

**"Решая реальные задачи ИБ,
выполняем ФЗ N152.
Продукты и решения компании Аладдин Р.Д."**



Максим Чирков

6 октября 2011 г.
г. Калуга

Аладдин Р.Д. сегодня

- **16 лет работы** на российском рынке
- Основные направления деятельности:
 - Обеспечение безопасного доступа к информационным ресурсам (аутентификация)
 - Контентная фильтрация
 - Шифрование дисков, защита БД
 - Защита ПО
- Собственный **отдел R&D**
- **Сертифицированные** специалисты
- **Лицензии** ФСТЭК, ФСБ, Минэкономразвития
- **Сертифицированные продукты**
- **Партнерская сеть** на территории России, представительства в Украине и Казахстане



Задачи решаемые продуктами Аладдин Р.Д.

- Аутентификация
- Защищённое хранения ключевой информации
- Централизованное управление средствами аутентификации
- Централизованное управление доступом в парольные (унаследованные) приложения
- Защита от НСД (защита при хранении)
 - На персональных раб.станциях и ноутбуках
 - На серверах
 - В масштабах организации/предприятия
- Защита в СУБД Oracle
- Контентная фильтрация

Аутентификация – первый шаг к ЗИ



Что такое eToken?

- **eToken – персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП).**



*Двухфакторная аутентификация
(знать – PIN-код,
иметь – смарт-карту)*

- **Аппаратное выполнение криптографических операций в доверенной среде**

- **Поддерживаемые ОС:**



- **Единственный на рынке сертифицированный ФСТЭК России**
«Программно-аппаратный комплекс аутентификации и хранения ключевой информации пользователей».

✓ **Windows 2008 R2 и Windows 7 (32/64-bit) указаны в сертификате**

Интеграция с СКУД

- **Единое устройство**

- Физический доступ
- Логический доступ

- **Технология RFID**

- Ангстрем БИМ-002
- HID ISOProxII
- Mifare
- EM-Marine
- и другие



- 1** Чип смарт-карты
- 2** Фото, логотип
- 3** RFID-метка



еToken

Сценарии аутентификации/идентификации



eToken в задачах аутентификации



- ✓ Аутентификация на рабочей станции (ноутбуке)

