Технические решения по защите персональных данных с использованием продуктов компании Аладдин Р.Д.

Мороз Константин

Консультант по продуктам и решениям

Лето. Москва

Зачем нужны продукты Аладдин ?

- Массовые утечки информации
- Требования закона о Защите ПД (ФЗ-152)
- Требования регуляторов (ФСБ, ФСТЭК) к государственным организациям
- «Мобильность» сотрудников офисов
- Кражи ноутбуков и внешних носителей
- Ужесточение конкуренции, кражи конфиденциальной информации (баз данных клиентов)
- Возросшее количество угроз со стороны интернета

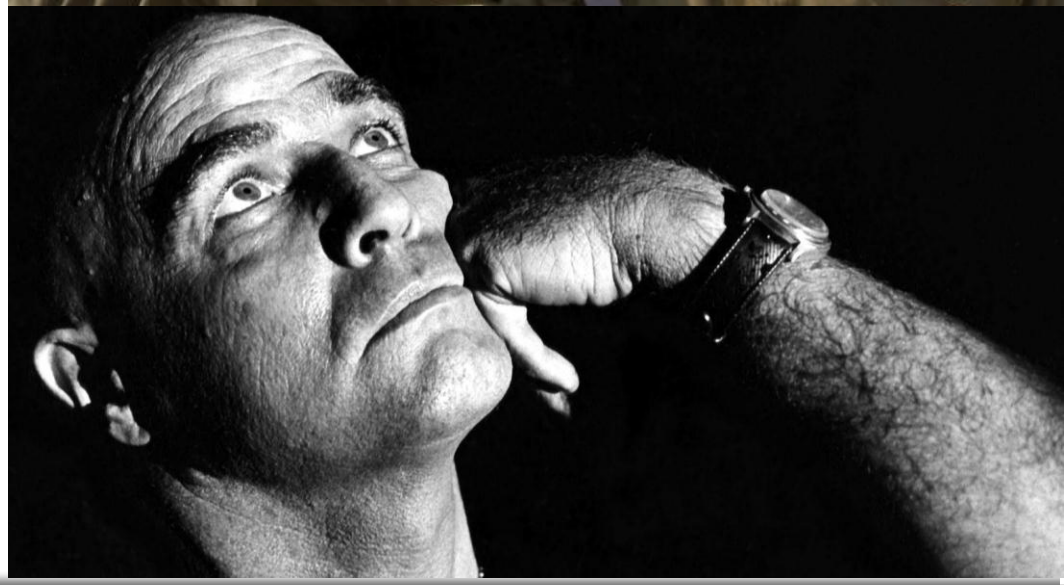
Актуальные задачи по обеспечению ИБ

- **Безопасный доступ к сети**:
  - Строгая аутентификация пользователей, одноразовые пароли
  - Организация защищенного удаленного доступа (VPN)
  - Решение проблемы «слабых» и «золотых» паролей
  - К защищенным Web - ресурсам
- **Безопасность данных:**
  - Защита конфиденциальной информации и ПДн
  - Защита серверов и рабочих станций от НСД
  - Электронно-цифровая подпись (ЭЦП)
  - Безопасная электронная почта
- **Хранение ключевой информации**
- **Контроль доступа в помещение**


PASSPORT CONTROL
CUSTOMS
REISEPASS

Что может eToken?

- Защитить деньги
- Сохранить секреты
- Разгрузить мозг
- Сэкономить время



Задачи решаемые eToken

Строгая аутентификация пользователей

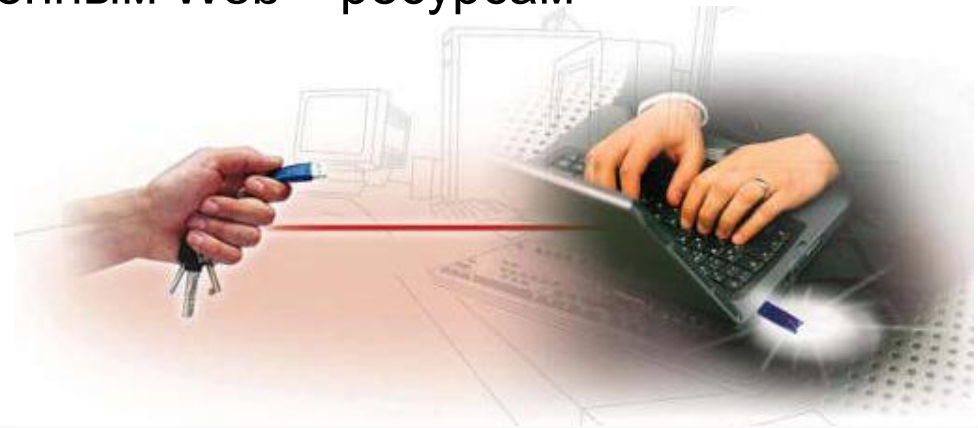
Терминальный доступ, тонкие клиенты

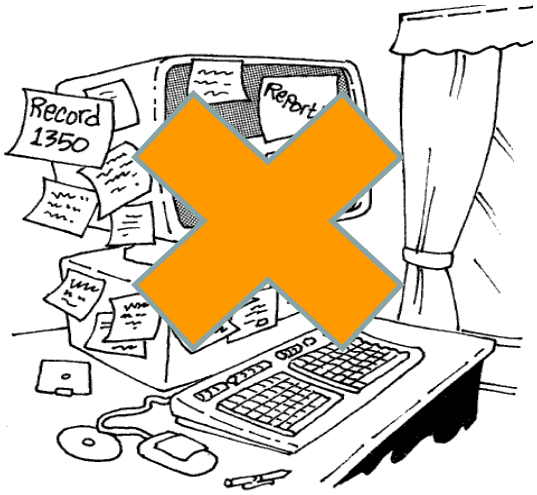
Организация защищенного удаленного доступа (VPN)

Использование одноразовых паролей

Решение проблемы «слабых» и «золотых» паролей

К защищенным Web – ресурсам





Задачи решаемые eToken

Хранение ключевой информации

Электронно-цифровая подпись (ЭЦП)

Безопасная электронная почта

Контроль доступа в помещение

Может использоваться в качестве единого устройства доступа

Модельный ряд eToken

eToken PASS

eToken Pro Java/ГОСТ

eToken NG-Flash

eToken Pro Smartcard

eToken NG-OTP

Сертифицированный eToken

- Электронный ключ eToken – средство аутентификации и хранения ключевой информации пользователей
- Сертифицированы все модели электронных ключей eToken
- Сертификат соответствия ФСТЭК России №1883 от 11 августа 2009 г.

