Новые Требования 117-го Приказа ФСТЭК России к защите информации в ГИС

Методические материалы и тренинг
для заказчиков и партнёров компании Аладдин

Октябрь, 2025 г. V3

Сергей Груздев

ген. директор "Аладдин Р.Д."

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

Новые Требования ФСТЭК России к защите информации в ГИС

- Подготовлены на замену устаревшим Требованиям
  - Утверждённых 17-м Приказом ФСТЭК России от 11.02.2013 и соответствующих Мер защиты
- Содержат
  - **Минимально необходимые требования** к защите информации на всех стадиях (этапах) обработки, хранения, создания, развития (модернизации), эксплуатации, вывода из эксплуатации
  - Обязательны для защиты
    - **От несанкционированного доступа** (НСД)
    - **От специальных воздействий** на информацию (**носители информации**)
- Распространяются на владельцев и операторов
  - Государственных ИС (федеральных, региональных, объектовых ИС на территории РФ - далее ГИС)
  - ИС гос. органов
  - ИС гос. унитарных предприятий
  - ИС гос. учреждений
  - Муниципальных и др. ИС
  - 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
- Вводятся в действие
  - **С 1 марта 2026 г.**

✓ **Времени на реализацию Требований очень мало!**

Новые Требования ФСТЭК России к защите информации в ГИС

- Применяются совместно
  - С **Требованиями 117-го Приказа ФСБ России** о защите информации, содержащейся в ГИС, с использованием шифровальных (криптографических) средств (когда средств защиты от НСД недостаточно)
    - **Защита каналов** передачи данных (удалённый доступ)
    - **Защита данных** на машинных носителя информации
  - Являются базовыми (минимально необходимыми) для КИИ
    - К ним планируется выпустить дополнительные требования с учётом специфики и категории КИИ
- Описывают и регламентируют
  - **ЧТО должно быть сделано** для защиты информации в ГИС
  - **КАК это должно быть сделано?** - планируется дать в Методическом документе "Меры защиты"
    - *Проект требований по идентификации и аутентификации (ИАФ), УПД, ЗНИ - подготовлен*
- Цели защиты информации в ГИС
  - Недопущение (снижение возможности) наступления негативных последствий (событий)

✓ **Оператор должен определить цели и приоритеты работ по обеспечению ИБ и сосредоточиться на главном**

Денег, ресурсов и времени на всё не хватит - **20% усилий должны давать 80% результата**
Начинать надо с главного

Новые Требования - класс защищённости ГИС

- Определяется
  - Степенью возможного ущерба в результате инцидента ИБ
    - Нарушение функционирования (блокирование) ИТ-инфраструктуры
    - Нарушение безопасности информации (конфиденциальности, целостности, доступности)
  - Масштабом ИС
    - Федеральный
    - Региональный
    - Объектовый
  - По наивысшему значению степени возможного ущерба (при обработке нескольких видов информации)
- Допускается сегментирование ИС с присвоением разных классов
- Зависит
  - От класса защищённости
    - **Информационно-телекоммуникационной (ИТ) инфраструктуры, на которой функционирует данная ГИС** NEW
    - Взаимодействующей с ней ИС (в т.ч. **подрядных организаций**)
  - От наличия информации ограниченного распространения (с пометкой **ДСП**)
    - Автоматически поднимает класс защищённости ИС до уровня К1
    - Для подключения ИС к ГИС и получению информации из ГИС класс защищённости такой ИС и её ИТ-инфраструктуры должен быть не ниже класса защищённости ГИС
- Влияет
  - На класс применяемых СЗИ (К1 - не ниже УД4, К2 - не ниже УД5, К3 - не ниже УД6)
- Должен подтверждаться аттестацией 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

Новые Требования к ГИС

- ГИС как система
  - ГИС надо рассматривать не как изолированную самодостаточную сущность, а как комплексную систему, работающую в ИТ-инфраструктуре (на различном оборудовании, в корпоративной сети, с использованием различных протоколов, сервисов и т.п.)

✓ **Задача #1 - обеспечить безопасность и доверие ИТ-инфраструктуре (п.8 Требований)**

  - К ГИС подключаются
    - Другие ИС (разработчики, контрагенты, системные интеграторы, сопровождающие и поддерживающие ИС)
    - Удалённые пользователи
    - Привилегированные, обладающие повышенными полномочиями
    - Администраторы
  - Многие инциденты с ИС происходят именно по их вине, из-за атак на них ("по цепочкам поставок"), поэтому в Требованиях уделено особое внимание:
    - Идентификации и аутентификации внутренних и внешних пользователей
    - Обеспечению безопасного удалённого доступа и дистанционной работе с информацией (в т.ч. с ДСП)
    - Защите конечных, мобильных, личных устройств, точек беспроводного доступа
    - Безопасности использования носителей информации

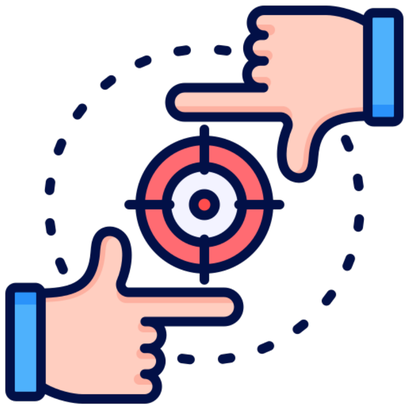
Новые Требования ФСТЭК России к защите информации в ГИС

- Основные приоритеты (фокус)

✓ **#1 - функционирование инфраструктуры, устранение в ней точек отказа**

✓ **#2 - устранение основных причин угроз ИБ, а не борьба с последствиями инцидентов:**

- (#1) **Идентификация и аутентификация** оборудования, ПО, внутренних и внешних пользователей
- (#2) Обеспечение безопасного **удалённого доступа и дистанционной работы** с информацией (с ДСП)
- (#3) **Защита конечных, мобильных (переносных) устройств**
- (#4) Безопасность использования **машинных носителей информации**



Выполнение этих приоритетных задач потребует 20% усилий и даст 80% результата

Рынок - ключевые изменения, конкуренция, стратегия

Зачем нам этим заниматься?

Ключевые изменения на рынках ГИС и КИИ

- Рынки ГИС и КИИ
  - Новые Требования ФСТЭК кардинально меняют требования к идентификации и аутентификации
  - Вводятся
    - Понятие **Доверие к ИС**
    - **Запрет на использование паролей** и **переход на 2ФА** (токены) для пользователей - усиленную и строгую, **запрет на аутентификацию оборудования по MAC-адресам**
    - Требования построения **корпоративной PKI** (доверие ко всем компонентам ИТ-инфраструктуры, ИС, пользователям)

- Оценка объёмов рынков (по нашей теме и нашим продуктам)
  - ГИС - **30 млрд. руб.**
    - Более 874 федеральных ГИС, порядка 3,300 региональных, более 100,000 объектовых
  - ГИС объектов КИИ - ещё **20-25 млрд. руб.**
    - Порядка 40,000 ИС

✓ **Суммарный объём рынка порядка 50-55 млрд. руб., мы претендуем на 20% ~10-12 млрд. руб.**

- Время
  - Новые требования вступает в действие с 1 марта 2026 г.
  - По опыту - всё пойдёт медленнее - **2,5 - 3 года** (новый продукт на новом рынке, урезание бюджетов, переносы проектов)
  - Необходимо использовать окно возможностей - правильно сформировать устойчивый спрос (под своё предложение) и вовремя удовлетворить его

Конкуренция

- По каждому отдельному продукту - достаточно сильная
- Единого комплексного решения пока нет ни у кого (кроме нас)
- Комплексное решени от одного вендора избавит заказчиков от состояния "вечного ремонта"

Стратегия - создание нового рынка ("голубой океан") под себя, игра на нём по своим правилам 5-7 лет

Основные требования 117-го Приказа ФСТЭК России

(по приоритетам важности их выполнения)

Приоритет #1

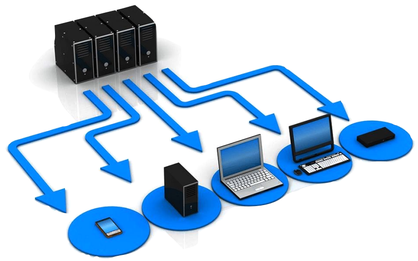
Как обеспечить безопасное функционирование ИТ-инфраструктуры, доверенное взаимодействие всех её компонентов,
устранить точки отказа

NEW

п. 8 Требований

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**



Что такое ДОВЕРИЕ (немного матчасти)

Доверие

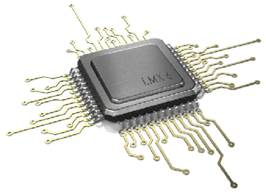
- Между людьми
  - Это уверенность в порядочности и ответственности другого, что он не воспользуется полученной от нас информацией нам во вред
- В ИТ-инфраструктуре (ИС)
  - Это уверенность в том, что
    - Каждый элемент (объект) ИТ-инфраструктуры работает так, как мы ожидаем
    - Этот элемент не подменили
    - Мы можем доверять получаемой от него информации и обмениваться с ним важной для нас информацией
    - Доступ в ИС получили только легальные пользователи (субъекты)
  - Доверие обеспечивается **идентификацией** и **аутентификацией** каждого элемента инфраструктуры
    - Объектов (оборудования, ПО)
    - Субъектов (пользователей)

Подтверждение идентификационных данных (подлинности)

Пирамида доверия

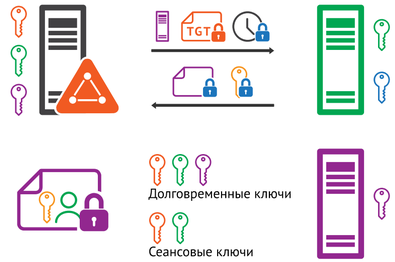
Доверие

- пришло из ISO 15408



Гарантии доверия:
- доверенная (своя) электроника
- своё производство
- проверенные/безопасные протоколы
- собственные стеки ПО
- сертификация (проверка и подтверждение независимыми экспертами)

▶ **На всё это нам нужно лет 10-15, не меньше**



3

Trust — Уверенность на основе **гарантий**

Пока нет своей микроэлектроники (полного цикла) - **для нас это недостижимо**

Не сейчас...

2

Assurance — **Подтверждённая уверенность**
- Кем?
- Третьей доверенной стороной

Никто никому не верит, но все верят своему корпоративному "нотариусу"

Корп. нотариус обеспечивает **доверенное взаимодействие** всех компонентов ИТ/ИС
- Оборудования
- ПО
- Пользователей

Это корпоративный PKI

Нам сюда!

