Инфраструктура доверия

Ключевые компоненты для построения безопасной доверенной ИТ-инфраструктуры

Сергей Груздев

ген. директор АО "Аладдин Р.Д."

Изменение и переоценка киберугроз после начала СВО

- С чем столкнулись после 2022 г?
  - Беспрецедентный рост успешных атак
    - Одна из причин (1) - неправильно спроектированная и реализованная **аутентификация** пользователей, использование паролей (ПРОСТАЯ аутентификация вместо СТРОГОЙ)
    - Вторая причина (2) - **удалённый доступ** - использование небезопасного "самопала"

    ✓ **После инцидента - начинается устранение последствий, а не причин**
  - Массовые утечки баз данных и персональных данных
    - Причины - вместо **обезличивания** ПДн и **защиты** самих критически важных данных - **главных информационных активов**, усиливают защиту периметра, средства мониторинга и аналитики
  - Переоценка рисков и угроз (политических, архитектурных), от которых зависит работоспособность всех наших ИТ-инфраструктур
    - Главный приоритет - **выявление и устранение точек отказа**
    - Вместо этого часто движемся по инерции - боремся с навязанными нам угрозами ("плохие парни" - хакеры, вирусы-шифровальщики…)

    ✓ **Необходимо сфокусироваться на главном**
- Мир изменился, мы перестали доверять Западу и их технологиям
  - Нам необходимо самим создавать свою безопасную **доверенную** ИТ-инфраструктуру

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 часто происходит **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

Как обеспечивается доверие в ИС

- Основа доверия в ИС - ИДЕНТИФИКАЦИЯ и АУТЕНТИФИКАЦИЯ
- Что такое идентификация?
  - Это ответ на вопрос - **ты кто?** - способ/процесс определения личности пользователя (субъекта) или объекта (сущности)
- Что такое аутентификация?
  - Это **доказательство** того, что ты - это ты (процедура "установление подлинности")
- Идентификация и аутентификация неразрывно связаны
- Цели аутентификации в ИС
  - (1) **Установление доверительных отношений** между всеми участниками обмена
    - Аутентификация источника данных
    - Аутентификация сторон (элементов ИТ-инфраструктуры)

    ✓ **Крайне важно для создания безопасной доверенной инфраструктуры!**
  - (2) **Предоставление доступа**

ИБ начинается с правильной идентификации и аутентификации

Как обеспечивается доверие в ИС

- Уровни доверия к аутентификации
  - **Простая** (для предоставления доступа, однофакторная, односторонняя)
    - 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") и др.
  - **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)

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

Без этого построить безопасную доверенную ИТ-инфраструктуру нельзя!

Нац. стандарты по идентификации и аутентификации

- Действующие стандарты
  - ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения
  - ГОСТ Р 70262.1-2022 Защита информации. Идентификация и аутентификация. **Уровни доверия идентификации**
  - ГОСТ Р 59381-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции
  - ГОСТ ISO/IEC 24760-2-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования.
  - ГОСТ Р 59382-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы
  - ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом
  - ГОСТ Р 59515-2021 Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности
- Проекты стандартов
  - Защита информации. Идентификация и аутентификация. **Уровни доверия аутентификации**
  - Защита информации. Идентификация и аутентификация. Управления идентификацией и аутентификацией
  - Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости идентификации и аутентификации
  - Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией

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

Вероятность и размер возможного ущерба

Уровень значимости информации в ИС

Уровень доверия	Низкая	**Средняя**	**Высокая**
Высокая	Средний	**Высокий**	**Высокий**
Средняя	Низкий	Средний	**Высокий**
Низкая	Низкий	Низкий	Средний

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

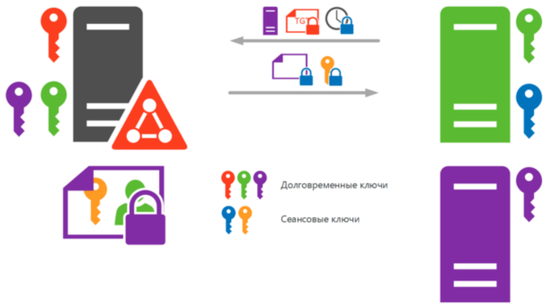
✓ **Здесь важнее не доверие, а ГАРАНТИИ**