- Следует использовать:
  - Для **создания АС**, обрабатывающих конфиденциальную информацию, до класса защищенности **1Г включительно**
  - Для использования в ИСПДн до **1 класса включительно**

- Входит в состав комплектов поставки сертифицированных версий ОС Microsoft Windows

eToken ГОСТ

- Назначение
  - Персональное средство криптографической защиты информации для формирования Электронной подписи по **ГОСТ Р 34.10-2001** с **неизвлекаемым закрытым ключом**
- Особенности
  - Возможность работы на разных платформах
  - Наличие нескольких вариантов исполнения
  - Наличие комплекта разработчика

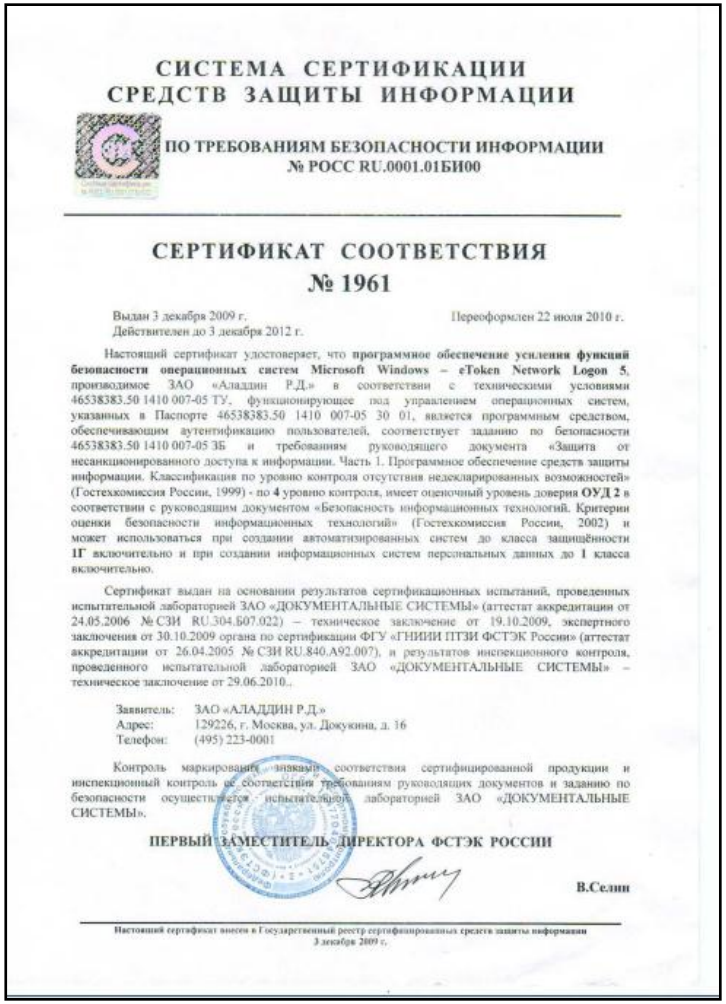
- Применение eToken ГОСТ
  - в системах ДБО (дистанционного банковского обслуживания);
  - для Web-сервисов, где требуется усиленная аутентификация пользователей и квалифицированная ЭЦП документов;
  - в системах электронных торгов;
  - в системах сдачи электронной отчетности через Интернет и др.
- Сертификация
  - Сертификат ФСБ № СФ/124-1671 от 11 мая 2011 г. по уровням КС1 и КС2

eToken Network Logon

- Усиление функций парольной безопасности ОС Microsoft Windows
- Двухфакторная аутентификация (eToken + PIN-код)
  - На локальном компьютере
  - В домене Microsoft Windows

Автоматическая блокировка рабочей станции **при отсоединении eToken**

ПО eToken Network Logon



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 1961

Выдан 3 декабря 2009 г. Переоформлен 22 июля 2010 г.
Действителен до 3 декабря 2012 г.

Настоящий сертификат удостоверяет, что **программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5**, производимое ЗАО «Аладдин Р.Д.» в соответствии с техническими условиями 46538383.50 1410 007-05 ТУ, функционирующее под управлением операционных систем, указанных в Паспорте 46538383.50 1410 007-05 30 01, является программным средством, обеспечивающим аутентификацию пользователей, соответствует заданию по безопасности 46538383.50 1410 007-05 3Б и требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 4 уровню контроля, имеет оценочный уровень доверия **ОУД 2** в соответствии с руководящим документом «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Гостехкомиссия России, 2002) и может использоваться при создании автоматизированных систем до класса защищённости **1Г** включительно и при создании информационных систем персональных данных до **1** класса включительно.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 24.05.2006 № СЗИ RU.304.507.022) – техническое заключение от 19.10.2009, экспертного заключения от 30.10.2009 органа по сертификации ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.A92.007), и результатов инспекционного контроля, проведенного испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» – техническое заключение от 29.06.2010..

Заявитель: ЗАО «АЛАДДИН Р.Д.»
Адрес: 129226, г. Москва, ул. Докукина, д. 16
Телефон: (495) 223-0001

Контроль маркированных знаком соответствия сертифицированной продукции и инспекционный контроль за соответствием требованиям руководящих документов и заданию по безопасности осуществляется испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ».

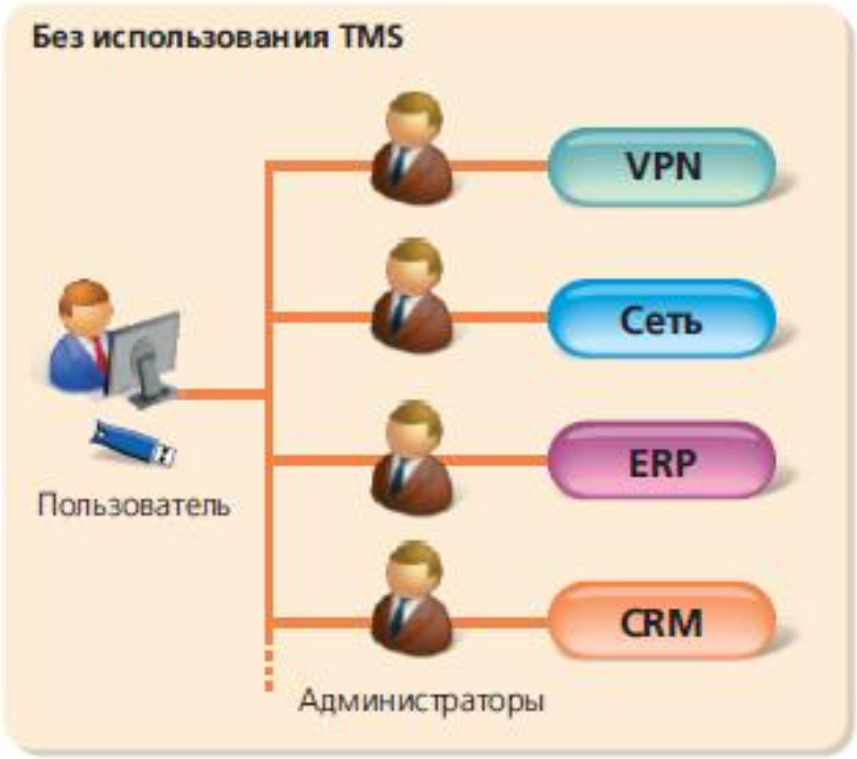
ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