1

Confidence — **Уверенность на основе предположения**

Верим "на слово", что нас не обманывают

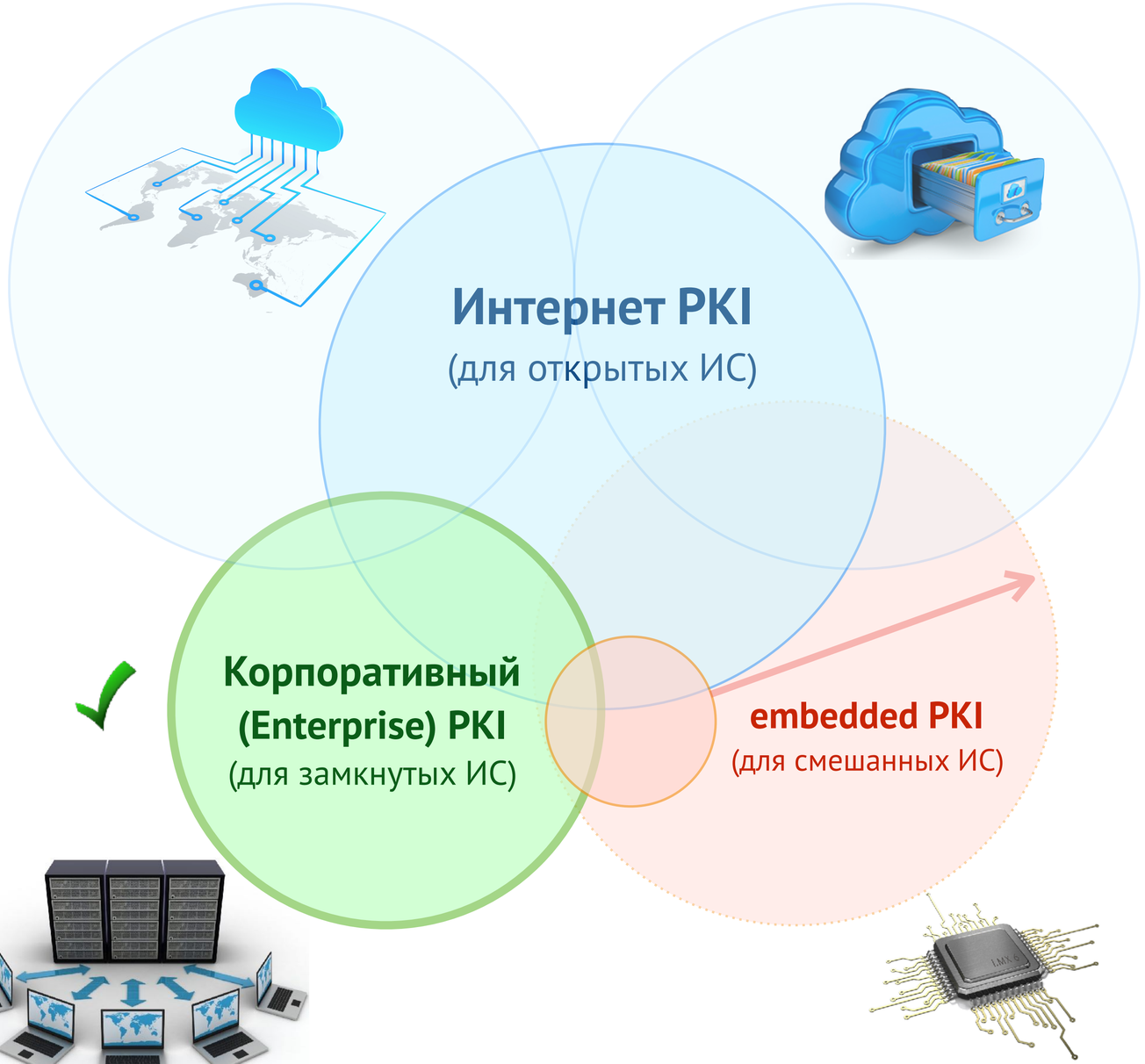
Предполагаем, что система работает так, как нам обещали

Нужно уходить отсюда

Сейчас мы здесь (#1)
Уровень доверия - низкий

Наша цель - усилить доверие, перейти на уровень #2

Мир PKI



- Цели, принципы и технологии практически одинаковые
- Задачи немного разные
- Проблема - часто смешиваем их и путаем

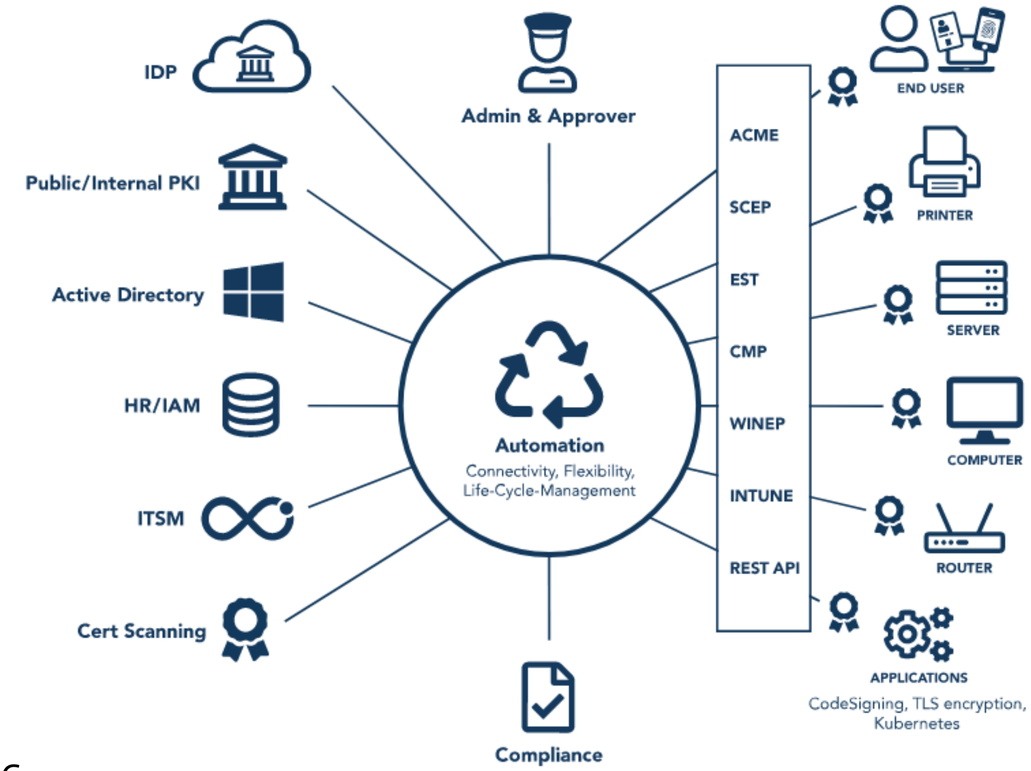
- Доверенное взаимодействие Web-сайтов (аутентификация)
- Защита сессий (SSL, TLS)
- **Обеспечение юридической значимости документов** (УКЭП для неограниченного круга лиц)

- Доверенное взаимодействие всех элементов ИТ-инфраструктуры, ИС, пользователей (**аутентификация**)
- Защита данных (БД, на дисках)
- Защита каналов передачи данных (VPN)

- Доверие к источнику информации
- Защита канала управления
- **Защита жизненного цикла устройства** (IIoT, M2M)

Корпоративный PKI

- Что такое корпоративный PKI
  - Это **технология**, базирующаяся на использовании цифровых сертификатов (электронных удостоверений - паспортов), выданных **корпоративным** Центром Сертификации (CA)
  - Это **инфраструктура**, построенная на базе
    - **Оборудования**, составляющего основу ИТ-инфраструктуры
    - **Программного обеспечения**
    - **Пользователей** (людей - физ. лиц)
    - **Процессов** (специальных служб, сервисов)
    - **Протоколов, политик и процедур**, необходимых для выпуска и обслуживания цифровых сертификатов, их проверки, управления жизненным циклом
- Цели внедрения PKI
  - Для обеспечения **доверенного взаимодействия** всех элементов корпоративной ИТ-инфраструктуры - используемого оборудования, программного обеспечения (ПО), пользователей
  - Для **строгой аутентификации пользователей** при доступе в корпоративную ИС
  - Для **корпоративного электронного документооборота** с использованием усиленной неквалифицированной ЭП
  - Для **защиты данных**
    - **Обеспечение доверия в ИС, достижение уровня Assurance**



Далее PKI рассматриваем только применительно к закрытым корпоративным системам

Элементы ИС - пирамида доверия

3 **Пользователи,** подключающиеся и работающие в ИС

2 **ПО,** используемое в ИС

1 **Оборудование,** на котором построена ИТ-инфраструктура

Цепочка доверия должна строиться от оборудования к ИС, от ИС к пользователям

- Доверие к ИС
  - Можно получить лишь тогда, когда все её элементы идентифицированы и аутентифицированы
  - Система считается доверенной, когда каждый её элемент является доверенным
  - Уровень доверия напрямую влияет на уровень безопасности в ИС
  - Уровень доверия к системе определяется по её самому слабому звену - по самому низкому уровню доверия элементов, составляющих ИТ-инфраструктуру и ИС
- Высокий уровень доверия к ИС
  - **Assurance** (уверенность, подтверждённая доказательствами, полученными от третьей стороны)
  - Необходим для МО, ОПК, гос. и Федеральных структур, организаций КИИ, крупного бизнеса, операторов ИСПДн
  - **Обеспечивается с использованием PKI** (инфраструктуры открытых ключей)
    - Позволяет установить **доверие между сторонами**, когда они не доверяют друг другу, но доверяют третьей стороне (корпоративному электронному “нотариусу” - CA)

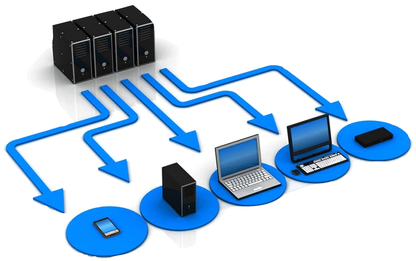
Приоритет #1

Как обеспечить безопасное функционирование ИТ-инфраструктуры, доверенное взаимодействие всех её компонентов,
устранить точки отказа

п. 8 Требований

Функционирование ИС на базе информационно-телекоммуникационной инфраструктуры **допускается при условии защиты** информационно-телекоммуникационной инфраструктуры в соответствии с Требованиями

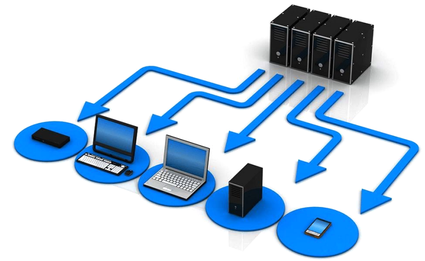
Защита ИТ-инфраструктуры - это:
- обеспечение **доверия** между всеми её компонентами и
- **безопасное взаимодействие**



Ключевые компоненты для обеспечения доверия в ИС

Приоритет #1

- Корпоративный Центр Сертификации (ЦС / CA)
  - Ключевой элемент доверия в ИС
    - От его функционирования зависит **работоспособность** всей ИТ-инфраструктуры и ИС
  - Выполняет функцию третьей доверенной стороны (корп. нотариуса)
    - **Правило**: никто никому не верит, но все доверяют корп. нотариусу (ЦС), а он проверяет и подтверждает подлинность объекта или субъекта и даёт разрешение на подключение и обмен
  - Выпускает и обслуживает **цифровые сертификаты** (эл. паспорта, используемые для строгой аутентификации)
    - Машинные (для всех устройств в ИТ-инфраструктуре)
    - Программные (для VDI, VPN, RDP-шлюзов, сервисов, Kubernetes и др.)
    - Пользовательские



Не путать с УЦ и сертификатами открытого ключа ЭП (УКЭП)

Использовать сертификаты ЭП для аутентификации категорически не допускается!

