# Система защиты конфиденциальной информации «StrongDisk»

Многие думают, что средства криптографической защиты — это сложно, неудобно и ненадежно. Другие предпочитают создавать архивы с паролем, что опять же неудобно, а уровень надежности подобных защит невысок. Однако, на рынке программного обеспечения существует немало продуктов, которые могут удовлетворить как требованиям легкости в использовании, так и профессионализма (надежность защиты информации и богатые функциональные возможности). Один из самых успешных подобных продуктов — программа StrongDisk, выпущенная компанией Физтех-софт. Физтех-софт — российская IT-компания, образованная в 1991 году.

Принцип работы программы StrongDisk очень прост — она создает логический диск с любым именем (скажем, Z:), с которым можно работать как с любым другим диском. Физически же диск представляет собой файл с произвольным именем, который может находиться где угодно: от жесткого диска до оптического носителя. Причем этот файл-диск можно открыть на любом другом компьютере, после установки на него программы StrongDisk. Таким образом, файл является зашифрованным образом диска. Для шифрования используются алгоритмы с открытыми исходными текстами, что обеспечивает надежность защиты. Для защиты можно использовать пароль, файл-ключ или электронный USB-ключ. Возможна произвольная комбинация этих методов — к примеру, использование файл-ключа и пароля. Такая комбинация повышает степень защиты, поскольку владение только одним элементом, файл-ключом или паролем, не дает доступа к информации. Файл-ключ можно затем записать на любой удобный внешний носитель (например во внутреннюю память смартфона) и носить с собой.

StrongDisk выпускается в двух версиях: Pro и Server, первая предназначена для обычных пользователей, а вторая расширяет возможности StrongDisk для использования в сети, когда конфиденциальная информация храниться на сервере. Ниже мы рассмотрим общие принципы работы обеих версий, а потом остановимся на их отличиях.

## Основные возможности StrongDisk

### Создание нового диска

По умолчанию программа запускается при старте Windows, после чего ее значок помещается в правую часть панели задач, рядом с часами компьютера. При вызове программы перед пользователем появляется окно с двумя основными возможностями: создание нового диска и подключение уже существующего (рис. 1).

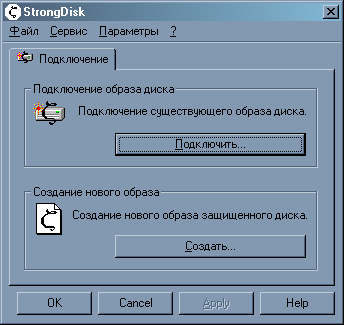


Рисунок 1. Первый запуск программы

При подключении существующего диска программа предложит указать файл-образ (рис. 2), причем ссылки на существующие файлы-образы могут быть запомнены в папке «StrongDisk Disks» в каталоге Windows, так что поиск файла не создаст проблем. Впрочем, в новых версиях программы подобная возможность опциональна.

Затем следует ввести все необходимые данные для открытия — пароль, файл-образ (если он есть) и вставить электронный ключ (если он есть). Ниже можно указать букву для защищенного диска, а также запретить запись на диск (подключить его только для чтения, но такой режим доступен только для FAT дисков). Если необходимо, StrongDisk может автоматически запустить программы на диске — они должны размещаться в папке StartUp защищенного диска (плюс должна быть помечена соответствующая галочка).

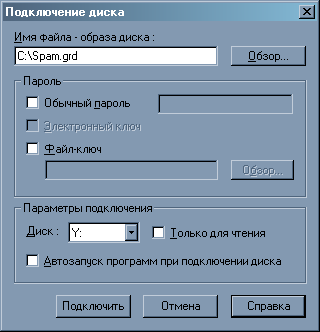


Рисунок 2. Подключение диска

После подключения пользователь сможет работать с подключенным диском как обычно: записывать на него файлы, считывать файлы, изменять на нем информацию. После окончания работы диск отключается вручную, либо он будет отключен автоматически при завершении работы Windows (рис. 3).

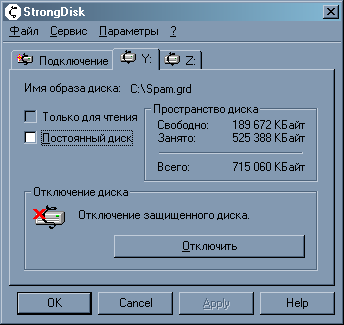


Рисунок 3. Информация о диске

Для ручного отключения необходимо вызвать программу StrongDisk (щелкнув по ее значку рядом с часами компьютера), после чего выбрать закладку соответствующего подключенного диска (в нашем случае «Y:») и нажать клавишу «Отключить». При этом следует убедиться, что закрыты все файлы, которые открывались с этого диска. Иначе программой будет выведено соответствующее предупреждение (рис. 4).