eToken + eToken Network Logon 5.0



eToken в задачах аутентификации

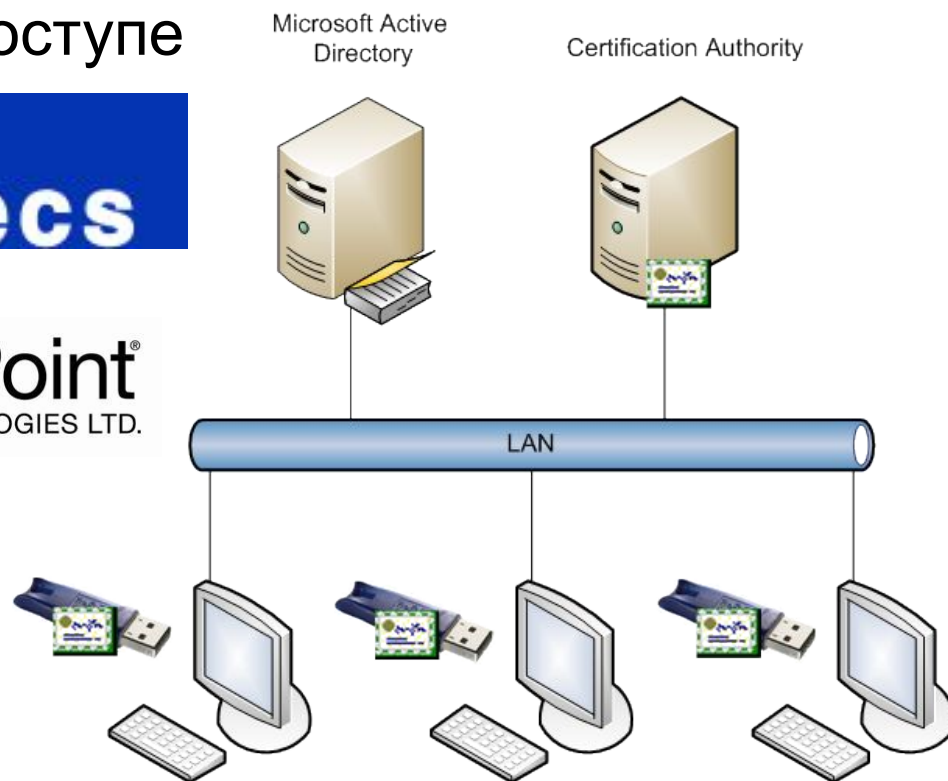


- ✓ Аутентификация в корпоративной сети (домене)*
- ✓ Аутентификация при терминальном доступе (RDP)*
- ✓ Аутентификация при терминальном доступе (Citrix)
- ✓ Аутентификация при VPN доступе
- ✓ Аутентификация



Check Point®
SOFTWARE TECHNOLOGIES LTD.

Microsoft®



Использование eToken с СЗИ от НСД

Наименование	Производитель
Соболь	ГК «Информзащита»
Secret Net	ГК «Информзащита»
Страж NT	ЗАО НПЦ "Модуль"
«Панцирь-С»	ЗАО "НПП "Информационные технологии в бизнесе"
«Dallas Lock»	ООО «Конфидент»

Применение eToken на практике. Электронно-цифровая подпись

- *ЭЦП в системе электронного документооборота*
Дело, Directum и др.



- *ЭЦП сообщений электронной почты их шифрование*
Microsoft Office Outlook и др.



- *ЭЦП в системе сдачи отчетности через интернет*
Калуга Астрал, и др.



- *ЭЦП в системах электронной торговли*
Федеральные ТП, B2B-Centr, NetTrader и др.



- *ЭЦП в системах банк-клиент*
Альфа-Банк, ВТБ и др.

**Централизованное управление
средствами аутентификации и
политиками ИБ**



Жизненный цикл средств аутентификации

- ✓ Инициализация (форматирование).
- ✓ Присвоение устройства пользователю.
- ✓ Определение списка приложений, с которыми данное устройство может быть использовано.
- ✓ Выпуск устройств.
- ✓ Отслеживание использования устройства.
- ✓ Работа с цифровыми сертификатами инфраструктуры PKI (запрос сертификата, отзыв).
- ✓ Обработка случаев утери/поломки устройств.
- ✓ Утилизация.

Централизованное управление



1. Сотрудник получает eToken



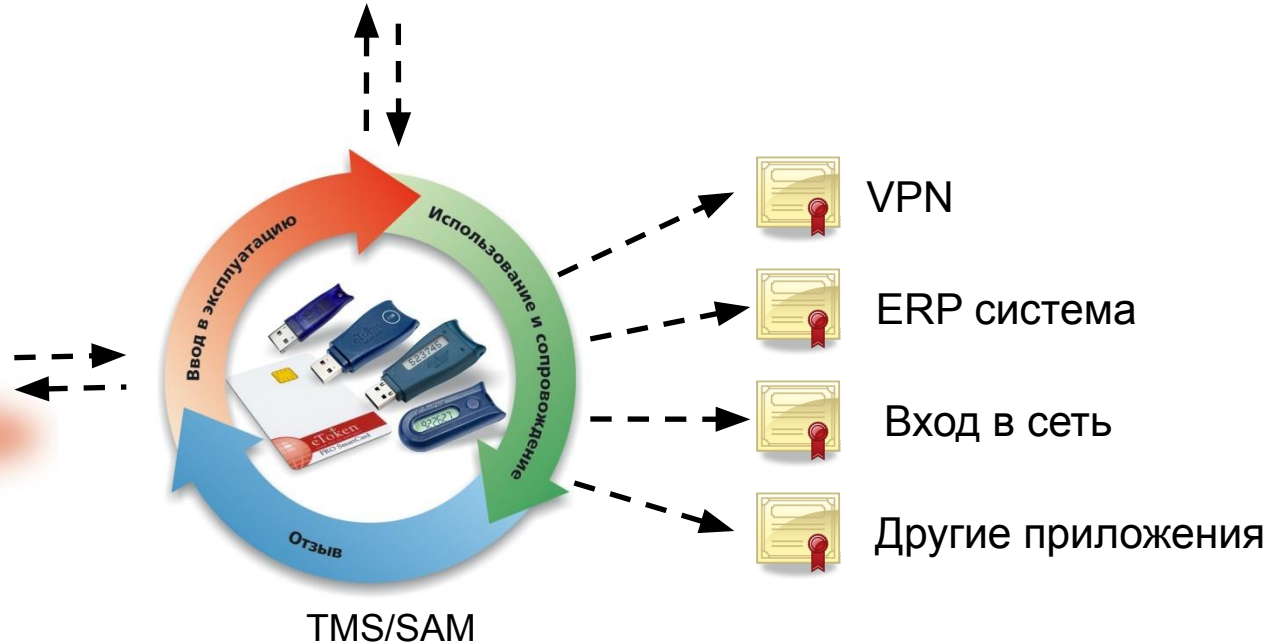
Active Directory
2. Регистрация пользователя