- Проблема (опасность)
  - Большинство ГИС используют MS CA
    - *Блокирование работы MS CA (Центра Валидации) парализует работу всей ИТ **в течение суток***

✓ **Это точка отказа всей ИТ-инфраструктуры, от неё надо избавляться в первую очередь**

- MS CA необходимо заменять - бесшовно, без остановки э-сервисов

✓ **Aladdin Enterprise CA (eCA)** - основа для построения корпоративной PKI

Требования к Центру Сертификации

- ЦС в ИТ-инфраструктуре
  - Является одним из ключевых элементов, от работоспособности которого зависит работа всей ИС
  - Нагрузка на подчинённый ЦС в крупной организации может быть достаточно большой, поэтому
    - должно использоваться несколько ЦС
    - ЦС должны быть территориально распределёны в соответствии с планируемыми нагрузками
    - ЦС и его службы (сервисы валидации и обслуживания сертификатов) должны собираться в отказоустойчивые и катастрофоустойчивые кластеры
- Владелец или оператор ИС должен иметь в своей инфраструктуре как минимум два ЦС
  - Корневой ЦС
  - Подчинённый (-ые) ЦС
- Корневой ЦС
  - Должен выпускать самоподписанные или подписанные сертификатом НУЦ цифровые сертификаты для подчинённых ЦС
  - Должен находиться в отключенном от ИС состоянии и после выпуска сертификатов подчиненным ЦС - отключаться или переводиться в **оффлайн** с предотвращением НСД к нему посторонних лиц

✓ **Дискредитация закрытого ключа корневого ЦС приведёт к полной потере доверия всей ИТ-инфраструктуры и ИС организации и потребует перевыпуск всех сертификатов безопасности**

Требования к Центру Сертификации

- Подчинённый ЦС
  - Должен обеспечивать
    - Регистрацию объектов и субъектов ИТ-инфраструктуры и ИС
    - Выпуск для них цифровых сертификатов безопасности (доступа) и возможность доставки выпущенных сертификатов с использованием различных (используемых в инфраструктуре владельца или оператора ГИС) протоколов (SCEP, ACME, CMP, EST, MS-WSTEP и др.)
    - Валидацию (проверку) сертификатов
    - Обслуживание сертификатов в рамках их жизненного цикла (отзыв, перевыпуск, блокирование, разблокирование и т.д.)
  - Должен
    - Функционировать в режиме 24x7 или в режиме функционирования ГИС
    - Быть доступным для всех сервисов и служб ИТ-инфраструктуры и ИС организации
    - Располагаться в пределах границ контролируемой зоны организации
    - Иметь **сертификат ФСТЭК России** (как СЗИ с зарубежной криптографией в объекте оценки, на УД-4), **заключение ФСБ**
  - Может
    - Использоваться для нескольких ИС и ИТ-инфраструктур владельца или оператора ГИС
- Сроки действия цифровых сертификатов
  - Не более 7 лет – для подчинённых ЦС (выдаются корневым ЦС владельца ИС)
  - Не более 3 лет – для пользователей ИС (выдаются подчинёнными ЦС владельца ИС)
  - Не более 1 года – для программных средств и оборудования (выдаются подчинёнными ЦС владельца ИС)

Не путать с сертификатами открытого ключа ЭП! (63-ФЗ)

Aladdin Enterprise CA

Доверенный корпоративный центр сертификации (CA)

- 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 отечественные ОС (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 (роутеров, маршрутизаторов, межсетевых экранов, VDI, VPN, RDP-шлюзов и пр.)
    - ПО
    - Пользователей
  - Одновременно работать с различными службами каталогов (Windows AD, Linux - ALD Pro, РЕД АДМ, Альт Домен 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, с Alt 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).

Приоритет #2

Требования по идентификации и аутентификации

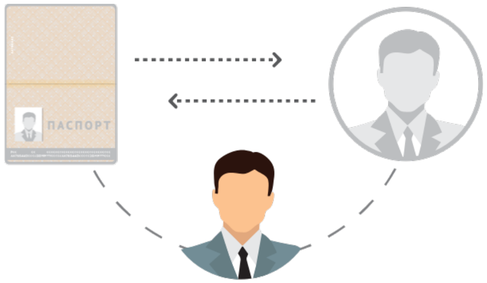
п.30а, б, 34д, е, ж, з, к, 40, 41, 42, 46, 48, 58, 63

- **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 80% всех проблем**
  - **Пример:** Госуслуги - неправильная реализация идентификации и аутентификации породила для пользователей массу проблем с использованием социальной инженерии. Проблема легко решается внедрением правильной технологии адаптивной аутентификации

Идентификация и аутентификация (немного матчасти)

- Что такое идентификация
  - Это способ или процесс определения личности пользователя или элемента ИС (объекта)
    - **Ответ на вопрос - ты кто?**
- Что такое аутентификация
  - Это процедура "установление подлинности" (объекта или субъекта ИС) и доказательства предъявленных идентификационных данных
    - **Докажи что ты это ты**
- Цели аутентификации в ИС
  - Подтверждение идентификационной информации (1)
  - Установление доверительных отношений (2) между всеми участниками обмена
    - Аутентификация источника данных (**односторонняя** аутентификация)
    - Аутентификация сторон (элементов ИТ-инфраструктуры - **взаимная** аутентификация)
  - Подтверждение возможности доступа (3) в ИС или в ИТ-инфраструктуру
  - Подтверждение личности владельца ЭП (4)

✓ **В Требованиях содержится прямое указание на необходимость использование ГОСТов по аутентификации (п.42), а в них - необходимые требования и процедуры**



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)

* - разработаны компанией "Аладдин"

Факторы аутентификации

- Фактор аутентификации
  - Вид (форма) аутентификационной информации, предъявляемой пользователем (субъектом) в процессе аутентификации
  - Существует всего 3 фактора:
    - **Фактор знания** - знание общего с ИС секрета (пароль, PIN-код, графический или одноразовый пароль)
    - **Фактор владения** - обладание определённым устройством/предметом, содержащим аутентификационную информацию
    - **Биометрический фактор** - свойственный конкретному человеку (субъекту) определённый признак ("контактная биометрия" - отпечатки пальцев, геометрия руки, шаблон поведения и пр.)

✓ **Типичные ошибки**

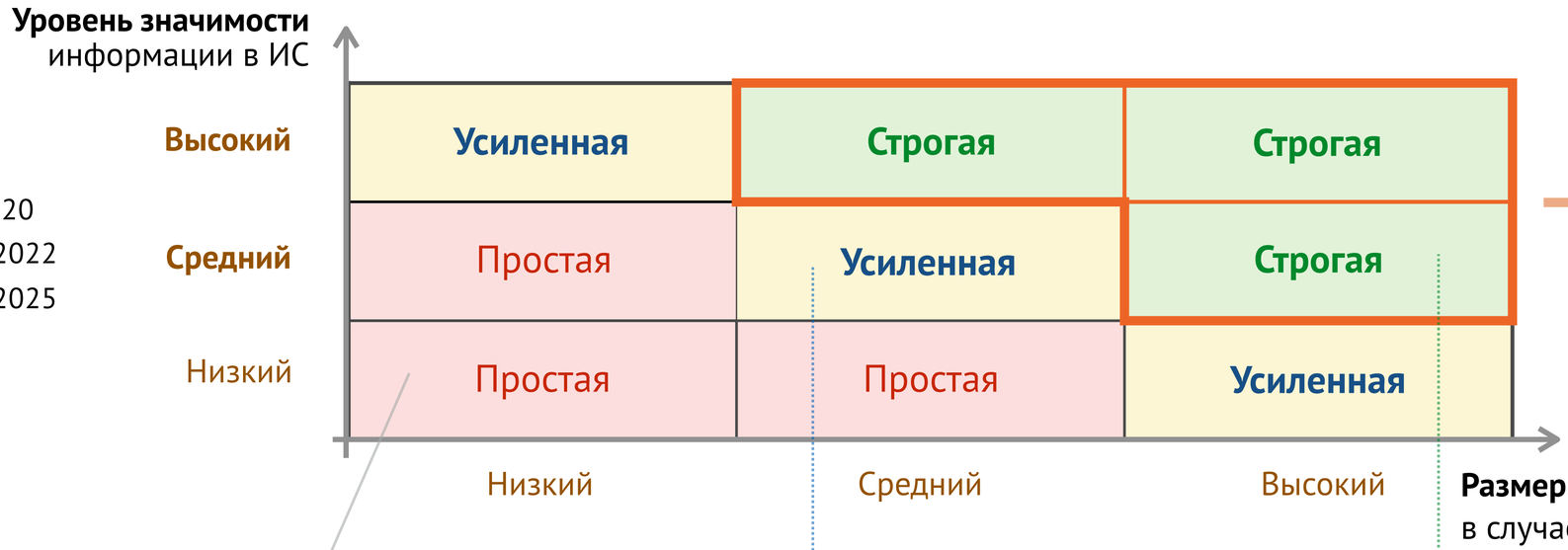
- Факторы аутентификации часто путают с дополнительными аутентификаторами (SMS-код, Push, QR-код и пр.) - *это двухэтапная аутентификация*
- Использование "бесконтактную биометрию" (лицо, голос) в качестве единственного фактора аутентификации в ИС и для прохода на объекты КИИ, МО не допускается (из-за возможностей современного генеративного искусственного интеллекта)

- Типы аутентификации (основные, всего 8)
  - Локальная
  - Доменная
  - Браузерная

Аутентификация в ИС

Требования к применяемым видам аутентификации в ИС

- ГОСТ Р 58833-2020
- ГОСТ Р 70262.1-2022
- ГОСТ Р 70262.2-2025

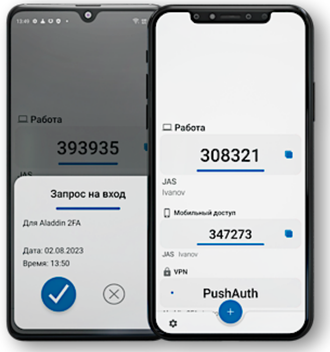


Низкий уровень доверия

Пароли
(однофакторная односторонняя)

Средний уровень доверия

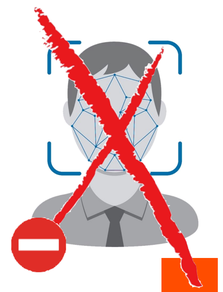
Содержит секрет



Высокий уровень доверия

PKI-токены

+BIO
для привязки к личности



Нельзя
Бесконтактная BIO

Приоритет #2

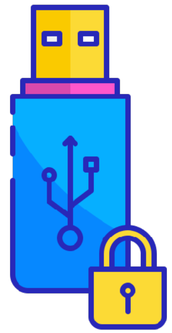
Требования по идентификации и аутентификации

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

Требования по идентификации и аутентификации (117-й Приказ)

- В ИС должны быть реализованы **базовые меры** защиты (п.63)
  - Идентификация и аутентификация
  - Управление доступом
- Мероприятия по защите информации должны быть направлены (п.30)
  - (а) исключение утечки информации ограниченного доступа и иной конфиденциальной информации
  - (б) предотвращение несанкционированного доступа к ИС и содержащейся в них информации
  - (в, г, д) предотвращение несанкционированной модификации, подмены, удаления информации

✓ **Обеспечивается отказом от использования паролей и использованием строгой аутентификации (2ФА)**



- Доступ в ИС должен осуществляться с применением **СТРОГОЙ аутентификации**
  - Для **привилегированных** пользователей (администраторов, VIP-пользователей, сотрудников подрядных организаций / п.48, 58)
    - В случае технической невозможности допускается использование **усиленной многофакторной аутентификации**
  - Для пользователей **мобильных** устройств (ноутбуки, планшеты / п.42)
  - **Для удалённых пользователей** при доступе в ИС (п.46)

✓ **Для реализации необходима корпоративная PKI (Центр Сертификации, PKI-клиент, Система Управления ЖЦ)**

Классы защищённости ИС и требования по аутентификации

Масштаб ИС

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

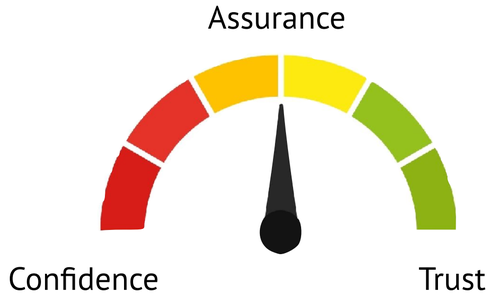
Пользователи, подключающиеся и работающие в ИС