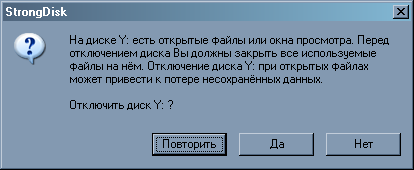


Рисунок 4. Предупреждение об открытых файлах

Возможно, также, «насильственное» отключение, когда диски будут отключены вне зависимости от наличия на них открытых файлов. Это может пригодиться в случае, когда отключение нужно произвести срочно. Такое экстренное отключение может происходить при нажатии «горячей» комбинации клавиш, заданной пользователем.

Теперь перейдем к созданию защищенных дисков. Для этого следует нажать клавишу «Создать», после чего запустится мастер создания дисков, в котором необходимо указать имя и место расположения образа диска, ввести размер диска и тип файловой системы, ввести емкость создаваемого защищенного диска. Емкость диска приблизительно равна длине образа диска, так как последний состоит из заголовка и собственно закодированных данных, а сжатия данных или увеличения их объема при кодировании не происходит. Для динамических («резиновых») дисков значение размера диска интерпретируется как максимальный размер образа диска. Емкость защищенного диска не может превышать количество свободного пространства на том диске, где создается образ диска (рис. 5).

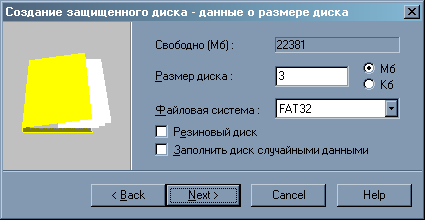


Рисунок 5. Создание защищённого диска

«Резиновый» диск — это защищенный диск, у которого размер образа увеличивается по мере заполнения данными. Начальный размер резинового диска мал - в нем нет ничего, кроме заголовка. Максимальный размер «резинового» диска вводится в поле «Размер диска (Мб)». При создании «резиновый» диск не может быть заполнен случайными данными. Следует крайне осторожно работать с резиновыми дисками, когда на диске, где расположен образ, мало места. Нехватка места может привести к потере записываемых на защищенный диск данных.

Если необходимо заполнить новый файл-образ диска случайными данными, то нужно установить в настройках соответствующую галочку. Заполнение диска случайными данными не позволит злоумышленникам узнать, сколько полезных данных записано на защищенном диске.

Диск лучше создавать в файловой системе NTFS, чтобы пользоваться всеми ее преимуществами, тем не менее, возможно использование и файловых систем типа FAT16 и FAT32.

Следует помнить, что файловая система NTFS не может использоваться на «резиновых» дисках. Кроме того, защищенные диски с NTFS невозможно подключать в режиме «только чтение», что может создавать препятствия при подключении защищенных дисков, образы которых расположены на таких носителях, как CD-диски.

Образ диска может располагаться в разделе с любой файловой системой, независимо от того, какая файловая система используется в нем самом.

При создании диска также можно указать необходимые алгоритмы кодирования ключей и данных, а также алгоритм хэширования (рис. 6).

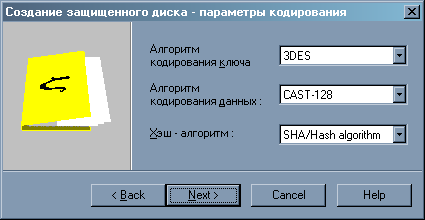


Рисунок 6. Выбор алгоритмов при создании диска

Перед тем как можно будет использовать электронный ключ или файл-ключ, его нужно проинициализировать. Пароль не хранится нигде, даже в самом файле защищенного диска. Содержимое внешних ключей также не хранится нигде, кроме самого электронного ключа или файл-ключа. Если пользователь забудет заданный им пароль или потеряет внешний ключ, не сделав его копию, никто (включая разработчиков системы StrongDisk), не сможет восстановить их.

