с оснасткой **Управление Secret Disk Server**.
2. Щёлкните правой кнопкой мыши по значку **Диски** в дереве консоли.
3. В появившемся меню выберите **Восстановить доступ к защищённому тому**.
4. В окне **Выберите файл с резервной копией мастер-ключа** выберите файл и нажмите **Открыть**.
5. Введите пароль файла резервной копии мастер-ключа защищённого тома и нажмите **OK**.
6. При необходимости выберите считыватель и введите PIN-код (интерфейс зависит от поставщика криптографии).

Восстановление сервера после сигнала «тревога»

Для того чтобы восстановить сервер после сигнала «тревога», выполните следующее.

1. Если сервер был настроен на удаление защищённого хранилища при получении сигнала «тревога»:
   - запустите на сервере службу `Secret Disk Server NG`;

     Примечание: При запуске службы будет создано новое защищённое хранилище, не содержащее ни информацию об администраторах Secret Disk Server NG, ни зашифрованные копии мастер-ключей защищённых дисков.
   - откройте сеанс управления, зарегистрировав нового администратора Secret Disk Server NG;
   - если вы располагаете резервной копией защищённого хранилища, восстановите его; в противном случае:
     - зарегистрируйте остальных администраторов Secret Disk Server NG;
     - каждый из администраторов Secret Disk Server NG должен восстановить доступ ко всем защищённым дискам.
2. Подключите все защищённые диски, отключенные по сигналу «тревога».
3. Проверьте все защищённые диски, оключавшиеся по сигналу «тревога», на наличие ошибок.

© 2006, Aladdin

SECRET DISK NG ALARM 3.1

Назначение

Инструменты Secret Disk NG Alarm 3.1 предназначены для подачи сигнала «тревога» серверам Secret Disk Server NG 3.x. В зависимости от настроек сервера и защищённых дисков, получение сигнала «тревога» приводит к:

- отключению защищённых дисков;
- уничтожению защищённого хранилища.

Уничтожение защищённого хранилища сигналом «тревога» означает полное удаление ключевой информации: даже если злоумышленники завладеют электронным ключом или смарт-картой eToken, узнают PIN-код и будут обладать полным доступом к серверу, без защищённого хранилища они не смогут прочесть информацию.

Состав

Инструменты Secret Disk NG Alarm 3.1:

- основная утилита Secret Disk NG Alarm 3.1 — утилита для настройки и отправки сигнала «тревога» с помощью графического интерфейса пользователя;
- «красная кнопка» — устройство, подключаемое к порту COM (кнопка с проводом или радиоприёмник с радиобрелоком);
- `sdsalrm.exe` — утилита для подачи сигнала «тревога» из командной строки.

Новое в версии

Secret Disk NG Alarm 3.1 имеет два основных отличия от Secret Disk NG Alarm 3.0:

- возможность настраивать время удержания кнопки;
- новая схема подключения кнопки к разъёмам порта COM.

Введение настройки времени удержания кнопки не означает, что вместо обычной кнопки в Secret Disk NG Alarm 3.1 нельзя использовать датчики пожарной или охранной сигнализации и т. п. Однако для того чтобы подача сигнала «тревога» происходила при каждом изменении разности потенциалов на соответствующих контактах порта COM необходима специальная настройка: вам потребуется установить время удержания кнопки равным нулю.

Использование в Secret Disk NG Alarm 3.1 новой схемы подключения кнопки к разъёмам порта COM не вносит несовместимости:

- при необходимости кнопки с новой схемой моожно использовать с программным обеспечением Secret Disk NG Alarm 3.0;
- при необходимости в Secret Disk NG Alarm 3.1 можно использовать кнопки Secret Disk NG Alarm 3.0.

© 2006, Aladdin

Требования к рабочей станции для сигнала «тревога»

Требования к программному обеспечению

Инструменты для сигнала «тревога» могут быть установлены на компьютере, работающем под управлением одной из следующих 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.

Требования к аппаратному обеспечению

1. Рабочая станция должна удовлетворять требованиям к аппаратному обеспечению соответствующей операционной системы.
2. Для подключения «красной кнопки» необходим свободный порт COM.

Установка и удаление программного обеспечения

Необходимые полномочия

Для установки и удаления Secret Disk NG Alarm 3.1 необходимы полномочия локального администратора.

Установка

Для того чтобы установить Secret Disk NG Alarm 3.1, выполните следующую последовательность действий.

1. Убедитесь в том, что компьютер удовлетворяет системным требованиям.
2. Для запуска программы установки Secret Disk NG Alarm 3.1 в меню компакт-диска Secret Disk Server NG 3.x нажмите **Установить утилиту подачи сигнала «тревога»**.

   Примечание: Более подробная информация о меню компакт-диска изложена в документации Secret Disk Server NG 3.x.
3. В окне приветствия программы установки нажмите **Далее**.
4. Для начала процесса установки нажмите **Установить**.
5. Процесс установки займёт некоторое время.
6. Убедитесь в том, что процесс установки завершён успешно, и нажмите **Готово**.