ПО, используемое в ИС

Оборудование, на котором построена ИТ-инфраструктура

Цепочка доверия должна строиться от оборудования к ИС, от ИС к пользователям

- Основа доверия в ИС - надёжная первичная идентификация и аутентификация
  - Всего оборудования в ИС (без исключения)
  - ПО
  - Пользователей
- Высокий уровень доверия (К1, К2)
  - В ИС никто никому не доверяет (Zero Trust), но все доверяют корпоративному "нотариусу" (CA в PKI)
  - Должна использоваться **СТРОГАЯ аутентификация**
- Средний уровень доверия (К3)
  - Допускается использовать **УСИЛЕННУЮ аутентификацию** (2ФА, без PKI)



Требования к аутентификации пользователей

Строгая аутентификация пользователей (для классов К1, К2-К3)

Первичная идентификация пользователей должна производиться **лично**

- Должна обеспечиваться при доступе пользователей
  - К программно-аппаратным средствам (компьютеру, терминальному оборудования) - *локальная 2ФА*
  - К ИС - *доменная и/или браузерная 2ФА*
- Должна быть
  - **Взаимной** - аутентификация обеих сторон взаимодействия: пользователь-ИС, ИС-пользователь
  - **Двухфакторной** (фактор владения аппаратным устройством, фактор знания – ПИН-код или биометрический фактор, подтверждающие факт владения данным устройством)
  - С использованием
    - **Специализированных защищённых аппаратных устройств** (средств аутентификации) с поддержкой криптографии **с неизвлекаемым закрытым ключом** *основа безопасности PKI - безопасность закрытого ключа*)
    - **Цифровых сертификатов доступа**, выдаваемых **собственным** корпоративным Центром Сертификации (*использование УКЭП и сертификатов, выданным публичным УЦ - грубейшая ошибка*)
    - **Третьей доверенной стороны** - корпоративного **Центра Валидации**, обеспечивающего проверку и подтверждение цифровых сертификатов взаимодействующих сторон (пользователя и ИС)
    - В организации владельца или оператора ИС с доменной архитектурой должен функционировать корпоративный ЦС и на его основе развёрнута инфраструктура открытых ключей (**PKI**)
    - Для малых ИС (**без PKI**) в качестве компенсирующей меры рекомендуется использовать средства 3ФА (с использованием **биометрии** по отпечаткам пальцев - *лучший способ подтверждения личности пользователя*)

Что нужно для реализации строгой аутентификации

Что нужно для реализации строгой аутентификации

Орг. меры

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

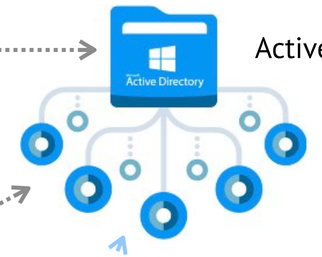
Меры защиты (ИАФ, УПД) - *проект*

Технические средства

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

HSM (опция)

Служба каталога/контроллер домена
- ALD Pro, РЭД АДМ, Альт Домен и др.



Active Directory

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

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

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

Средства 2ФА/3ФА

Ресурсная система

Защищённое хранилище

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

Проблемы миграции и внедрения строгой аутентификации в Linux

В экосистеме Windows

- **Корп. центр сертификации**
  - MS CA (CS), входит в состав MS Windows Server
  - ✓ **Отвечает за выпуск и валидацию сертификатов**
- **Служба каталога/контроллер домена**
  - MS Active Directory (AD)
  - ✓ **Отвечает за доменную аутентификацию**
- **Клиент PKI и 2ФА**
  - MS Windows Smart Card Logon
  - ✓ **Отвечает за аутентификацию пользователей**

- Все необходимые компоненты для построения корпоративной PKI **встроены** в MS Windows
- MS CA выпускает и обслуживает
  - машинные сертификаты (для аутентификации оборудования в ИТ-инфраструктуре)
  - программные сертификаты (code signing)
  - пользовательские сертификаты

- **PKI-токены, смарт-карты, BIO-токены**

- **Система централизованного управления ЖЦ токенов и сертификатов**

- Для внедрения строгой 2ФА пользователей достаточно приобрести
  - средства 2ФА
  - систему централизованного управления ЖЦ токенов и сертификатов

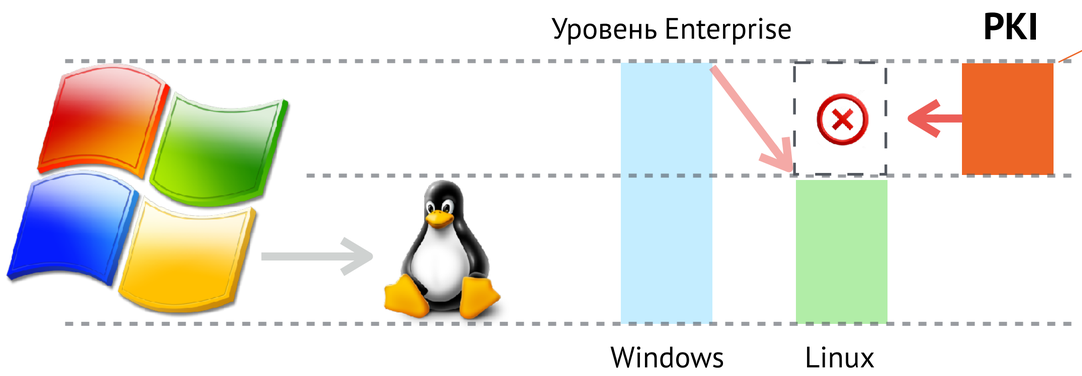
Проблемы миграции и внедрения строгой аутентификации в Linux

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



- Чтобы подняться до уровня **Enterprise** и обеспечить такой же уровень безопасности и управляемости как в Windows, **необходимо внедрить полноценный PKI**

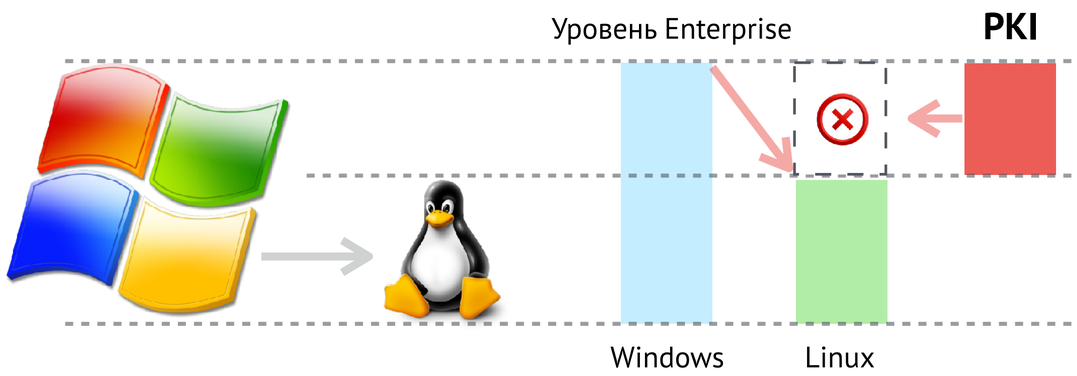
Проблемы миграции и внедрения строгой аутентификации в Linux

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
  - ALD Pro, РЭД АДМ, Альт Домен
- Клиент PKI (полный стек PKI)
- Клиент 2ФА/3ФА
- PKI-токены, смарт-карты, BIO-токены
- Система централизованного управления ЖЦ токенов и сертификатов

Аладдин

Проблемы миграции и внедрения строгой аутентификации в Linux

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, РЭД АДМ, Альт Домен
◆ 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**	◆ Система централизованного управления ЖЦ токенов и сертификатов

+

Ключевые компоненты для защиты ИТ-инфраструктуры

Компоненты корпоративной PKI

- Центр Сертификации (ЦР, ЦС, ЦВ) - центр доверия (корпоративный "нотариус")
- Служба каталога (доменная служба)

Центр Сертификации и Служба каталога (доменная служба)

1. Центр Сертификации - **Aladdin eCA**

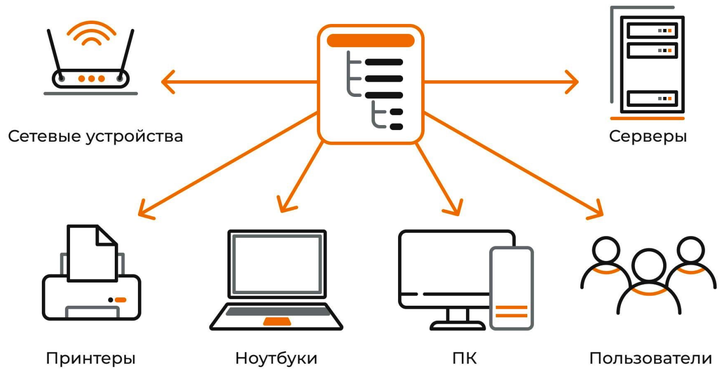
2. Служба каталога

- В MS Windows - Active Directory
- В Linux
  - ALD Pro (Астра Линукс)
  - Альт Домен (Альт Линукс)
  - РЕД АДМ (РЕД ОС)
  - Dynamic Directory (РОСА)
  - *Samba DC*
  - *FreeIPA и др.*

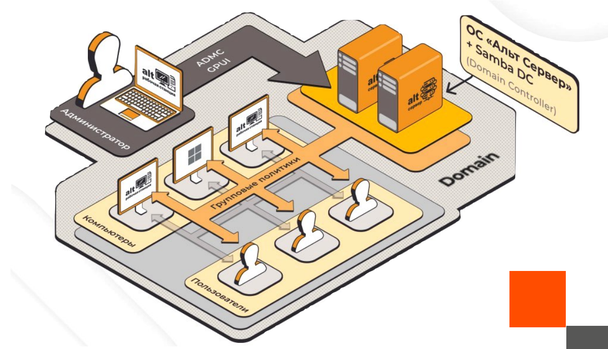
Есть у всех производителей российских ОС

Aladdin eCA

Служба каталогов



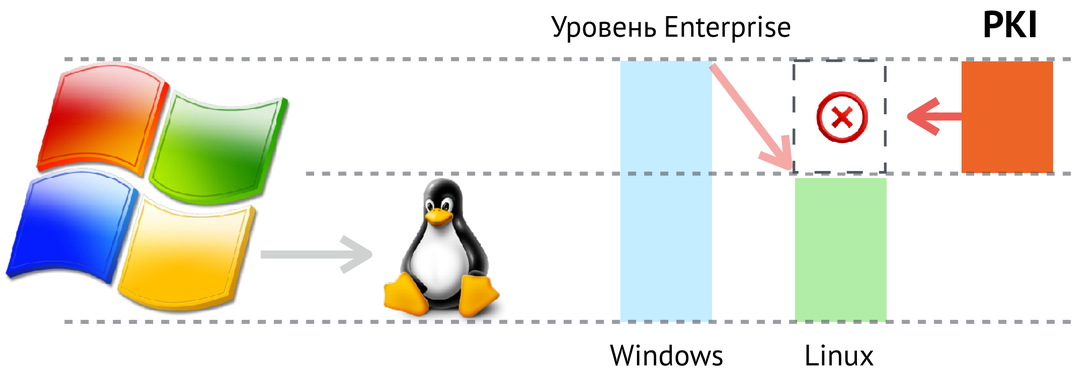
✓ **Главное при защите ИТ-инфраструктуры — обеспечить правильную первичную идентификацию и строгую аутентификация всего используемого оборудования с использованием машинных сертификатов**



В составе Linux нет полноценного PKI Enterprise-уровня

- Нельзя обеспечить строгую аутентификацию (по сертификатам) "из коробки"
  - оборудования
  - ПО
  - пользователей

