Инфраструктура доверия

Ключевые компоненты для построения безопасной доверенной ИТ-инфраструктуры

Сергей Груздев

ген. директор АО "Аладдин Р.Д."

18 января 2024 г.

Что такое **доверие** и зачем оно нам?

Постоянно слышим про доверие

Начинаем сами про него твердить

Большинство не понимает ЧТО ЭТО, КАК обеспечивается, и ЗАЧЕМ оно нам?

Из-за этого идёт **подмена понятий и целей**, и мы начинаем делать не то, что нужно

Что такое ДОВЕРИЕ

- Доверие
  - Между людьми
    - Это уверенность в порядочности и ответственности другого, что он не воспользуется полученной от нас информацией нам во вред
  - В ИТ-инфраструктуре
    - Это уверенность в том, что каждый элемент инфраструктуры (сети) работает так, как мы ожидаем, что этот элемент не подменили, что мы можем доверять получаемой информации
    - Система считается доверенной, когда каждый её элемент является доверенным
    - Доверие обеспечивается идентификацией и аутентификацией каждого элемента инфраструктуры (компоненты системы)
    - Надёжность (доверие) системы определяется по её самому слабому звену
- Уровни доверия
    - Низкий
    - Средний
    - Высокий

Уровни доверия в ИС

Для ИС с высокой значимостью информации и высоким (недопустимым) размером возможного ущерба необходим ВЫСОКИЙ уровень доверия

Здесь важнее не доверие, а ГАРАНТИИ

- Уровни доверия в ИС

Как обеспечивается доверие в ИС

- Основа доверия в ИС - АУТЕНТИФИКАЦИЯ
- Что такое аутентификация?
  - Это процедура "установление подлинности" (перевод с латинского)
    - Доказательство того, что ты - это ты
- Цели аутентификации в ИС
  - Установление доверительных отношений между всеми участниками обмена
    - Аутентификация источника данных (односторонняя аутентификация)
    - Аутентификация сторон (элементов ИТ-инфраструктуры - взаимная аутентификация)
  - Предоставление доступа
- Надёжность аутентификации и уровни доверия
  - Простая - низкий уровень доверия
  - Усиленная - средний уровень доверия
  - **Строгая** - высокий уровень доверия

ИБ начинается с аутентификации

Как обеспечивается доверие в ИС

- Как обеспечивается аутентификация (доверие)
  - **Простая** (для предоставления доступа, однофакторная, односторонняя)
    - Логин / Пароль
    - Двухэтапная - с QR-кодом или кодом подтверждения, присылаемым на телефон (не путать с 2ФА!)
  - **Усиленная** (для предоставления доступа, двухфакторная, одно- или двухсторонняя)
    - OTP (с хранением секретного ключа на токене или смартфоне)
    - U2F (стандарт FIDO Alliance - "Мир без паролей")
  - **Строгая** (для установления доверительных отношений в ИС и предоставления доступа, двухсторонняя, с использованием криптографии, PKI и сертификатов)
    - Машинные сертификаты (для аутентификации "железа" в ИТ-инфраструктуре)
    - Программные сертификаты (для использования только разрешённого/доверенного ПО)
    - Пользовательские сертификаты (для 2ФА/3ФА пользователей в ИС)

Без этого построить безопасную доверенную ИТ-инфраструктуру нельзя!

✓ **Типовое заблуждение: 2ФА - не всегда строгая**

Требования к аутентификации в различных ИС

Тип аутентификации в ИС должен определяться

- по уровню значимости информации

- по вероятности и размеру возможного ущерба в случае взлома и утечки

- 70% взломов и утечек после начала СВО - из-за некорректной подсистемы аутентификации

- Требуемые типы аутентификации в ИС

Вероятность и размер возможного ущерба

Уровень значимости информации в ИС

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

- Гос. организации
- Федеральные структуры
- Организации КИИ
- Крупный и ср. бизнес
- Операторы ИСПДн (оборотные штрафы)

