Многофакторная аутентификация при работе с Termidesk VDI

Как выполнить требования регуляторов по ИБ (117-й приказ ФСТЭК)

Сергей Груздев

ген. директор "Аладдин Р.Д."

Ноябрь, 2025 г. V1

Груздев Сергей Львович

- Более 30 лет возглавляет компанию Аладдин
- Один из трёх авторов, в своё время придумавших USB-токен для аутентификации и ЭП
- Один из авторов и редакторов учебного пособия "Аутентификация - теория и практика"
- Один из авторов концепции и требований, заложенных в основу российских ГОСТов по идентификации и аутентификации (14 шт.)
- Награждён
  - Двумя медалями ФСТЭК России I и II степени "За укрепление государственной системы защиты информации"
  - Медалью Министерства обороны "Генерал армии Штеменко" за заслуги по защите государственной тайны ВС РФ

Аладдин

- Российский разработчик и производитель средств ИБ:
  - Ключевых компонентов для построения безопасной доверенной ИТ-инфраструктуры
  - Средств аутентификации, ЭП и защиты данных
- Разработчик 14-ти национальных стандартов (ГОСТов) по идентификации и аутентификации
- 30 лет на рынке ИБ

Кто, зачем и почему внедряет российские продукты?

Кто, зачем и почему внедряет российские продукты группы Астра?

- Кто?
  - Гос. организации (ГИС)
  - КИИ (ИС ЗО КИИ)
  - Крупный и средний бизнес
- Зачем?
  - Обязаны выполнять требования регуляторов (ФСТЭК, ФСБ, Минобороны, Минцифры, Минпромторг) - **Compliance**
  - **Снизить потери -** финансовые и репутационные, **избежать ответственности** в случае инцидента ИБ
    - Оборотные штрафы (ИСПДн)
    - Административная и уголовная ответственность (ЗО КИИ)
      - Планируется ввести уголовную ответственность за использование иностранного ПО, если произошел инцидент ИБ в ЗО КИИ

✓ **Все помним инцидент с Аэрофлотом…**

- Почему?
  - Технологический суверенитет (независимость от зарубежных вендоров)
    - Невозможность вырубить/блокировать ИТ-инфраструктуру из-за рубежа
  - Доверие и подтверждённая **безопасность**

Termidesk VDI
- Compliance
- Безопасность

Назначение:
обеспечение удалённого доступа к виртуальным и физическим рабочим местам пользователей

Требования ФСТЭК (117й Приказ)
Требования ФСБ (117й Приказ)

Требования к аутентификации пользователей и защите носителей информации (данных на дисках)
Требования к защите носителей информации (данных на дисках)

Новые требования 117-го Приказа ФСТЭК России

- Содержат
  - **Минимально необходимые требования** к защите информации
  - Обязательны для защиты
    - **От несанкционированного доступа** в ИС (НСД)
- Распространяются на владельцев и операторов
  - Государственных ИС (ГИС)
  - ИС **подрядных организаций**, осуществляющих взаимодействие с ГИС, получающие информацию из ГИС
    - Многие крупные коммерческие компании рассматривают эти требования как **лучшие практики** и берут их на вооружение

✓ **Рассматриваются как базовые требования для КИИ**

- Вводятся в действие
  - **С 1 марта 2026 г.**
- Класс защищённости ГИС определяется
  - Степенью возможного ущерба в результате инцидента ИБ
    - Нарушение функционирования (блокирование) ИТ-инфраструктуры
    - Нарушение безопасности информации (конфиденциальности, целостности, доступности)
  - Масштабом ИС

Уровень значимости (УЗ) информации	Федеральный	Региональный	Объектовый
УЗ 1 (высокий)	**К1**	**К1**	**К1**
УЗ 2 (средний)	**К1**	**К2**	**К2**
УЗ 3 (низкий)	**К2**	К3	К3

Строгая аутентификация
- привилегированных пользователей (администраторов, VIP-пользователей (п.48, 58)
- пользователей мобильных устройств - ноутбуков, планшетов (п.42)
- удалённых пользователей (п.46)
- сотрудников подрядных организаций (п.48, 58)

Допускается
Усиленная аутентификация

Требования к аутентификации пользователей

Идентификация и аутентификация

- Что такое идентификация
  - Это способ или процесс определения личности пользователя (субъекта)
- Что такое аутентификация
  - Это технология и процесс подтверждения идентификационных данных (личности пользователя)
- Виды аутентификации и уровни доверия/надёжности

	Вид аутентификации	Уровень доверия (надёжности)	Характеристика	Примеры
Запрещено	**Простая**	**Низкий**	Однофакторная, односторонняя	• Пароль • Эл. идентификатор (iButton)
Для К3	**Усиленная**	**Средний**	2ФА/3ФА, двух/многоэтапная (коды доступа, OTP, SMS, push, QR-коды и пр.)	Программные токены для смартфона: • Яндекс Ключ, Google Authenticator, **Aladdin 2FA** Эл. идентификаторы: • OTP-токен, U2F-токен, USB-токен, iButton+PIN
Для К2-К1 Если есть ДСП	**Строгая**	**Высокий**	2ФА/3ФА, взаимная, защищённый неклонируемый **токен с аппаратной криптографией**, с неизвлекаемым закрытым ключом, с использованием цифровых сертификатов и **PKI** (с третьей доверенной стороной) или другим надёжным подтверждением личности (контактная **биометрия**)	• Аппаратные криптографические токены • Смарт-карты • BIO-токены

Понятия, определения, требования

- Определены в национальных стандартах РФ (14 шт.), основные из них:
  - ГОСТ Р 58833-2020 (Идентификация и аутентификация. Общие положения)
  - ГОСТ Р 70262.1-2022 (Идентификация и аутентификация. Уровни доверия идентификации)
  - ГОСТ Р 70262.2-2025 (Идентификация и аутентификация. Уровни доверия идентификации)

