

## Настройка и использование StrongDisk Server

### Часто задаваемые вопросы

**Вопрос:** Почему программы в папках **Startup** и **Dismount** не запускаются при подключении диска?

**Ответ:** Необходимо в эту папку помещать не сами программы, а ярлыки на эти программы.

---

**Вопрос:** Если в процессе работы при подключенном защищенном диске выключится питание компьютера, останутся ли файлы с защищенного диска в открытом виде?

**Ответ:** Нет. Кодирование происходит "на лету", т.е. **StrongDisk Server** не хранит данные в открытом виде, когда подключен диск. Раскодируются данные только при чтении, но на жесткий диск в открытом виде они не записываются. Тем не менее, есть риск, что какая-то часть данных, с которыми Вы работали, может оказаться в файле подкачки системы Windows, поэтому следует избегать таких ситуаций.

---

**Вопрос:** Насколько сильную защиту данных обеспечивает **StrongDisk Server**?

**Ответ:** Алгоритмы кодирования и длины ключей, используемые в системе **StrongDisk Server**, проверены временем и признаны во всем мире. Защита, которую предоставляет система **StrongDisk Server**, в подавляющем большинстве случаев более чем достаточна. Для взлома системы потребуются, по меньшей мере, месяцы и десятки-сотни миллионов долларов. Наибольшую опасность представляет утечка информации и плохие пароли без использования внешних ключей. По этой причине в системе **StrongDisk Server** предусмотрены средства, снижающие риск утечки практически до нуля, а также даны рекомендации по выбору хороших паролей.

---

**Вопрос:** Можно ли защищенный диск, созданный на одном компьютере, подключить на другом?

**Ответ:** Да. Если на другом компьютере установлена система **StrongDisk Server** и его пользователь обладает необходимым паролем и внешним ключом, то он может подключить созданный Вами защищенный диск. Это может быть использовано, в частности, для пересылки по электронной почте данных внутри файлов-образов защищенных дисков.

---

**Вопрос:** Где хранится пароль к защищенному диску?

**Ответ:** Пароль к защищенному диску не хранится ни где.

---

**Вопрос:** Почему мне не удается получить доступ (прямо с **CD-ROM**) к диску, созданному в системе **Windows NT/2000**, файл-образ которого был записан на **CD-ROM**?

**Ответ:** Если защищенный диск содержит файловую систему **NTFS**, то это действительно невозможно. Дело в том, что при доступе к диску с системой **NTFS** Windows пытается производить служебные операции записи на диск, даже если Вы хотите только прочитать с него информацию. Естественно, запись на **CD-ROM** не удастся. Если на защищенном диске файловая система **FAT**, то такой проблемы не существует.

## Электронные ключи

Системы **StrongDisk™** поддерживают работу с электронными USB-ключами через стандарт **PKCS#11(Cryptoki)**. Реализована встроенная поддержка следующих типов электронных USB-ключей:

- **iKey 1000/1032 by Rainbow**



- **iKey 2000/2032 by Rainbow**



- **Crypto Identity 5 by Eutron**



- **ePass 1000 by Fetian**



- **ePass 2000 by Fetian**

- **eToken Pro by Aladdin**



- **eToken R2 by Aladdin**

Системы **StrongDisk™** также поддерживают работу с электронным ключом **Dallas iButton** (touch memory), подключаемым к COM-порту.

- **iButton by Dallas Semiconductors**



## Часто задаваемые вопросы

**Вопрос:** Программа **StrongDisk Pro**, **StrongDisk Server** или **StrongDisk Remote Administrator** запрашивает **SO PIN**, как его узнать?

**Ответ:** Необходимо посмотреть в файл **ekey.txt** соответствующее описание электронного ключа или в **Таблице 3** на странице "**Дополнительные сведения**".

---

**Вопрос:** Что необходимо сделать, чтобы электронный ключ, проинициализированный в предыдущей версии работал в **StrongDisk Pro 3.0** или **StrongDisk Server 3.1**

**Ответ:** Необходимо воспользоваться утилитами производителя ключей для форматирования ключа, а затем этот электронный ключ проинициализировать в **StrongDisk Pro 3.0** или в **StrongDisk Server 3.1**.

---

**Вопрос:** В чем отличие работы электронного ключа в **обычном** и **защищенном** режимах?

**Ответ:** В **обычном** режиме код в электронном ключе считывается, перезаписывается и удаляется без запроса **ПИН**, а в **защищенном** режиме все операции с электронным ключом выполняются только после ввода **ПИН**.

**Вопрос:** Можно ли использовать электронный USB-ключ сразу в нескольких приложениях вместе с программой **StrongDisk Pro** или **StrongDisk Server**?

**Ответ:** Да, если другое приложение не перехватывает управление ключом полностью на себя.

---

**Вопрос:** Можно ли использовать электронный ключ **iButton** сразу в нескольких приложениях вместе с программой **StrongDisk Pro** или **StrongDisk Server**?

**Ответ:** Нет, так как электронный ключ **iButton** подключен к COM-порту, то к нему может одновременно обращаться только одно приложение. Особенно это критично, если электронный ключ **iButton** используется в функции "**Красная кнопка**".

