Инфраструктурные продукты и решения компании Аладдин для построения полноценной корпоративной PKI на Linux

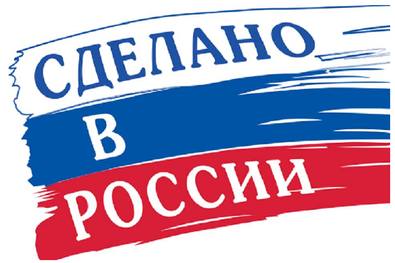
Сергей Груздев

ген. директор АО "Аладдин Р.Д."

Импортозамещение, санкционная и технологическая независимость

Прошел год с начала СВО…

- Вся ИТ-инфраструктура в стране построена на зарубежных решениях
- Западные вендоры ушли
  - Как минимум, мы остались без поддержки и развития
  - Риски блокирования работы ПО и "окирпичивания" оборудования висят как Дамоклов меч
  - Произошли массовые утечки - персональных данных, различных баз данных, чувствительной информации
  - Продолжаются массовые атаки на ИТ-инфраструктуры российских организаций
    - В 2012 г. США запустили программу "закладки кибербомб в критическую инфраструктуру России" (Cloud Act, PPD-20)
- Сильно недооценено влияние внутреннего нарушителя
  - Он везде
  - Он знает всё (принимал или принимает участие в разработке/обслуживании ИС, ИТ-инфраструктуры, СЗИ)



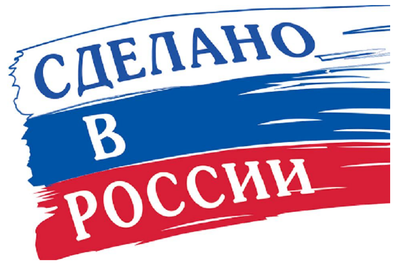
Импортозамещение, санкционная и технологическая независимость

- К практическому импортозамещению в ИТ мы не готовы
  - Последние 5-7 лет страна занималась имитацией импортозамещения и красивой отчётностью
  - Маразм продолжается - KPI по импортозамещению ставят по количеству рабочих станций, переведённых на Linux

  ✓ **Начинать надо с главного - с ключевых инфраструктурных решений, с защиты главных информационных активов**

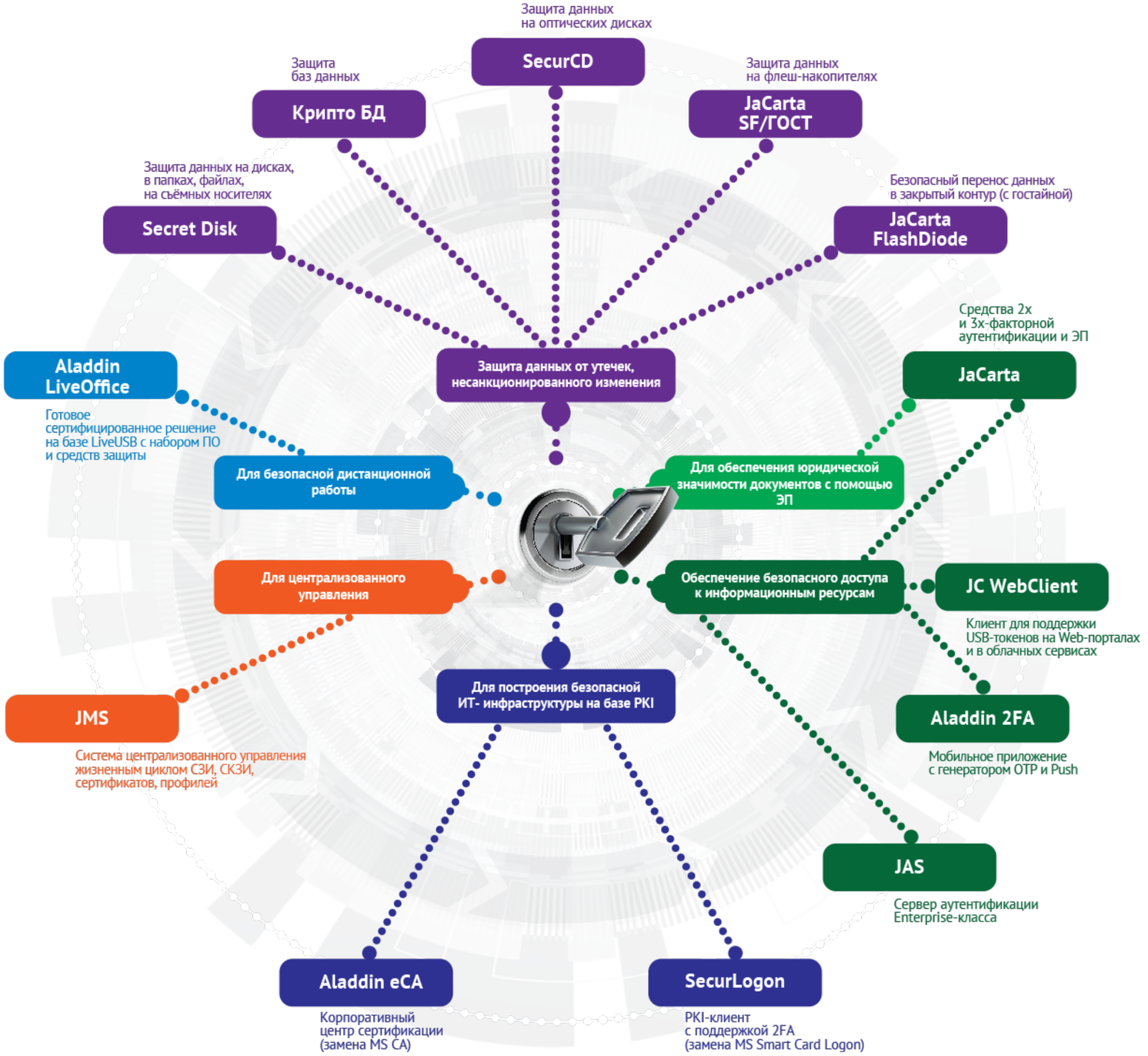
- Нам дали уникальную возможность сделать всё правильно
  - Не точечно замещать импортные продукты на аналоги (менять шило на мыло), а **заново перепроектировать свою ИТ-инфраструктуру**, без наследования "родимых пятен"
  - В основу подхода сразу заложить принципы Secure by Design

