



Проблемы обеспечения безопасности и доверия в корпоративной ИТ-инфраструктуре при переходе на Linux

Ключевые элементы и точки отказа

Сергей Груздев

ген. директор АО "Аладдин Р.Д."

13 октября 2023 г.

Линейка продуктов

Изменение позиционирования компании

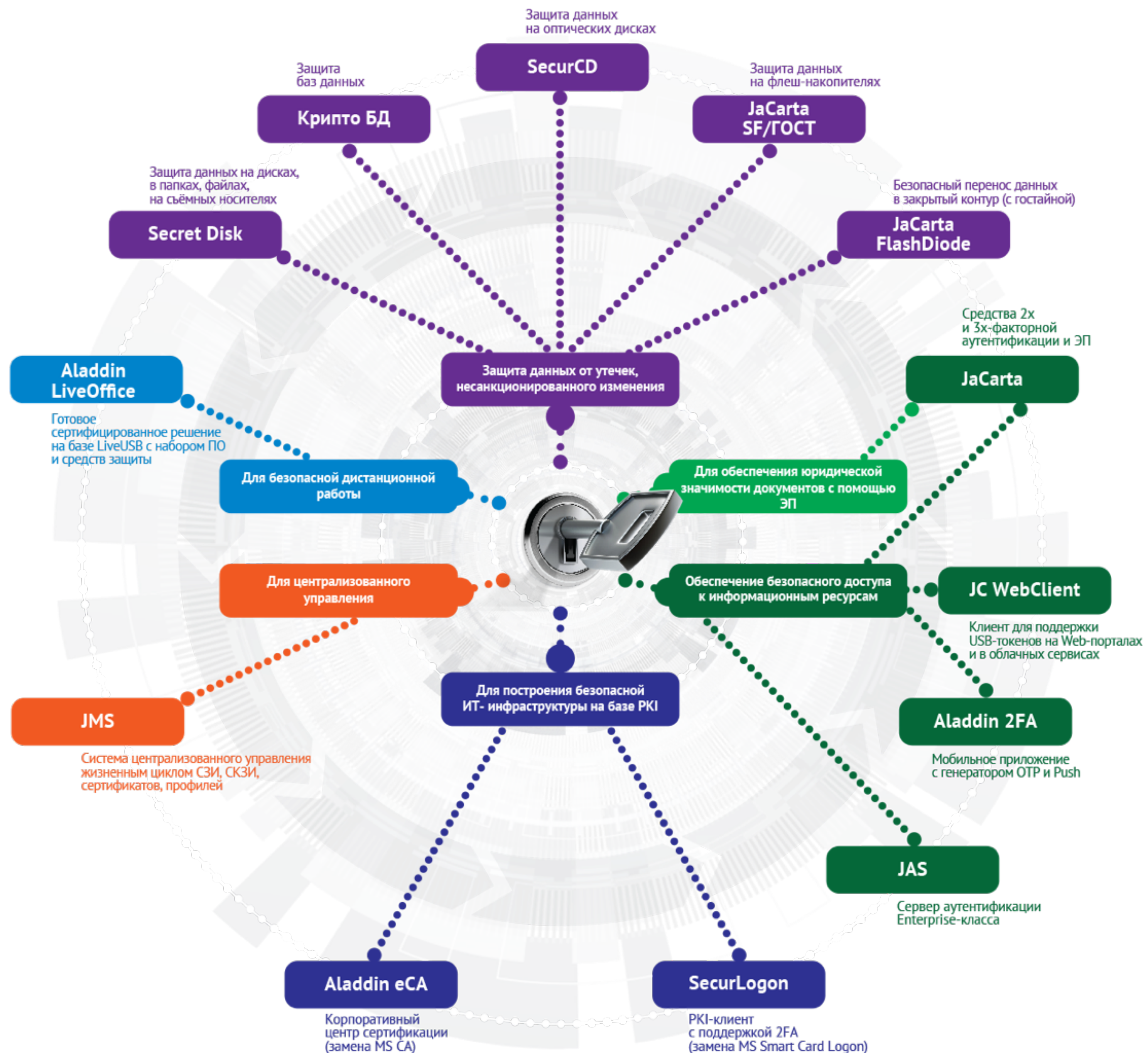
NASP - eToken - JaCarta - ...

Линейка продуктов сильно выросла и изменилась, продукты группируем по двум фокусным направлениям для рынков КИИ, Enterprise, госов, меняем позиционирование компании:

1. Ключевые инфраструктурные решения для построения безопасной доверенной ИТ-инфраструктуры (и PKI на Linux)
2. Средства защиты главных информационных активов (CRM, ИСПДн и пр. - базы данных, информация на дисках)

Используем тренды:

- Импортзамещения, миграция на Linux
- Доверие и безопасность ИТ-инфраструктуры (безопасность должна закладываться на стадии проектирования и развёртывания ИТ-инфраструктуры)



Изменение и оценка киберугроз с началом СВО

- ◆ Посетил 7-8 конференций - что обсуждается?
 - Чем заместить прикладное ПО ушедших из РФ зарубежных вендоров
 - Беспрецедентный рост успешных атак из-за слабой или неправильной аутентификации пользователей
 - Массовые утечки баз данных и персональных данных
 - Блокирование поставок и производства для РФ микроэлектроники
 - Необходимость всеобщего перехода на Linux
- ✓ Все просто фиксируют факты, приводят статистику, предлагают средства мониторинга вместо противодействия...
- ✓ Никто системно и всерьёз не предлагает переоценить риски - в первую очередь, связанные с работоспособностью всей нашей ИТ-инфраструктуры, найти и в первую очередь устранить ТОЧКИ ОТКАЗА
- ✓ Движемся по инерции, боремся с навязанными нам угрозами (плохие парни-хакеры - взломы ресурсов, эксплуатация уязвимостей, вирусы-шифровальщики...)



Изменение и оценка киберугроз с началом СВО

“Мы порвём экономику России в клочья!”

- Барак Обама – помните? 2012 г. - PPD-20, CloudAct
 - Решение о закладке в объекты критической информационной инфраструктуры России **кибербомб**, которые можно привести в действие для **вывода из строя** системы командования и контроля вооруженных сил противника, **объектов его критически важной инфраструктуры**
 - Решение, обязывающее американских вендоров осуществлять сбор и передачу в АНБ, ЦРУ и ФБР т.н. “**телеметрии**”
 - **Запрет** американским вендорам **на передачу и/или раскрытие исходных кодов ПО и прошивок** “железа” другим государствам
 - Задание ЦРУ по разработке маскировочных программных средств проведения компьютерных атак, в том числе под “чужим флагом”



✓ Это были не пустые слова

◆ Национальная стратегия кибербезопасности США

- Март 2023
 - “Мы задействуем все имеющиеся у нас возможности, весь заложенный арсенал средств для **блокирования и вывода из строя ИТ-инфраструктуры организаций КИИ противника** - и с помощью кибератак, и с проведением военных операций (силами зависимых партнёров)”

✓ С нами пока только играют, основной арсенал средств ещё не задействован

Насколько уязвимы наши ИТ-инфраструктуры?