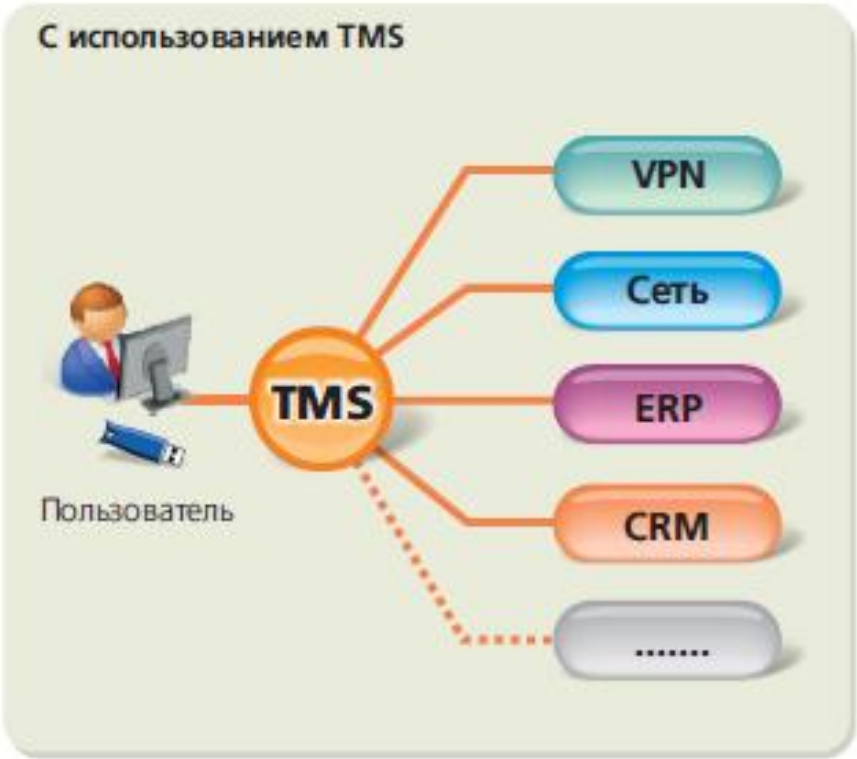
В.Селин

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
3 декабря 2009 г.

- Сертификат ФСТЭК России №1961 от 03.12.2009 г.
  - Для **создания АС**, обрабатывающих конфиденциальную информацию, **до класса защищенности 1Г включительно**
  - Для использования в **ИСПДн** до **1 класса включительно**

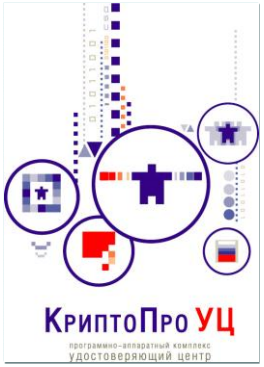
Централизованное администрирование и управление доступом





Основные возможности eToken TMS

- Поэкземплярный учет и регистрация ключей eToken
- Ускорение ввода ключей в эксплуатацию
- Управление жизненным циклом ключей eToken
- Аудит использования ключей eToken
- Техническая поддержка пользователей
- Подготовка отчетов
- Самообслуживание пользователя
- Управление классическими паролями
- Поддержка УЦ
  - УЦ “Крипто Про УЦ”, УЦ “RSA Keon”, Microsoft CA



Сертифицированная версия eToken TMS

- Назначение
  - Централизованное управление средствами аутентификации и хранения ключевой информации – eToken
- Особенности
  - Поддержка всей линейки электронных ключей eToken
  - Поддержка российских УЦ
- Сертификат ФСТЭК России №1700 от 16.10.2008 г.
  - Для создания АС, обрабатывающих конфиденциальную информацию, до класса защищенности **1Г включительно**
  - Для использования в ИСПДн до **2 класса включительно**
- Применение eToken TMS
  - Управление жизненным циклом средств аутентификации
  - Централизованное администрирование
  - Подготовка детализированных отчетов
  - Возможность самостоятельного решения пользователями проблем, возникающих в процессе использования средств аутентификации
  - Отказоустойчивость и масштабируемость системы

Система управления TMS

Способы потерять информацию

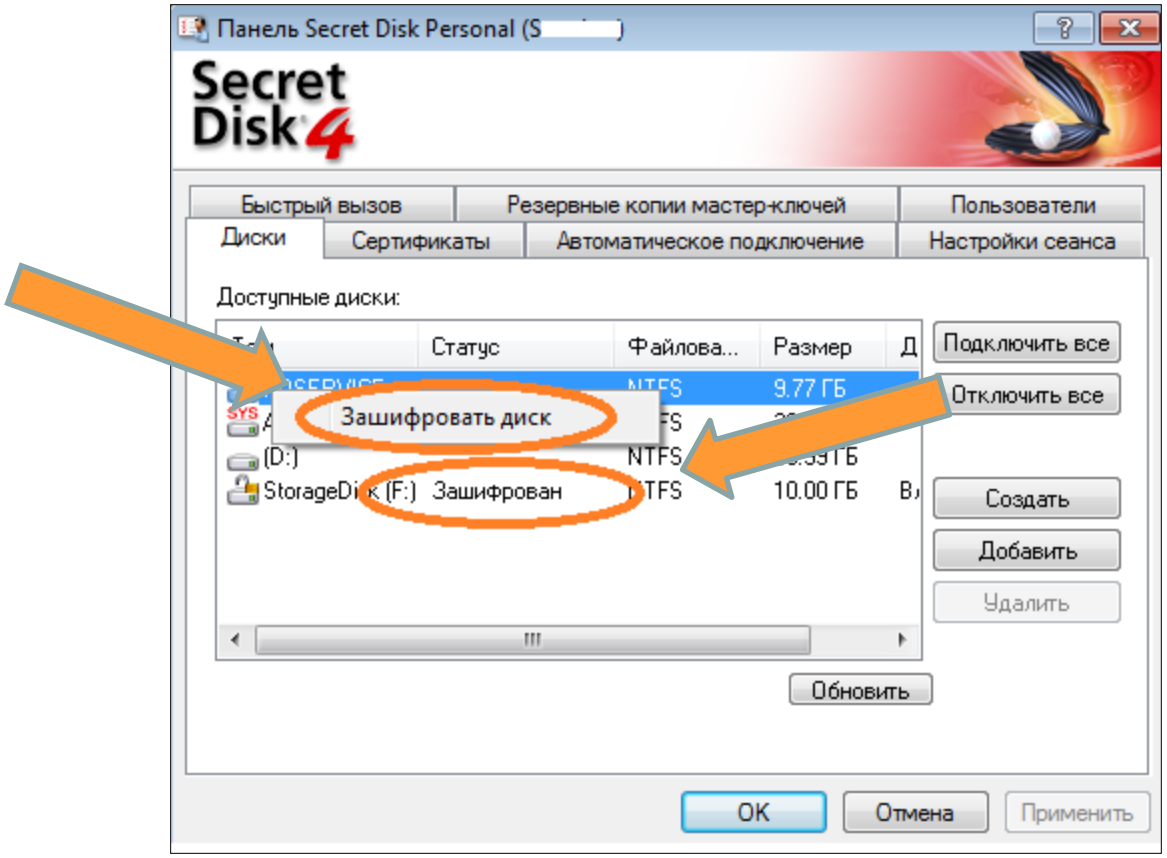
Как защититься?