* - экспертная оценка компании Аладдин

Виды аутентификации в ИС

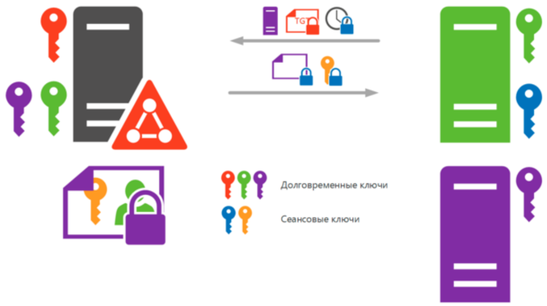
Всего 8 видов аутентификации

- Локальная
  - Службы аутентификации и валидации (принимающая решение о предоставлении доступа) находятся на каждом локальном устройстве (ПК, смартфон и пр.)
- Прямая
  - Владелец ресурса доверяет одному валидатору, расположенному внутри защищённого периметра
  - Все пользователя локальной сети проходят процесс аутентификации и валидации напрямую
    - Применяется в небольших организациях численностью до 20-30 рабочих мест
- Доменная
  - Владельцы многих ресурсов в локальной сети доверяют одному валидатору, расположенному внутри защищённого периметра локальной сети
    - Применяется в сегментах малого и среднего бизнеса
- Иерархическая
  - Отличается от доменной наличием подчинённых доменов, доступ пользователям могут предоставляться ими, однако в центре имеется база данных учётных записей всех пользователей и право управления доступом
    - Применяется в организациях с филиальной сетью



Типы аутентификации в ИС

- Распределённая сетевая
  - Отличается от доменной наличием множества доменов, связанных между собой трассовыми (доверенными) отношениями
  - В каждом домене независимо производится процесс аутентификации и принимается решение о доступе
    - Применяется в крупных корпорациях и холдингах
- Мостовая
  - Отличается от распределённой сетевой наличием доверенной третьей стороны (ДТС)
    - Применяется для межведомственного взаимодействия с развитым электронным документооборотом (ЭДО)
- Браузерная
  - Отличается от мостовой механизмом аутентификации, основанном на организации защищённого канала связи клиент-сервер на сессионном уровне
  - ДТС может находится на том сервере
    - Применяется для порталов госуслуг
- Браузерная с трансляцией доверия
  - Отличается от браузерной транслированием доверия к аутентификации, которую пользователь успешно прошёл в первичной ИС, в другие публичные/облачные ИС
  - Решается с применением федеративной системы трансляции доверия
    - Применяется для ведомственных, региональных порталов (ФНС, mos.ru и др.) с трансляцией доверия, например, от портала gosuslugi.ru



Требования к аутентификации в различных ИС

Для каждой ИС должен применяться свой правильный вид и тип аутентификации

Тип аутентификации в ИС должен определяться

- по уровню значимости информации
- по вероятности и размеру возможного ущерба в случае взлома и утечки
  - **Причины взломов и утечек многих ИС - некорректная подсистема первичной идентификации и 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

✓ **Здесь важнее не доверие, а ГАРАНТИИ**

Требования к идентификации и аутентификации в ИС

Уровень значимости информации и размер возможного ущерба	**Низкий**	**Средний**	**Высокий**
Первичная идентификация			
Удалённо	●		
При личной явке		●	
Только при личной явке с проверкой и подтверждением личности			●
Вторичная идентификация			
По предъявлению идентификатора без дополнительной проверки	●		
По предъявлению идентификатора и дополнительных атрибутов идентификации (Знание, Владение, Биометрия)		●	●●
Дополнительные атрибуты и факторы (степень связанности с пользователем)			
Двухэтапная проверка при идентификации (Знание - код доступа)		●	
Электронный идентификатор (Владение)		●	
Электронный идентификатор и одноразовый пароль (Владение и Знание - общий секрет)		●	
Электронный идентификатор и сертификат (Владение и Знание - ПИН-код)		●	
Электронный идентификатор с встроенной криптографией, неизвлекаемым закрытым ключом, сертификатом пользователя, **развёрнутой PKI** (Владение и Знание - ПИН-код)			●●
Электронный идентификатор с встроенным полупроводниковым сканером отпечатков пальцев, реализацией технологии Match-On-Device (Владение и Биометрия)			●

