Новые требования ФСТЭК России

к защите ГИС, обеспечению доверия в ИС и ИТ-инфраструктуре

V2

Сергей Груздев

ген. директор АО "Аладдин Р.Д."

19 сентября 2024 г.

Новые Требования ФСТЭК России

Для кого

- К защите информации, содержащейся в
  - ГИС
  - ИС гос. органов, гос. унитарных предприятий, гос. учреждений
  - ИСПДн (совместно с Требованиями по 1119-ПП от 1.11.2012)
  - ИС значимых объектов КИИ (с дополнениями в зависимости от категории значимости)
  - Иных ИС (в т.ч. муниципальных) в случае обработки и хранения в них информации
    - Доступ к которой ограничен законодательством РФ
    - Переданной из ГИС
- Обязательны для защиты
  - Общедоступной информации
  - Информации ограниченного доступа (служебная тайна, ДСП)

✓ **Замена 17-го Приказа ФСТЭК России от 11.02.2013 и Мер защиты…**

Новые Требования ФСТЭК России

Статус

- Требования, обязательные к исполнению (ЧТО должно быть сделано)
  - КАК делать - планируется определить в Методических рекомендациях
  - Началась проработка в рабочих группах
- Проект
  - Вступят в действие через 1 год после утверждения
  - Пункт 50 (про обеспечение доверия в ГИС на базе PKI) - отложенная мера - через 2 года

Классы защищённости ГИС

Масштаб ИС

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

При определении класса защищённости ГИС должны учитываться

- Класс защищённости ИТ-инфраструктуры (д.б. не ниже класса защищённости ГИС)
- Наличие информации ограниченного распространения (с пометкой **ДСП**) - сразу **К1**

Уровни доверия к ИС

- К1 - высокий
- К2 - средний
- К3 - низкий

Важнейшие изменения в подходе к защите ГИС

Важнейшие изменения в подходе к защите ГИС

Системный подход

- ГИС - это не "сферический конь в вакууме"
- ГИС надо рассматривать как комплексную систему, работающую в ИТ-инфраструктуре (оборудование, сети, протоколы, сервисы…)
- К ГИС подключаются
  - Администраторы
  - Удалённые пользователи
  - Другие ИС (разработчики, контрагенты, системные интеграторы)

✓ **ИС часто атакуют через них!**

Ключевые изменения

- Доверие к ГИС напрямую связано
  - С обеспечением доверенного безопасного взаимодействия между собой всех элементов **ИТ-инфраструктуры, ПО,** пользователей
    - Требуется **строгая** аутентификация оборудования и ПО
  - С отказом от использования паролей
    - Только 2ФА (строгая и усиленная)

✓ **Для этого нужен корпоративный PKI**

Элементы ИС - пирамида доверия

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

2 **ПО,** используемое в ИС (встроенное, системное, прикладное)

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
  - Уверенность, подтверждённая доказательствами, полученными от третьей доверенной стороны (корп. CA)
  - **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)

Цели внедрения PKI в ГИС

- ИС делятся:
  - Открытые (публичные) - с неограниченным количеством пользователей (УЦ, ЭП, 63-ФЗ…)
  - Закрытые (замкнутые, корпоративные)
- Большинство ГИС надо рассматривать как **закрытые корпоративные системы**

✓ **PKI в новых Требованиях рассматривается только применительно к закрытым корпоративным системам**

- PKI в ГИС необходим для
  - Обеспечения доверенного **взаимодействия** всех элементов корпоративной ИТ-инфраструктуры - используемого оборудования, программного обеспечения (ПО), пользователей
  - **Строгой аутентификации** пользователей при доступе в корпоративную ИС
  - Корпоративного электронного документооборота с использованием усиленной **неквалифицированной** ЭП
  - Защиты данных
- PKI должен разворачиваться **в распределённых ГИС с доменной архитектурой**
  - В ГИС без доменной архитектуры может использоваться **усиленная** аутентификация пользователей
    - Обязательно 2ФА, не пароли!