Если организация использует пароли, значит она не контролирует доступ к своим ресурсам

* - разработаны компанией "Аладдин"

Проблемы реализации
строгой аутентификации пользователей в ОС Linux

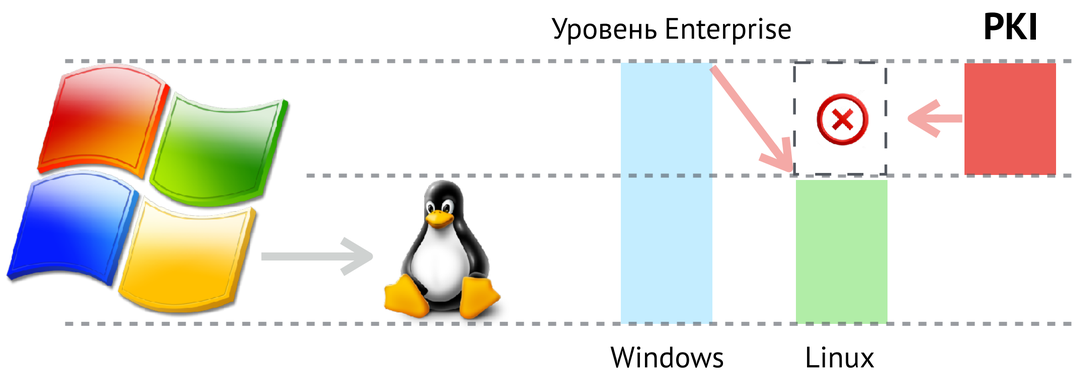
Проблемы реализации строгой аутентификации в Linux

Импортозамещение

- Возможна ли полноценная миграция на Linux без кардинального снижения безопасности в ИС?
- Возможна ли бесшовная миграция на Linux?

- **В составе Linux нет полноценного PKI Enterprise-уровня**

- **Нельзя обеспечить строгую аутентификацию** (по сертификатам)
  - оборудования
  - ПО
  - пользователей



В экосистеме отечественных ОС (Linux)

- Корп. центр сертификации (CA)
- Служба каталога/контроллер домена
- Клиент PKI (полный стек PKI)
- Клиент 2ФА/3ФА
- PKI-токены, смарт-карты, BIO-токены
- Система централизованного управления ЖЦ токенов и сертификатов

Аладдин

Необходимые компоненты для внедрения строгой аутентификации

Aladdin ePKI

В экосистеме Windows — Бесшовная миграция и работа в двух экосистемах → В экосистеме отечественных ОС (Linux)

В экосистеме Windows	Aladdin ePKI	В экосистеме отечественных ОС (Linux)
◆ Корп. центр сертификации - MS CA (CS), входит в состав MS Windows Server	**Aladdin eCA**	◆ Корп. центр сертификации (CA)
◆ Служба каталога/контроллер домена - MS Active Directory (AD)		◆ Служба каталога/контроллер домена - ALD Pro
◆ Клиент PKI и 2ФА - MS Windows Smart Card Logon	**Aladdin SecurLogon**	◆ Клиент PKI (полный стек PKI) ◆ Клиент 2ФА/3ФА
◆ PKI-токены, смарт-карты, BIO-токены	**JaCarta-3 PKI/ГОСТ** **JaCarta Virtual Token** **JaCarta SecurBIO** **JaCarta Mobile** **Aladdin 2FA + JAS**	◆ PKI-токены, смарт-карты, BIO-токены
◆ Система централизованного управления ЖЦ токенов и сертификатов	**Aladdin JMS/JAS/JIP**	◆ Система централизованного управления ЖЦ токенов и сертификатов ◆ JIP - Identity Provider, SSO, IAM

+

НОВИНКА

Что нужно для реализации строгой аутентификации пользователей в ОС Linux и при работе с Termidesk VDI

Идентификация и аутентификация - основа (фундамент) ИБ

- Неправильно реализованная подсистема идентификации и аутентификации - основной источник инцидентов в ИС
- После инцидента часто начинается не устранение его причин, а борьба с последствиями атак, взломов, кражи чувствительной информации, блокирования инфраструктуры
- ИБ-бюджеты часто тратятся на модные ИБ-технологии и продукты, а не на системы аутентификации - то, что способно устранить до 70% всех проблем

Требования 117-го Приказа ФСТЭК в части аутентификации пользователей

- п.30а, б, 34д, е, ж, з, к, 40, 41, 42, 46, 48, 58, 63

Что нужно для реализации строгой аутентификации

Орг. меры

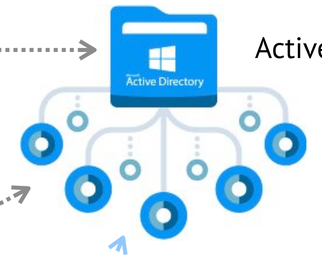
Правильно реализованная **система первичной идентификации и аутентификации**
- Всего оборудования в ИТ-инфраструктуре
- ПО (программных сервисов, шлюзов, VDI и пр.)
- Пользователей

Меры защиты (ИАФ, УПД) - *проект*

Технические средства

Корп. центр сертификации (CA)
- Корневой CA (offline)
- Подчинённые CA (online)
  - Центр Регистрации (выпуск)
  - Центр Сертификации (обслуживание)
  - Центр Валидации (проверка и подтверждение)

Служба каталога/контроллер домена
- ALD Pro и др.



Active Directory

Клиент PKI
- Полный стек PKI для Linux и Windows (!)