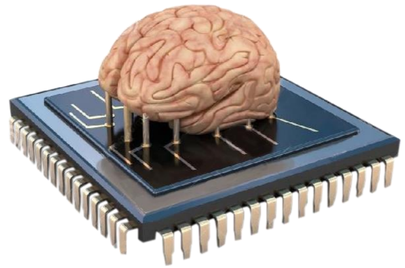
* - на уровне гарантий
** - опция

Ключевые компоненты,

обеспечивающие высокий уровень доверия ИТ-инфраструктуры

Компоненты для обеспечения высокого уровня доверия в ИС

- Идентификация
  - Правильные процедуры, требования и регламенты
    - С обязательной личной явкой, проверкой предоставленных документов
- Аутентификация (строгая)
  - (1) **Персональный USB-токен или смарт-карта** - второй фактор аутентификации пользователей
    - С ПИН-кодом, установленным самим пользователем (фактор знания)
    - С аппаратной реализацией криптографии с известной стойкостью
    - С неизвлекаемым закрытым ключом
    - С цифровым сертификатом X.509
  - (2) **Secure Element** (**не TPM!**) для доверенного оборудования в критически важных системах
    - Для безопасного взаимодействия, дистанционного управления, обновления ПО
    - С аппаратной реализацией криптографии
    - С неизвлекаемым закрытым ключом
    - С машинным сертификатом X.509
  - (3) **Оборудование без Secure Element**
    - С машинным сертификатом X.509, сохраняемым в памяти устройства
    - С поддержкой стандарта IEEE 802.1X



Security Island - "островок безопасности на процессоре" позволить себе сегодня не можем, у нас нет таких технологий и возможностей производства

Компоненты для обеспечения высокого уровня доверия в ИС

- Инфраструктура
  - (4) **Корпоративный центр выпуска и обслуживания сертификатов** (CA)
    - **Машинные** (каждое устройство в ИТ-инфраструктуре должно быть идентифицировано и аутентифицировано)
    - **Программные** - разрешённое ПО должно быть подписано не только сертификатом разработчика, но и эксплуатирующей организацией
    - **Пользовательские** (выпущенные на их персональные USB-токены или смарт-карты)

      ✓ **Это не должен быть Microsoft CA - ему больше нельзя доверять!**
    - С поддержкой работы в двух экосистемах - Linux и Windows
  - (5) **Клиентское ПО** (под российские ОС на базе Linux)
    - С поддержкой средств 2ФА
    - С поддержкой PKI
    - С возможностью одновременно работать и в Linux, и в Windows, с разными домен-контроллерами
  - (6) **Корпоративная система централизованного управления жизненным циклом**
    - Средств 2ФА (с возможностью обновления сертификатов и "прошивок")
    - Сертификатов и др. объектов PKI
    - Профилей пользователей, СЗИ, СКЗИ и пр.

Ключевые компоненты

для построения безопасной доверенной ИТ-инфраструктуры

MS CA - единая точка отказа в любой ИТ-инфраструктуре

Его необходимо срочно заменять

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, приложений (ПО), пользователей
  - Работоспособность доменов безопасности/службы каталога
  - Работа различных сервисов (удалённого доступа, VDI, VPN, RDP-шлюзы и др.)
- Мало кто 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, даёт доступ в ИС)?
  - Как это будет работать при переходе на Linux?
  - Есть ли полноценный PKI Enterprise-класса под Linux?

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

✓ **Риски блокирования работы сервиса MS CA - достаточно большие**

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

НОВИНКА!