Ахиллесова пята всех наших ИТ-инфраструктур

Все помним Ахиллеса...

◆ Провожу аналогию

- Тратим силы и бюджеты на внешний периметр, на борьбу с плохими парнями
- А прилетит в другое место - куда не ждёшь
- Мы не правильно оценивали политические риски, архитектурные уязвимости (критические зависимости) и продолжаем плыть по течению...
 - Недавно так было с производством российских процессоров - все яйца сложили в одну корзину - TSMC, с ИБ-сервисами (облачная аутентификация пользователей)

◆ ВОПРОСЫ

- ✓ **Что является единой точкой отказа для всех наших ИТ-инфраструктур?**
- ✓ **Приведёт ли такой отказ к недопустимому ущербу?**
- ✓ **Удастся ли отсидеться, изолировав свою сеть от Интернета?**
- ✓ **Верите ли, что Они этого не сделают?**
- ✓ **Какой приоритет следует поставить решению этой задачи?**



Что является единой точкой отказа для всех наших ИТ-инфраструктур?

Корпоративный центр выпуска и обслуживания сертификатов - MS CA

- ◆ От него зависят
 - Доверенное взаимодействие всех объектов и компонентов ИТ-инфраструктуры
 - Аутентификация всех объектов системы - оборудования, пользователей, приложений (ПО)
 - Работоспособность доменов безопасности/службы каталога
 - Работа различных сервисов (удалённого доступа, VDI, VPN, RDP-шлюзы и др.)
- ◆ Никто не задумывается над вопросами
 - Что такое ДОВЕРИЕ, как оно обеспечивается, КОМУ мы доверяем?
 - Откуда берутся сертификаты доступа (машинные, пользовательские, ПО)?
 - Кто принимает решение "свой-чужой" (проверяет валидность сертификатов, пускает пользователей в систему)?
- ✓ Как это будет работать при переходе на Linux? (ожидаем, что так же как в Windows?)
- ✓ Есть ли PKI под Linux?



Что такое доверие и как оно обеспечивается?

Что такое ДОВЕРИЕ и как оно обеспечивается

- ◆ Доверие
 - Это открытые взаимоотношения между людьми (субъектами), содержащие уверенность в порядочности другого, в возможности поделиться с ним личной или сокровенной информацией, в его ответственности не воспользоваться этой информацией вам во вред...
- ◆ Применительно к ИТ-инфраструктуре - это определение тоже работает
 - Система является **доверенной**, когда каждый её элемент надёжно (**гарантированно**) идентифицирован и аутентифицирован
 - ✓ **Для ИБ важнее не доверие, а ГАРАНТИИ**
 - Гарантии даёт криптография (гарантированная стойкость), PKI (централизованная инфраструктура), безопасность закрытых ключей
 - Основа доверительных отношений - АУТЕНТИФИКАЦИЯ, для критических систем - **строгая (2ФА)**
 - Для СТРОГОЙ аутентификации между всеми компонентами ИТ-инфраструктуры необходимо разворачивание PKI (инфраструктуры открытых ключей)
 - Основа PKI - центр выпуска и обслуживания сертификатов (**корпоративный СА**)
 - ✓ **Построить безопасную доверенную ИТ-инфраструктуру крупной организации без PKI нельзя**



Основа создания доверительных отношений - аутентификация

Нац. стандарты по идентификации и аутентификации

◆ Действующие стандарты

- ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения
- ГОСТ Р 70262.1-2022 Защита информации. Идентификация и аутентификация. **Уровни доверия идентификации**
- ГОСТ Р 59381-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции
- ГОСТ ISO/IEC 24760-2-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования.
- ГОСТ Р 59382-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы
- ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом
- ГОСТ Р 59515-2021 Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности

◆ Проекты стандартов (в работе)

- Защита информации. Идентификация и аутентификация. **Уровни доверия аутентификации**
- Защита информации. Идентификация и аутентификация. Управления идентификацией и аутентификацией
- Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости идентификации и аутентификации
- Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией

Требования к аутентификации

- ◆ Что обеспечивает ДОВЕРИЕ и даёт гарантии?
 - Какой тип аутентификации нужен для критически важных систем?
 - Как его реализовать?

Вероятность и размер возможного ущерба

Тип аутентификации	Низкая	Средняя	Высокая
Высокая	Усиленная	Строгая	Строгая
Средняя	Простая	Усиленная	Строгая
Низкая	Простая	Простая	Усиленная

Уровень значимости информации в ИС

Кому:

- Гос. организации
- Федеральные структуры
- **Организации КИИ**
- Крупный и ср. бизнес
- **Производители СЗИ**

Для кого:

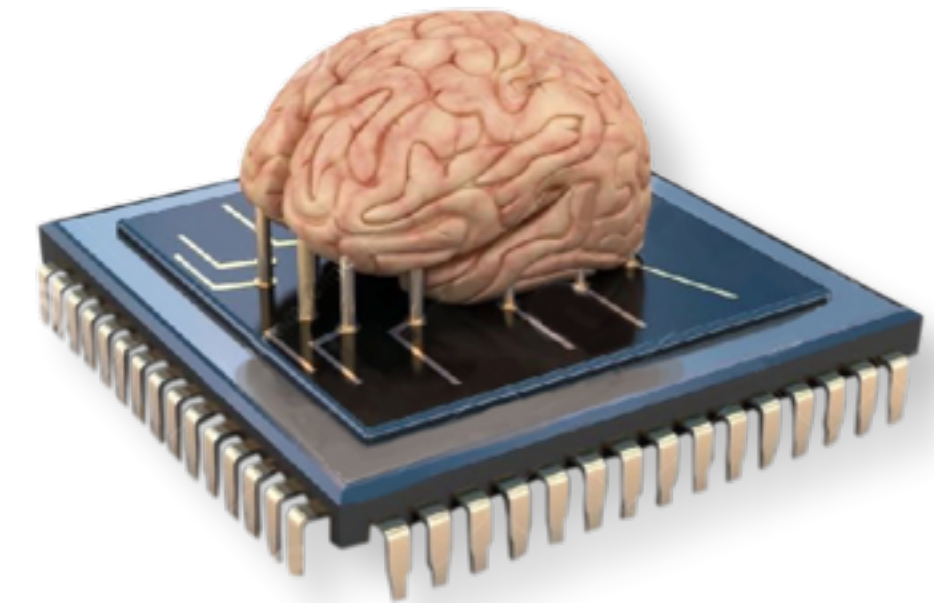
- **Для всех пользователей ИС**
- Для администраторов
- **Для удалённых пользователей**

С началом СВО на первое место выходит **внутренний нарушитель** (был сильно недооценён)