3. Сотрудник начинает работать

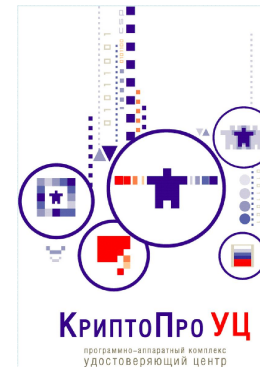
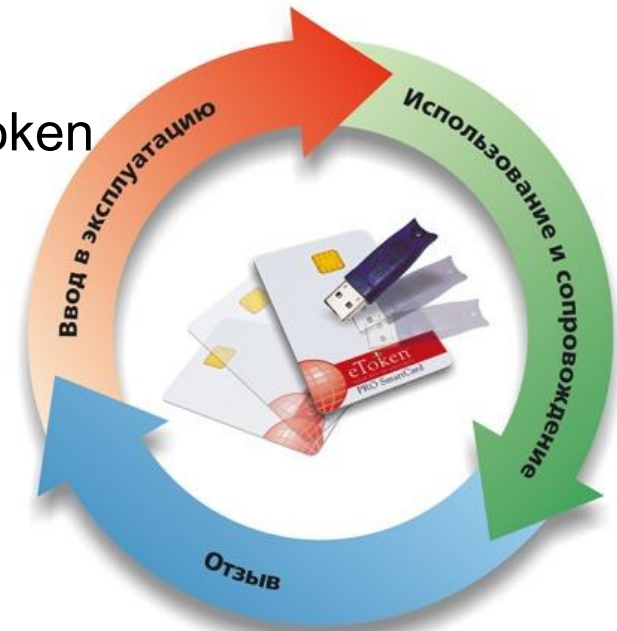


Политики организации



Основные возможности eToken TMS/SAM

- ✓ 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»
 - Microsoft CA



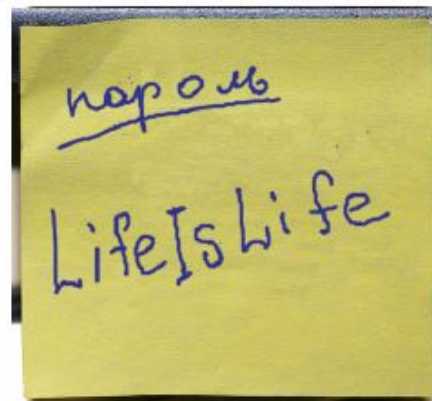
«Прозрачный доступ» к бизнес приложениям



Текущая ситуация и тенденции

Имя пользователя:

Пароль:



- ✓ В средних и крупных организациях используется более 20-ти систем и приложений
- ✓ В течении дня пользователь несколько раз получает доступ в 5-9 приложений

Microsoft Active Directory	Почтовая система	Терминальный сервер
Система документооборота	ERP/CRM	Citrix среда
Биллинговая система	Service Desk	Система бухгалтерского учета
Корпоративные порталы	Internet ресурсы	Базы данных
...

