Более 100 000 пользователей в России выбрали Secret Disk!

Безопасность

- Защита сеанса загрузки операционной системы: для загрузки операционной системы пользователь должен подключить свой eToken и ввести его PIN-код.
- Двухфакторная аутентификация: для доступа к зашифрованной информации пользователь должен подключить свой eToken и ввести его PIN-код.
- Отключенные защищаемые диски выглядят в системе как неформатированные.
- Поддержка «спящего» режима с сохранением образа оперативной памяти в зашифрованном виде. Помимо файлов спящего режима Secret Disk 4 защищает файл подкачки и дампы памяти, сохраняемые на диск операционной системой.
- Блокирование компьютера в перерывах между работой и возможность автоматического отключения защищенных дисков при отсоединении eToken.

Надежность

- Защита от программных и аппаратных сбоев во время выполнения операций шифрования, включая перебои электропитания.
- Защита от случайного / умышленного уничтожения или повреждения защищенных данных.
- Аварийное восстановление главной загрузочной записи (Master Boot Record) с использованием специального загрузочного Rescue CD.
- Резервное копирование / восстановление ключей шифрования.
- Возможность использования алгоритмов шифрования AES-128, AES-256 и Twofish-256 после установки бесплатного пакета Secret Disk Crypto Pack.
- Возможность использования российских сертифицированных криптопровайдеров КриптоПро CSP, Signal-COM CSP, Infotecs CSP.

Удобство

- Фоновое шифрование: операции зашифрования, расшифрования и перешифрования дисков проводятся в фоновом режиме с возможностью приостановки и дальнейшего продолжения выполнения этих операций, что позволяет быстро ввести систему в эксплуатацию.
- Прозрачность для приложений: работа с Secret Disk не требует перенастройки ПО и смены привычек пользователя, с любыми приложениями можно работать как обычно.
- Многопользовательская работа: несколько пользователей (каждый со своим eToken) могут загружать ОС с защищенного системного раздела и получать доступ к своим зашифрованным дискам.
- Гибкость настроек Secret Disk 4 позволяет найти разумный баланс между удобством работы и обеспечением необходимого уровня безопасности.
- Быстрый ввод в эксплуатацию: в составе операционной системы Windows уже есть поставщик криптографии, который поддерживается Secret Disk. Таким образом сразу после установки продукт готов к работе.
- Режим энергосбережения для ноутбуков – операции шифрования, перешифрования и расшифрования диска приостанавливаются, если ноутбук переходит на питание от внутренних батарей. При возобновлении питания от сети приостановленный процесс автоматически продолжится.
- Полная интеграция в Windows 2000, XP, Vista, 7.

Сертификация

Secret Disk 4 сертифицирован ФСТЭК России(сертификат №1742 от 24 декабря 2008 года) на соответствие Заданию по безопасности и имеет оценочный уровень доверия ОУД1 (усиленный) в соответствии с требованиями руководящего документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», (Гостехкомиссия России, 2002). Secret Disk 4 может использоваться при создании автоматизированных систем до класса защищенности 1Г включительно, а также ИСПДн до класса 2 включительно.

Secret Disk® более 10 лет на рынке!