Сейчас они есть у всех!
Но и этого недостаточно

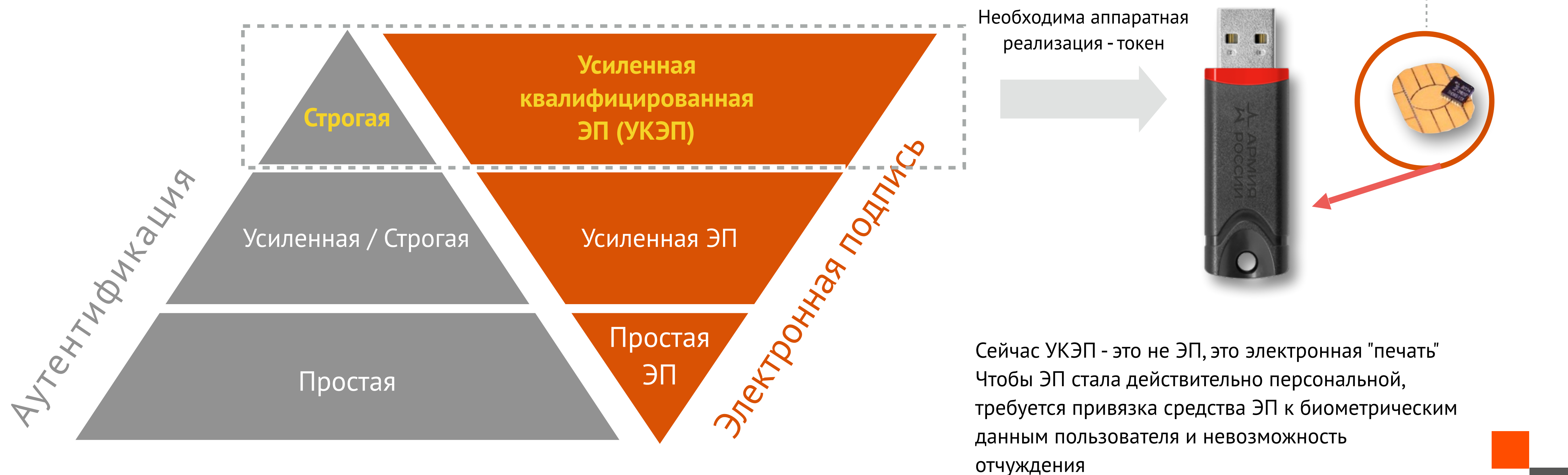
Что нужно для реализации СТРОГОЙ аутентификации

- ◆ В ИС с высокой важностью информации и высоким размером возможного ущерба
 - Должна применяться **строгая** взаимная двухфакторная аутентификация пользователей (2ФА)
- ◆ Строгая аутентификация обеспечивается использованием
 - Инфраструктуры открытых ключей (PKI) - **сертификатов доступа**
 - Специализированных защищённых и сертифицированных аппаратных средств аутентификации (**второго фактора**):
 - Хранение цифрового **сертификата** пользователя
 - Выполнение **криптографических** операций с использованием **неизвлекаемых** закрытых ключей пользователя (требуется для поддержки защищённых протоколов аутентификации)
 - Возможность использования только **аутентифицированным** пользователем
- ✓ **Программные токены, смартфоны, генераторы одноразовых паролей (ОТР) не обеспечивают СТРОГУЮ 2ФА**
 - Централизованным управлением и поддержкой жизненного цикла сертификатов, средств 2ФА
 - Сервисом аутентификации (локальным или доменным)
 - Он должен быть своим, доверенным, а **не как в Windows** - чужим!



Тип аутентификации определяет тип ЭП в ИС

- ◆ Надёжность системы определяется по её самому слабому звену
 - Если в ИС необходимо обеспечить **юридически значимую ЭП**, приравненную к собственноручной, то для получения усиленной квалифицированной ЭП (УКЭП) должна быть обеспечена **СТРОГАЯ** аутентификация пользователей
 - Строгая аутентификация предполагает **ДВУХФАКТОРНУЮ** (с использованием защищённого неклонировемого аппаратного устройства с поддержкой криптографии "на борту" с неизвлекаемым закрытым ключом ЭП)



Мигрируем на Linux...

А будет ли там также удобно, привычно и безопасно как в Windows?

Ответ: НЕТ

Построить безопасную доверенную
ИТ-инфраструктуру крупной организации без РКІ
нельзя

Ключевые элементы и точки отказа в ИТ-инфраструктуре

Все смотрели фильм “Стиляги”?

Помните сцену - В Америке нет стилиг!

Для многих такое же откровение, что **в Linux нет полноценного РКІ...**

Ключевой элемент и точка отказа всей ИТ-инфраструктуры

Проблема №1

- ◆ Ключевой и самый критичный элемент во всей ИТ-инфраструктуре - **центр выпуска и обслуживания цифровых сертификатов (CA)**
 - CA - основа доверенного взаимодействия всех объектов и компонентов в сети
- ◆ Практически все ИТ-инфраструктуры в России построены на базе MS CA (CS)
 - ...и на 100% зависят от его работоспособности
 - В 2022 г. Microsoft ушла из России, представительство закрыто, поддержки MS CA больше нет, купить его тоже нельзя
 - С 30 сентября 2023 г. Microsoft перестаёт продлевать подписки корпоративным клиентам из России
- ◆ Полноценных аналогов корпоративного MS CA в Open Source проектах нет
 - Коммерческие Enterprise-версии CA под Linux - стратегический товар - под строгим запретом, в Россию не поставляются
 - ✓ **Не путать корп. CA с УЦ для ЭП (63-ФЗ) – разные задачи и разные требования!**
 - ✓ **MS CA - ключевая точка отказа для всей ИТ-инфраструктуры**
 - ✓ **Риски блокирования работы сервиса MS CA - очень большие (в т.ч. через закладки)**
 - ✓ **Мы сделали альтернативу MS CA - Aladdin Enterprise CA (под Linux)**



Проблемы построения PKI под Linux

Проблема №2

- ◆ Импортозамещаемся, переходим на отечественные ОС (Linux)
 - Одновременно перейти на Linux и отказаться от Windows никто не сможет
 - В Linux свои службы каталогов и домены безопасности (FreeIPA, Samba DC, ALD Pro)
 - ✓ **Корпоративный CA должен уметь одновременно работать и с MS AD, и со службами каталогов/контроллерами доменов всех отечественных ОС (Linux)**
 - ✓ **Простого аналога MS CA (CS) недостаточно - заткнём дыру, но задачи импортозамещения и санкционной независимости не решим**