  ✓ **Сначала безопасность, потом функциональность**
    - Если делать по-другому, то получится "как всегда"
    - Сейчас у нас есть шанс сделать сразу всё правильно



Линейка продуктов

Аладдин



Корпоративный центр сертификации (CA)

- ключевой компонент

для построения безопасной доверенной ИТ-инфраструктуры на базе PKI

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

В Реестре отечественного ПО

Импортозамещение: Microsoft Certificate Services (MS CA)

Актуальность и важность замещения MS CA

- Корпоративный центр выпуска и обслуживания сертификатов (CA)
  - Основа (сердце) всей ИТ-инфраструктуры современной организации
    - работоспособности доменов безопасности/службы каталога
    - различных сервисов
    - аутентификации устройств, пользователей, приложений
    - доверенного взаимодействия всех объектов и компонентов
- Риски
  - Практически все ИТ-инфраструктуры в России построены на базе MS CA и на 100% зависят от его работоспособности
  - В 2022 г. Microsoft ушла из России, представительство закрыто, поддержка MS CA больше не осуществляется, купить его тоже нельзя
  - Полноценных аналогов MS CA в Open Source проектах нет
  - Коммерческие Enterprise-версии CA под Linux в Россию не поставляются (под строгим запретом)

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

Aladdin Enterprise CA под Linux

- Обеспечивает
  - Создание и функционирование корпоративной инфраструктуры открытых ключей (PKI)
  - Управление жизненным циклом цифровых сертификатов
  - Объединение всех компонентов ИТ-инфраструктуры в единый домен безопасности, их аутентификацию и безопасное взаимодействие
  - Обслуживание в автоматическом режиме всех объектов и компонентов корпоративной инфраструктуры ключами и цифровыми сертификатами
    - контроллеров доменов
    - серверов, Web-серверов, эл. почты
    - роутеров, маршрутизаторов, межсетевых экранов, VDI, VPN, RDP-шлюзов
    - компьютеров и др. устройств в доменах
    - M2M, IIoT-устройств
    - пользователей
  - Построение доверенной безопасной ИТ-инфраструктуры на базе PKI в сложных гетерогенных, облачных и мультиарендных инфраструктурах с разделением ролей и полномочий
  - Масштабирование, отказоустойчивость и разделение ролей
    - каждая функциональная роль центра сертификации (CA, RA, WebEnrol, CDP, DB и др.) может быть развёрнута на отдельном сервере в отказоустойчивой конфигурации