099(4A008ge248J%6sn6e@7Pn4vj=
SO93ES)4SM141b423x21U13y0@H

Решение

Шифрование

Самый простой и надежный метод защиты



Линейка продуктов Secret Disk

Защита данных на рабочих станциях, ноутбуках и съёмных носителях

От несанкционированного доступа и …

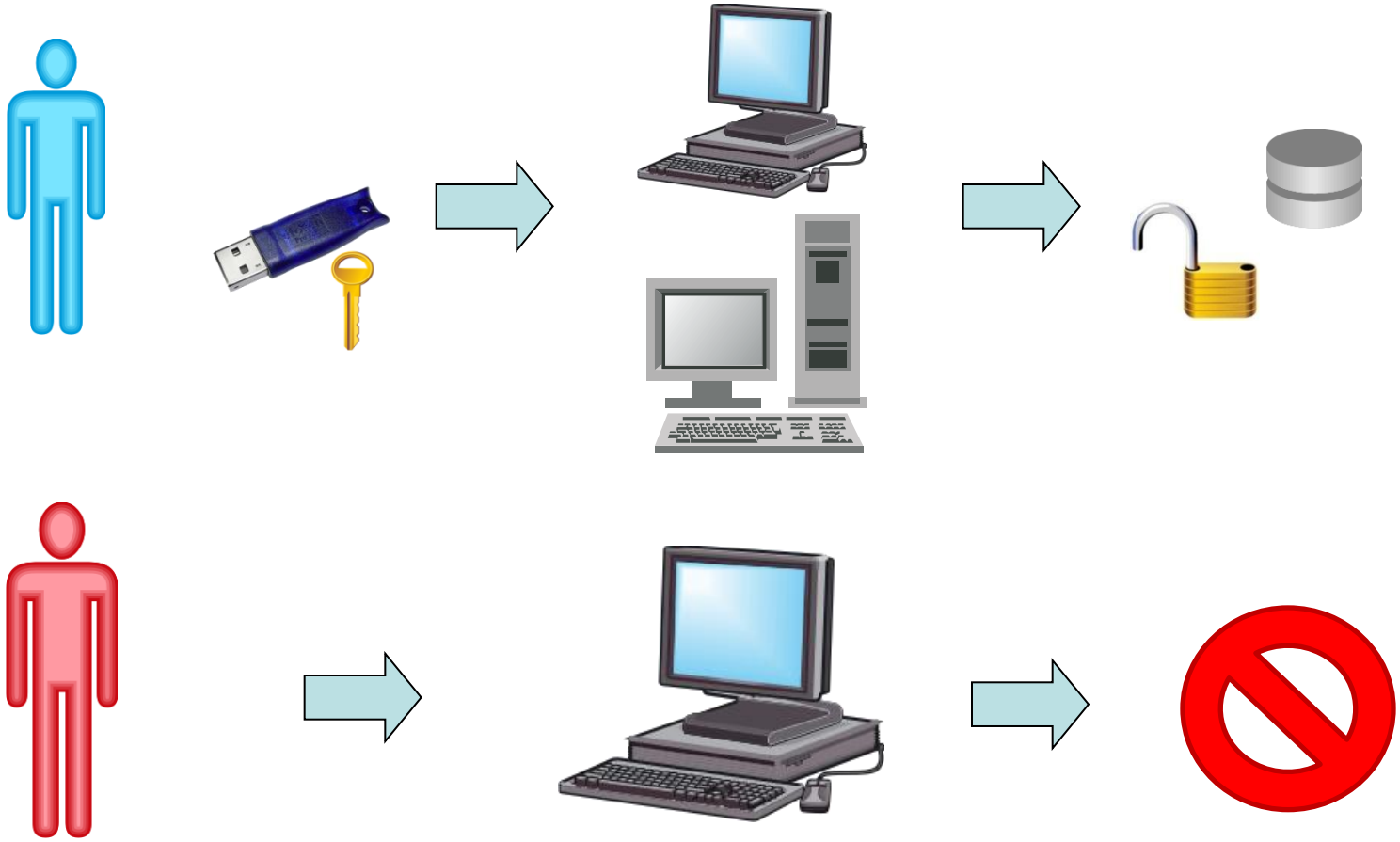
Secret Disk 4

Secret Disk 4 Workgroup Edition

Кому в необходим Secret Disk

- Руководство компании
- Топ менеджмент
- Бухгалтерам
- Финансисты
- Кадровики
- …
- …

Логика работы Secret Disk



Доступ к зашифрованным данным может получить только **авторизованный** пользователь

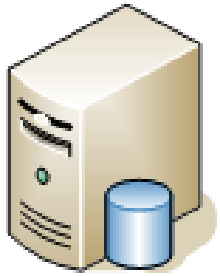
ПАК Secret Disk 4

- Назначение
  - Реализация разрешительной системы допуска к информационным ресурсам рабочей станции пользователя
  - Разграничение доступа к информационным ресурсам
  - Защита от НСД к информации на рабочей станции
- Особенности
  - Контроль начальной загрузки ОС, аутентификация пользователя до загрузки ОС
  - Двухфакторная аутентификация доступа к информационным ресурсам (eToken + пароль)
  - Защита от НСД информации на жёстких дисках рабочей станции, а также съёмных носителях
  - Поддержка сертифицированных ФСБ России СКЗИ (КриптоПро CSP, Сигнал-ком CSP, Инфотекс CSP)
  - Запрет сетевого доступа к данным
- Сертифицированная версия
  - Сертификация производства (сертификат соответствия ФСТЭК России №1742/1 от 06.05.2010 г.)
  - Оценочный уровень доверия ОУД1+
  - Может использоваться при проектировании АС до класса защищённости 1Г включительно и ИСПДн до 2 класса включительно

SECRET DISK® SERVER NG New Generation

Область применения Secret Disk Server

Защита шифрованием конфиденциальной информации и персональных данных на серверах



и её сокрытие

Возможности Secret Disk Server NG

- **Шифрование** данных на логических дисках **HDD, RAID, SAN,** создание виртуальных зашифрованных дисков

- **Контроль доступа** к зашифрованным дискам по сети

- **Аутентификация администраторов** с использованием **eToken**

Особенности Secret Disk Server NG

Экстренное предотвращение

несанкционированного **доступа** к данным

- **Гибкая** система подачи сигнала **«Тревога»**
  - Красная кнопка
  - Радио-брелок
  - GSM-модуль
- Поддержка **скриптов**