В пароле к диску должно быть не менее восьми символов. Следует иметь в виду, что неудачный пароль может свести на нет (если, конечно, не используется внешний ключ) все преимущества, которые дают мощные методы шифрования. Даже обзаведясь очень длинным и абсолютно бессмысленным паролем, следует соблюдать ряд мер предосторожности. В противном случае этот пароль может стать известным посторонним.

В конце следует внимательно проверить все параметры нового диска, а затем нажать клавишу «Создать». После этого будет создан и подключен новый защищенный диск.

### Электронные ключи

Системы защиты информации StrongDisk Pro и StrongDisk Server поддерживают работу с электронными ключами. На электронный ключ владелец информации записывает код, который будет паролем для доступа к защищенной информации. Этот код генерируется случайным образом и имеет большую длину, что полностью исключает возможность его подбора. Электронные ключи выполнены в виде брелоков, что позволяет носить их вместе с обычными ключами. Они очень удобны в использовании и обеспечивают следующие преимущества:

* для получения доступа к защищенной информации необходим не только пароль, но и электронный ключ. До тех пор, пока ключ находится у пользователя, можно быть уверенным, что информация надежно защищена;
* код, хранимый на электронном ключе, генерируется случайным образом, имеет большую длину и является двоичным, что делает его подбор нереальной задачей;
* использование электронных ключей не требует запоминание сложного пароля;
* возможность доступа к защищенной информации может быть мгновенно заблокирована при извлечении электронного ключа, если такая опция указана. На основе этого можно организовать функцию «Красная кнопка»;
* при использовании в StrongDisk Server электронные ключи обеспечивают значительно более простой и надежный процесс аутентификации при удаленном управлении сервером.

## Особенности StrongDisk Server

Если StrongDisk Pro прекрасно подойдет отдельным пользователям, то для развертывания системы безопасного хранения данных в организации следует воспользоваться StrongDisk Server. При этом конфиденциальная информация хранится централизованно на защищенных дисках сервера, которые являются для сервера обычными локальными дисками. Для предоставления пользователям доступа к защищенным дискам, используются стандартные средства Windows (Sharing). При этом никто не может получить доступ к конфиденциальной информации, пока на сервере не подключен соответствующий защищенный диск. После того, как на сервере администратор подключит защищенный диск, введя нужный пароль и подключив соответствующие внешние ключи, общие сетевые ресурсы на дисках становятся доступными тем пользователям, которых администратор наделил необходимыми правами. То есть для доступа к ресурсам на защищенных дисках пользователи также должны указывать пароль, но не тот, который позволяет декодировать данные на защищенном диске, а пароль, который идентифицирует их как пользователей. В случае домена в Windows, это будет пароль, вводимый пользователем при входе в систему.

Все действия, связанные с предоставлением доступа к защищенным дискам, такие как отключение дисков, смена паролей и кодов, записанных на внешних ключах, производятся централизованно администратором. Обычные пользователи могут и не знать, что их данные хранятся на сервере в закодированном виде.

StrongDisk Server позволяет подключать и отключать защищенные диски на сервере удаленно, без использования консоли сервера. Для этого в комплект поставки включена программа «Удаленный администратор».

Установка на сервере StrongDisk Server, даёт уверенность в том, что злоумышленник, получивший доступ к локальной сети или непосредственно к серверу, не сможет прочитать файлы, содержащие конфиденциальную информацию. Более того, даже в случае похищения или изъятия сервера, доступ к файлам, защищенным с помощью StrongDisk Server, будет невозможен, так как вся информация на защищенных дисках хранится в закодированном виде.

То обстоятельство, что для хранения защищенного диска используется файл, позволяет несколько расширить сферу применения StrongDisk Server. Так, например, можно использовать его для защиты данных, отправляемых по электронной почте, пересылая файлы в формате StrongDisk как вложения.

Таким образом, российские разработчики программного обеспечения создали хороший продукт по защите информации от несанкционированного доступа — StrongDisk. Программа предельно проста в использовании, и в то же время она выполнена на высоком технологическом и профессиональном уровне.

## Продукты и решения

Существуют разные модификации продукта StrongDisk. О некоторых их них (Pro и Server) уже было сказано выше. Остальные представлены ниже:

### Решения для рабочих станций

* StrongDisk Pro Standard
  + все что необходимо для надежной защиты конфиденциальной информации на персональном компьютере, ноутбуке и сменных носителях;
  + поддержка электронных ключей на выбор;
  + безграничные возможности традиционного продукта для коммерческого использования;
* StrongDisk Pro Corporate
  + криптографическая защита информации на рабочих станциях и ноутбуках в корпоративной сети;
  + удаленная работы с защищенными дисками и криптографическими устройствами (электронными ключами и смарт-картами);
  + поддержка групповых операций;
  + контроль запуска приложений;
  + администраторский ключ.