Цели внедрения PKI в ГИС

- Строгая аутентификация
  - Объектов ИТ-инфраструктуры, ИС (ПО)
  - Пользователей
    - Всех без исключения (администраторов, удалённых, контрагентов)
    - Взаимная, 2ФА (обязательно с использованием аппаратного устройства с поддержкой криптографии, неизвлекаемыми закрытыми ключами, по цифровым пользовательским сертификатам, выдаваемым ЦС владельца ГИС)

- *Цели внедрения* PKI *в открытых информационных системах* ***другие***
  - *Для аутентификации Web-сайтов и защиты сессий (SSL, TLS-сертификаты)*
  - *Для организации юридически значимого электронного документооборота с использованием квалифицированной электронной подписи (ЭП)*
    - *Сервисы ФНС, портал госуслуг, ДБО и др.*

Разные цели внедрения PKI - разная терминология

ПНСТ 799-2022

Требует корректировки

Открытые ИС (в части электронной подписи в соответствии с 63-ФЗ)	**Закрытые ИС** (в части строгой аутентификации в соотв. с ГОСТ Р 58833-2020)
Удостоверяющий центр	**Центр сертификации (ЦС)**
Электронная подпись	**Цифровая подпись**
Сертификат ключа проверки электронной подписи	**Сертификат безопасности** (Цифровой сертификат)

Сертификаты безопасности

- Типы цифровых сертификатов
  - Машинные
    - Для взаимной аутентификации оборудования в ИТ-инфраструктуре
  - Программные
    - Для проверки подлинности (аутентичности) ПО и возможности использовать его в данной ИТ-инфраструктуре (подпись кода, подпись программных объектов)
  - Пользовательские
    - Для строгой аутентификации пользователей в ИС
- Сроки действия сертификатов
  - Для подчинённых ЦС - 7 лет
  - Для пользователей - 3 года
  - Для оборудования и ПО - 1 год

Требования к аутентификации в ГИС

- Аутентификация оборудования
  - По цифровым сертификатам (машинным)
  - С использованием модуля безопасности (Secure Element)
    - Неизвлекаемый закрытый ключ
    - Поддержка зарубежной криптографии (для совместимости с применяемыми протоколами аутентификации - SCEP, ACME, MS-WSTEP и др.) и российских ГОСТов - «на вырост»
    - Для доверенной загрузки оборудования и его строгой аутентификации при подключении к сетевой инфраструктуре
    - Для проверки цифровой подписи ПО (прошивки, UEFI, ядра ОС, обновлений)
- Аутентификация пользователей
  - Строгая (для распределенных ГИС с доменной архитектурой)
    - Двухфакторная (или 3х-факторная) - обязателен физический носитель!
    - С использованием цифровых сертификатов и неизвлекаемых закрытых ключей
  - Усиленная (допускается для малых ГИС)
    - Двухфакторная (или 3х-факторная) - обязателен физический носитель!

✓ ***Простая (парольная) - не допускается!***

✓ **Большая задача - разработка протоколов аутентификации оборудования с поддержкой российских ГОСТов**

Требования к аутентификации ПО

- Подпись кода (ПО)
  - ПО должно подписываться
    - Цифровой подписью **разработчика** (1)
    - Цифровой подписью **владельца ИС** (2) - это обеспечивает возможность установки/использования только разрешённого (подписанного владельцем ИС) ПО
  - При установке ПО и обновлений в ГИС должны проверяться их аутентичность и целостность с использованием цифровых сертификатов
  - ОС должны включать в себя
    - Средства, обеспечивающие поддержку модулей безопасности
    - Средств 2ФА пользователей
    - Средства проверки цифровой подписи ПО

✓ **Создана рабочая группа (разработчики российских ОС) для разработки Методических рекомендаций**