© 2006, Aladdin

Отказ от установки

Отказаться от установки Secret Disk NG Alarm 3.1 можно в любом диалоговом окне программы установки, кроме последнего. Для этого:

- нажмите **Отмена**;
- в окне подтверждения нажмите **Да**;
- нажмите **Готово**.

Удаление

Для того чтобы удалить Secret Disk NG Alarm 3.1, выполните следующее.

1. Щёлкните **Пуск**/**Start** > **Все программы** (**All Programs**) / **Программы** (**Programs**) > **Secret Disk NG** > **Alarm** > **Удаление**.
2. В окне подтверждения нажмите **Да**/**Yes**.
3. При необходимости закройте требуемые окна и нажмите **Повторить**.

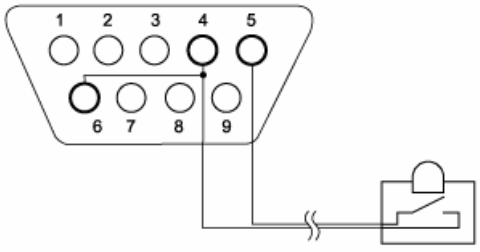
Подключение и отключение «красной кнопки»

Переделка устаревших кнопок

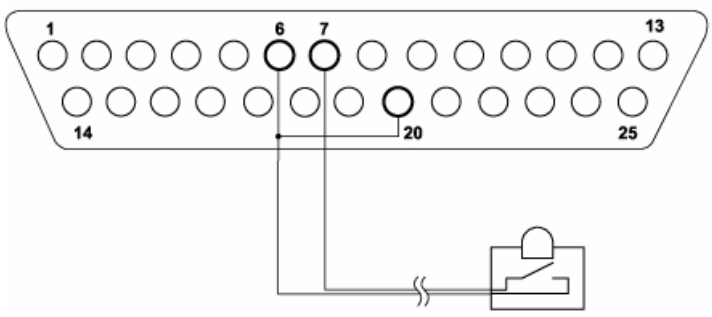
В «красной кнопке», использовавшейся с Secret Disk Server 1.x, замыкались контакты 2 и 3 штекера DB-9 (контакты 3 и 2 штекера DB-25). В «красной кнопке» Secret Disk NG Alarm 3.0 замыкались контакты 4 и 6 штекера DB-9 (контакты 20 и 6 штекера DB-25). Если вы хотите использовать устаревшую кнопку в комплексе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



Примечание:

Переделка кнопки Secret Disk NG Alarm 3.0 рекомендуется, но не является обязательной, поскольку Secret Disk NG Alarm 3.1 поддерживает кнопки, входившие в состав Secret Disk NG Alarm 3.0.

Подключение «красной кнопки»

Для того чтобы подключить «красную кнопку», выполните следующее:

1. Выключите компьютер.
2. Отсоедините провод электропитания.
3. Подключите разъём к порту COM.
4. Закрепите кнопку. Место крепления должно удовлетворять двум условиям:
   - оно должно быть легкодоступным;
   - случайное нажатие «красной кнопки» должно быть исключено.

Отключение «красной кнопки»

Для того чтобы отключить «красную кнопку», выполните следующее:

1. Выключите компьютер.
2. Отсоедините провод электропитания.
3. Отключите разъём от порта COM.

Настройка

Для настройки Secret Disk NG Alarm 3.1 необходимо иметь полный доступ к разделам реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Alarm\Plugins\ALRMCfg\Parameters`, `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Alarm\Plugins\RBEvents\Parameters` и `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Alarm\Plugins\SDNotifier\Parameters`. По умолчанию такой доступ есть только у администраторов.

Для того чтобы осуществить настройку Secret Disk NG Alarm 3.1, выполните следующее:

1. Убедитесь в том, что программное и аппаратное обеспечение установлено.
2. Щёлкните **Пуск**/**Start** > **Все программы** (**All Programs**) / **Программы** (**Programs**) > **Secret Disk NG** > **Alarm** > **Alarm**.
3. На экране появится окно **Secret Disk NG Alarm**.
4. Укажите серверы и соответствующие пароли сигнала «тревога»:

   Примечание: нажатие «красной кнопки» будет приводить к подаче сигнала «тревога» на все указанные серверы одновременно.

   - для добавления сервера:
     - нажмите **Добавить**;
     - в окне **Свойства сервера** введите имя или IP-адрес сервера;

 © 2006, Aladdin

- введите пароль сигнала «тревога» в поля **Пароль** и **Подтверждение**;
- нажмите **ОК**;

- для редактирования свойств сервера:
  - выберите сервер из списка;
  - нажмите **Редактировать**;
  - в окне **Свойства сервера** измените полное доменное имя или IP-адрес сервера;
  - введите пароль сигнала «тревога» в поля **Пароль** и **Подтверждение**;
  - нажмите **ОК**;
- для того чтобы нажатие «красной кнопки» и подача сигнала с помощью основной утилиты не влияли на какой-либо сервер:
  - выберите сервер из списка;
  - нажмите **Удалить**;
  - в окне подтверждения нажмите **Да**.

