# Ключевые компоненты
## для построения безопасной доверенной ИТ-инфраструктуры

Аладдин


- Импортозамещение критически важных инфраструктурных продуктов
- Защита главных информационных активов
- Организация безопасной дистанционной работы
- Построение корпоративной PKI на Linux

ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

2024 г.

# Продукты и решения компании "Аладдин"

## Для чего

- Для построения доверенной безопасной ИТ-инфраструктуры предприятия на базе PKI
- Для надёжной идентификации и аутентификации пользователей информационных систем и онлайн-сервисов, а также устройств (M2M, IIoT)
- Для обеспечения безопасной дистанционной работы сотрудников и контрагентов
- Для защиты ценной информации на серверах, ноутбуках сотрудников, на съёмных носителях
- Для централизованного управления средствами защиты, сертификатами, профилями и политиками

## Для кого

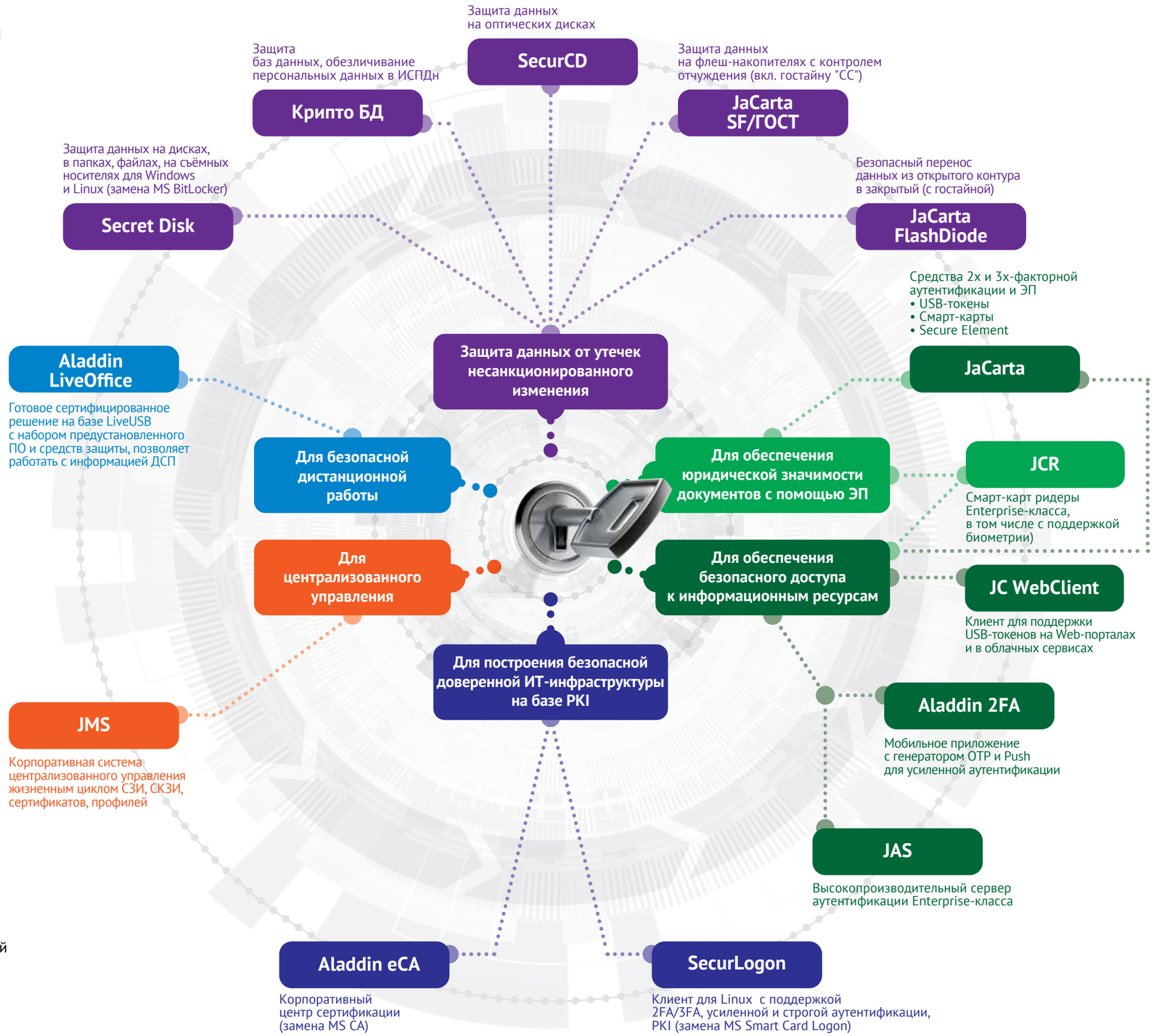
- Для гос. организаций, организаций КИИ, ОПК, Минобороны
- Для корпоративных пользователей со сложной и развитой ИТ-инфраструктурой
  - начавших замещение импортных продуктов ушедших с российского рынка зарубежных вендоров
  - внедряющих отечественные ОС (Linux), но вынужденных продолжать использовать Windows
  - приводящих свои АС, ГИС, ИСПДн, АСУ ТП, КИИ в соответствие требованиям законодательства РФ по защите информации
- Для предпринимателей, физлиц – всех, кто пользуется массовыми онлайн сервисами с применением ЭП