Особенности Secret Disk Server NG

- **Удаленное управление** несколькими **серверами**
- Возможность регистрации **нескольких администраторов**

- **Два режима** экстренного **отключения** дисков
- **Несколько точек** подачи сигнала **«Тревога»**

ПАК Secret Disk Server NG 3.2

- Назначение
  - Защита конфиденциальных данных на серверах с использованием шифрования и контроля сетевого доступа

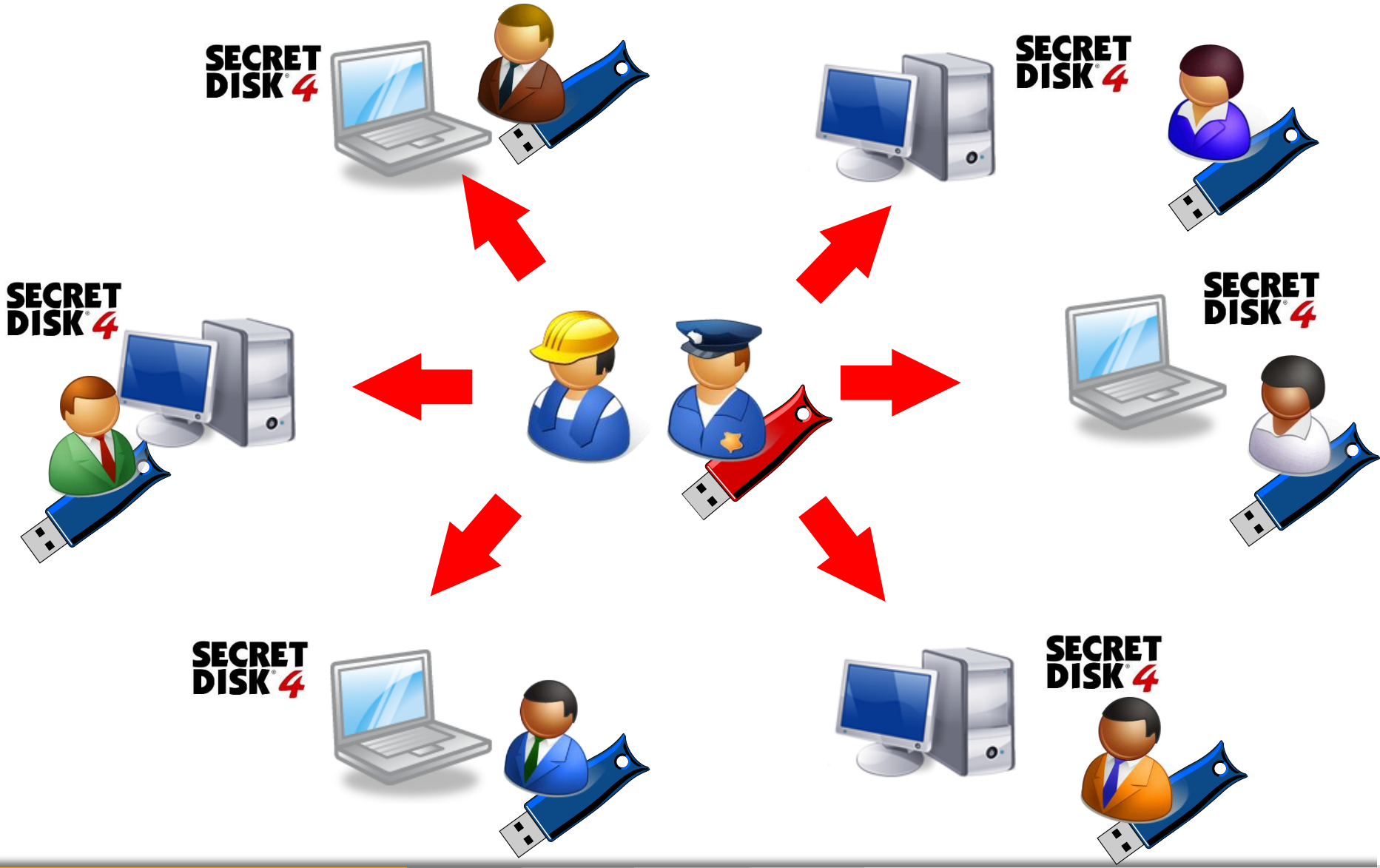
- Особенности
  - Двухфакторная аутентификация (eToken + пароль)
  - Поддержка российской криптографии
  - Контроль сетевого доступа к данным

- Сертифицированная версия
  - Сертификация производства во ФСТЭК РФ (сертификат ФСТЭК РФ №1487 от 02.11.2007 г.)
  - На соответствие 3Б («Общие Критерии»)
  - На отсутствие НДВ (по 4 уровню контроля)
  - Может использоваться при проектировании АС до класса защищённости 1Г включительно и ИСПДн до 1 класса включительно

Secret Disk® Enterprise

Корпоративная система защиты конфиденциальной информации с централизованным управлением

До Secret Disk Enterprise …



До Secret Disk Enterprise …

Secret Disk очень сложен для меня, там столько кнопок, кнопочек и функций, для чего они нужны…