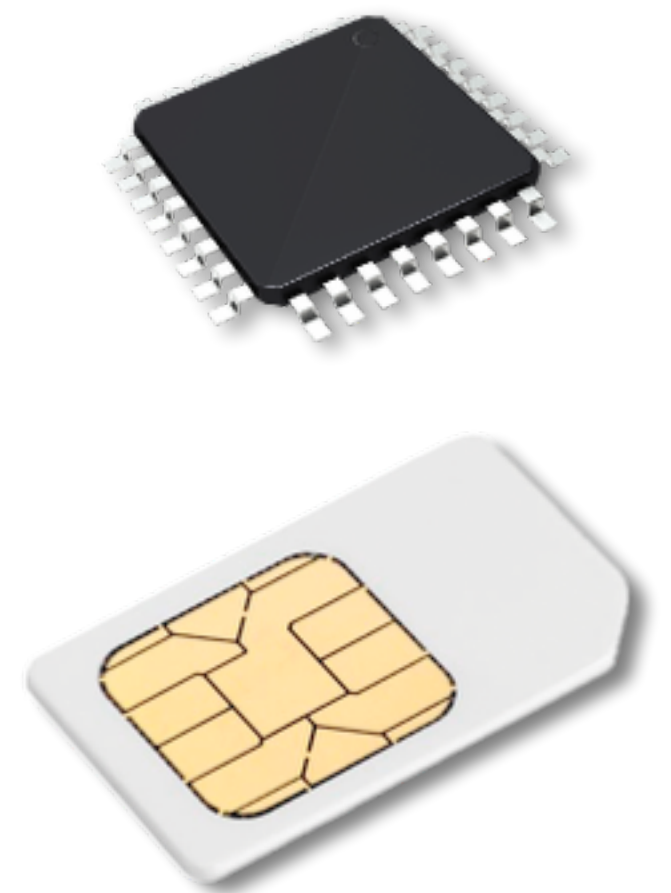
Проблема №3

- ◆ В Linux нет полноценной поддержки PKI и 2ФА пользователей
 - В Windows аутентификацию пользователей (2ФА) реализуют **встроенные сервисы** (вкл. MS Smart Card Logon)
 - Полноценного аналога для Linux нет (клиента PKI и 2ФА)
 - ✓ **Реализовать строгую аутентификацию пользователей для Linux можно (руками), но достаточно сложно**



Проблема №4

- ◆ M2M, IIoT и пр. оборудование которое работает "в полях", на новых территориях... (с большими рисками компрометации)
 - Необходима строгая аутентификация подключаемых устройств
 - Мы должны быть точно уверены, что это именно то устройство, что его не подменили, не перепрошили
 - Должно быть доверенное взаимодействие
 - Мы должны доверять данным, получаемым из этого источника
 - Для "слабых" устройств нужны "лёгкие" защищённые протоколы (DTLS,...) и машинные сертификаты
 - Мы должны иметь доверенный защищённый канал управления, передачи данных, **обновления**
 - Большой парк устройств невозможно обслуживать без системы централизованного управления
 - Мы замещаем особо критичные импортные M2M-устройства в режиме "ошпаренной кошки" чтобы успеть к 1.01.2025 г. (Указ Президента)
 - Как будем исправлять ошибки, устранять обнаруженные уязвимости, обновлять ПО и прошивки?
- ✓ **В каждом устройстве, работающем в КИИ, должен быть аппаратный модуль безопасности (Secure Element) и машинный сертификат**



Что нужно сделать СРОЧНО,
чтобы не вырубили всю ИТ-инфраструктуру?

Что нужно сделать СРОЧНО

- ◆ Молиться, чтобы не заблокировали MS CA
 - ◆ Параллельно MS CA поставить Aladdin Enterprise CA (на Linux)
 - ◆ От корневого MS CA (пока работает) для него выпустить подчинённый сертификат
 - Невозможность выпуска сертификата для подчинённого CA от корневого CA полностью парализует работу всех сервисов и всей ИТ-инфраструктуры
 - ◆ Для Aladdin Enterprise CA настроить автоматический выпуск новых сертификатов
 - Чтобы он постепенно перехватывал на себя выпуск/перевыпуск и обслуживание сертификатов
 - Это позволит произвести постепенный бесшовный переход на него (постепенное замещение MS CA - если Бог даст нам на это время...)
- ✓ **Делать это надо немедленно!**



Как и чем заменить MS CA

НОВИНКА!

Aladdin Enterprise CA

Корпоративный центр сертификации (CA) под Linux
- ключевой компонент
для обеспечения доверия в ИТ-инфраструктуре на базе PKI

Сертификация: по линии ФСТЭК России (до гостайны вкл.)
В Реестре отечественного ПО
Импортозамещение: Microsoft Certificate Services (MS CA)

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ



Aladdin Enterprise CA под Linux

- ◆ Обеспечивает

- Создание и функционирование корпоративной инфраструктуры открытых ключей (PKI)
- Управление жизненным циклом цифровых сертификатов
- Объединение всех компонентов ИТ-инфраструктуры в **единый домен безопасности**, их аутентификацию и безопасное взаимодействие
- Обслуживание в **автоматическом** режиме всех объектов и компонентов корпоративной инфраструктуры ключами и цифровыми сертификатами
 - контроллеров доменов
 - серверов, Web-серверов, эл. почты
 - роутеров, маршрутизаторов, межсетевых экранов, VDI, VPN, RDP-шлюзов
 - компьютеров и др. устройств в доменах
 - M2M, IoT-устройств
 - пользователей
- Построение доверенной безопасной ИТ-инфраструктуры на базе PKI в сложных гетерогенных, облачных и мультиарендных инфраструктурах с разделением ролей и полномочий
- Масштабирование, отказоустойчивость и разделение ролей
 - каждая функциональная роль центра сертификации (CA, RA, WebEnrol, CDP, DB и др.) может быть развёрнута на отдельном сервере в отказоустойчивой конфигурации