Клиент для средств 2ФА/3ФА
- Для локальной, доменной и браузерной аутентификации

Средства 2ФА/3ФА

Аппаратные средства 2ФА/3ФА
- PKI-токены, смарт-карты, BIO-токены

Ресурсная система

Защищённое хранилище

Система централизованного управления ЖЦ
- Токенов, сертификатов, СЗИ, СКЗИ
- Доставка сертификатов для оборудования и ПО вне домена

Aladdin Enterprise CA

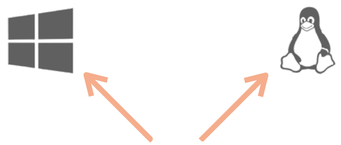
Доверенный корпоративный центр сертификации (CA) - основа PKI

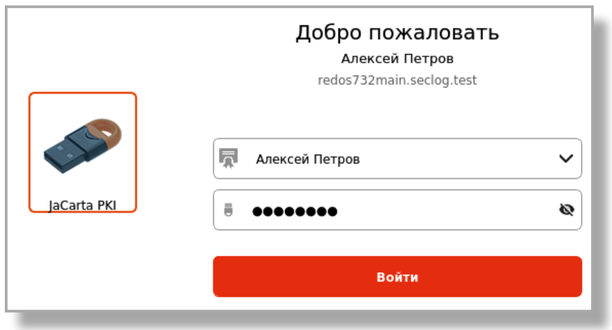
- Для замещения MS CA (CS)
  - MS CA - **единая точка отказа** для всей ИТ-инфраструктуры
- Обеспечивает
  - Создание и функционирование корпоративной инфраструктуры открытых ключей (PKI)
  - Объединение всех компонентов ИТ-инфраструктуры в **единый домен безопасности,** их аутентификацию и безопасное взаимодействие
- Позволяет
  - Бесшовно (без остановки сервисов) полноценно заместить MS CA, работать **параллельно** с ним (под Linux)
  - Переехать на отечественную ОС (Astra Linux) без снижения уровня ИБ и управления
  - **Построить полноценный PKI в сложной гетерогенной инфраструктуре**
  - Одновременно работать в двух экосистемах (Windows / Linux)
  - **Реализовать строгую аутентификацию** (по цифровым сертификатам)
    - Используемого оборудования и ПО (роутеров, маршрутизаторов, МСЭ, VDI, VPN, RDP-шлюзов и пр.)
    - Пользователей
  - Одновременно работать с различными службами каталогов (Windows AD, ALD Pro и др.)

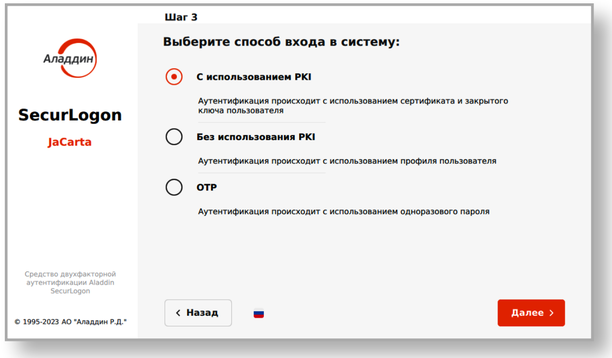
Aladdin Enterprise CA

Импортозамещение	Microsoft Certificate Authority (MS Certificate Services - MSCS)
Сертификация	**Сертификат ФСТЭК России №4835** (для работы с конфиденциальной информацией) *Ведётся работа по увеличения класса до УД-2 для работы с гостайной до степени секретности "СС" вкл.* **Положительное Заключение ФСБ России № 149/3/4/794**
В Реестре отечественного ПО	№14433, 25921
Возможность поставки в рамках госзакупок и ГОЗ (по ПП-1875, 44-ФЗ, (вкл. возможность закупки у единственного поставщика), 223-ФЗ, ПП-325)	Да
Входит в совместный бандл	"**Домен безопасности**" с Astra Linux
Выполняет требования 117-го Приказа ФСТЭК	**п. 8** - Функционирование ИС на базе информационно-телекоммуникационной инфраструктуры допускается при условии защиты информационно-телекоммуникационной инфраструктуры в соответствии с Требованиями. ***Защита ИТ-инфраструктуры*** *- подразумевает обеспечение доверия между всеми её компонентами и безопасное взаимодействие.* п.30а, б, в, г, з, и, 34д, е, ж, з, к, р, 40, **42, 46, 48, 58**, 63а, б, ж, и, к, **л, м, с,** 70, 71 **–** для реализации **строгой** аутентификации в ИТ-инфраструктуре необходим собственный доверенный Центр Сертификации (требования ГОСТ Р 58833-2020, ГОСТ Р 70262.1-2022, ГОСТ Р 70262.2-2025).

Aladdin SecurLogon







PKI-клиент и поддержка средств МФА в Linux

- Обеспечивает
  - Полноценную альтернативу Windows Smartcard Logon на Linux в привычном для пользователей интерфейсе
  - Усиленную аутентификацию пользователей
    - С использованием автоматически сгенерированного сложного пароля длиной до 63 символов, который **неизвестен пользователю**
  - Строгую аутентификацию пользователей
  - 2ФА/3ФА
    - Локальную
    - Доменную - в различных службах каталога (**Windows AD**, ALD Pro, РЕД АДМ, Альт Домен, Samba DC, FreeIPA и др.)
  - Применение различных групповых политик для 2ФА/3ФА
  - Групповое развёртывание
  - Удалённое администрирование и настройку с рабочего места администратора
  - Дополнительные сервисные функции, позволяющие до входа в ОС
    - Разблокировать токен
    - Сменить ПИН-код пользователя
    - Кастомизировать окно приветствия и др.