Что нужно для реализации
высокого уровня доверия в ГИС

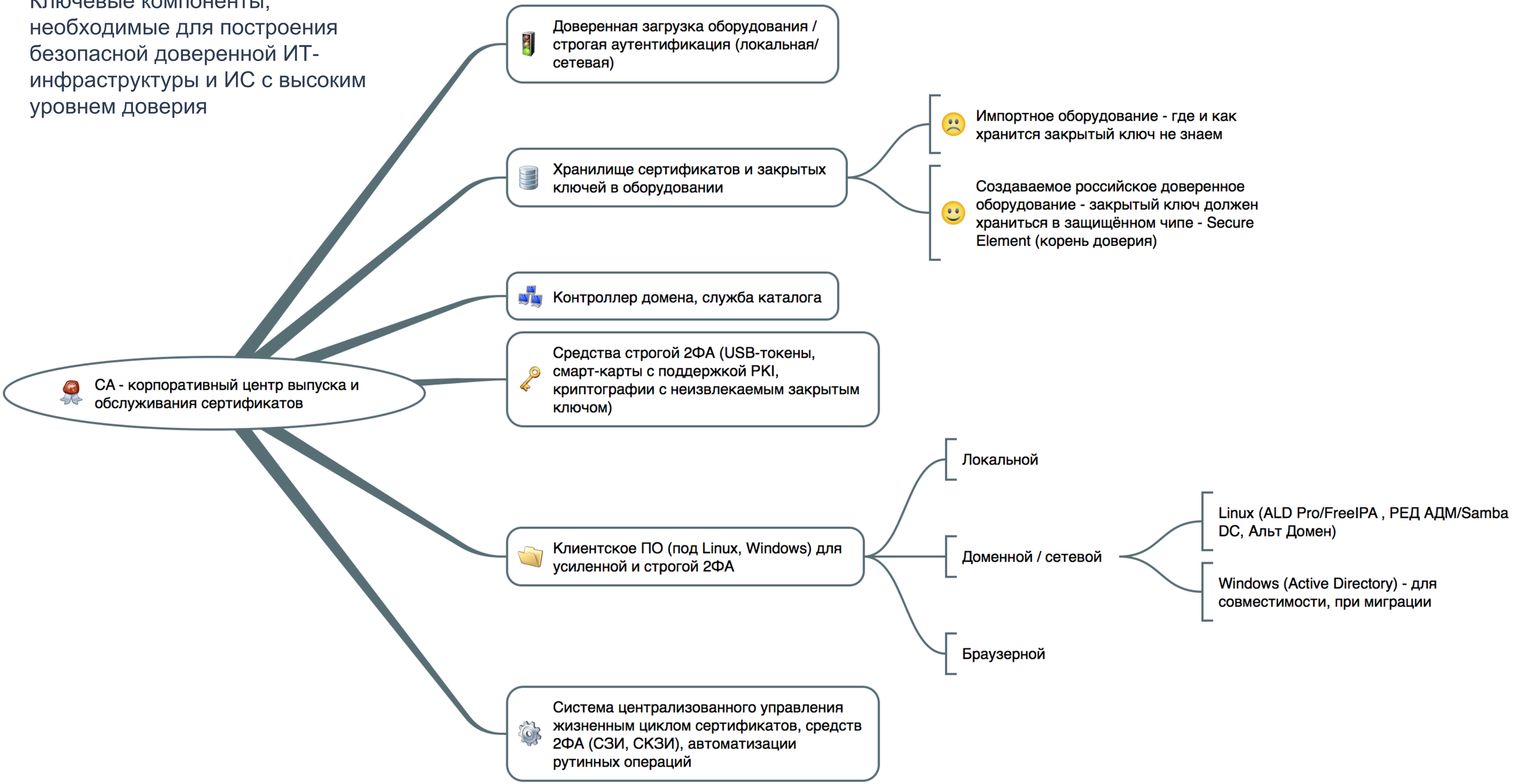
Ключевые компоненты

- Корпоративный Центр сертификации
  - Владелец (оператор) ГИС должен иметь **собственный** доверенный Центр Сертификации, сертифицированный ФСТЭК России
    - Не MS CA! Это единая точка отказа всей ИТ-инфраструктуры
    - Корневой и подчинённые ЦС

  ✓ **Aladdin Enterprise CA (eCA) - сертификат на оформлении**

- Средства строгой аутентификации
  - Пользователей (USB-токены, смарт-карты с поддержкой PKI)
- Клиентское ПО (в составе российских ОС)
  - Реализация всего стека PKI
    - Полноценного PKI для Linux нет ни в Open Source, ни в российских ОС
  - Поддержка средств 2ФА, строгой и усиленной аутентификации пользователей
    - Локальной, доменной (MS AD, домены Linux), браузерной
    - Аналог MS Smartcard logon (**Aladdin SecurLogon**)
  - Поддержка модулей безопасности (встраиваемых в оборудование)
- Централизованное управление жизненным циклом цифровых сертификатов, средств 2ФА

Ключевые компоненты, необходимые для построения безопасной доверенной ИТ-инфраструктуры и ИС с высоким уровнем доверия



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