Aladdin Enterprise CA

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

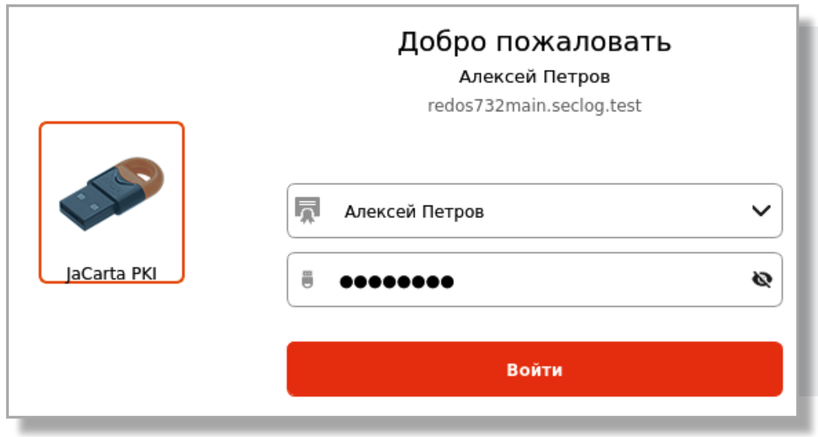
Сертификация: по линии ФСТЭК России (до гостайны вкл.)
В Реестре отечественного ПО
Импортозамещение: Microsoft Certificate Services (MS CA)

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

Поддержка PKI и 2ФА на клиенте Linux

Aladdin SecurLogon

НОВИНКА!



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

Проблемы:

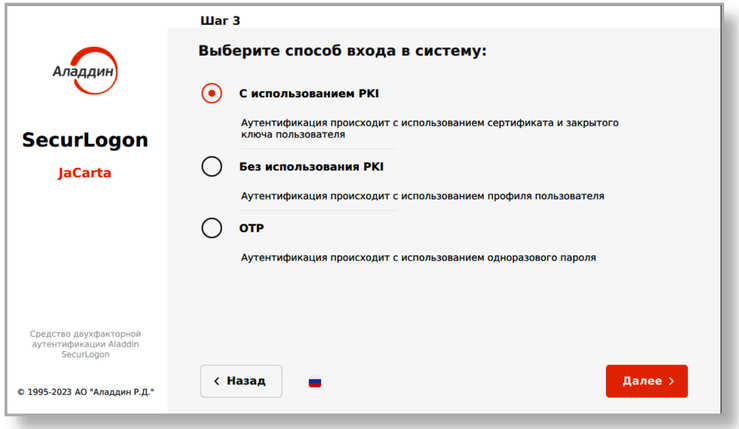
В MS Windows 2ФА пользователей реализует встроенная подсистема Windows Smart Card Logon

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

Aladdin SecurLogon

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

✓ **Полноценная альтернатива Microsoft Smart Card Logon на отечественных ОС на базе Linux**



Работает с USB-токенами и смарт-картами JaCarta

Средства для строгой двухфакторной аутентификации (2ФА) и ЭП

- безопасный доступ в Linux по сертификатам (PKI)

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

2ФА - не значит СТРОГАЯ

Строгая аутентификация для Linux

- Что значит СТРОГАЯ
  - Двухфакторная (2ФА), с использованием персонального специализированного защищённого устройства (требования новых ГОСТов)
    - с аппаратной реализацией криптографии с неизвлекаемым закрытым ключом
    - с хранением сертификатов доступа с памяти устройства
    - с возможностью его использования только авторизованным пользователем
    - неклонируемого (Secure by design)
  - Взаимная (аутентификация обеих сторон)
  - С использованием защищённых протоколов
- Требуется
  - Во всех системах, обрабатывающих значимую информацию
    - гос. организации, КИИ, АСУ ТП и др.
  - Для администраторов, пользователей, удалённых пользователей
  - Развёрнутая инфраструктура открытых ключей (PKI)
  - Централизованное управление жизненным циклом сертификатов, средств 2ФА
  - Модуль поддержки средств 2ФА и PKI для Linux
    - **В Linux нет аналога MS Smart Card Logon**

Линейка USB-токенов и смарт-карт JaCarta
(вкл. российские чипы I и II категории)
с сертификацией до КС-3 (ФСБ) и УД-4 (ФСТЭК)

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

Включает высокопроизводительный сервер аутентификации Enterprise-класса - JAS

Импортозамещение: любого импортного аналога

Версии: Linux, Windows

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

JMS - система централизованного управления Enterprise-класса

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

JMS - система централизованного управления Enterprise-класса

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

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 "оправославливания" зарубежных СУБД
- Аутентификация и электронная подпись для Secure Element (SE), USB-токенов, смарт-карт, IIoT-устройств, Web-порталов и эл. сервисов.