Aladdin Enterprise CA под Linux

◆ Позволяет

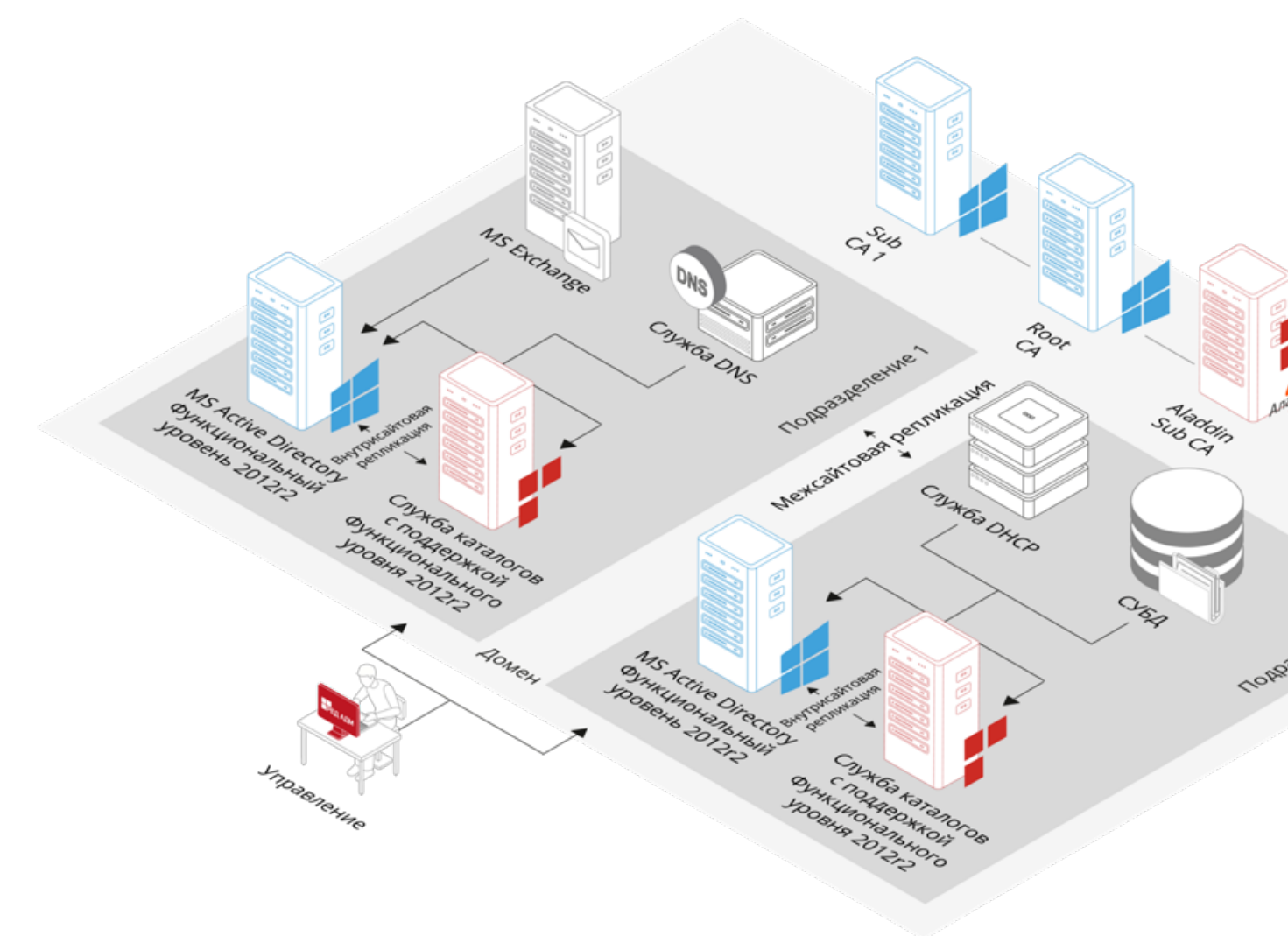
- Поставить Aladdin eCA параллельно с действующим MS CA
 - Выпустить на него подчинённый сертификат (от действующего корневого CA)
 - Настроить автоматический выпуск новых сертификатов
 - Импортировать и использовать действующие шаблоны сертификатов Microsoft CA, создавать новые
- Одновременно работать с различными службами каталогов (**как Windows, так и Linux**)
 - MS Active Directory
 - Samba DC
 - FreeIPA
 - ALD Pro
 - **РЕД АДМ** (промышленная редакция) - **отработаны сценарии бесшовной миграции**
 - Альт Домен
- Интегрироваться с различными внешними системами через REST API
 - IdM, IAM, IGA, SIEM, **JMS** и др.
- Обеспечить строгую двухфакторную аутентификацию (в т.ч. под Linux)
- Использовать различные архитектуры аппаратных платформ, отечественные ОС, виртуальные среды



Поддержка РКІ и 2ФА на клиенте Linux

Aladdin eCA в домене РЕД АДМ – сценарий миграции


- ◆ Процедура миграции PKI
 - Разработаны и протестированы подробные инструкции и методики по бесшовной миграции
 - Новая ветка ROOT
 - Действующий ROOT CA
 - Миграция шаблонов
- ✓ **Сертификаты работают в Windows и Linux**
- ◆ Репликация с MS AD 2003, 2008_R2, 2012_R2, 2016 в домен РЕД АДМ:
 - Структуры домена
 - Пользователей
 - Двухсторонняя репликация групповых политик
- ◆ В итоге получаем
 - Комплексную и бесшовную миграцию AD и CA
 - Плавный вывод продуктов Microsoft без остановки сервисов
 - Гарантию работоспособности инфраструктуры в случае отключения MS CA



Aladdin SecurLogon

НОВИНКА!

Добро пожаловать
Алексей Петров
redos732main.seclog.test



▼
Алексей Петров

●●●●●●●●
✖

Войти

PKI-клиент и поддержка средств 2ФА в Linux - замена MS Smart Card Logon

Проблемы:

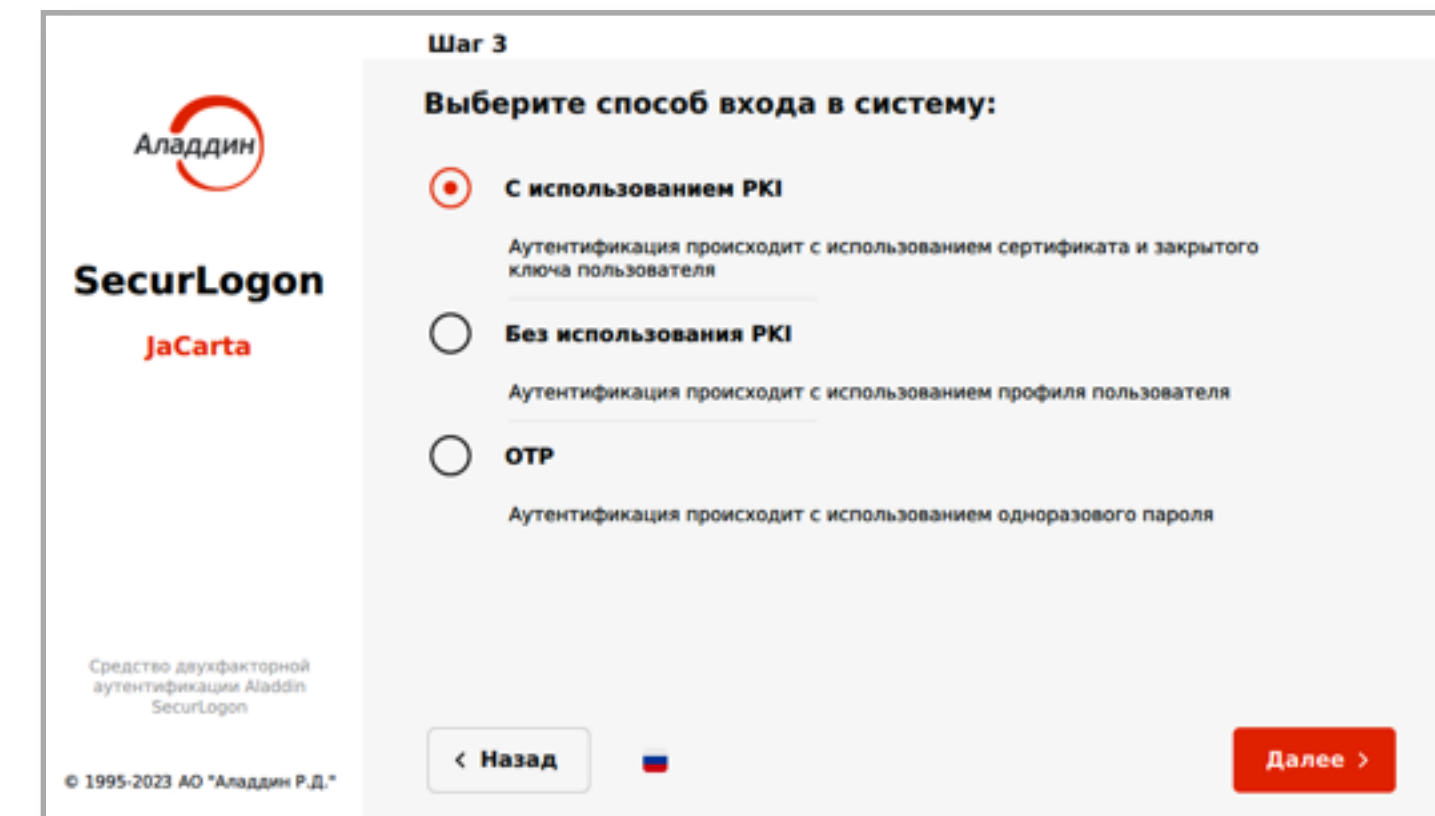
В MS Windows 2ФА пользователей реализует встроенная подсистема Windows Smart Card Logon