5. При необходимости укажите порт, к которому подключена «красная кнопка».
6. По умолчанию для подачи сигнала «тревога» с помощью «красной кнопки» нужно нажать и отпустить кнопку. При этом время удержания кнопки должно составлять не менее 90 мс. Такое значение параметра обеспечивает:
   - подачу сигнала «тревога» обычным чётким кратковременным нажатием кнопки;
   - предотвращение случайного срабатывания.

   В некоторых случаях вам потребуется изменить минимальное время удержания кнопки:
   - увеличить его, если при текущих настройках наблюдается самопроизвольная подача сигнала «тревога»;
   - уменьшить его, если при текущих настройках кратковременное нажатие «красной кнопки» не приводит к подаче сигнала «тревога»;
   - назначить параметру значение 0, если для подачи сигнала «тревога» вы используете датчик пожарной или охранной сигнализации и т. п.

   Примечания:
   - Чем больше минимальное время удержания кнопки, тем дольше надо удерживать кнопку. Чрезмерное увеличение значения этого параметра может привести к тому, что кратковременное нажатие «красной кнопки» не будет приводить к подаче сигнала «тревога».
   - Если параметр принимает значение `0`, то подача сигнала «тревога» происходит при каждом изменении разности потенциалов на соответствующих контактах порта COM. Это необходимо, когда вместо обычной кнопки контакты подключены к датчику пожарной или охранной сигнализации и т. п. При использовании обычной кнопки нулевое значение параметра может приводить к самопроизвольной подаче сигнала «тревога». Для того чтобы предотвратить

самопроизвольное срабатывание при подключении к датчикам используйте экранированные кабели с заземлением.

Для того чтобы увеличить минимальное время удержания кнопки, переместите ползунок вправо, а для того чтобы уменьшить — влево.

7. Если вы хотите подавать сигнал «тревога» с помощью мыши, установите флажок **Значок на панели задач**.
8. Нажмите **OK**.

Подача сигнала «тревога»

Использование «красной кнопки»

Для того чтобы подать сигнал «тревога» с помощью «красной кнопки», просто нажмите кнопку (обычную или на радиобрелоке).

Подача сигнала «тревога» с помощью мыши

Основная утилита Secret Disk NG Alarm 3.1 позволяет подавать сигнал «тревога» без нажатия «красной кнопки». Для этого:

- на панели задач щёлкните правой кнопкой мыши по значку **сигнал «тревога»** ();
- щёлкните **Подать сигнал «тревога»**.

Подача сигнала «тревога» из командной строки

Если Secret Disk NG Alarm 3.1 настроен на подачу сигнала «тревога» нескольким серверам Secret Disk Server NG 3.x, то использование командной строки — единственный способ подачи сигнала лишь одному или некоторым из них.

Для отправки сигнала «тревога» одному или нескольким серверам Secret Disk Server NG 3.x из командной строки предназначена утилита `sdsalrm.exe`. Для того чтобы послать сигнал «тревога» серверу, вы должны знать:

• имя или IP-адрес сервера;

• пароль сигнала «тревога».

Для того чтобы отправить сигнал «тревога» с помощью утилиты `sdsalrm.exe`, выполните следующее:

1. Убедитесь в том, что на рабочей станции установлен Secret Disk NG Alarm 3.1.
2. В меню **Пуск**/**Start** выберите **Выполнить**/**Run**.
3. В поле **Открыть**/**Open** введите:

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

   где:

   `<парольN>` — пароль сигнала «тревога» для сервера N.

   `<серверN>` — имя или IP-адрес сервера N.

 © 2006, Aladdin

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>" ...].`

ИЗВЕСТНЫЕ ПРОБЛЕМЫ И ИХ РЕШЕНИЕ

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 3.2.
4. Запустите программу установки компонентов Secret Disk Server NG 3.2 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 3.2 снова.

© 2006, Aladdin

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 3.2 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.

© 2006, Aladdin

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:

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.

Срок действия сертификата не начался или истёк.

Сертификат отозван.

Решение:

1. Нажмите **OK**.

Сверьте срок действия сертификата с текущими датой и временем.

Проверьте, не является ли сертификат отозванным.

При необходимости добавьте необходимые сертификаты центров сертификации в соответствующие хранилища на рабочей станции администратора или выберите другой сертификат.

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.

 © 2006, Aladdin

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.
```

Возможная причина:

Вы ввели неверный пароль файла резервной копии.

Решение:

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

Проблема:

Сертификат, созданный с помощью КриптоПро CSP на другом компьютере, не отображается в окне **Secret Disk Server NG: выбор сертификата**.

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 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.

 © 2006, Aladdin

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».

© 2006, Aladdin

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.
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.

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 3.2.

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.

© 2006, Aladdin

Защищённый диск — диск, использующийся для безопасного хранения конфиденциальной информации в зашифрованном виде. В Secret Disk Server NG 3.2 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 — 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 3.2 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 3.2 может использовать Signal-COM CSP и КриптоПро CSP.

См. также: Signal-COM CSP, КриптоПро CSP, 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.

 © 2006, Aladdin

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

© 2006, Aladdin

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

 © 2006, Aladdin

 © 2006, Aladdin