## Дополнительные сведения об электронных ключах

**Таблица 1.** Поддерживает ли ОС работу с электронным ключом определенного типа.

Тип ключа	Windows 98 SE	Windows ME	Windows NT4(SP6)	Windows 2000	Windows XP	PKCS#11-библиотека
iKey 1000/1032	Да	Да	Да	Да	Да	k1pk112.dll
iKey 2000/2032	Да	Да	Да	Да	Да	dkck232.dll
Crypto Identity 5	Да	Да	Да	Да	Да	sadaptor.dll
ePass 1000	Да	Да	Да	Да	Да	ep1pk111.dll
ePass 2000	Да	Нет	Да	Да	Да	ep2pk11.dll
eToken R2	Да	Да	Да	Да	Да	etpkcs11.dll
eToken PRO	Да	Да	Да	Да	Да	etpkcs11.dll

**Таблица 2.** Расположение необходимых библиотек в системных папках.

Операционная система	Расположение библиотеки
Windows 98 SE/ME	..\WINDOWS\SYSTEM
Windows NT4/2000	..\WINNT\SYSTEM32
Windows XP/2003	..\WINDOWS\SYSTEM32

**Таблица 3.** Утилиты форматирования электронного ключа и установленные производителем **SO PIN** и **USER PIN (PIN)**.

Тип ключа	Утилита	SO PIN	PIN	Сайт производителя
iKey 1000/1032	iKeyTU.exe	Rainbow	Не задан	<a href="http://www.rainbow.msk.ru">http://www.rainbow.msk.ru</a>
iKey 2000/2032	CIPUtils.exe	Отсутствует	PASSWORD	<a href="http://www.rainbow.msk.ru">http://www.rainbow.msk.ru</a>
Crypto Identity 5	INITOKEN.EXE	Не задан	Не задан	<a href="http://www.eutron.com">http://www.eutron.com</a>
ePass 1000	epassmgr.exe	ROCKEY	Не задан	<a href="http://www.fetian.com">http://www.fetian.com</a>
ePass 2000	ePassMgr2K.exe	Не задан	Не задан	<a href="http://www.fetian.com">http://www.fetian.com</a>
eToken R2	eTEdit	Отсутствует	Не задан	<a href="http://www.aladdin.ru">http://www.aladdin.ru</a>
eToken PRO	eTFormat.exe	1234567890	Не задан	<a href="http://www.aladdin.ru">http://www.aladdin.ru</a>

В электронных USB-ключках при их инициализации программами **StrongDisk Pro** и **StrongDisk Server** не изменяется **SO PIN**.

Электронный ключ **iButton** в отличие от USB-ключей требует адаптера, считывателя и соединяющего их кабеля.

- Используемые типы адаптеров к COM-порту: **DS9097** и **DS9097U**
- Тип используемого считывателя: **DS1402D-DR8**
- Тип поддерживаемого электронного ключа: **DS1994L-F5**

Адаптер **DS9097** может быть использован для удлинения соединительного кабеля только до 15 метров, адаптер **DS9097U** позволяет увеличить длину соединительного кабеля до 100 метров.

Если Вы не смогли найти ответ на вопрос, связанный с электронным ключом, обратитесь в службу технической поддержки производителя электронного ключа.

## Уничтожение данных

Файловая система, используемая в системе Windows, устроена таким образом, что при удалении файлов они только помечаются как удаленные, но информация, содержащаяся в них, остается на диске, даже если Вы очистите 'Корзину'. Существует множество средств для восстановления таким образом удаленных файлов, которыми может воспользоваться даже школьник. В действительности информация будет затерта (частично или полностью), только когда система запишет на место удаленного файла другой файл. Но это может произойти нескоро. Поэтому при работе с конфиденциальной информацией удаление файлов с обычных дисков, используя стандартные средства, является недопустимым.

В состав систем **StrongDisk™** входит утилита **Burner**, предназначенная для уничтожения файлов с полным затиранием содержащихся в них данных без возможности восстановления. Настоятельно рекомендуется использовать утилиту **Burner**, если в процессе работы конфиденциальные данные попали на жесткий диск и были удалены средствами Windows.

## Часто задаваемые вопросы

**Вопрос:** Как происходит уничтожение файлов и каталогов при помощи утилиты **Burner.exe**?

**Ответ:** На то место, где расположен файл (папка) записывается случайно сгенерированная двоичная последовательность, а после этого файл (каталог) удаляется. Таким образом, при восстановлении файла (папки) в нем будет "информационный мусор".

---

**Вопрос:** Как происходит затирание свободного места на диске при помощи утилиты **Burner.exe**?

**Ответ:** На диске сначала создается папка **\$\$Burner\$\$**. Затем в этой папке создаются файлы с ничего не значащими именами, заполненные случайно сгенерированными двоичными последовательностями. Так происходит до тех пор, пока диск не будет заполнен. После этого папка **\$\$Burner\$\$** вместе с содержимым удаляется.