Максимально простой пользовательский интерфейс для неспециалистов в IT

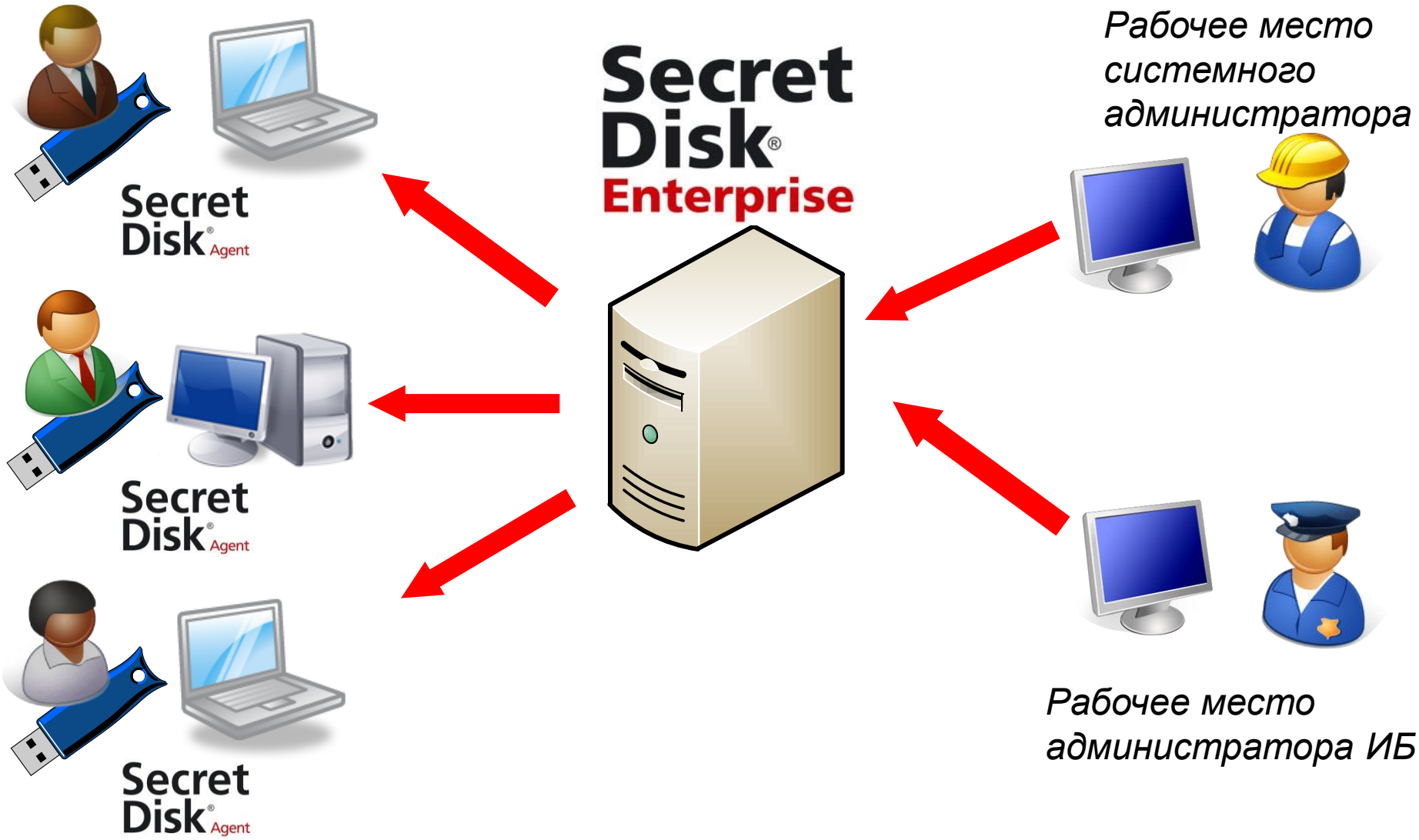
У нас уже не хватает времени и сил устанавливать и конфигурировать SD вручную на каждом компьютере, делать резервные копии всех ключей шифрования

Централизованное управление установкой, настройками и конфигурацией, обслуживание, аудит

А я сам себе зашифровал диск, а пользоваться не понимаю…

Ролевая модель, пользователь не должен иметь возможность изменять настройки или конфигурацию ПО, а также создать ситуацию, грозящую потерей данных

Secret Disk Enterprise – наводим порядок!



Назначение

Система Secret Disk Enterprise предназначена для решения в масштабе предприятия следующих задач:

- Защита информации от несанкционированного доступа, обеспечение конфиденциальности информации, хранящейся и обрабатываемой на серверах, персональных компьютерах и ноутбуках
- Централизованное управление защищенными ресурсами и доступом к ним
- Разграничение прав доступа, исключающее несанкционированный доступ к защищенным данным даже системных администраторов

Возможности

- Защита данных на системных, логических и виртуальных дисках
- Аутентификация пользователя до загрузки операционной системы по USB-ключу или смарт-карте
- Поддержка различных алгоритмов шифрования данных, в т.ч. по ГОСТ 28147-89 из состава КриптоПро CSP
- Аутентификация доступа по электронному ключу eToken — обеспечение надежной двухфакторной аутентификации

Возможности

- Управление настройками, мониторинг работоспособности и диагностика состояния клиентского ПО на каждом рабочем месте
- Работа с защищенными данными вне корпоративной сети — сотрудник, уехавший в командировку, может продолжать работать с этими данными на своем ноутбуке
- Гибкая ролевая модель: наличие предопределенных ролей, возможность их настройки и создание новых
- Аудит использования защищенных ресурсов

Ролевая модель

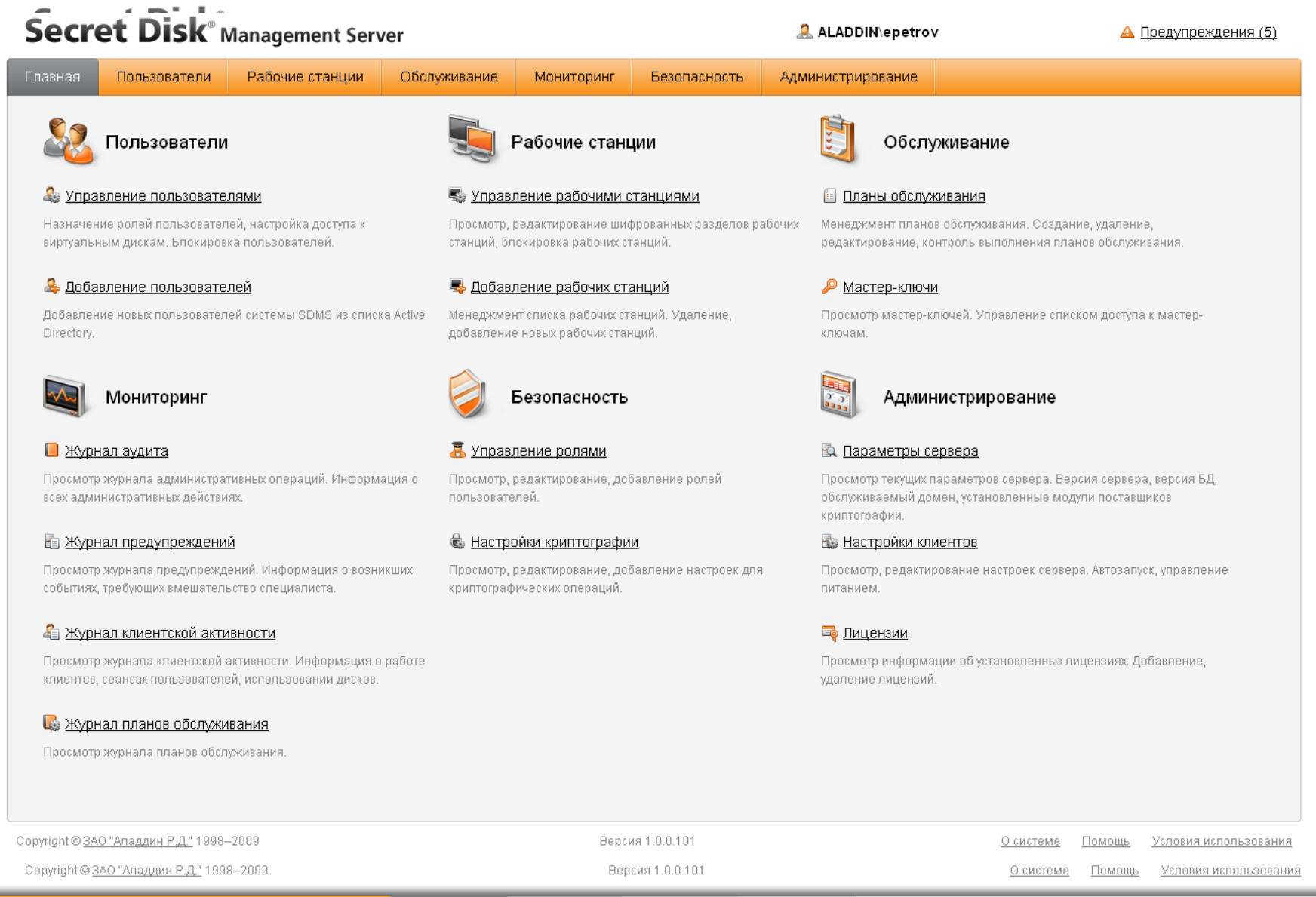
- **Встроенные роли**
  - Оператор
  - Администратор информационной безопасности
  - Аудитор
  - Пользователь
  - Агент восстановления ключей
  - Инженер по обслуживанию