В российских ОС на базе Linux подобного механизма нет, всё надо делать руками (34 доп. пакета), но это будет только вход в Linux (замкнутая экосистема)

Aladdin SecurLogon

◆ Обеспечивает

- **Полноценную поддержку PKI**, двух- и трёхфакторную **строгую** аутентификацию пользователей в смешанных гетерогенных средах, в ОС на базе Linux, Windows и macOS
 - Работу с доменами Microsoft AD, FreeIPA, Samba DC, ALD Pro
 - Усиленную аутентификацию пользователей с использованием автоматически сгенерированного сложного пароля длиной до 63 символов
 - Для инфраструктур, где **PKI ещё не развёрнута**
 - Применение политик входа на основе принадлежности пользователя к группе безопасности (только токен, токен или пароль, только пароль)
 - Групповое развёртывание и удалённую настройку с рабочего места администратора
 - Защиту удалённых соединений (RDP, SSH)
 - Дополнительные сервисные функции, позволяющие до входа в ОС разблокировать токен, сменить ПИН-код пользователя, кастомизировать окно приветствия и др.
- ✓ **Полноценная альтернатива Microsoft Smart Card Logon на отечественных ОС на базе Linux**



Работает с USB-токенами и смарт-картами JaCarta

СТРОГАЯ аутентификация пользователей

Строгая аутентификация для Linux

◆ Что значит СТРОГАЯ

- Двухфакторная (2ФА), с использованием персонального специализированного защищённого устройства (требования новых ГОСТов)
 - с аппаратной реализацией криптографии с неизвлекаемым закрытым ключом
 - с хранением сертификатов доступа с памяти устройства
 - с возможностью его использования только авторизованным пользователем
 - неклонировемого (Secure by design)
- Взаимная (аутентификация обеих сторон)
- С использованием защищённых протоколов

◆ Требуется

- Во всех системах, обрабатывающих значимую информацию
 - гос. организации, КИИ, АСУ ТП и др.
- Для администраторов, пользователей, удалённых пользователей
- Развёрнутая инфраструктура открытых ключей (PKI)
- Централизованное управление жизненным циклом сертификатов, средств 2ФА
- Модуль поддержки средств 2ФА и PKI для Linux
 - **В Linux нет аналога MS Smart Card Logon**



Линейка USB-токенов и смарт-карт JaCarta (вкл. российские чипы I и II категории) с сертификацией по КС-3 (ФСБ) и УД-2 (ФСТЭК)



Средства для строгой двухфакторной аутентификации (2ФА) и ЭП

- безопасный доступ в Linux по сертификатам (PKI)

Проблемы:

В российских ОС на базе Linux нет поддержки средств 2ФА пользователей и PKI

Во многих ИТ-инфраструктурах в РФ до сих пор не используется 2ФА!

ВІО-токен

АНОНС



2ФА на базе смарт-карт и USB-токенов уже недостаточно!

Нужна дополнительная надёжная биометрическая идентификация пользователей

ВАЖНО:

Для противодействия ВНУТРЕННЕМУ нарушителю

Чтобы ЭП стала действительно подписью, а не эл. печатью (физически не привязанной к своему владельцу)!



Готовое сертифицированное средство
для организации безопасной дистанционной работы
с возможностью подключения к ГИС, обработки информации
ограниченного распространения

◆ Позволяет

- Использовать специализированное защищённое USB-устройство Aladdin LiveOffice вместо служебного ноутбука
 - как удалённое рабочее место (терминал) с набором предустановленного и преднастроенного ПО
 - работать в замкнутой доверенной программно-аппаратной среде
- Автоматически выполнить все требования и политики безопасности
- Полностью соответствовать требованиям ФСТЭК и ФСБ России по организации безопасной дистанционной работы
- Обеспечить централизованное управление (с использованием JMS)
- Решается проблема контролируемой зоны, не требуется аттестация рабочего места сотрудника
- В 5-7 раз экономить бюджет при организации дистанционной работы сотрудников и контрагентов



◆ Примеры кейсов

- Работа с внешними контрагентами (не сотрудниками организации)
 - Заказчик ведёт базу эл. полисов, оформляют полисы - контрагенты (не сотрудники)
 - Выдать всем им служебные защищённые ноутбуки - дорого, а заставить всех их выполнять требования безопасности - невозможно
 - Риски утечки информации, компрометации учётных данных, атак на ИС, внесение несанкционированных изменений в базу - огромны
 - Решение - подключать к работе с ИС только тех, кто самостоятельно приобрел правильное сертифицированное средство, обеспечивающее безопасную дистанционную работу
- Онлайн-работа и дистанционное обслуживание 1С-бухгалтерии, ERP, фреш
 - Практически все организации КИИ, гос., ФОИВы работают на 1С - установлено **в закрытом контуре, информация критически важная**
 - Администрирование, обслуживание, поддержку осуществляют 1С-франчайзи, используя **удалённое подключение**
 - Требуется выдача служебного компьютера (являющегося частью ГИС), аттестация рабочего места, организация контролируемой зоны - очень сложно и дорого





◆ Обеспечивает

- Полноценную дистанционную работу с любого недоверенного компьютера, например, с личного
 - в ГИС, КИИ, АСУ ТП, МИС и др. до 1-го класса защищённости
 - в ИСПДн до 1-й уровня защищённости персональных данных
- Возможность обработки персональных данных
- Возможность обработки коммерческой, служебной тайны
 - налоговой, врачебной, банковской, нотариальной, аудиторской, в области обороны и др.
- Защиту от внутреннего нарушителя - **пользователь не сможет:**
 - скопировать, распечатать, переслать служебный документ
 - передать посторонним и скомпрометировать свой аккаунт, пароль, параметры подключения
 - загрузить в информационную систему троян или вирус

✓ **Является альтернативой служебному ноутбуку с набором установленных приложений и сертифицированных средств защиты**

- ## ◆ Сертификаты: ФСТЭК России, ФСБ России (на компоненты, содержащие криптографию)



Защита данных на дисках - замена MS BitLocker

Вся служебная информация, выносимая за пределы организации, должна быть зашифрована