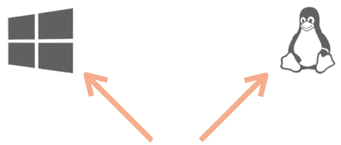
PKI-клиент и поддержка средств МФА в Linux

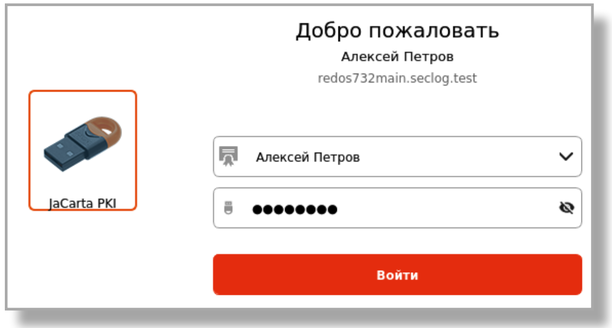


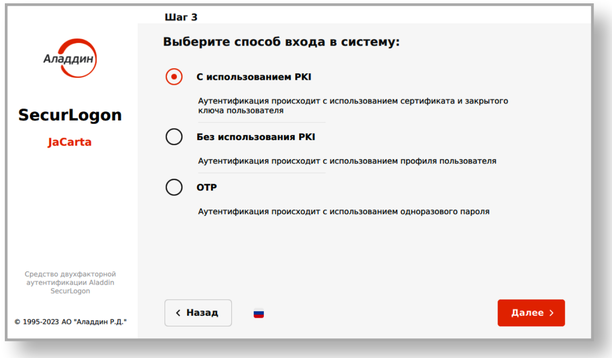
Чтобы подняться до уровня **Enterprise** и обеспечить такой же уровень безопасности и управляемости как в Windows, **необходимо внедрить полноценный PKI на стороне клиента**

Полноценный PKI-клиент для Linux пока есть только у Аладдина

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

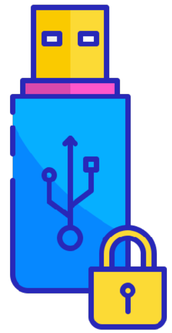
Импортозамещение	Microsoft SmartCard Logon
Сертификация	Сертификат ФСТЭК России №4809 (для работы с конфиденциальной информацией) *Планируется увеличение класса до УД-2 для работы с гостайной до степени секретности "СС" вкл.*
В Реестре отечественного ПО	№10043
Возможность поставки в рамках госзакупок 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 строгой аутентификации

с поддержкой PKI

Требования к средствам строгой аутентификации пользователей

- Должны быть реализованы в виде персонального, защищённого от взлома и клонирования аппаратного устройства
  - С аппаратной реализацией необходимого набора криптографических алгоритмов **с неизвлекаемым закрытым ключом**
  - Реализованные в устройстве криптографические алгоритмы должны иметь заявленную **стойкость** не менее $4*10^{33}$ (реализуется алгоритмами RSA с длиной ключа не менее 2048 или ECDSA с длиной ключа не менее 224)
    - Рекомендуется использовать современный и более быстрый алгоритм ECDSA с длиной ключа 304 бита (заявленная стойкость $4*10^{45}$)
  - С хранением цифровых сертификатов доступа в памяти устройства (не менее двух)
  - С возможностью генерации ключевых пар и обновления цифровых (пользовательских) сертификатов
  - С возможностью его инициализации только уполномоченными администраторами ИС
  - С возможностью его использования только авторизованным пользователем
- Должны поддерживаться в качестве средства 2ФА/3ФА для **локальной, доменной и браузерной** аутентификации пользователей ИС на базе PKI (цифровых сертификатов доступа), а также
  - В средствах доверенной загрузки используемого оборудования
  - В ОС и приложениях
  - В Службах Каталога и домен-контроллерах
- Должны поддерживаться корпоративной системой централизованного управления жизненным циклом
- Должны быть сертифицированы ФСТЭК России (как СЗИ, на УД-4)



✓ **Использование сертификатов электронной подписи (УКЭП), выпущенных внешним УЦ, для строгой аутентификации пользователей в ГИС не допускается**

Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены

JaCarta-3 PKI/ГОСТ

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

С NFC

JaCarta-3 PKI/ГОСТ/NFC

JaCarta PKI/ГОСТ/NFC

SecurRing PKI/ЭП

Терминальный клиент

Aladdin LiveOffice

LiveUSB+ОС+VPN+RDP/VDI+PKI+УКЭП

Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены

JaCarta-3 PKI/ГОСТ

MicroUSB

для M2M

USB Type-C

С биометрией

SecurBIO PKI [ЭП]

SecurBIO Reader
JCR-761

JaCarta PKI/ГОСТ/BIO

Смарт-карты и ридеры

JaCarta PKI/ГОСТ/SC **+ JCR-721**

SecurBIO Reader
JCR-781

С NFC

JaCarta-3 PKI/ГОСТ/NFC

JaCarta PKI/ГОСТ/NFC

SecurRing PKI/ЭП

Терминальный клиент

Aladdin LiveOffice

LiveUSB+ОС+VPN+RDP/VDI+PKI+УКЭП

Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены

JaCarta-3 PKI/ГОСТ

MicroUSB

для M2M

USB Type-C

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

С NFC

JaCarta-3 PKI/ГОСТ/NFC

JaCarta PKI/ГОСТ/NFC

SecurRing PKI/ЭП

Терминальный клиент

Aladdin LiveOffice

LiveUSB+ОС+VPN+RDP/VDI+PKI+УКЭП

Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены

JaCarta-3 PKI/ГОСТ

MicroUSB

для M2M

USB Type-C

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

С NFC

JaCarta-3 PKI/ГОСТ/NFC

JaCarta PKI/ГОСТ/NFC

NEW

SecurRing PKI/ЭП

Терминальный клиент

Aladdin LiveOffice

LiveUSB+ОС+VPN+RDP/VDI+PKI+УКЭП

Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены

JaCarta-3 PKI/ГОСТ

MicroUSB

для M2M

USB Type-C

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

С NFC

JaCarta-3 PKI/ГОСТ/NFC

JaCarta PKI/ГОСТ/NFC

SecurRing PKI/ЭП

Терминальный клиент

Aladdin LiveOffice

LiveUSB+ОС+VPN+RDP/VDI+PKI+УКЭП

Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены

JaCarta-3 PKI/ГОСТ

С биометрией

SecurBIO PKI [ЭП]

Смарт-карты и ридеры

JaCarta PKI/ГОСТ/SC **+ JCR-721**

JaCarta PKI/ГОСТ/BIO

С NFC

JaCarta-3 PKI/ГОСТ/NFC

JaCarta PKI/ГОСТ/NFC

SecurRing PKI/ЭП

Терминальный клиент

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

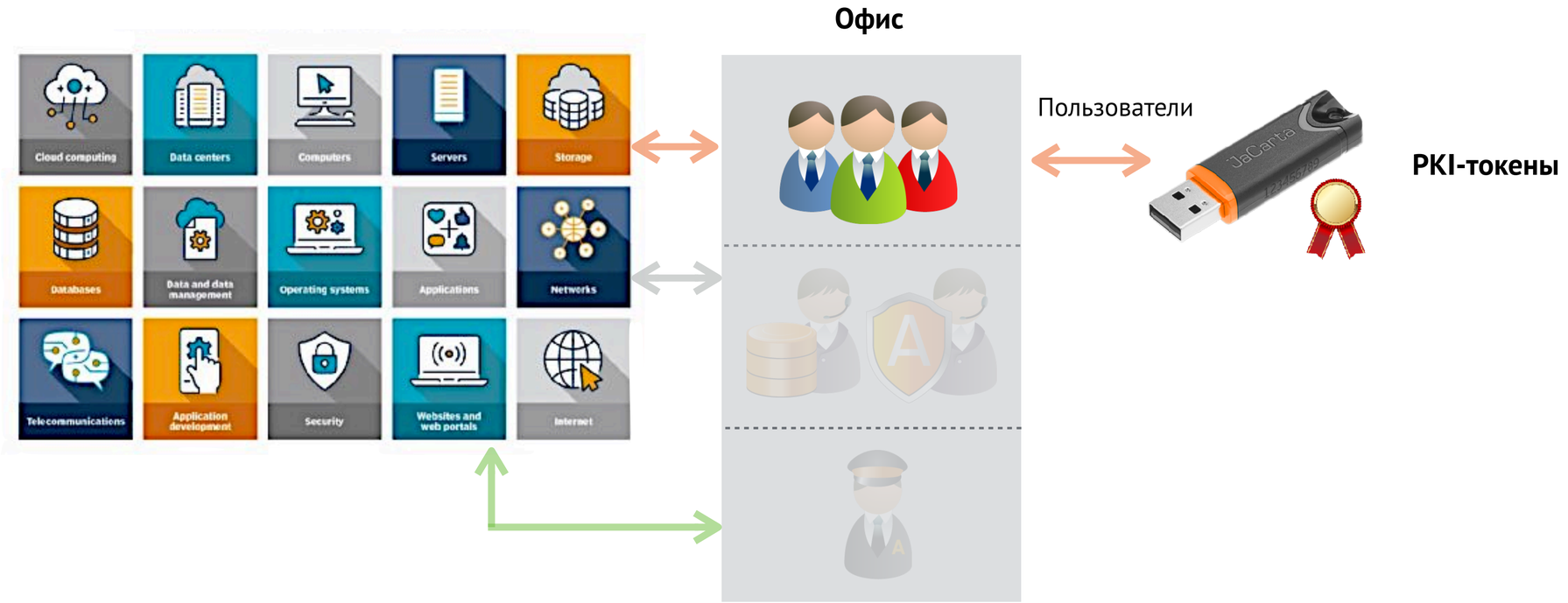
Адаптивная МФА

Концепция и реализация

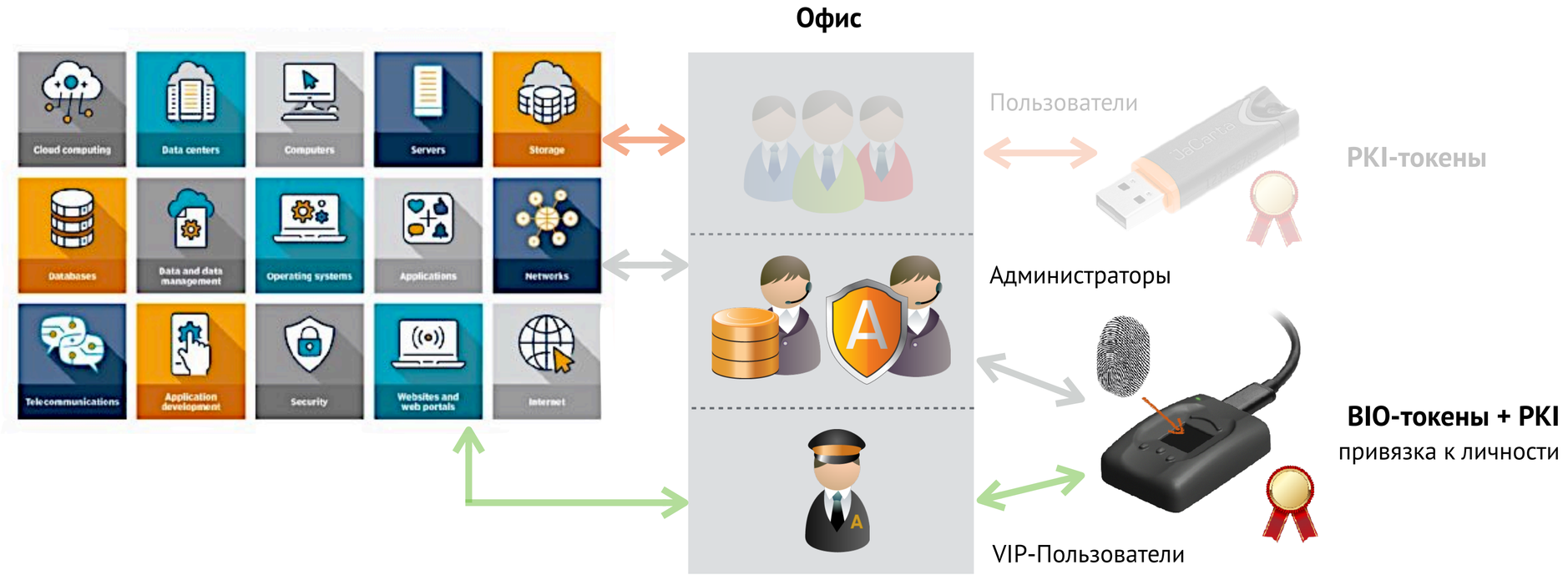
Для разных сред функционирования, условий работы, сегментов ИС должен быть определён РАЗНЫЙ набор факторов и методов для подтверждения идентификационных данных и их связи с личностью пользователя