## Сертификаты

Практически все продукты компании:

- имеют сертификаты соответствия ФСТЭК России, ФСБ и/или Минобороны России, сертификат происхождения СТ-1
- могут использоваться для защиты конфиденциальной информации, а ряд из них – для гостайны со степенью секретности до "СС" включительно
- включены в реестры:
  - Реестр заключений Минпромторга РФ о подтверждении производства промышленной продукции на территории Российской Федерации (ПП719)
  - Единый реестр радиоэлектронной продукции Минпромторга РФ (ПП878)
  - Единый реестр Минцифры РФ российских программ для электронных вычислительных машин и баз данных
  - Единый реестр Минцифры РФ программно-аппаратных комплексов российского производства
- имеют сертификаты совместимости с продуктами ведущих российских производителей и иностранных вендоров

*Все продукты спроектированы в соответствии с принципами* **Secure by design** *– сначала безопасность, потом функциональность.*



# Aladdin Enterprise CA

## корпоративный центр сертификации под Linux – основа для построения корпоративной PKI

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


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.

### Актуальность и важность замещения MS CA

- Корпоративный центр сертификации – основа (сердце) всей ИТ-инфраструктуры современной организации, работоспособности доменов безопасности, службы каталога, различных сервисов, аутентификации устройств, пользователей, приложений, основа доверенного взаимодействия всех объектов и компонентов
- 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

***Импортозамещение:*** *Microsoft Certificate Services (MS CA)*

***Сертификаты:*** *по линии ФСТЭК России (до гостайны вкл.)*

***В Реестре отечественного ПО***

# JaCarta

## средства аутентификации и ЭП

- USB-токены
- Смарт-карты и ридеры
- Встраиваемые модули безопасности

Обеспечивают

- **двухфакторную** аутентификацию пользователей
  - строгую – на базе PKI
  - усиленную для ИТ-инфраструктур без PKI
- **трёхфакторную** аутентификацию пользователей с использованием биометрии по отпечатку пальца
  - Дополнительная идентификация пользователей (особенно привилегированных) крайне важна при доступе к критически важным информационным ресурсам предприятия, при проведении крупных финансовых транзакций
  - Применение биометрии гарантирует, что средством аутентификации (смарт-картой) сможет воспользоваться только его владелец
- **электронную подпись** (в т.ч. усиленную квалифицированную - УКЭП) в корпоративных и гос. системах электронного документооборота, на Web-порталах.
  - Все криптографические алгоритмы реализованы аппаратно[1], закрытые ключи никогда не покидают чип и не могут быть украдены или склонированы, поэтому, в отличие от программных СКЗИ, срок действия ключей составляет 3 года вместо одного


1. – кроме модели JaCarta LT


Позволяют

- применять токены и смарт-карты в корпоративной инфраструктуре в качестве
  - **персонального средства** аутентификации и ЭП для безопасного доступа в информационную систему предприятия, для работы с эл. сервисами и обеспечения юридической значимости подписываемых документов (госуслуги, эл. сервисы ФНС, Росреестр, Казначейство и др.)
  - **автоматического средства ЭП** в автоматизированных системах (ЕГАИС, АБС и др.), имеющего повышенный ресурс – более 10М операций подписи
  - **электронного удостоверения сотрудника**, объединяющего в себе идентификационную карту (бейдж) с именем, фото и должностью сотрудника, бесконтактным эл. пропуском (RFID-метку для СКУД) для прохода через турникеты, в помещения организации, персональное средство двухфакторной аутентификации и ЭП пользователя
- единообразно работать на различных устройствах и в различных средах на базе
  - Windows,
  - Linux,
  - Mac OS,
  - Android,
  - Аврора и др.