Enterprise Single Sing-On

Single Sing-On (SSO) - технология избавления:

- ✓ сотрудников от использования паролей
- ✓ службы ИТ от инцидентов “забытый пароль”
- ✓ службы ИБ от присутствия слабых паролей и липких стикеров

Нет SSO



Есть SSO



Принцип работы Аладдин Indeed-ID ESSO



Аладдин Indeed-ID ESSO – основные преимущества

Form-based SSO

не требуется модификация приложений

Все типы приложений

Windows, Java,
Web, Citrix, SSH

Отказоустойчивость

multi-master режим,
работа без сервера,
данные на ключе

Разные сценарии

1-к-1, N-к-1,
делегирование доступа,
командировка

Интеграция с CMS

реализована интеграция с
Aladdin TMS 2.0 и выше

PKI - aware

поддержка x509
сертификатов



Защита данных

Способы потерять информацию

Сервисное обслуживание компьютеров и серверов сторонними организациями



Способы потерять информацию

Потеря или кража ноутбуков, съемных носителей



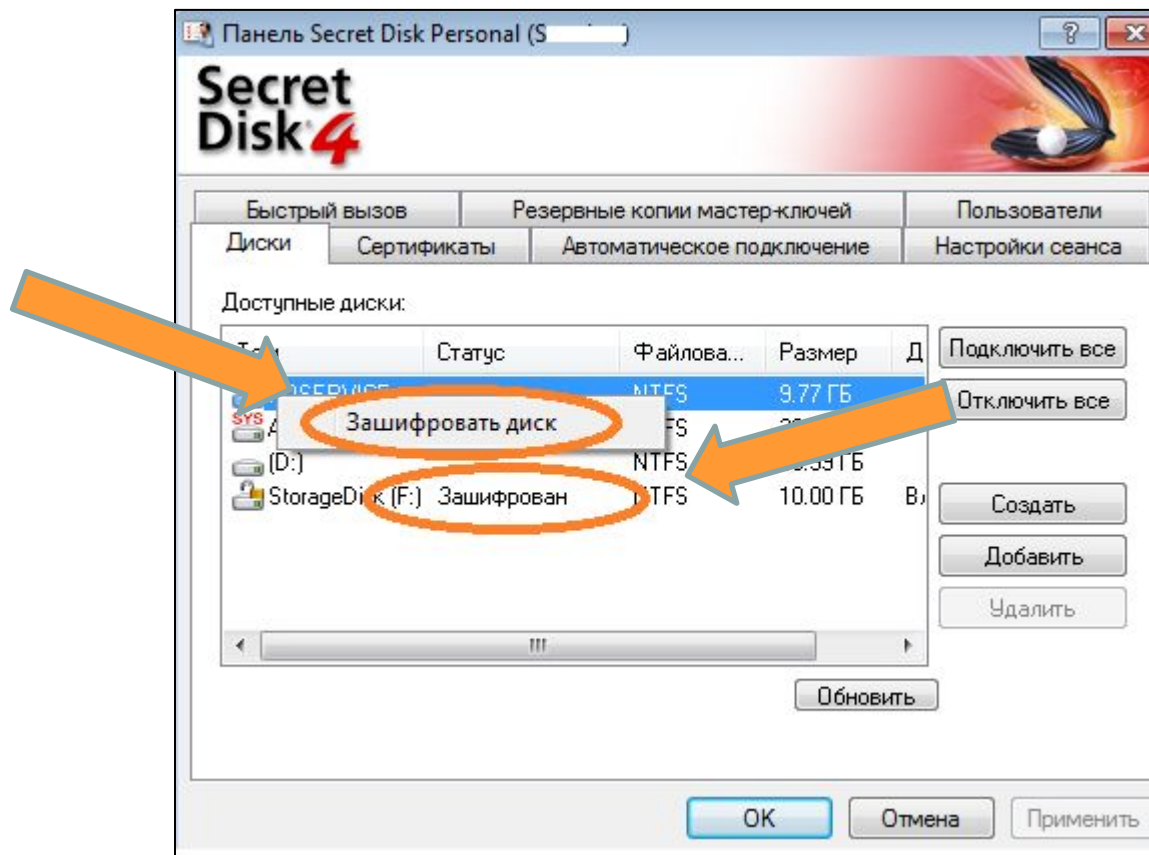
Он не рассчитывал увидеть
свои фото в сети



Как защититься?

Шифрование

Самый простой и надежный метод защиты



Линейка продуктов Secret Disk.