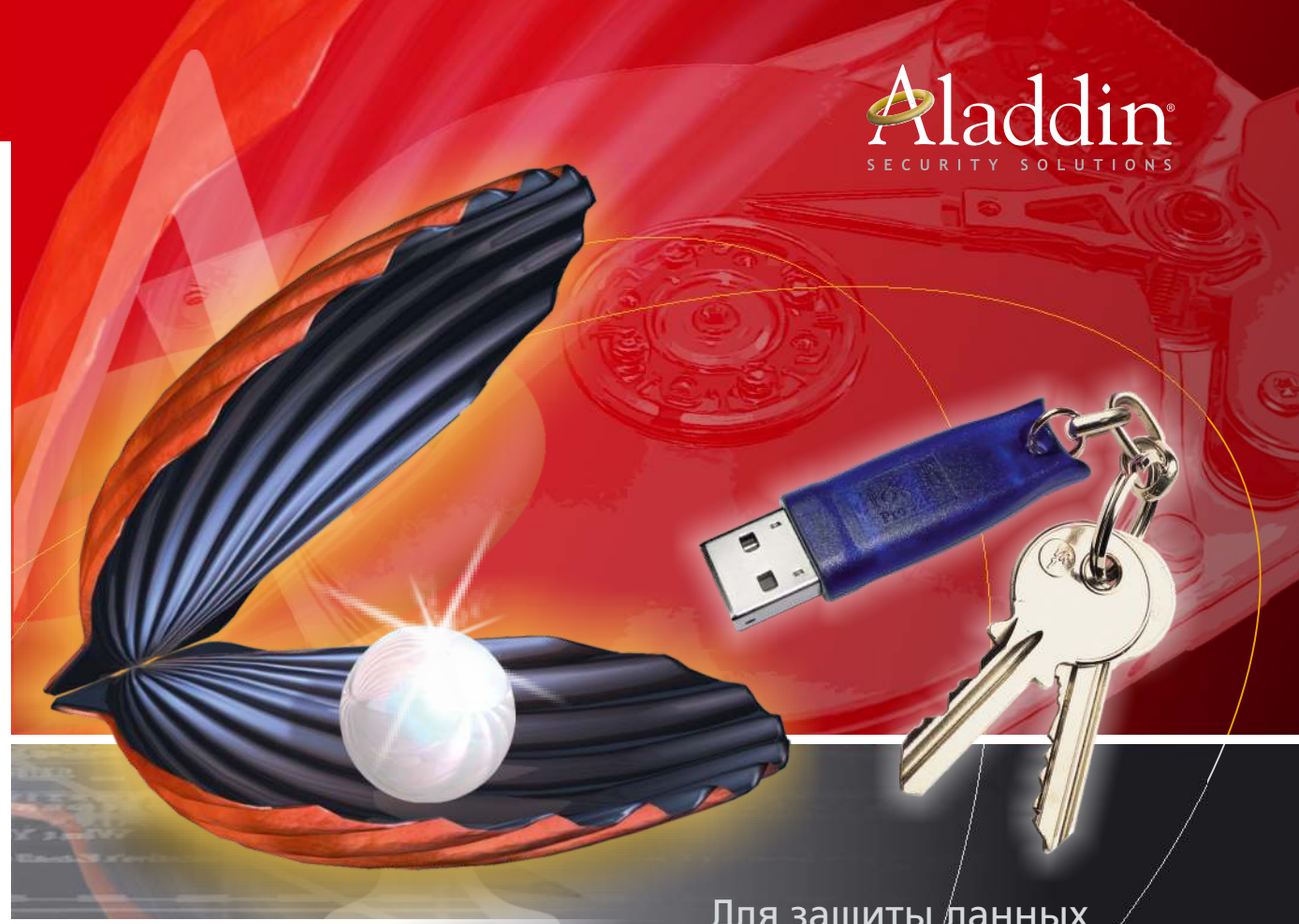
- Secert Disk 4 занял первое место в открытом конкурсе «Продукт года – 2007» в номинации «Защита Информации»
- «Продукт года-2003» - диплом и памятный знак от Аппарата Совета Безопасности РФ, Комитета Государственной Думы по безопасности за разработку Secret Disk NG - высокотехнологичного программно-аппаратного средства защиты конфиденциальной информации
- Лучший инновационный продукт MIPS'2001
- Победитель конкурса «КомпьюЛог-Экономика'2000»
- Победитель конкурса «Бизнес-Софт'99»
- Золотая медаль ВДНХ (ВВЦ)

ID: 02964-0609

Aladdin SECURITY SOLUTIONS
© 2009, Aladdin Software Security R.D.
Тел.: (495) 223-0001
E-mail: aladdin@aladdin.ru
Web: www.aladdin.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (продлены до 18.02.13)
Лицензии ФСБ России № 2683Р от 02.09.05, №№ 4205П, 4206Х, 4207Р от 22.06.07 и № 4898П от 14.12.07
Microsoft Certified Partner, IBM Business Partner, Oracle Business Partner