Aladdin SecurLogon

Импортозамещение	Microsoft SmartCard Logon
Сертификация	Сертификат ФСТЭК России №4809 (для работы с конфиденциальной информацией) *Планируется увеличение класса до УД-2 для работы с гостайной до степени секретности "СС" вкл.*
В Реестре отечественного ПО	№10043
Возможность поставки в рамках госзакупок и ГОЗ (по ПП-1875, 44-ФЗ, 223-ФЗ, ПП-325)	Да
Входит в совместный бандл	"Домен безопасности" с Astra Linux, Alt Linux
Выполняет требования 117-го Приказа ФСТЭК	п.30а, б, 34д, е, ж, з, к, 40, 41, **42, 46, 48, 58**, 63 - строгая/усиленная аутентификация пользователей (в первую очередь привилегированных, администраторов, удалённых, сотрудников подрядных организаций) в соответствие с требованиями ГОСТ Р 58833-2020, ГОСТ Р 70262.1-2022, ГОСТ Р 70262.2-2025

Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены

JaCarta-3 PKI/ГОСТ

MicroUSB

для M2M

USB Type-C

Для работы из доверенной среды

С биометрией

SecurBIO PKI [ЭП]

SecurBIO Reader
JCR-761

Смарт-карты и ридеры

JaCarta PKI/ГОСТ/SC **+ JCR-721**

SecurBIO Reader
JCR-781

JaCarta PKI/ГОСТ/BIO

Терминальный клиент

Termidesk VDI
"на борту"

Для работы из недоверенной среды (домашний/чужой ПК)

Aladdin LiveOffice

LiveUSB+ОС+VPN+RDP/**VDI**+PKI+УКЭП

Аппаратные средства от Аладдин для строгой аутентификации

Импортозамещение	Любой аналогичный продукт
Сертификация	Сертификат ФСТЭК России №4446 Сертификаты ФСБ России №СФ/124-4641, СФ/124-4611, СФ/124-5060, СФ/124-5061, СФ/124-5062
В Реестре отечественного ПО	№4300, 4301
В Реестре радиоэлектронной промышленности Минпромторга (ПП-878, ПП-719)	№10522179, 10457431, 10495356, 10382754, 10522180, 10457432, 10522178, 10457430 №10598244, 10598245, 10598246, 10598247, 10598248
В Реестре ПАКов (Минцифры)	№18780, 19311, 19312, 19313
Возможность поставки в рамках госзакупок и ГОЗ (по ПП-1875, 44-ФЗ, 223-ФЗ, ПП-325)	Да
Выполняет требования 117-го Приказа ФСТЭК	п.30а, б, **42, 46, 48, 58**, 63 - строгая/усиленная аутентификация пользователей в соответствие с требованиями ГОСТ Р 58833-2020, ГОСТ Р 70262.1-2022, ГОСТ Р 70262.2-2025.
Выполняет требования ФСБ к СКЗИ	Соответствует требованиям 63-ФЗ и Приказа ФСБ России № 796 к средствам ЭП, 117-го Приказа ФСБ - п.1, 3, 6 (СКЗИ и ЭП для защиты данных, придания юридической значимости, шифрование данных на носителях вне контролируемой зоны).

Доп. способы аутентификации (подтверждения личности)

- Адаптивная МФА
  - **Достоверность результатов аутентификации зависит от условий работы, сред функционирования**
  - В зависимости от рисков (работа вне контролируемой зоны, повышенные привилегии или доступ ко всем ресурсам ИС, удалённая работа и пр.) должен быть определён РАЗНЫЙ набор средств, методов и способов подтверждения личности пользователя

✓ **Больше рисков - больше дополнительных способов, методов, средств и компенсационных мер**

- Рекомендуется в случаях
  - Отсутствия/невозможности использования PKI (Центра Валидации)
  - При удалённом доступе
  - Для привилегированных пользователей

✓ **Биометрия - лучший способ подтверждения личности пользователя**

  - Подтверждается факт владения пользователем своим персональным устройством (токеном, смарт-картой с поддержкой PKI)
  - Может использоваться как **третий фактор** (вместе с вводом PIN-кода) или как **второй фактор** (вместо ввода PIN-кода)
  - Тип биометрической идентификации
    - **Контактный - по отпечаткам пальцев** (ВАЖНО: если сканер отпечатков расположен "на борту" устройства и отпечатки пальцев не попадают в ПК и/или в ИС, владелец ИС не становится оператором персональных биометрических данных)
    - **Бесконтактный** - по распознаванию лица или голоса (настоятельно не рекомендуется из-за возможностей генеративного ИИ, из-за законодательных ограничений - только через ЕБС, существенно дороже)

Высокий уровень доверия

Aladdin SecurBIO-токен

Централизованное управление жизненным циклом
средств 2ФА/3ФА, сертификатов, СЗИ, СКЗИ

Требования 117-го Приказа ФСТЭК: п.30а, б, **42, 46, 48, 58**, 63, 70, 71

JMS (JaCarta Management System)