Для персонального использования

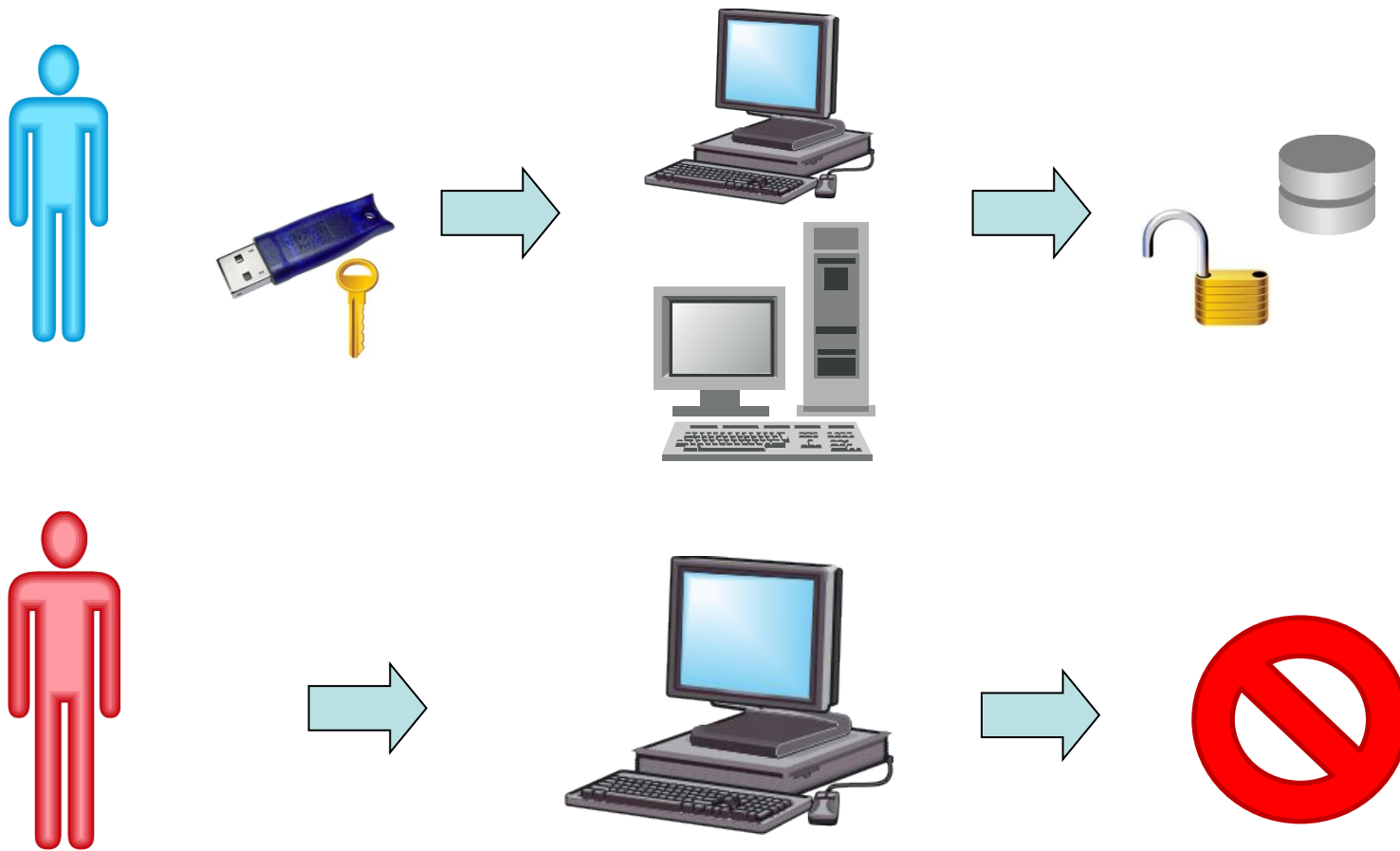
Защита данных на рабочих станциях, мобильных компьютерах и съёмных носителях

Secret Disk 4



**Secret Disk 4
Workgroup Edition**

Логика работы Secret Disk



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

Преимущества Secret Disk 4

- Защита **системного раздела**, контроль **начальной загрузки**
- **Шифрование** логических и внешних дисков
- Поддержка различных алгоритмов шифрования данных, в т.ч.
ViPNet (Домен-К), КриптоПро CSP
- **Запрет доступа по сети** к зашифрованным данным для всех пользователей, включая системного администратора
- Многопользовательская работа

Возможности Secret Disk 4

□ Расширенная безопасность

- Поддержка ждущего и спящего режимов
- Тестовое шифрование системного раздела

□ **Автоматическое отключение** зашифрованных ДИСКОВ

- При отсоединении eToken
- Нажатием горячих клавиш

Линейка продуктов Secret Disk.