Microsoft CERTIFIED Partner



Aladdin SECURITY SOLUTIONS

Для защиты данных

Система защиты

конфиденциальной информации и персональных данных для Microsoft® Windows® 2000 / XP / Vista / 7

Secret Disk® 4

- Загрузка компьютера только с электронным ключом
- Защита системного раздела
- Шифрование пользовательских данных и съемных носителей
- Прозрачная работа для пользователя
- Соответствие требованиям ФСТЭК по защите персональных данных

Secret Disk® 4

Система защиты конфиденциальной информации и персональных данных для Microsoft® Windows® 2000 / XP / Vista /7

Утечка информации о клиентах и поставщиках, финансовых потоках, планах развития может стать для компании причиной многих бед и нанести бизнесу значительный ущерб.
Защищая информацию, Вы защищаете свой бизнес.

Назначение

- Защита от несанкционированного доступа и раскрытия конфиденциальной информации, хранящейся и обрабатываемой на персональном компьютере или ноутбуке.
- Защита информации при переносе и хранении на съемных носителях.
- Разграничение прав пользователей на доступ к защищенной информации с использованием надежной двухфакторной аутентификации (владение электронным ключом eToken и знание PIN-кода).

Возможности

- Защита системного раздела, шифрование разделов на жестких дисках, томов на динамических дисках, виртуальных дисков и съемных носителей (USB-диски, Flash-диски, ZIP-диски, различные карты памяти и т. п.).
- Аутентификация пользователя по USB-ключу eToken как для загрузки операционной системы, так и для доступа к зашифрованным данным.
- Запрет доступа по сети к зашифрованным данным для всех пользователей, включая системного администратора.
- Восстановление доступа к данным в случае утери eToken.
- Сохранность защищенных данных при внезапном отключении питания.
- Поддержка режима энергосбережения для ноутбуков.

eToken®

USB-ключи eToken – персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП.

Поддерживаемые модели USB-ключей и смарт-карт:

- eToken PRO / 32K, 64K, 72K (Java).
- eToken NG-FLASH, имеет встроенную Flash-память объемом до 4ГБ.
- eToken NG-OTP имеет встроенный генератор одноразовых паролей.

Когда необходим Secret Disk 4

- **При работе на ноутбуке**
  Утеря или кража ноутбука, несанкционированное использование посторонними лицами (во время деловых поездок, на отдыхе или в домашних условиях).
- **При работе на персональном компьютере в офисе**
  Несанкционированный доступ к данным по локальной сети или неправомерное использование посторонними лицами во время отсутствия пользователя на рабочем месте.
- **Компьютер передается на сервисное обслуживание**
  Несанкционированный доступ к данным во время проведения ремонтных и сервисных работ внутренней IT-службой или внешней сервисной компанией.
- **Конфиденциальная информация переносится или пересылается на съемных носителях**
  Утеря или кража носителей.
- **Необходимо обеспечить выполнение требований Федерального закона о персональных данных №152-ФЗ от 27 июля 2006 г.**
  Нарушение конфиденциальности персональных данных, которые хранятся и обрабатываются на персональных компьютерах в организации.

«Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных».
ФЗ о персональных данных от 27 июля 2006 г. №152-ФЗ, Статья 7. Конфиденциальность персональных данных.