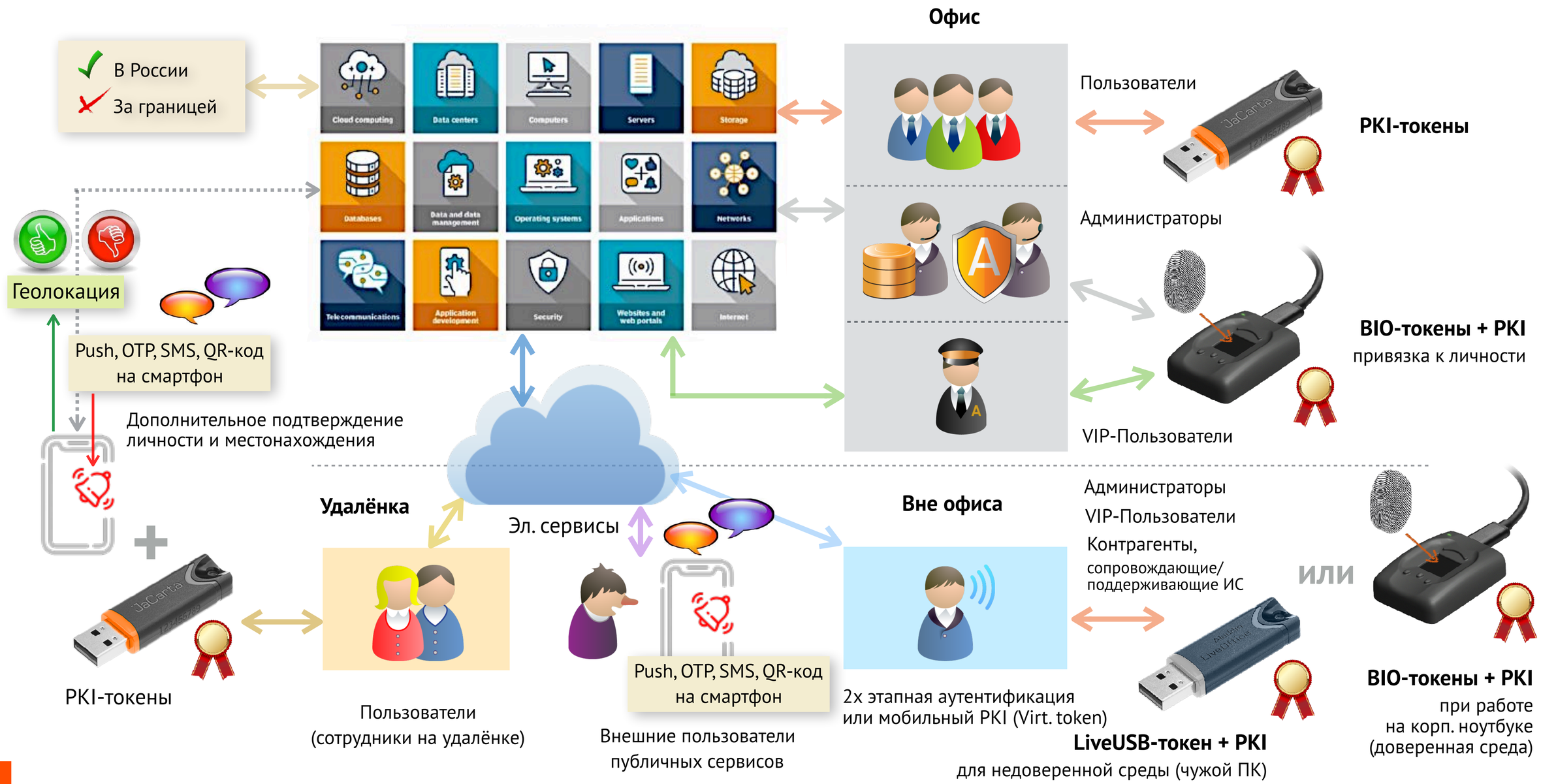
Система централизованного управления жизненным циклом сертификатов, токенов, СЗИ, СКЗИ

- Обеспечивает
  - Учёт и управление жизненным циклом
    - Аппаратных USB-токенов, BIO-токенов, смарт-карт, U2F-токенов, смарт-карт ридеров, BIO-ридеров
    - Программных (виртуальных) токенов, OTP/PUSH/SMS-аутентификаторов
    - Специализированных средств безопасной дистанционной работы (Aladdin LiveOffice)
    - Защищённых съёмных носителей (флеш-накопителей)
    - СЗИ, СКЗИ
    - Цифровых сертификатов доступа и ЭП
    - Объектов PKI, профилей
  - Автоматическое взятие под управление средств 2ФА/3ФА
    - Ранее введённых в эксплуатацию (до внедрения JMS)
    - Новых
  - Автоматизацию большинства рутинных операций и применения политик безопасности (например, требований к ПИН-кодам)
  - Автоматическую рассылку уведомлений
  - Быструю подготовку типовых профилей и конфигураций для разных групп пользователей
  - Мониторинг и аудит действий пользователей и администраторов
  - Удобный сервис самообслуживания пользователей (Web-портал)
- Включает
  - Высокопроизводительный **сервер аутентификации** Enterprise-класса - JAS для усиленной и адаптивной 2ФА/3ФА

JMS (JaCarta Management System)

Импортозамещение	Любой аналогичный продукт
Сертификация	Сертификаты ФСТЭК России №4411, №4516 (для работы с конфиденциальной информацией) Сертификат Минобороны №5444 (для работы с гостайной до "Совершенно секретно")
В Реестре отечественного ПО	№311, 11260
Возможность поставки в рамках госзакупок и ГОЗ (по ПП-1875, 44-ФЗ, 223-ФЗ, ПП-325)	Да
Выполняет требования 117-го Приказа ФСТЭК	п.30а, б, **42, 46, 48, 58**, 63, 70, 71 – управление цифровыми сертификатами и средствами строгой и усиленной аутентификации пользователей в соответствие с требованиями ГОСТ Р 58833-2020, ГОСТ Р 70262.1-2022, ГОСТ Р 70262.2-2025.