Для использования на Windows серверах



FWRU

Возможности Secret Disk Server NG

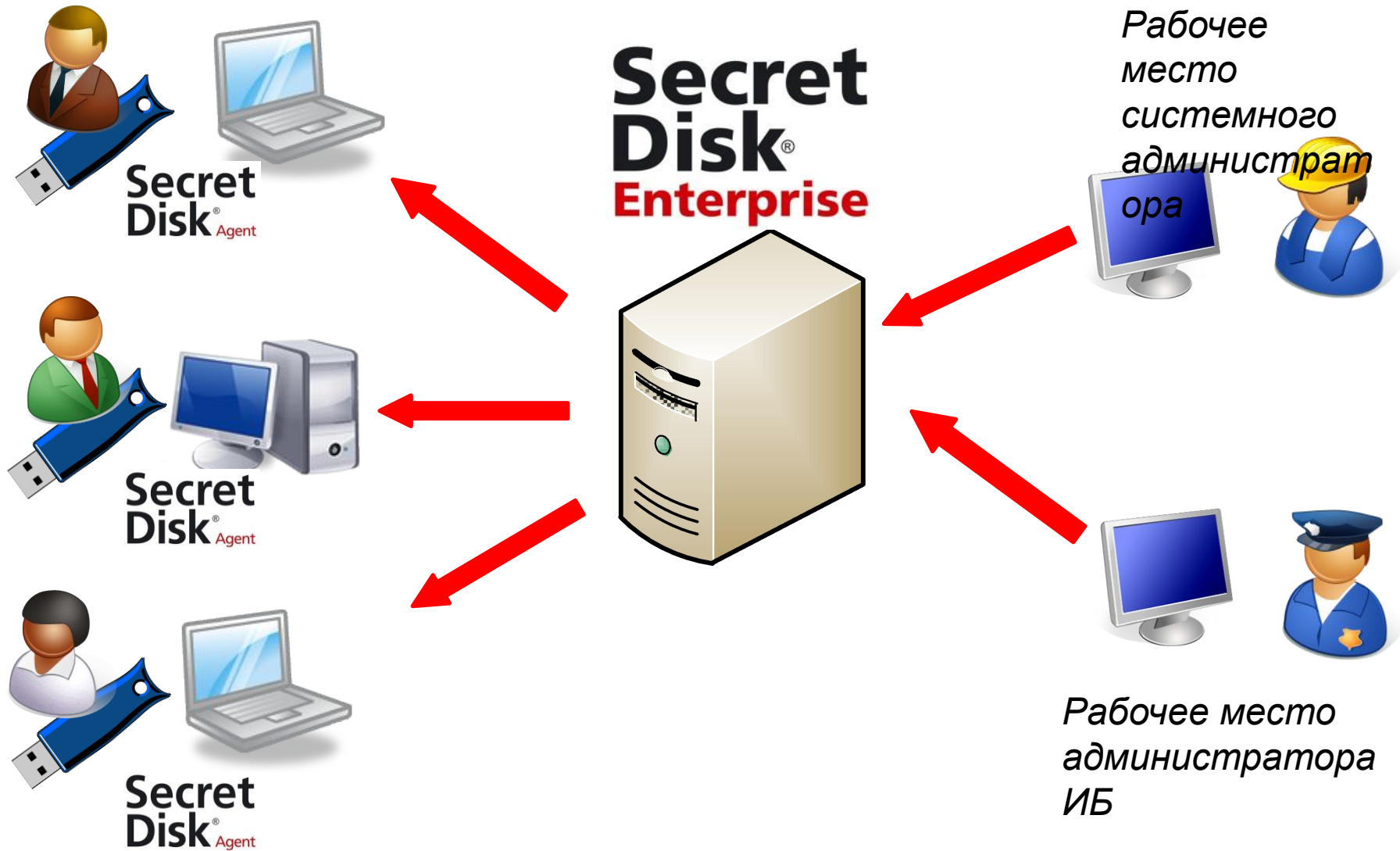
- Шифрование данных на HDD, RAID, SAN
- Контроль доступа к зашифрованным дискам по сети
- Аутентификация администраторов с использованием eToken
- Защита от сбоев и система восстановления