- Больше рисков - больше дополнительных атрибутов и компенсационных мер

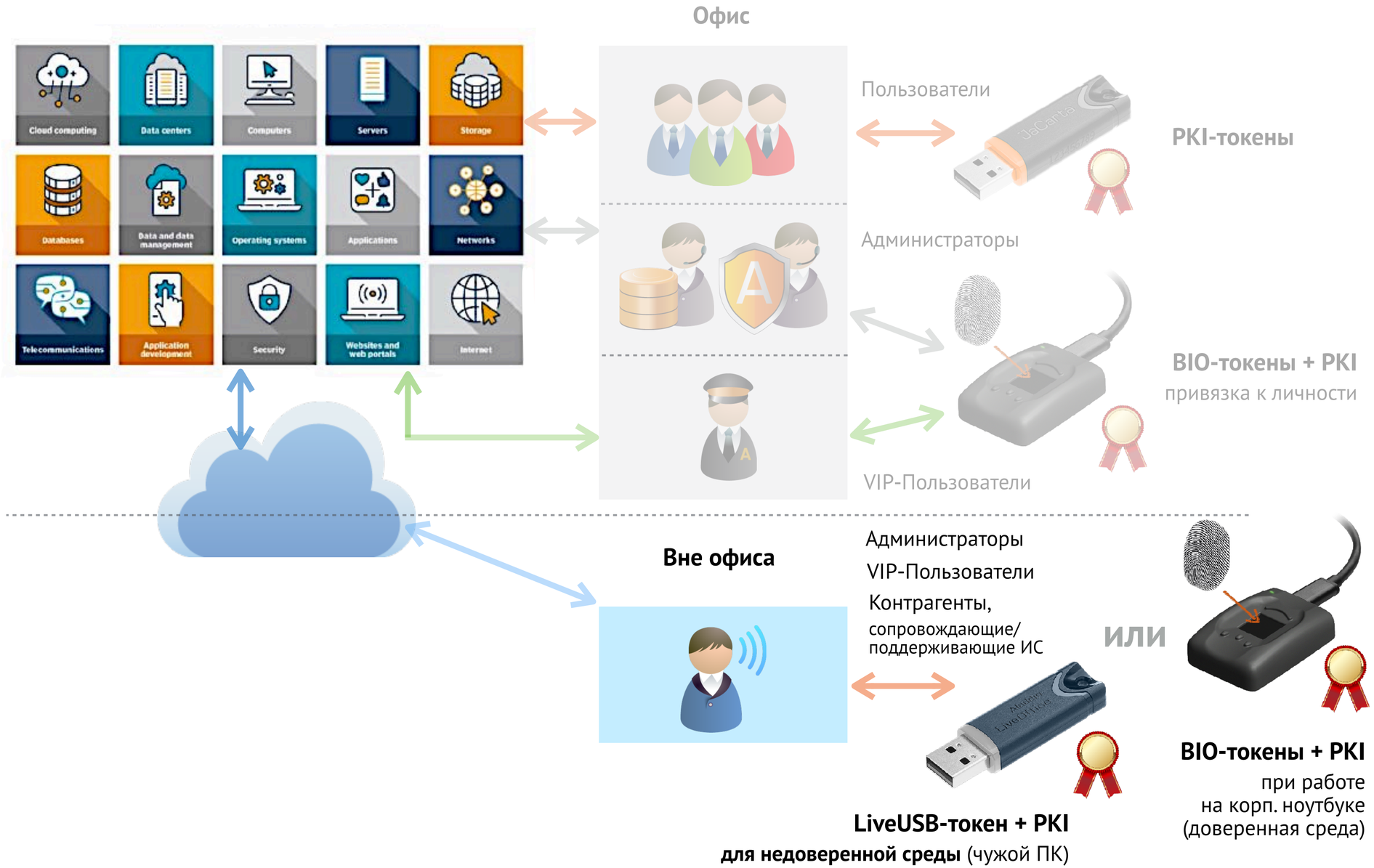
Адаптивная МФА в ИС



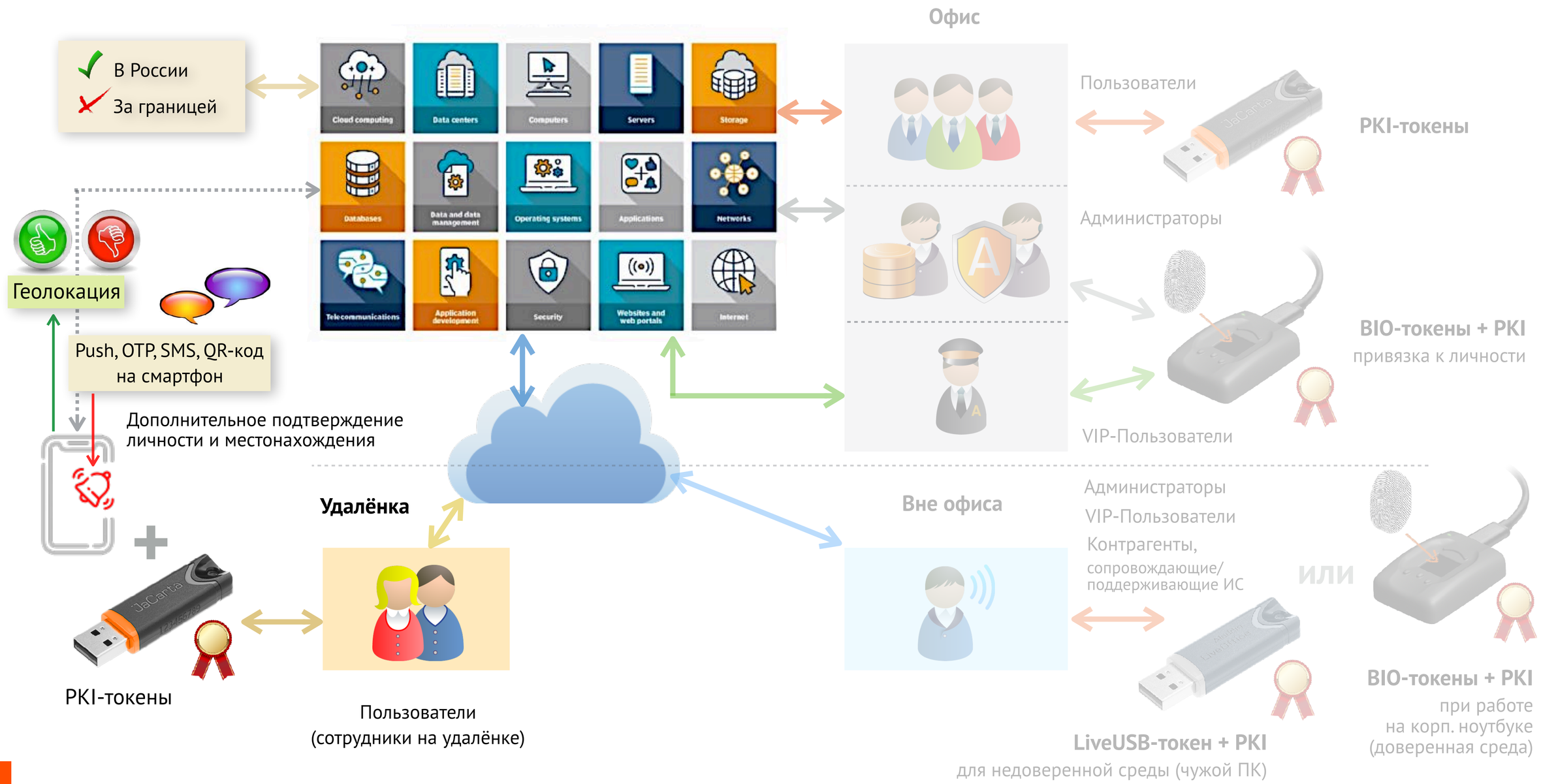
Адаптивная МФА в ИС



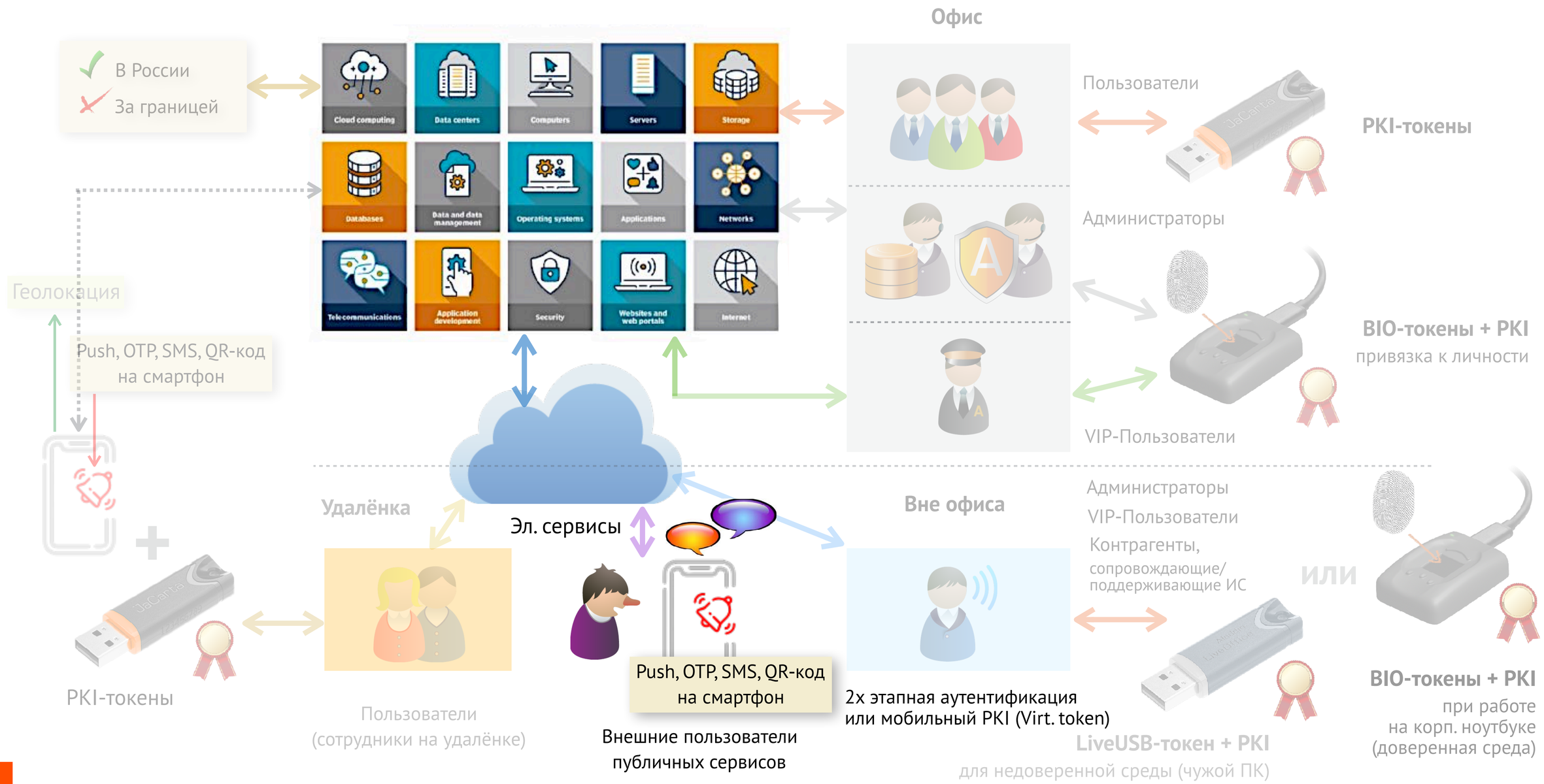
Адаптивная МФА в ИС



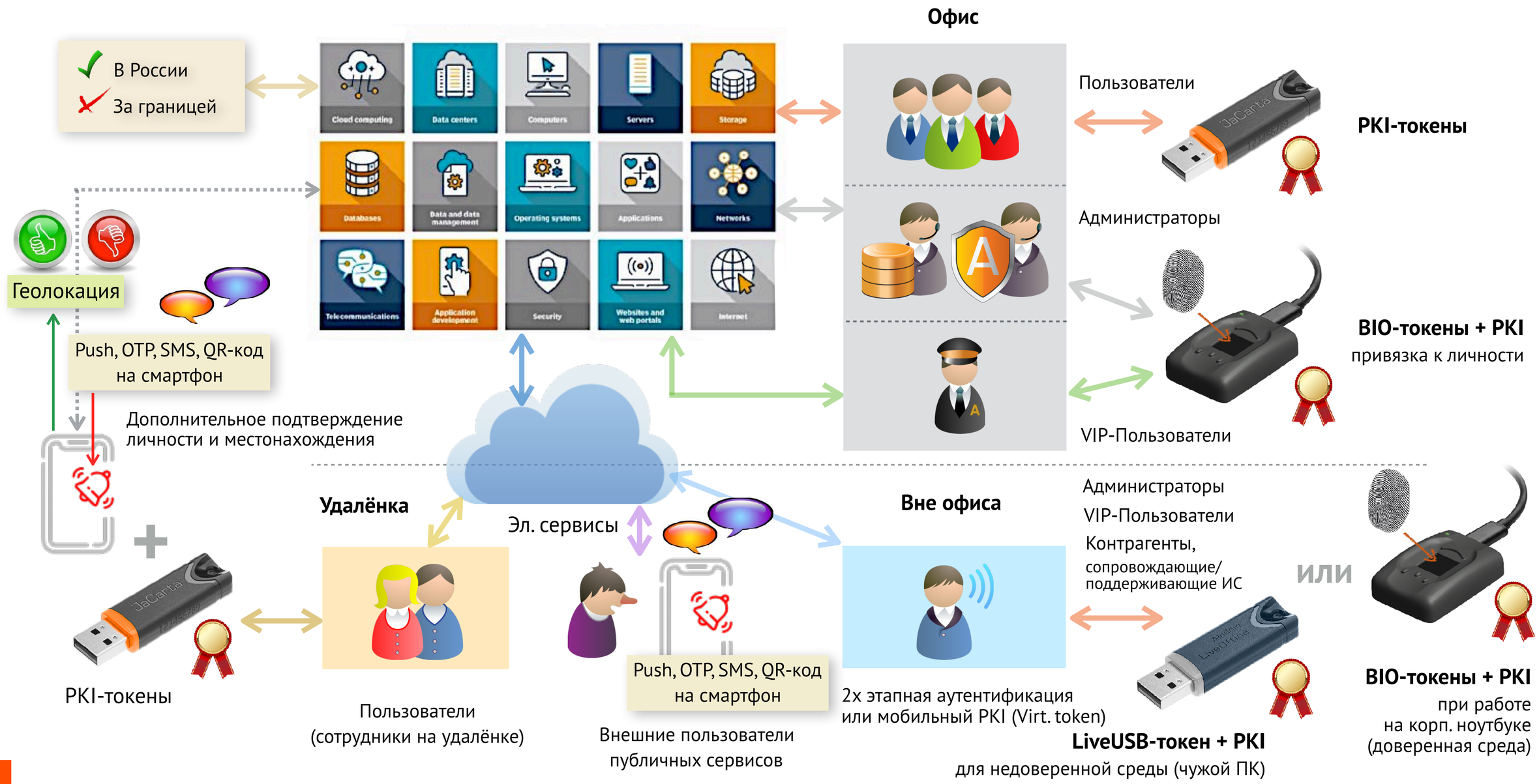
Адаптивная МФА в ИС



Адаптивная МФА в ИС



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)

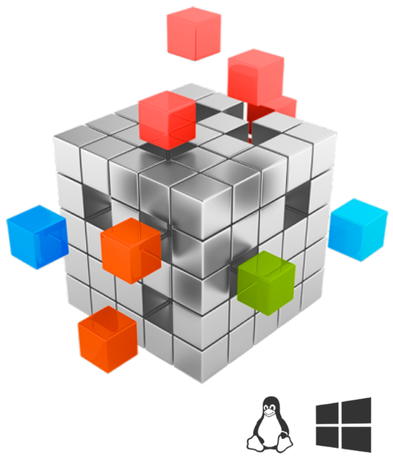
- Усиленная 2ФА — п. 48 Требований
  - Обязательно должен быть **фактор ВЛАДЕНИЯ** (1)
    - Электронный идентификатор (защищённое неклонируемое устройство)
    - [**Смартфон**] + [QR-код, SMS, push, OTP]
  - ✓ **Только при работе на компьютере - чтобы было разделение сред**
  - ✓ **Если работа на смартфоне - 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)

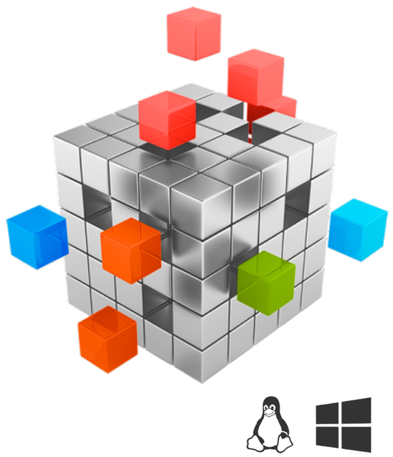


Глубоко интегрирован с JMS (системой централизованного управления ЖЦ токенов)

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.

Мобильные приложения для усиленной 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

Программные средства для 2ФА/3ФА и адаптивной аутентификации

Aladdin 2FA

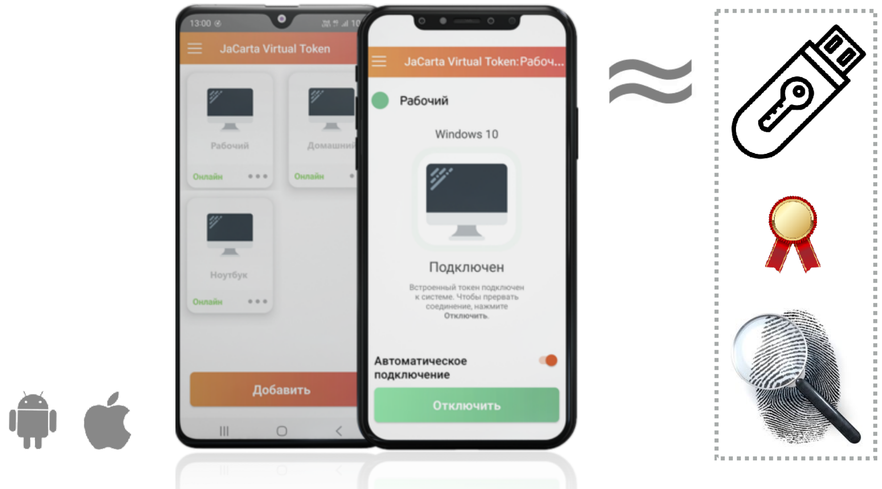
Мобильное приложение

- 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



Программные средства для 2ФА/3ФА и адаптивной аутентификации

Aladdin 2FA

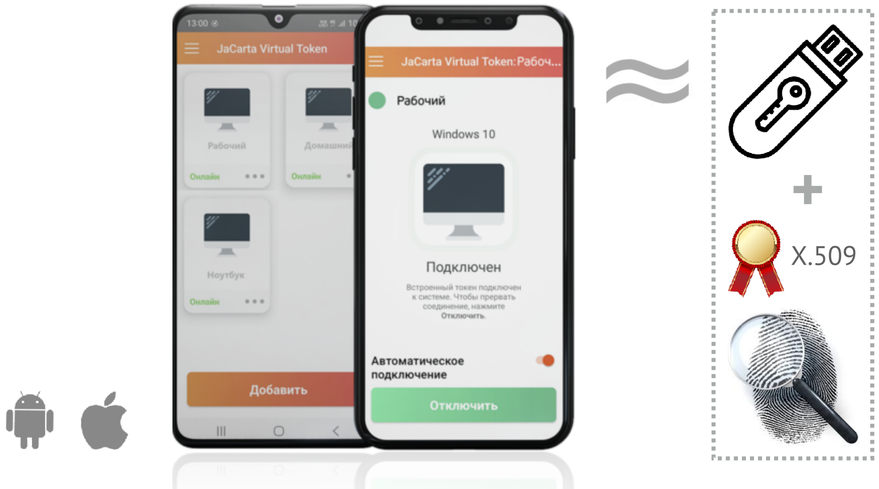
Мобильное приложение

- 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