### Решения для серверных систем

* StrongDisk Server
  + криптографическая защита информации при ее обработке и хранении на сервере;
  + сокрытие факта наличия защищенных данных на сервере;
  + экстренное реагирование на внешние угрозы;
* StrongDisk Server Standalone
  + защита корпоративных баз данных, почтовых приложений, бизнес-приложений, CRM-систем и любых других приложений;
  + блокирование прямого доступа пользователей.

## Активная защита

Система активной защиты StrongDisk объединяет модули экстренного реагирования для продуктов StrongDisk Server, StrongDisk Server Standalone и StrongDisk Corporate. Главной целью системы является защитить информацию в экстренной ситуации, а также удаленное администрирование систем защиты информации StrongDisk.

|  |  |  |
| --- | --- | --- |
| **Возможные ситуации** | **Возможные действия для серверной станции и любых выбранных защищенных дисков** | **Возможные действия для рабочей станции и любых выбранных защищенных дисков** |
| 1. Внезапное появление злоумышленников или посторонних в зоне физического доступа к серверным или рабочим станциям. 2. Необходимость управлять защищенными данными в условиях ограничения передвижения. 3. Необходимость управлять защищенными данными в удалении от рабочего места администратора или вне офиса (вне города, страны, континента). | 1. Отключение дисков. 2. Подключение дисков. 3. Уничтожение ключа/заголовка диска. 4. Уничтожение диска. 5. Подмена дисков на ложные. 6. Запуск или остановка любых приложений, скриптов. 7. Отправка сигнала тревоги по локальной сети для других серверных или рабочих станций. 8. Отправка отчета о срабатывании конкретного сценария. 9. Перезагрузка станции. 10. Выключение станции. | 1. Отключение дисков. 2. Подключение дисков. 3. Уничтожение ключа/заголовка диска. 4. Уничтожение диска. 5. Подмена дисков на ложные. 6. Запуск или остановка любых приложений, скриптов. 7. Отправка отчета о срабатывании конкретного сценария. 8. Перезагрузка станции. 9. Выключение станции. |

## Удаление файлов

Когда файл удаляется стандартными средствами Windows, он помечается как удалённый и считается системой несуществующим, однако, его содержимое по-прежнему остается на диске до тех пор, пока на его место не запишутся новые файлы. Таким образом, злоумышленники, захватив жёсткий диск, смогут получить доступ к секретным файлам, даже если они были удалены, и «Корзина» была очищена. Поэтому при работе с конфиденциальной информацией удаление файлов с обычных дисков, используя стандартные средства, является недопустимым.

Утилита Burner, входящая в комплект поставки StrongDisk, предназначена для уничтожения файлов без возможности их восстановления. Эта утилита забивает место на диске, которое занимал файл, случайными данными, то есть при восстановлении файла в нём будет «информационный мусор».

Также Burner содержит функцию затирания «хвостов» файлов и затирания свободного места на диске. Дело в том, что минимальной единицей размещения информации на жёстком диске является кластер. Размер кластера зависит от объёма жёсткого диска и файловой системы. Файл всегда занимает некоторое целое количество кластеров. Иными словами, если размер кластера равен 512 байт, а размер файла — 520 байт, то файлу выделятся два кластера. Оставшееся место кластера, которое выделено файлу, но не используются им, называется «хвостом» файла. В «хвосте» файла может содержаться конфиденциальная информация, даже если сам файл удален. Чтобы предотвратить утечку конфиденциальной информации, остающейся в «хвостах» файлов, в утилите Burner существует опция «Затирать хвосты файлов». Если эта опция включена, то Burner надёжно удаляет не только сам файл, но и его «хвост», после чего никакую информацию из файла восстановить будет невозможно.

Опция затирания свободного места на диске утилиты Burner может быть полезна в том случае, когда было удалено несколько конфиденциальных файлов или папок на жёстком диске стандартными средствами Windows, после чего стало необходимым обеспечить невозможность их восстановления. При работе в режиме затирания свободного места на диске утилита Burner проходит по всему жёсткому диску, заполняя случайными данными те области, которые обозначены системой как свободные. Таким образом, восстановление недавно удалённых с этого диска файлов становится невозможным.