Secret Disk® Enterprise

Корпоративная система защиты
конфиденциальной информации с
централизованным управлением

Secret Disk Enterprise – наводим порядок!



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

Линейка Secret Disk – 12 лет на страже Вашей информации

- **Secret Disk 4 и Secret Disk 4 Workgroup Edition** – для дома и бизнеса
- **Secret Disk Server NG** – для файловых серверов и серверов приложений
- **Secret Disk Enterprise** – корпоративная система защиты
- **Сертифицированные версии Secret Disk** – для ИСПДн и защиты конфиденциальной информации



Доверенная среда – мифы и реальность



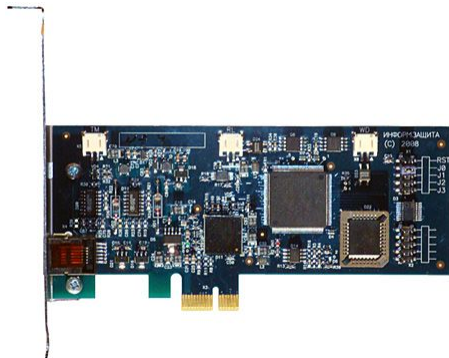
Электронный замок, АПМДЗ

Электронные замки (аппаратно-программные модули доверенной загрузки - АПМДЗ) решают следующие задачи:

- Предотвращение несанкционированного доступа к ресурсам компьютера;
- Предотвращение загрузки операционной системы с внешнего носителя;
- Контроль целостности программной среды компьютера;
- Регистрация событий доступа (в том числе несанкционированного) к ресурсам компьютера.

Традиционные АПМДЗ

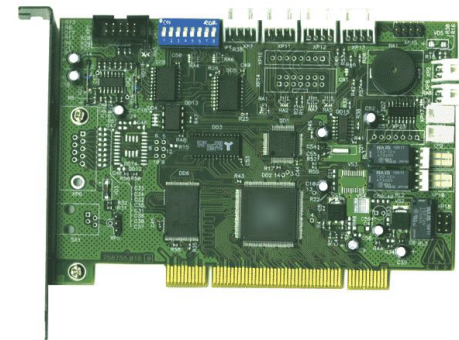
- «Традиционные» АПМДЗ выполняются в виде специализированного контроллера, подключаемого к компьютеру посредством шины PCI/PCI-X, PCI-E.



ПАК «Соболь»



AMD3 Аккорд-5.5.e



АПМДЗ «КРИПТОН-ЗАМОК»

Проект «Защищенный компьютер»



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

- Современная аппаратная платформа и программное обеспечение
- Aladdin Trusted Security Module
- Модифицированный BIOS
 - Разграничение прав доступа (защита от перезаписи, ограничение прав чтения) к секциям BIOS, TSM
 - Защита от несанкционированной модификации CMOS (Complementary Metal-Oxide-Semiconductor, область хранения настроек BIOS);
 - Ограничение доступа к BIOS SETUP по роли пользователя из TSM;
 - Интеграция с TSM для защиты от НСД.