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

п.30а, б, **42, 46, 48, 58**, 63, 70, 71

Централизованное управление - требования

- Жизненный цикл средств аутентификации и цифровых сертификатов в ИС должен управляться с использованием специализированной системы
- Должен обеспечиваться
  - Учёт и автоматизация процессов регистрации, персонализации, выдачи, обслуживания, управления жизненным циклом
    - Средств аутентификации пользователей (средства 2ФА/3ФА) и оборудования с использованием модулей безопасности
    - Цифровых сертификатов с возможностью их автоматической верификации и обслуживания (выпуск Центром Сертификации, запись в память устройства, блокирование, отзыв, перевыпуск)
    - Профилей зарегистрированных в ИС объектов и субъектов, требующих аутентификации при доступе в ИС
  - Безопасное хранение и обработка всех идентификационных данных объектов и субъектов ИС
    - Защищённое хранилище (*нет ни у одного конкурента, а это дыра в ИБ)*
  - Распознавание используемых средств 2ФА/3ФА и их автоматическая регистрацию в системе учёта и управления жизненным циклом
  - Учёт используемых средств 2ФА/3ФА, СКЗИ, выданных и обслуживаемых цифровых сертификатов, сроков их действия и необходимости их перевыпуска
  - Автоматизация рутинных операций, связанных с выдачей и обслуживанием цифровых сертификатов в соответствии с принятыми политиками безопасности
- Необходимо наличие сертификата ФСТЭК России (как СЗИ, на УД-4)

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.