В условиях санкций, атак на КИИ, "окирпичивания" многих зарубежных продуктов продолжать использовать встроенный в MS Windows BitLocker - лучший способ похоронить свои данные



Secret Disk

- ◆ Обеспечивает
 - Предотвращение утечки и несанкционированного доступа к ценной информации при утере, краже, изъятии, ремонте, неправильной утилизации компьютеров, серверов, носителей информации
 - Прозрачное шифрование данных
 - на ноутбуках, ПК, планшетах сотрудников
 - на файл-серверах и серверах приложений (в т.ч. баз данных)
 - на съёмных носителях
 - Соккрытие наличия ценной информации на защищённом компьютере, сервере или носителе
 - Гарантированное необратимое удаление данных
 - Экстренное блокирование доступа к защищённым разделам на серверах (базы данных, корпоративная почта и др.) по сигналу "тревога"
 - Безопасную передачу конфиденциальной информации по незащищённым каналам связи
 - Фиксацию фактов доступа к защищённой информации
 - Защиту от действий привилегированных пользователей (системных администраторов)
 - Централизованное управление, интеграцию с системой управления JMS (для Enterprise-версии)



- Персональная версия
- Для серверов (приложений, файловых)
- С централизованным управлением (Enterprise)
- Версия под Linux - имеет сертификат МО для работы с ГТ ("СС")



Защита баз данных импортозамещение встроенных в зарубежные СУБД средств защиты на отечественные, сертифицированные

Не всегда можно отказаться от использования Oracle и др.
зарубежных СУБД

- огромные базы, которые российские аналоги не потянут
- огромное количество работающих приложений, для переноса которых могут потребоваться десятилетия

Технология "оправославливания" зарубежных СУБД позволяет существенно снизить риски и продолжить их использование



Крипто БД

◆ Обеспечивает

- Защиту главных информационных активов организации (ERP, CRM, ИБС, ИСПДн и др.)
 - от утечек и кражи
 - от внесения несанкционированных изменений и искажения чувствительной информации
 - от несанкционированного доступа к критически важным данным администраторов СУБД (внутренних нарушителей)
- Обезличивание персональные данные
- Прозрачное селективное (выборочное) шифрование критически важных данных в СУБД с использование российских алгоритмов
- Двухфакторную аутентификацию пользователей при доступе к данным в СУБД
- Централизованное управления ключами шифрования, исключающее возможные несанкционированные действия администраторов БД
- Реализацию требований регуляторов
 - по обеспечению конфиденциальности и целостности информации в СУБД
 - по защите персональных данных, PCI DSS, ИС организаций КИИ
 - по моделям разделения доступа - дискретной и мандатной
- Получение некорректируемой юридически значимой доказательной базы для проведения расследований инцидентов информационной безопасности

◆ Сертификаты ФСБ России до класса КС-3



Для СУБД Oracle,
MS SQL, Tibero, PostgreSQL,
Postgres Pro, Jatoba

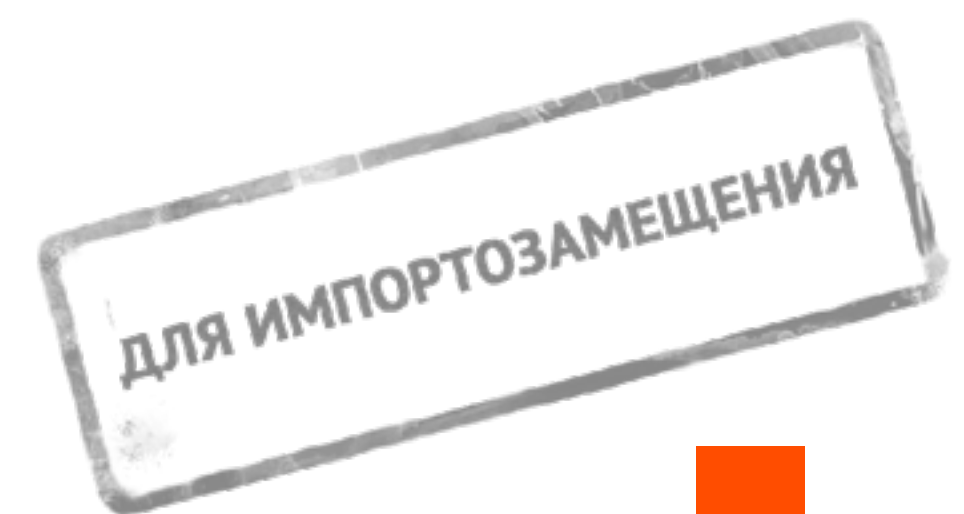


Система централизованного управления жизненным циклом сертификатов, токенов, СЗИ, СКЗИ

Включает высокопроизводительный сервер аутентификации
Enterprise-класса - JAS

Импортозамещение: любого импортного аналога

Версии: Linux, Windows



JMS - система централизованного управления Enterprise-класса

◆ Обеспечивает

- Учёт и управление жизненным циклом
 - токенов, смарт-карт, "облачных", программных токенов, OTP/PUSH/SMS аутентификаторов, U2F-токенов
 - защищённых съёмных носителей
 - смарт-карт ридеров
 - средств безопасной дистанционной работы
 - СЗИ, СКЗИ, сертификатов, объектов РКІ, профилей
- Автоматизацию большинства рутинных операций и применения политик безопасности (например, требований к ПИН-кодам)
- Быструю подготовку типовых профилей, конфигураций для разных групп пользователей, ввод в эксплуатацию новых средств, "взятие под управление" выпущенных до внедрения JMS
- Удобный сервис самообслуживания пользователей (Web-портал)



JMS - система централизованного управления Enterprise-класса

◆ Позволяет

- Интегрироваться с внешними ресурсными системами - источниками информации о пользователях и рабочих станциях, с сервисом "облачной" подписи КристоПро DSS и др.
- Связывать учётные записи пользователей из различных ресурсных систем
- Обслуживать сертификаты для аутентификации и ЭП, выданных различными удостоверяющими центрами
- Вести мониторинг и аудит действий пользователей и администраторов с выгрузкой на сервер Syslog для интеграции с SIEM
- Автоматически рассылать уведомления
- Дистанционно и безопасно обновлять "прошивки" устройств (firmware), образы встроенных ОС и приложений (только для своих продуктов!)
- Добавлять необходимую функциональность за счёт разработки и подключения дополнительных модулей и коннекторов
- Использовать версию для Linux или для Windows