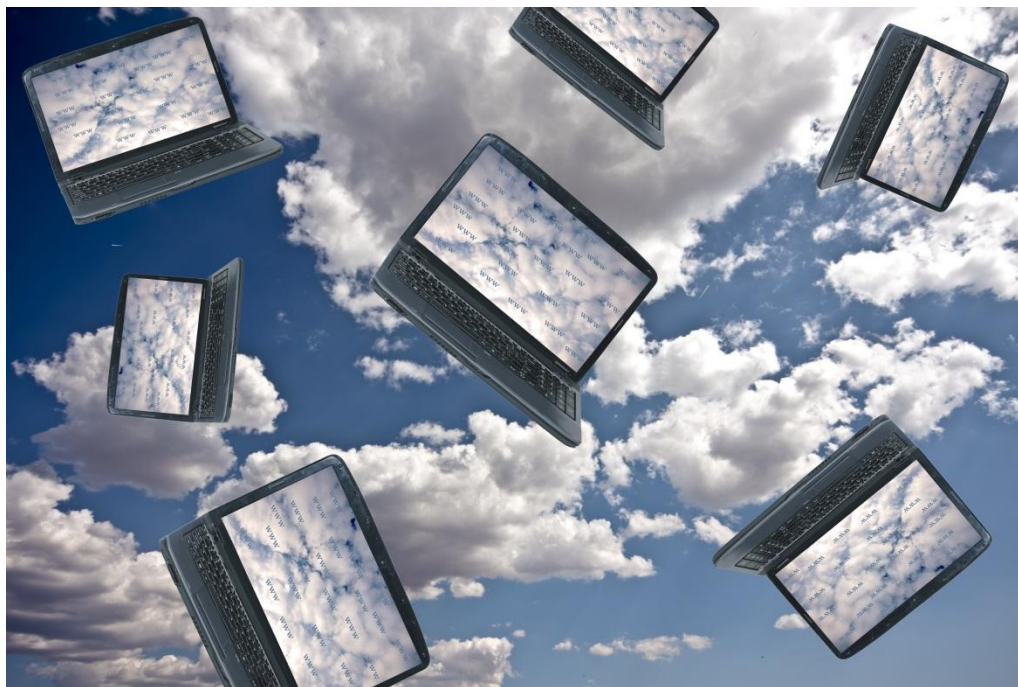


«Квалифицированная» подпись в Web



Web-based приложения

Использование облачных вычислений и web-based приложений стало устойчивой тенденцией



*"Не частично, а все госуслуги должны быть переведены в электронный вид к 2015 году»
Д.А. Медведев*

Требования к технологиям аутентификации и ЭЦП физических лиц на Портале

- Настройка и работа с Порталом не должна требовать высокой квалификации в области IT
- Поддержка всех популярных пользовательских ОС (Windows, Linux, MAC)
- Поддержка всех популярных браузеров
- Доступность с любого места
- Отсутствие необходимости установки специальных дистрибутивов

Выбор технологии для физ.лиц

Криптоконтейнер



ПО CSP



Требуется обучать
устанавливать ПО и
пользоваться им

Только одна
операционная
система



Только собственный
компьютер

Аппаратная ЭЦП



Не требуется обучать
пользователей



Любой интернет
браузер



Любая ОС



Любой компьютер

eToken ГОСТ

- *Самостоятельное СКЗИ*
 - *USB-токен*
 - *смарт-карта*
- *Аппаратная реализация российских криптографических алгоритмов*
 - *ГОСТ Р 34.10-2001*
 - *ГОСТ Р 34.11-94*
 - *ГОСТ 28147-89*
- *Работа без установки дополнительного ПО*
 - *USB CCID*



От концепции к технологии – JC-WebClient

- *Мультибраузерный кроссплатформенный плагин JC-WebClient:*
 - *Internet Explorer, Firefox, Chrome, Opera, Safari*
 - *Windows, Linux, Mac OS*



- *Возможность работы с eToken ГОСТ*
 - *из контекста веб-страницы*
 - *при помощи Java Script*



Требование безопасности

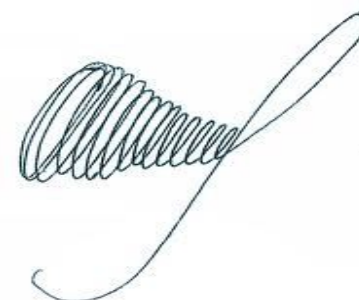
- ***Строгая аутентификация***



- ***Целостность и конфиденциальность при информационном обмене***



- ***Аутентичность информации, юридическая значимость***



Система Безопасности Вашей Организации

*Решение реальных
задач ЗИ*

*Минимальное влияние
на бизнес-процессы*



*Выполнение
требования
«Регуляторов»*

*Низкая стоимость
владения*



Спасибо за внимание

Максим Чирков

eToken@aladdin-rd.ru

www.aladdin-rd.ru