Адаптивная МФА в ИС



Что нужно
для внедрения усиленной аутентификации

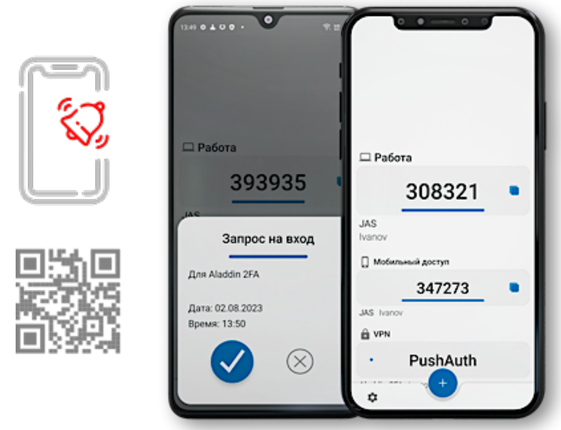
Усиленная аутентификация:

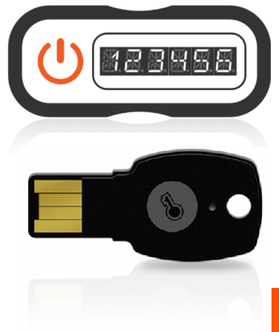
- **Только для класса К3**
- Допускается использовать для классов К2, К1 при обоснованной невозможности реализовать строгую аутентификацию (отсутствие домена, малый размер ИС, когда разворачивать PKI не целесообразно и дорого)

Усиленная аутентификация (если невозможно реализовать строгую)

- Усиленная 2ФА — п. 48 Требований
  - Обязательно должен быть **фактор ВЛАДЕНИЯ** (1)
    - Электронный идентификатор (защищённое неклонируемое устройство)
    - [**Смартфон**] + [QR-код, SMS, push, OTP]
  - ✓ **Только при работе на компьютере - чтобы было разделение сред**
  - ✓ **Если работа на смартфоне - это 2х этапная аутентификация (не 2ФА)**
  - Второй фактор (2) - **ЗНАНИЕ** (PIN-код устройства) или **БИОМЕТРИЯ**
- Первичная идентификация — *- важно, про неё все забывают*
  - **Личная явка** (вручение эл. идентификатора)
  - **Допускается удалённая**, но с обязательным использованием доп. средств идентификации
    - [**Смартфон**] + [**QR-код, SMS, push, OTP**] и/или [**Биометрия** (лицо, голос)]
    - Должна быть **безопасная передача общего секрета** (нет практически ни у кого)
- Необходимые компоненты
  - **Сервер аутентификации**
    - Важно: база данных с ключами, профилями и аутентификационной информацией должна быть надёжно защищена с помощью СКЗИ (нет практически ни у кого)
  - **Клиентское ПО** (приложение)
  - **Система централизованного управления ЖЦ**
  - **Эл. идентификаторы** / смартфон пользователя

Аутентификация
- это подтверждение идентификационных данных

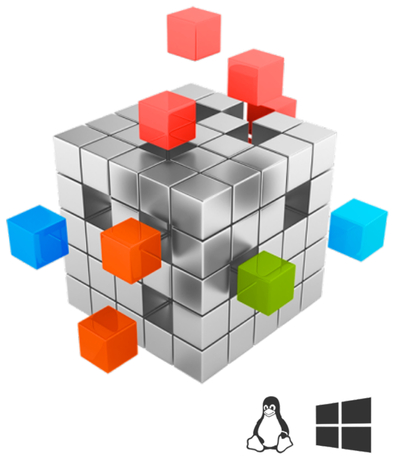




Геолокация

Блокирование доступа к ИС из-за рубежа
п. 46 Требований

JAS (JaCarta Authentication Server)

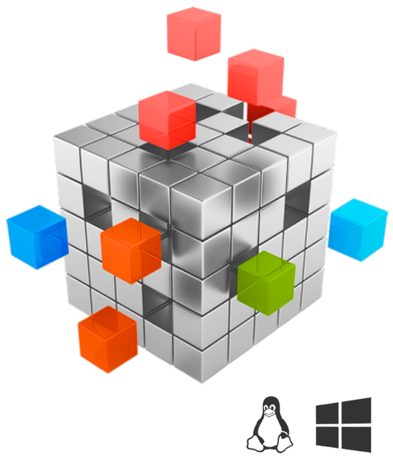


Глубоко интегрирован с JMS (системой централизованного управления ЖЦ токенов)

Высокопроизводительный сервер аутентификации Enterprise-класса

- Обеспечивает
  - Усиленную и/или адаптивную (дополнительную) аутентификацию пользователей
    - В инфраструктурах без PKI
    - В ОС Linux, Windows, macOS
    - В сервисах и приложениях с использованием U2F-совместимых токенов и OTP, SMS, PUSH, Telegram OTP – аутентификаторов
  - Безопасный доступ внешних и внутренних пользователей к информационным системам и сервисам:
    - шлюзам удалённого доступа КриптоПро NGate, UserGate, Microsoft, Cisco, Citrix, Palo Alto, Check Point, VMware, Fortinet и др.
    - шлюзам к рабочим столам Microsoft RDG
    - CRM, ERP, MS SharePoint, MS Outlook Web App, эл. почте
    - web-приложениям, облачным сервисам
    - системам ДБО, ЭДО и др
  - Высокую отказоустойчивость (Failover Cluster) и производительность (более 5,000 аутентификаций в сек.)
- Позволяет
  - Использовать **смартфон в качестве второго фактора** при работе на ПК (ВЛАДЕНИЕ)
  - Работать с различными приложениями
    - **Aladdin 2FA** (с безопасной передачей общего секрета - QR-код)
    - Яндекс.Ключ
    - Google Authenticator и др.
  - Использовать стандартные протоколы (RADIUS, REST, WCF, WS-Federation (ADFS), HTTP и SMPP (для интеграции с SMS-шлюзами)

JAS (JaCarta Authentication Server)



Импортозамещение	Любой аналогичный продукт
Сертификация	Сертификат ФСТЭК России №4516 (для работы с конфиденциальной информацией)
В Реестре отечественного ПО	№11260
Возможность поставки в рамках госзакупок и ГОЗ (по ПП-1875, 44-ФЗ, 223-ФЗ, ПП-325)	Да
Выполняет требования 117-го Приказа ФСТЭК	п.30а, б, **42, 46, 48, 58**, 63, 70, 71 - строгая/усиленная аутентификация пользователей в соответствие с требованиями ГОСТ Р 58833-2020, ГОСТ Р 70262.1-2022, ГОСТ Р 70262.2-2025.