Приоритет #3

Требования к обеспечению удалённого доступа

п. 46 Требований

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**

Средства удалённого доступа к ИС

- Должны быть
  - Определены оператором ГИС и согласованы со службой ИБ или специализированным структурным подразделением, отвечающим за ИБ
    - Программно-аппаратные средства (ПАК)
    - Состав ПО, минимально необходимый и достаточный для удалённого доступа и работы в ГИС
    - Средства контроля целостности используемого ПО (доверенной загрузки)
    - Сертифицированные шифровальные (криптографические) средства для защиты канала передачи данных
    - Средства 2ФА для строгой или усиленной аутентификации пользователей и администраторов ИС
    - Средства мониторинга и журналирования действий работников и администраторов с сохранением данных на машинных носителях
    - Используемые средства геопозиционирования для определения местонахождения работника, получающего удалённый доступ
    - Блокирование удалённого доступа из-за пределов территории РФ (***реализовали в нашем продукте Aladdin 2FA***)
    - Невозможность изменения конфигураций и настроек средства удалённого доступа, влияющих на безопасность, самим пользователем.

- При условии применения **специализированных сертифицированных средств безопасной дистанционной работы** допускается:
  - Использование **недоверенных**, в том числе **личных СВТ**
    - работников оператора ГИС (пользователей)
    - администраторов
    - привилегированных пользователей (VIP)
    - работников подрядных организаций, обеспечивающих внедрение ИС, её сопровождение, техническую поддержку и пр.

NEW

Требования к средства безопасной дистанционной работы, утв. Приказом ФСТЭК России №32 от 16.02.2021

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

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)

Приоритет #4

Защита конечных, мобильных (переносных) устройств и съёмных носителей

п. 34д, е, ж, к, 37, 40, 41,42, 51, 63, 70, 71 Требований

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)

NEW

Средства хранения и обработки конфиденциальной информации

- В организации должен быть определён
  - Перечень конфиденциальных сведений
  - Список программно-аппаратных средств, предназначенных для хранения и обработки конфиденциальной информации

✓ **Базы данных, хранилища массивов данных (серверы)**

✓ **Машинные носители информации**

- Установленные в конечных устройствах – компьютерах, ноутбуках, планшетах, рабочих станциях и т.д.

✓ **Съёмные носители информации**

- USB-флешки, съёмные жесткие диски и др. носители информации

- Порядок учёта конечных устройств (ПАК)
  - Тип, модель устройства
  - Состав используемого ПО
  - Перечень СЗИ, в т.ч. обеспечивающего контроль целостности используемого ПО
  - Список работников, имеющих право работать на данном конечном устройстве (ПАК) и пр.

Требования к защите конечных и мобильных (переносных) устройств

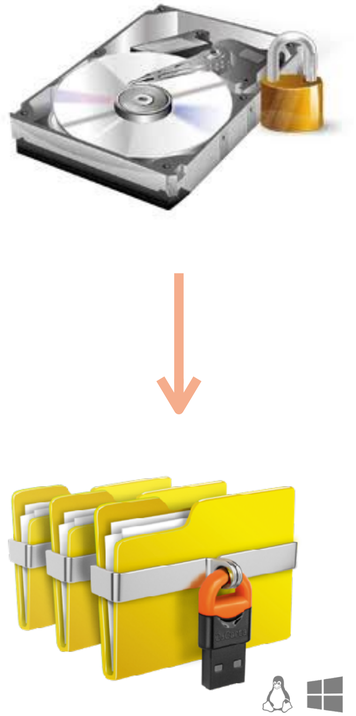
- Конечные и мобильные устройства - средства хранения и обработки конфиденциальной информации
  - Доступ к ним должны иметь только те работники, на которых возложены данные функции (обязанности)
  - Должны храниться в пределах контролируемой зоны, несанкционированный доступ в которую лиц, не являющихся работниками оператора ГИС, должен быть исключён
  - При необходимости хранения и/или использования средств хранения и обработки конфиденциальной информации вне контролируемой зоны, конфиденциальная информация должна быть защищена с использованием сертифицированных шифровальных (криптографических) средств защиты (СКЗИ) с доступом к информации только после успешной 2ФА

✓ **117-й Приказ ФСБ России от 18 марта 2025 г.**

- Информация, содержащаяся в ГИС, подлежит защите с использованием шифровальных (криптографических) средств защиты информации в случаях, если в ИС осуществляется хранение данных на носителях информации, предназначенных для записи, хранения и воспроизведения информации, обрабатываемой с использованием средств вычислительной техники, несанкционированный доступ к которым со стороны третьих лиц не может быть исключен с помощью некриптографических методов и способов.

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



Как обеспечить защиту машинных носителей информации

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).

Крипто БД - система защиты и обезличивания данных в СУБД

- Обеспечивает
  - Защиту главных информационных активов организации (данных в 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 персональных данных
  - Прозрачное селективное (выборочное) шифрование критически важных данных в СУБД с использованием российских алгоритмов
  - Двухфакторную аутентификацию пользователей при доступе к данным в СУБД
- Позволяет
  - "Импортозаместить" встроенные в СУБД зарубежные средства защиты на российские, сертифицированные, и продолжать использовать необходимые СУБД и приложения
  - Защищать критически важные данные в СУБД
    - в клиент-серверных ИС
    - в многозвенных приложениях ИС
    - в информационных системах с терминальным доступом
    - в виртуальных и облачных инфраструктурах (IaaS, SaaS)
  - Создавать защищённые ИС с использованием сертифицированного СКЗИ

Для СУБД Oracle, MS SQL, Tibero, PostgreSQL, Postgres PRO, Jatoba, Sybase

Крипто БД - система защиты и обезличивания данных в СУБД

Импортозамещение	Встроенные в импортные СУБД зарубежные средства защиты на российские
Сертификация	Сертификат ФСБ России №СФ/124-4638
В Реестре отечественного ПО	№509, 518, 4292, 4293
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, к, р, 40,** 42, 48, 49, 51, 58, 63а, б, ж, 70, 71 - Защита от НСД, МФА, шифрование данных вне контролируемой зоны - 117-го Приказа ФСБ - п.1, 3, 6 (шифрование данных если средствами защиты от НСД нельзя предотвратить утечку данных)

Требования к съёмным машинным носителям

✓ **Съёмные носители - "ящик Пандоры" для обеспечения ИБ**

- Имеют скрытую избыточную память, которая может использоваться для зеркалирования сохраняемой информации
- Не имеют возможности однозначной машинной идентификации/аутентификации
- Содержат заложенную уязвимость (закладку) на уровне спецификации
- Подвержены атакам BadUSB и достаточно легко клонируются и перепрограммируются для кражи информации и атак на целевые ИС

- Оператором ИС должны быть
  - Запрещены к использованию любые съёмные машинные носители информации (USB-флешки, съёмные жёсткие диски, смартфоны и пр.), кроме выдаваемых им самим (оператором ИС)
  - Проверены, разрешены к использованию в ИС, учтены и закреплены за конкретными пользователями ИС только такие съёмные машинные носители информации, которые:
    - Соответствуют требованиям безопасности
    - Выдаются самим оператором

✓ **Как выполнить эти требования, если любой флеш-накопитель можно клонировать и его нельзя идентифицировать?**

- Съёмные машинные носители информации должны обеспечивать
  - Невозможность изменения (подмены) встроенного программного обеспечения (прошивки) устройства, а также идентификационных параметров устройства – VID (Vendor ID), PID (Product ID)
  - Возможность визуальной и машинной идентификации устройства с помощью уникального неизменяемого серийного номера
  - Возможность аутентификации устройства до начала его использования средствами ОС и/или специализированными средствами защиты (доверенная загрузка, контроль съёмных носителей информации и др.)

Aladdin eFlash - доверенный корпоративный флеш-накопитель

- Имеет
  - Повышенный ресурс, скорость (USB 3.1) и встроенные функции безопасности
  - ✓ **Возможность аутентификации (свой/чужой)**
- Обеспечивает
  - Защиту контроллера флеш-памяти от атак BadUSB с подменой "прошивки" и его доверенную загрузку с контролем целостности из встроенного модуля безопасности
  - Контроль за избыточной памятью и невозможность скрытого копирования информации
  - Однозначную идентификацию и аутентификацию устройства с использованием уникального серийного номера и дополнительных функций безопасности
  - Защиту от использования клонов с поддельными значениями параметров VID (Vendor ID) и PID (Product ID) для атаки на ИС
  - Повышенный гарантированный ресурс флеш-памяти (не менее 1,500 циклов полной перезаписи)
  - Отсутствие деградации (снижения) надёжности и скорости чтения/записи по всему объёму памяти
  - Повышенную защиту от статического электричества (до 15 кВ) и электромагнитных помех
  - Высокую скорость чтения ~90 МБ/с и записи не менее 50 МБ/с при подключении к USB 3.0
  - Большой объём памяти (64 ГБ в базовой версии)

Aladdin eFlash - доверенный корпоративный флеш-накопитель

Импортозамещение	Любые USB флеш-накопители
Сертификация	В процессе по линии Минобороны (в т.ч. для работы с гостайной до СС) и по линии ФСТЭК России
В Реестре отечественного ПО	В процессе
В Реестре ПАКов (Минцифры)	В процессе
В Реестре радиоэлектронной промышленности Минпромторга (ПП-878, ПП-719)	№10658184, №10658185
Возможность поставки в рамках госзакупок и ГОЗ (по ПП-1875, 44-ФЗ, 223-ФЗ, ПП-325)	Да
Выполняет требования 117-го Приказа ФСТЭК	п.**51**, 66-б, 70 - Работа только с учтёнными и идентифицированными съёмными носителями, контроль использования, выявление несанкционированных)

JaCarta SF/ГОСТ - защищённый служебный флеш-накопитель

- Обеспечивает
  - Безопасное хранение и перенос данных в зашифрованном виде (аппаратная реализация) Доступ к данным только авторизованным пользователям и только на авторизованных служебных компьютерах
  - Защиту ценной информации от несанкционированного доступа и копирования со стороны внешних и внутренних нарушителей, в т.ч.
    - самого пользователя (владельца) флеш-накопителя (например, при попытке копирования данных на личный ноутбук)
    - системных администраторов (например, при попытке доступа к критически важным данным пользователя)
  - Сокрытие наличия записанной информации на служебном флеш-накопителе
- Позволяет
  - Обрабатывать и защищать информацию ограниченного доступа (ДСП), гостайну со степенью секретности "Совершенно секретно"
  - Реализовать **контроль отчуждения (переноса) информации** со съёмных машинных носителей
  - Вести мониторинг и аудит действий пользователей и администраторов

JaCarta SF/ГОСТ - защищённый служебный флеш-накопитель

Сертификация	Сертификат Минобороны №6114 (для работы с гостайной до "СС" включительно) Сертификат ФСБ №СФ/124-4641 (на используемое в составе изделия СКЗИ)
В Реестре отечественного ПО	№4320
В Реестре ПАКов (Минцифры)	№20809
В Реестре радиоэлектронной промышленности Минпромторга (ПП-878, ПП-719)	№10495357, 0520850
Возможность поставки в рамках госзакупок и ГОЗ (по ПП-1875, 44-ФЗ, 223-ФЗ, ПП-325)	Да
Выполняет требования 117-го Приказа ФСТЭК	п.51, 66-б, 70 - работа только с учтёнными и идентифицированными съёмными носителями, контроль использования, выявление несанкционированных Выполнение требований - приказов ФСТЭК России №17, 21, 25, 31, требований профилей защиты средств контроля отчуждения (переноса) информации со съёмных машинных носителей информации - МО России к ЗМНИ (защищённым машинным носителям информации) - 117-го Приказа ФСБ - п.1, 3, 6 (СКЗИ для шифрование данных на носителях вне контролируемой зоны) - СТР, СТО БР ИББС, 152-ФЗ "О персональных данных", 187-ФЗ "О безопасности КИИ"

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.