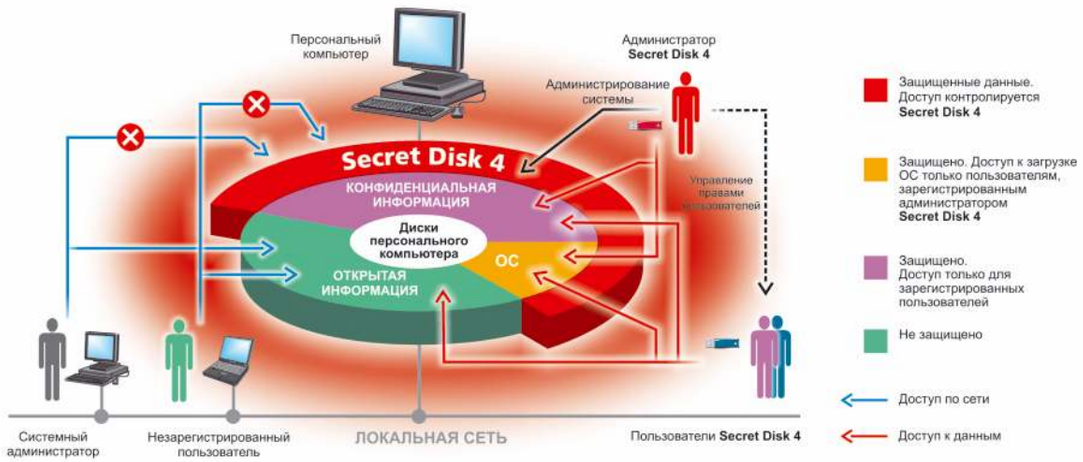
«Каждый десятый ноутбук становится жертвой воров, а каждый пятый – хозяин теряет сам».
Gartner Group, 2007

«Офисные служащие боятся сокращений и смогут ради работы пожертвовать любыми нормами морали. 46% опрошенных готовы скопировать себе ценную корпоративную информацию - базы данных, планы развития и т.д. - и будут использовать её как козырь при поисках новой работы».
Cyber-Ark, 2008

Линейка продуктов Secret Disk

- Персональная версия – Secret Disk 4
- Редакция Secret Disk 4 Workgroup Edition
- Серверная версия для файловых серверов и серверов приложений – Secret Disk Server NG
- Сертифицированные версии Secret Disk 4, Secret Disk NG и Secret Disk Server NG

Как работает Secret Disk 4



Данные, хранящиеся на зашифрованных дисках персонального компьютера, доступны только администратору безопасности и пользователям, владеющими eToken и зарегистрированными в Secret Disk 4. Остальные пользователи, включая системного администратора, не могут получить доступ к зашифрованным данным, а наличие лицензии Secret Disk 4 Workgroup Edition позволит организовать работу в сети с защищенными дисками для небольших групп пользователей.

Особенности Secret Disk 4

Защита системного раздела жесткого диска

Системный раздел жесткого диска содержит большое количество информации, представляющей особый интерес для хакеров, конкурентов или инсайдеров.

Например, в системном разделе хранятся учетные записи пользователей, логины и пароли к различным информационным ресурсам, электронная почта, лицензионная информация используемых программ и т.д.

Злоумышленники могут получить все эти данные, анализируя временные файлы ОС, файлы подкачки, файлы-журналы приложений, дампы памяти, а также образ, сохраняемый на диск при переходе системы в «спящий» режим.

Secret Disk 4, в отличие от многих конкурентов позволяет защитить системный раздел, а также хранящуюся на нем информацию.

Загрузка операционной системы по ключу eToken

Получив доступ к персональному компьютеру, злоумышленник или недобросовестный сотрудник может использовать его для получения доступа к закрытым ресурсам (например, к корпоративным серверам или платежной системе пользователя).

Стандартные средства авторизации Windows не могут надежно ограничить загрузку и работу в операционной системе. Использование eToken для аутентификации пользователей до загрузки ОС гарантирует доступ к компьютеру только доверенных лиц.

Secret Disk 4 предоставляет наиболее безопасную и надежную на сегодняшний день процедуру подтверждения прав пользователя – необходимо не только наличие USB-ключа но и знание PIN-кода для загрузки операционной системы.

Прозрачное шифрование

Операции начального зашифрования или полного перешифрования для современных дисков большого объема могут потребовать значительного времени, что может создать определенные неудобства для пользователя.

В Secret Disk 4 все операции зашифрования, перешифрования и расшифрования проводятся в фоновом режиме. Во время выполнения этих операций диск полностью доступен для работы, что дает возможность использовать компьютер не дожидаясь окончания процесса зашифрования.

Восстановление доступа к зашифрованным дискам

Злоумышленник не сможет получить доступ к компьютеру в обход системы Secret Disk. Если же добросовестный пользователь потерял или сломал eToken, то восстановить доступ к данным можно, если администратор Secret Disk заранее позаботился о сохранении в надежном месте резервной копии мастер-ключей шифрования.