- **Роли, определяемые заказчиком**
  - Позволяют гибко настроить продукт в соответствии с действующей на предприятии политикой ИБ

Мониторинг и аудит

- Четыре журнала:
  - Журнал аудита
  - Журнал предупреждений
  - Журнал клиентской активности
  - Журнал планов обслуживания
- Группировка событий
- Просмотр событий на конкретной рабочей станции
- Журналы событий хранятся в БД Microsoft SQL – можно строить свои отчёты или подключить источник к корпоративной системе мониторинга

Административный Web-портал



Secret Disk Enterprise как SD4 только …

- ✓**Централизованное**
  - Развертывание
  - Управление конфигурацией рабочих мест
  - Аудит
- ✓**Логирование действий** с защищенными объектами
- ✓**Защита от пользователей**
- ✓**Разделение ролей** управления системой

Secret Disk защищает

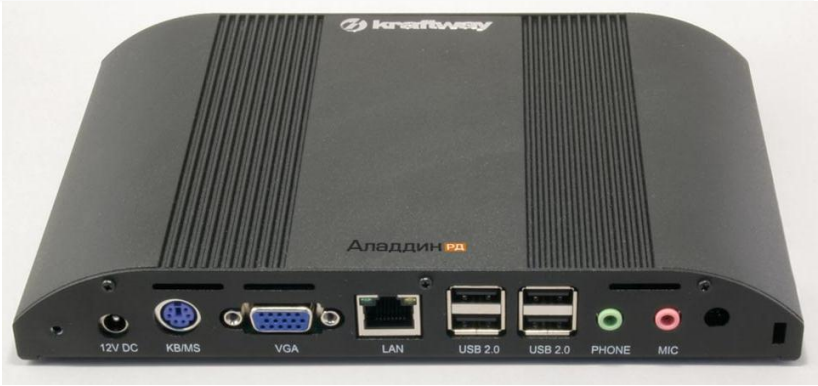
Конфиденциальность любой информации
Хранящейся и обрабатываемой на




Бизнес и Личную жизнь

Современные информационные риски

Trusted Security Module



Для противодействия современным угрозам и соответствия уровню развития техники, а так же для максимального удобства использования и управления средствами защиты компаниями **Kraftway, Fujitsu** и **ЗАО «Аладдин Р.Д.»** был разработан Защищенный компьютер:

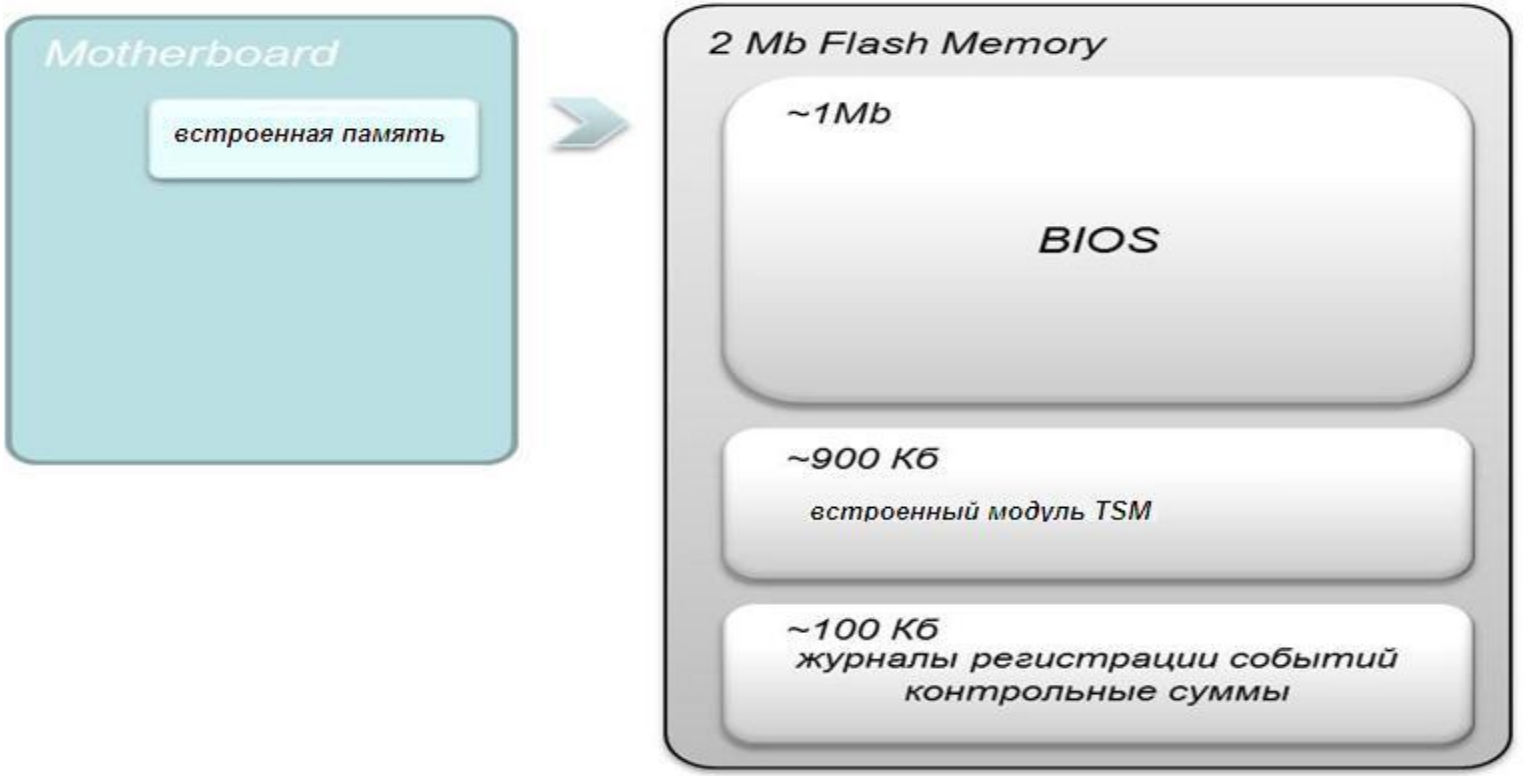
- Современная аппаратная платформа и программное обеспечение
- TSM
- Модифицированный BIOS

Аладдин РД

kraftway
ТЕХНОЛОГИИ ДЛЯ ЛЮДЕЙ

FUJITSU

Технические характеристики



- Вызывается на исполнение из BIOS после прохождения процедуры Power On Self-Test (POST).