Aladdin Enterprise CA под Linux

- Позволяет
  - Работать параллельно с действующим Microsoft CA
  - Импортировать и использовать действующие шаблоны сертификатов Microsoft CA, создавать новые
  - Одновременно работать с различными службами каталогов (как Windows, так и Linux)
    - MS Active Directory
    - Samba DC
    - FreeIPA
    - ALD Pro
  - Интегрироваться с различными внешними системами через REST API
    - IdM, IAM, IGA, SIEM, JMS и др.
  - Обеспечить строгую двухфакторную аутентификацию (в т.ч. под Linux)
  - Использовать различные архитектуры аппаратных платформ, отечественные ОС, виртуальные среды

✓ **Замена для Microsoft Certificate Services (MS CA)**

Средства для строгой двухфакторной аутентификации (2ФА) и ЭП

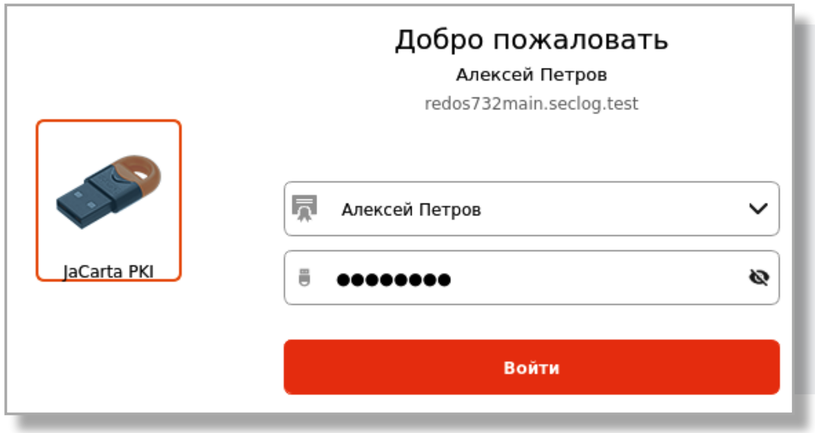
- безопасный доступ в Linux по сертификатам (PKI)

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

Строгая аутентификация для Linux

- Что значит СТРОГАЯ
  - Двухфакторная (2ФА), с использованием персонального специализированного защищённого устройства
    - 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



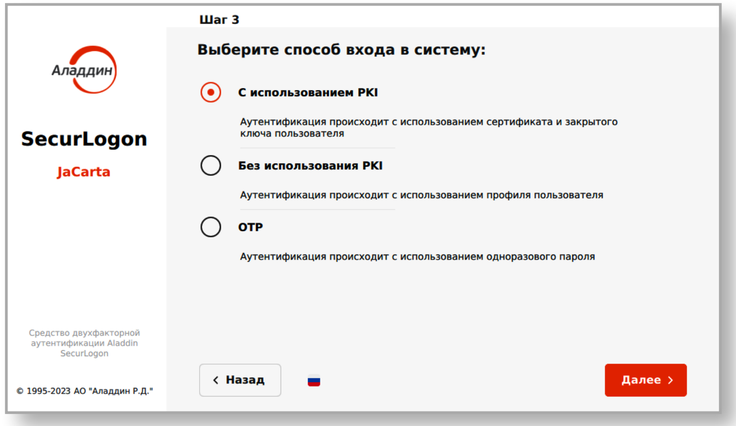
PKI-клиент и поддержка средств 2ФА в Linux

- замена MS Smart Card Logon

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

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**

Готовое сертифицированное средство для организации безопасной дистанционной работы

с возможностью подключения к ГИС, обработки информации ограниченного распространения

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

Aladdin LiveOffice

- Позволяет
  - Использовать специализированное защищённое USB-устройство Aladdin LiveOffice вместо служебного ноутбука
    - как удалённое рабочее место (терминал) с набором предустановленного и преднастроенного ПО
    - работать в замкнутой доверенной программно-аппаратной среде
  - Автоматически выполнить все требования и политики безопасности
  - Полностью соответствовать требованиям ФСТЭК и ФСБ России по организации безопасной дистанционной работы
  - Обеспечить централизованное управление (с использованием JMS)
  - В 5-7 раз экономить бюджет при организации дистанционной работы сотрудников и контрагентов
- Пример кейса
  - Заказчик ведёт базу эл. полисов, оформляют полисы - контрагенты (не сотрудники)
  - Выдать всем им служебные защищённые ноутбуки - дорого, а заставить всех их выполнять требования безопасности - невозможно
  - Риски утечки информации, компрометации учётных данных, атак на ИС, внесение несанкционированных изменений в базу - огромны
  - Решение - подключать к работе с ИС только тех, кто самостоятельно приобрел правильное сертифицированное средство, обеспечивающее безопасную дистанционную работу