Программные средства для 2ФА/3ФА и адаптивной аутентификации

Aladdin 2FA

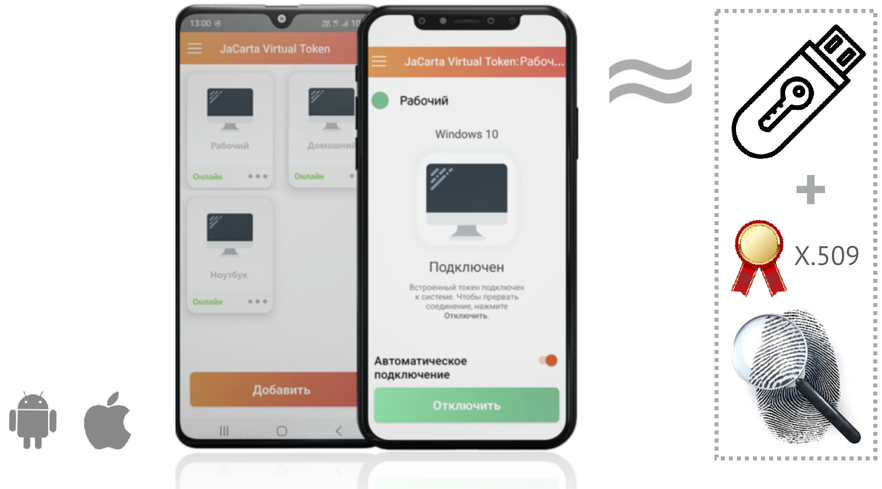
Мобильное приложение

- Обеспечивает
  - Аутентификацию пользователя с использованием OTP/Push
- Позволяет
  - Использовать смартфон в качестве второго фактора при работе на ПК
  - Выпускать неклонируемые аутентификаторы (важно!)
  - Безопасно получить вектор инициализации с помощью одноразового QR-кода
  - Получать и передавать в ИС геолокацию

JaCarta Virtual Token

Мобильное приложение

- Обеспечивает
  - Функциональность аппаратного токена JaCarta PKI
  - Строгую 2ФА пользователя по цифровым сертификатам (не для ГИС)
- Позволяет
  - Использовать смартфон в качестве второго фактора при работе на ПК (в т.ч. без Интернета)
  - Моментально получить дубликат USB-токена при его блокировании/утере (Rescue-token)
  - Быстро выдавать VT подрядчикам и контрагентам



Требования к обеспечению удалённого доступа

п. 46 Требований 117-го Приказа ФСТЭК

При удалённом доступе к ИС

- должна быть исключена возможность НСД (воздействия) к ИС и содержащейся в них информации, к СВТ пользователей через каналы передачи данных, интерфейсы, порты
- должны использоваться выделенные оператором ИС СВТ с установленными СЗИ и СКЗИ и соответствующие Требованиям
- могут использоваться личные (недоверенные) СВТ при условии применения специализированных сертифицированных ФСТЭК России средств обеспечения безопасной дистанционной работы
  - **Обеспечивается с помощью Aladdin LiveOffice**

Aladdin LiveOffice (ALO)

Специализированное средство обеспечения безопасной дистанционной работы

- Обеспечивает
  - Полноценную дистанционную работу с любого недоверенного компьютера, например, с личного компьютера сотрудника
    - 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, коммерческой, служебной тайны (ДСП)
    - 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 свою учётную запись, пароль, параметры удалённого подключения
    - загрузить в ИС троян или вирус
- Позволяет
  - В 5-7 раз экономить бюджет при организации удалённого доступа
  - Выполнить требования 117-го Приказа ФСТЭК и ФСБ России по организации безопасной дистанционной работы
  - Использовать USB-устройство Aladdin LiveOffice вместо служебного ноутбука как удалённое рабочее место (терминальный клиент) с предустановленным и преднастроенным ПО в замкнутой доверенной программно-аппаратной среде

Termidesk VDI
"на борту"

Aladdin LiveOffice (ALO)

Сертификация	Сертификат ФСТЭК России №4355 Сертификаты ФСБ России №СФ/124-4641, СФ/124-5060 (на СКЗИ в составе продукта)
В Реестре ПАКов (Минцифры)	№20648
В Реестре отечественного ПО	№4300, 4301
В Реестре радиоэлектронной промышленности Минпромторга (ПП-878, ПП-719)	№10495358, 10495359, 10495360
Возможность поставки в рамках госзакупок и ГОЗ (по ПП-1875, 44-ФЗ, 223-ФЗ, ПП-325)	Да
Выполняет требования 117-го Приказа ФСТЭК	п.30а, б, в, г, д, з, и, 34д, е, з, к, 37, 40, **41**, **42**, **46**, **48**, 49, **51**, 58, 63а, б, в, и, к, 70, 71 - удалённый доступ из недоверенной среды, защита конечных устройств, работа с ДСП, строгая/ усиленная аутентификация пользователей в соответствие с требованиями ГОСТ Р 58833-2020, ГОСТ Р 70262.1-2022, ГОСТ Р 70262.2-2025, защита канала передачи данных Соответствует требованиям 32-го Приказа ФСТЭК (Требования к средствам дистанционной работы)
Выполняет требования ФСБ к СКЗИ	Соответствует – требованиям 63-ФЗ и Приказа ФСБ России № 796 к средствам ЭП – 117-го Приказа ФСБ - п.1, 3, 6 (СКЗИ и ЭП для защиты данных, придания юридической значимости, шифрование данных на носителях вне контролируемой зоны, защита канала передачи данных)