Для кого:
- Для всех пользователей и администраторов ИС
- Для удалённых пользователей

Для государственных ИС, объектов КИИ необходимо создавать доверенную, безопасную, санкционно-независимую ИТ-инфраструктуру

Доверенная - с обеспечением строгой аутентификации всех элементов ИТ-инфраструктуры (здесь важны гарантии, а не доверие)

Санкционной-независимая - в инфраструктуре не должно быть точек отказа, которые можно бы было активировать из-за рубежа

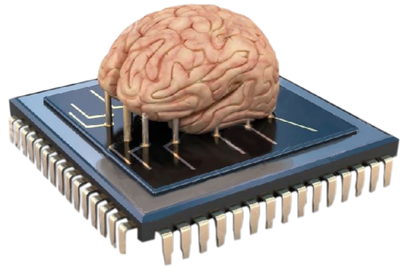
Что такое ДОВЕРИЕ и как оно обеспечивается

- Гарантии, обеспечивающие высокий уровень доверия
  - Криптография (гарантированная стойкость)
  - Строгая аутентификация (взаимная, многофакторная, с использованием криптографии)
  - Безопасность закрытых ключей (Secure Element, ~~*Security Island*~~)
  - PKI (централизованная инфраструктура)
    - Основа PKI - центр выпуска и обслуживания сертификатов (корпоративный CA)
      - Выпуск цифровых сертификатов (машинных, программный, пользовательских)
      - Валидация (проверка)

✓ **Это самый критический сервис во всей ИТ-инфраструктуре**

- Чем обеспечивается доверие и безопасность в наших ИТ-инфраструктурах?
  - Microsoft CA (Certificate Authority/Certificate Services)
    - В 2022 г. Microsoft ушла из России, представительство закрыто, поддержки MS CA больше нет, купить его тоже нельзя
  - Аналога Enterprise-класса в российских ОС на базе Linux нет, в OpenSource тоже нет

✓ **Это стратегический продукт, приравненный к ядерным технологиям**



Secure Element

Security Island - не можем сегодня себе это позволить - у нас нет таких технологий и возможностей производства

Требуется изменение приоритетов

Первый приоритет для ИТ/ИБ - устранение точек отказа - санкционно-зависимых (критических) компонентов в ИТ-инфраструктуре, невозможность вырубить её из-за рубежа

Второй - защита главных информационных активов (баз данных, хранилищ/дисков-носителей)

Приоритеты не определены, движемся по инерции, продолжаем бороться с плохими парнями и защищать периметр

Единая точка отказа для всех наших ИТ-инфраструктур - MS CA

MS CA - корпоративный центр выпуска и обслуживания сертификатов

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

✓ **Не путать корп. CA с УЦ для ЭП (63-ФЗ) — разные задачи и разные требования!**

✓ **Риски блокирования работы сервиса MS CA - очень большие (в т.ч. через закладки)**

Ключевые компоненты

для построения безопасной доверенной ИТ-инфраструктуры

Ключевые компоненты для построения доверенной ИТ-инфраструктуры

NEW

Корпоративный центр выпуска и обслуживания сертификатов

Aladdin Enterprise CA

- основа обеспечения доверия всех элементов ИТ-инфраструктуры

NEW

Клиент PKI и 2ФА для Linux

SecurLogon

- для строгой 2ФА пользователей
- аналог MS Smartcard logon

USB-токены, смарт-карты, Secure Element

JaCarta-2 PKI

- для строгой 2ФА пользователей и устройств (машин)

Корпоративная система централизованного управления токенами, сертификатами

JMS

- обязательный компонент для крупной ИТ-инфраструктуры

Aladdin Enterprise CA

НОВИНКА!

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

Сертификация: по линии ФСТЭК России (до гостайны вкл.)

В Реестре отечественного ПО

Импортозамещение: Microsoft Certificate Services (MS CA)

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

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 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.