Технические характеристики

- Microsoft Windows XP/2003/Vista/2008/7/2008R2 (x86/x64), Linux (LSB 3.6/4.1).
- Интеграция с BIOS материнской платы.
- Идентификация и аутентификация пользователей компьютера с применением аппаратных идентификаторов.
- Контроль целостности программной среды.
- Регистрация событий доступа (в том числе несанкционированного) к компьютеру.
- Невозможность неконтролируемой загрузки с внешних носителей.
- Невозможность извлечения встроенного модуля безопасности.
- Обеспечение интеграции с системами сбора, контроля, обработки, корреляции и реагирования на события информационной безопасности (требование PCI DSS, SOX, ISO 2700

Соответствие РД

- «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 3 уровню контроля.
- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (Гостехкомиссия России, 1992)» до 1Г включительно.
- «Положение о методах и способах защиты информации в информационных системах персональных данных (Утв. приказом ФСТЭК России от 5 февраля 2010 г. № 58) до 1 класса включительно.

Крипто БД - СКЗИ

- Шифрование данных по ГОСТ 28147-89;
- Защита ключей шифрования по ГОСТ 34.10-2001;
- Дискретное разграничение доступа к зашифрованным данным, для любых категорий пользователей, включая администраторов баз данных;
- Мандатное разграничение доступа;
- Возможность обезличивания и анонимизации данных;
- Контроль целостности собственного ПО;
- Персонализированный мониторинг и аудит доступа защищенным данным.

Крипто БД: важное отличие

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-1569*** от "***06***" ***ноября*** 201***0*** г.

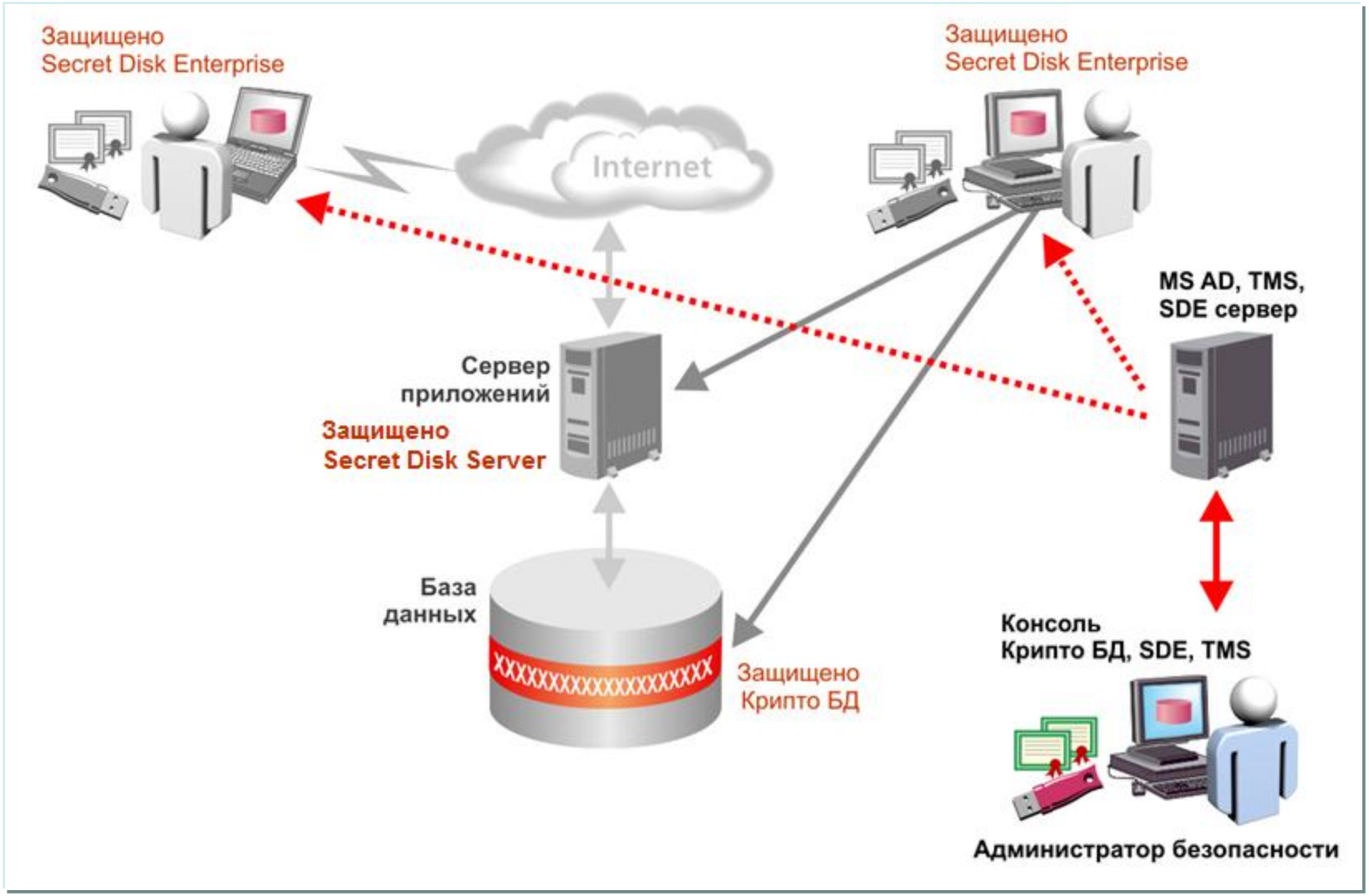
Действителен до "***06***" ***ноября*** 201***3*** г.

Выдан закрытому акционерному обществу «АЛАДДИН Р.Д.».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **«Крипто БД Версия 1.0»** (исполнения 1 и 2) в составе согласно формуляру 643.46538383.50 1430 005-01 30 01

соответствует требованиям ГОСТ 28147-89 и требованиям ФСБ России к СКЗИ класса КС1 (для исполнения 1) и КС2 (для исполнения 2) и может использоваться для криптографической защиты (генерация и управление ключевой информацией, шифрование и вычисление имитовставки пользовательских данных) информации, не содержащей сведений, составляющих государственную тайну, хранящейся в таблицах баз данных под управлением СУБД Oracle.

Концепция защиты ПДн в ИС от Аладдин Р.Д.



Спасибо за внимание!

Технические решения по защите персональных данных с использованием продуктов компании Аладдин Р.Д.

+7 495 223-00-01

Мороз Константин

dealer@aladdin-rd.ru

www.aladdin-rd.ru