Как обеспечить защиту машинных носителей информации

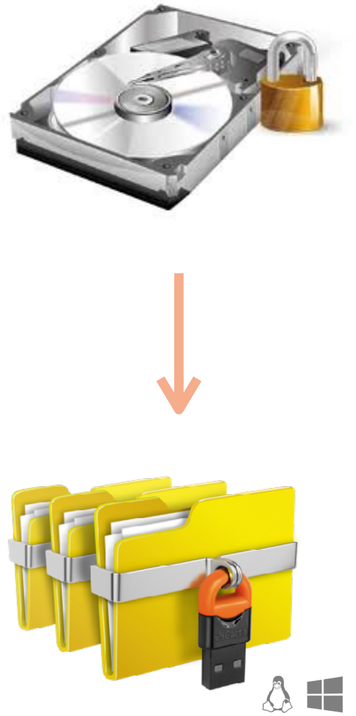
п. 34д, е, ж, к, 37, 40, 41,42, 51, 63, 70, 71 Требований 117-го Приказа ФСТЭК

Должны применяться:

- Защита конфиденциальной информации от НСД на машинных носителях конечных, переносных устройств, съёмных носителей
- Установка и хранение СВТ и съёмных носителей в помещениях, шкафах, сейфах, исключающий к ним физический доступ посторонних
- **Шифрование** данных на машинных носителях с использованием сертифицированных ФСБ России СКЗИ в случаях, если конечное/переносное устройство, машинный носитель хранится или используется вне контролируемой зоны (защищённого периметра организации)

Требования к защите конечных и мобильных (переносных) устройств

- Должна обеспечиваться
  - Невозможность получения доступа к конфиденциальной информации лицами, не имеющими на это права, злоумышленниками
  - Регистрация фактов физического доступа к ним
  - Гарантированное удаление (стирание) информации с машинных носителей (в случае утраты необходимости дальнейшего хранения такой информации, при передаче средств хранения (машинных носителей) в сторонние организации для ремонта, технического обслуживания и др.)
  - Невозможность изменения настроек и конфигураций пользователями



Secret Disk - система предотвращения утечек и шифрования данных на дисках

- Обеспечивает
  - Предотвращение утечки и несанкционированного доступа к ценной информации при утере, краже, изъятии, ремонте, неправильной утилизации компьютеров, серверов, носителей информации
  - Защиту данных
    - на ноутбуках, персональных компьютера, планшетах сотрудников
    - на файл-серверах и серверах приложений (в т.ч. баз данных)
    - на съёмных носителях
  - Сокрытие наличия конфиденциальной информации на защищённом компьютере или носителе
  - Гарантированно необратимое и, при необходимости, мгновенное уничтожение 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
  - Защиту от действий привилегированных пользователей (системных администраторов)
  - Централизованное управление, интеграцию с системой управления JMS
- Позволяет
  - Прозрачно (незаметно для пользователя, "на лету") шифровать
    - Системный раздел, содержащий информацию об учётной записи пользователя, логины и пароли к различным информационным ресурсам, лицензионную информацию, временные файлы ОС, файлы подкачки, файлы-журналы приложений, дампы памяти, образ системы, сохраняемый на диск при переходе в "спящий" режим
    - Разделы на жёстких, логических дисках, дисковых массивах (SAN, RAID)
    - Виртуальные диски
    - Съёмные диски (USB- и Flash-диски и др.)
    - Файлы и папки

Версии

- Персональная (для Windows и Linux)
- Серверная (для файл-сервера, сервера приложений)
- Корпоративная (с централизованным управлением)

Secret Disk - система предотвращения утечек и шифрования данных на дисках

Импортозамещение	Microsoft BitLocker, CheckPoint Endpoint Security и др.
Сертификация	Сертификаты ФСТЭК России №4765 (для работы с конфиденциальной информацией) Сертификаты ФСБ России №СФ/120-5019 Сертификат Минобороны (для работы с гостайной до "Совершенно секретно")
В Реестре отечественного ПО	№513, 514, 519, 4322
Возможность поставки в рамках госзакупок и ГОЗ (по ПП-1875, 44-ФЗ, 223-ФЗ, ПП-325)	Да
Выполняет требования 117-го Приказа ФСТЭК	**п.30а, б, в, г, д, з, и**, **34д, е, ж, к,** 37, 40, **41**, **42**, 43, 44, 45, 46, 50, **51**, 55, 58, 63а, б, в, и, к, 70, 71 - Защита от НСД, МФА, шифрование данных на носителях вне контролируемой зоны - 117-го Приказа ФСБ - п.1, 3, 6 (СКЗИ для шифрование данных на носителях вне контролируемой зоны).

Дополнительные материалы

- Краткая сводная таблица по 117му Приказу - как выполнить с помощью продуктов Аладдин
  https://dms.aladdin-rd.ru/ffa4019f-92b7-4562-a447-d04a649d8860
- Про адаптивную аутентификацию
  https://dms.aladdin-rd.ru/85417a9d-1dff-49bf-bae3-6a7c8cf87f7b
- 117-й приказ ФСТЭК России
  https://dms.aladdin-rd.ru/5b11f88c-2595-47fd-a2d2-4a516f6f4c6c
- Меры защиты информации в ГИС, методические материалы (проект)
  https://dms.aladdin-rd.ru/3ba624d2-8930-460a-9bc9-be0da0996c9e
- Про средство безопасной дистанционной работы Aladdin LiveOffice
  https://dms.aladdin-rd.ru/a88af4b4-42eb-410f-ba20-3602afd63ff2
- Материалы по продуктам компании Аладдин
  www.aladdin.ru

Аладдин

Спасибо!

Сергей Груздев

ген. директор
АО "Аладдин"

www.aladdin.ru

О компании

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 7 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, IIoT-устройств, Web-порталов и эл. сервисов.