◆ Сертификаты

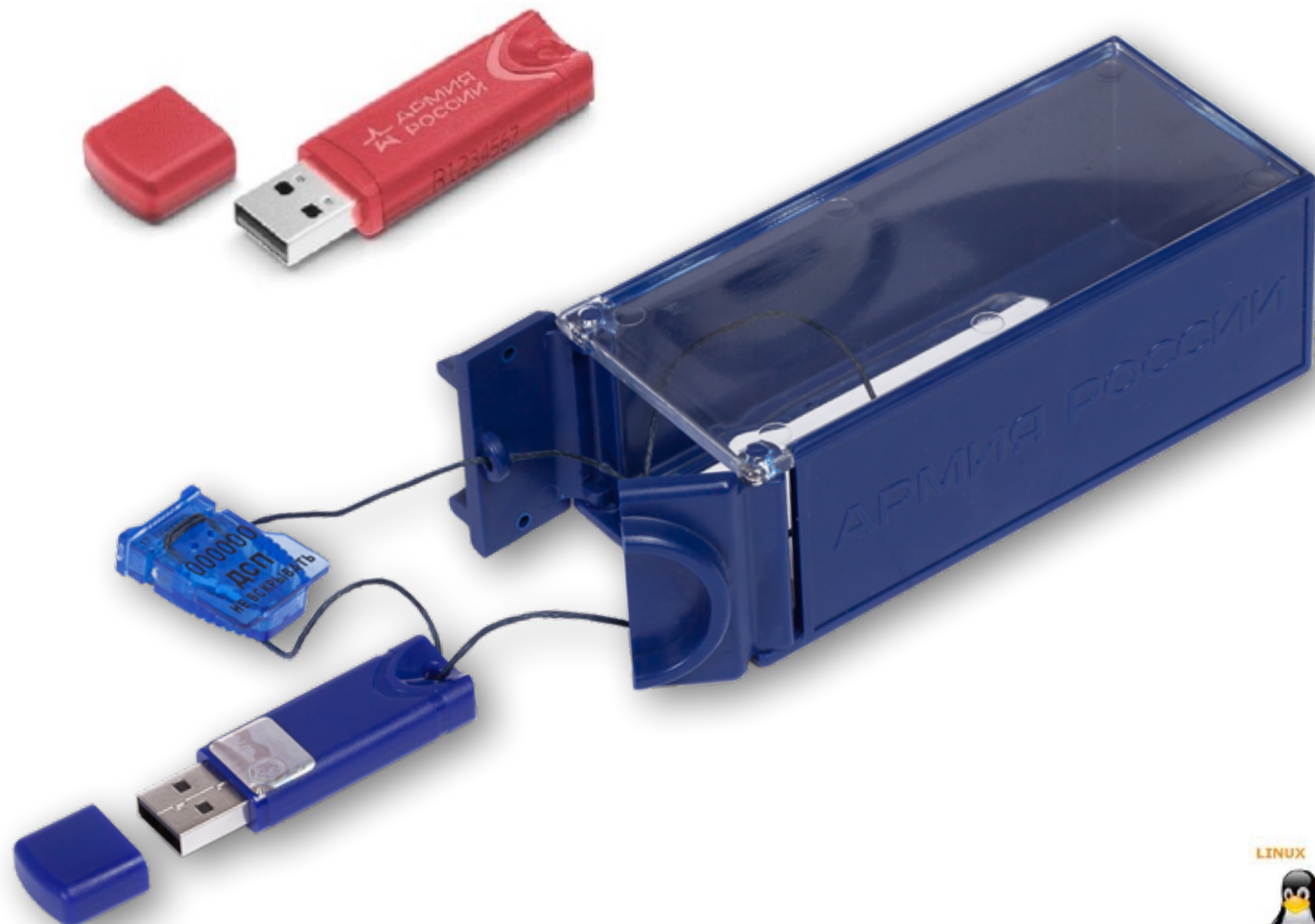
- ФСТЭК России
- Минобороны России (для работы с гостайной со степенью секретности "Совершенно секретно")



Что массово поставляем в силовые ведомства

ЗМНИ JaCarta SF/ГОСТ

Защищённый служебный USB-накопитель для безопасного хранения, переноса информации с контролем её отчуждения (разрешением копирования на данный компьютер или с него)



НОВИНКА!

JaCarta FlashDiode

Персональный специализированный однонаправленный USB-флеш-накопитель для безопасного переноса информации из открытого контура в закрытый (с ГТ)

- Для замены одноразовых (неперезаписываемых) оптических дисков CD-ROM и дорогих однонаправленных USB-шлюзов
- Для ускорения и удешевления процесса



НОВИНКА!

SecurCD

Защита данных от утечек при их передаче на CD-ROM



Давайте делать всё правильно и безопасно!

- ◆ Нам дали уникальную возможность сделать всё правильно
 - Не пытаться точечно заместить один продукт другим, а начать с проектирования правильной и безопасной ИТ-инфраструктуры
- ◆ На банковском рынке это удалось сделать
 - Россия совершила "квантовый скачок" - перепрыгнула целую эпоху платёжных карт с магнитной полосой, сразу на смарт-карты - и стала одним из лидеров
- ◆ У нас есть исторический шанс
 - Спроектировать наши ИТ-инфраструктуры изначально правильно и безопасно, без наследования "родимых пятен"
 - Давайте стараться делать всё правильно и безопасно! ...и немного на вырост
 - *PKI, сертификаты доступа, строгая аутентификация каждого субъекта инфраструктуры*



Аладдин - будь собой в электронном мире!



Спасибо!

Сергей Груздев

ген. директор
АО "Аладдин"

www.aladdin.ru



АЛАДДИН – ведущий российский разработчик и производитель ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры предприятий и защиты её главных информационных активов.

Компания работает на рынке с апреля 1995 г.

Многие продукты, решения и технологии компании стали лидерами в своих сегментах, а во многих крупных организациях и Федеральных структурах - стандартом де-факто.

Компания имеет все необходимые лицензии ФСТЭК, ФСБ и Минобороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной, производство, поставку и поддержку продукции в рамках гособоронзаказа.

Большинство продуктов компании имеют сертификаты соответствия ФСТЭК, ФСБ, Минобороны России и могут использоваться при работе с гостайной со степенью секретности до "Совершенно Секретно".

С 2012 г. в компании внедрена система менеджмента качества продукции (СМК), ежегодно проводится внешний аудит, имеются соответствующие сертификаты ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и ГОСТ РВ 0015.002-2020 на соответствие требованиями российского военного стандарта, необходимые для участия в реализации гособоронзаказа.

Ключевые компетенции

- ◆ Аутентификация
 - Подготовлено 12 национальных стандартов по идентификации и аутентификации (ГОСТ 58833-2020, ГОСТ Р 70262-2022)
 - Выпущено учебное пособие "Аутентификация – теория и практика"
 - Защищена докторская диссертация
- ◆ Доверенная загрузка и технология "стерилизации" импортных ARM-процессоров с TrustZone
- ◆ Разработка встраиваемых (embedded) Secure OS и криптографии для микроконтроллеров, смарт-карт, JavaCard
- ◆ Биометрическая идентификация и аутентификация по отпечаткам пальцев (Match On Card/Device)
- ◆ PKI для Linux и российских ОС
- ◆ Прозрачное шифрование на дисках, флеш-накопителях
- ◆ Защита баз данных и технология "опровославливания" зарубежных СУБД
- ◆ Аутентификация и электронная подпись для Secure Element (SE), USB-токенов, смарт-карт, IoT-устройств, Web-порталов и эл. сервисов.