Aladdin LiveOffice

- Обеспечивает
  - Полноценную дистанционную работу с любого недоверенного компьютера, например, с личного
    - 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
  - Возможность обработки коммерческой, служебной тайны
    - 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 свой аккаунт, пароль, параметры подключения
    - загрузить в информационную систему троян или вирус

✓ **Является альтернативой служебному ноутбуку с набором установленных приложений и сертифицированных средств защиты**

- Сертификаты: ФСТЭК России, ФСБ России (на компоненты, содержащие криптографию)

Защита данных на дисках

- замена MS BitLocker

Вся служебная информация, выносимая за пределы организации, должна быть зашифрована

В условиях санкций, атак на КИИ, "окирпичивания" многих зарубежных продуктов продолжать использовать встроенный в MS Windows BitLocker - лучший способ похоронить свои данные

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

Secret Disk

- Обеспечивает
  - Предотвращение утечки и несанкционированного доступа к ценной информации при утере, краже, изъятии, ремонте, неправильной утилизации компьютеров, серверов, носителей информации
  - Прозрачное шифрование данных
    - на ноутбуках, ПК, планшетах сотрудников
    - на файл-серверах и серверах приложений (в т.ч. баз данных)
    - на съёмных носителях
  - Сокрытие наличия ценной информации на защищённом компьютере, сервере или носителе
  - Гарантированное необратимое удаление 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
  - Фиксацию фактов доступа к защищённой информации
  - Защиту от действий привилегированных пользователей (системных администраторов)
  - Централизованное управление, интеграцию с системой управления JMS (для Enterprise-версии)

- Персональная версия
- Для серверов (приложений, файловых)
- С централизованным управлением (Enterprise)

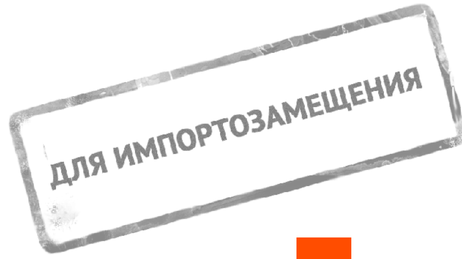
Защита баз данных

- импортозамещение встроенных в зарубежные СУБД средств защиты на отечественные, сертифицированные

Не всегда можно отказаться от использования Oracle и др. зарубежных СУБД

- огромные базы, которые российские аналоги не потянут
- огромное количество работающих приложений, для переноса которых могут потребоваться десятилетия

Технология "оправославливания" зарубежных СУБД позволяет существенно снизить риски и продолжить их использование



Крипто БД

- **Обеспечивает**
  - Защиту главных информационных активов организации (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 персональные данные
  - Прозрачное селективное (выборочное) шифрование критически важных данных в СУБД с использование российских алгоритмов
  - Двухфакторную аутентификацию пользователей при доступе к данным в СУБД
  - Централизованное управления ключами шифрования, исключающее возможные несанкционированные действия администраторов БД
  - Реализацию требований регуляторов
    - по обеспечению конфиденциальности и целостности информации в СУБД
    - по защите персональных данных, PCI DSS, ИС организаций КИИ
    - по моделям разделения доступа - дискретной и мандатной
  - Получение некорректируемой юридически значимой доказательной базы для проведения расследований инцидентов информационной безопасности
- **Сертификаты ФСБ России до класса КС-3**

Для СУБД Oracle, MS SQL, Tibero, PostgreSQL, Postgres Pro, Jatoba

Система централизованного управления

жизненным циклом сертификатов, токенов, СЗИ, СКЗИ

Включает высокопроизводительный сервер аутентификации Enterprise-класса - JAS

Импортозамещение: любого импортного аналога

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
  - 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")

Инфраструктурные продукты Аладдин для построения PKI на Linux

Стенд С-50

Сергей Груздев
ген. директор АО "Аладдин Р.Д."

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.