***Импортозамещение:***
*любых аналогичных продуктов, MS Smart Card Logon**

***Сертификаты:*** *ФСТЭК России, ФСБ России*

# JaCarta

## средства для защиты аккаунтов в онлайн сервисах

### JaCarta U2F

- поддерживает стандарт FIDO U2F – один токен для всех используемых эл. сервисов (доступ к облачным, почтовым сервисам, видео-, файловому хостингу, к ИТ-проектам на GitHub, в соцсети и пр.)

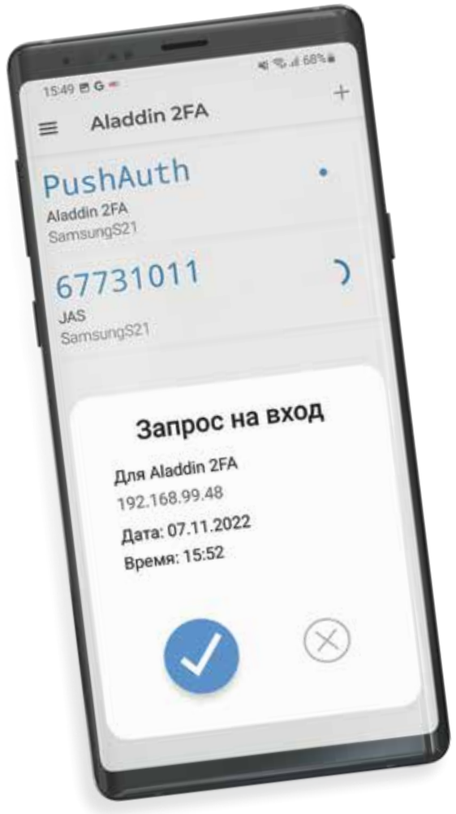
### JaCarta WebPass

- более удобная альтернатива классическим OTP-токенам с ручным вводом генерируемого ими одноразового пароля

кнопка для аутентификации и генерации одноразового пароля

### Позволяют

- защититься от фишинга - сохранять адреса нужных Web-ресурсов и автоматически переходить на них
- генерировать одноразовые пароли (OTP) и автоматически подставлять их в поля экранных форм
- генерировать, безопасно хранить и автоматически подставлять в поля экранных форм многоразовые сложные пароли
- организовать усиленную двухфакторую аутентификацию в инфраструктурах без PKI




## Смартфон вместо токена

Мобильное приложение Aladdin 2FA позволяет использовать смартфон вместо аппаратного OTP-токена для усиленной аутентификации в компьютере, в корпоративной сети, в различных эл. сервисах.

Оно более безопасно, чем коды подтверждения, передаваемые через SMS, и чем программные генераторы одноразовых паролей (OTP) типа Google Authenticator или Яндекс.Ключ.
Перехват секрета здесь невозможен.

## Централизованное управление

Задачи учёта, инвентаризации, централизованного управления жизненным циклом токенов и смарт-карт JaCarta, выпуска/отзыва сертификатов, учёта СКЗИ, автоматической подготовки отчётности по требованиям Регуляторов, обновление профилей, автоматизации практически всех рутинных операций решаются с помощью специализированной корпоративной системы централизованного управления JMS (JaCarta Management Systems).

# Aladdin SecurLogon

При миграции на Linux все сталкиваются с серьёзной проблемой – отсутствием полноценной поддержки PKI Enterprise-класса и двухфакторной аутентификации (аналога Windows Smart Card Logon)

### Aladdin SecurLogon обеспечивает

- полноценную поддержку PKI, двух- и трёхфакторную **строгую аутентификацию** пользователей в ОС на базе Linux, Windows и macOS, удобную работу в смешанных гетерогенных средах
- работу с доменами Microsoft AD, FreeIPA, Samba DC, ALD, Pro РЕД АДМ, Альт Домен
- усиленную аутентификацию пользователей с использованием автоматически сгенерированного сложного пароля длиной до 63 символов - для инфраструктур, где PKI ещё не развёрнута
  - Этот пароль хранится в защищённой памяти токенов JaCarta, в соответствии с установленными политиками безопасности он может автоматически меняться, например, раз в день, после каждого использования
  - После ввода правильного ПИН-кода токена SecurLogon использует этот пароль для доменной и/или локальной аутентификации на отдельно стоящих АРМах. При этом пользователь свой пароль не знает, следовательно, не сможет его скомпрометировать
- усиленную аутентификацию пользователей с использованием одноразовых паролей (OTP) или виртуального токена на мобильном устройстве
- применение политик входа на основе принадлежности пользовате к группе безопасности (только токен, токен или пароль, только пар
- аутентификацию любым из методов на отдельно стоящих АРМ или АРМ в одноранговых сетях (workgroup)
- дополнительные сервисные функции, позволяющие до входа в ОС р сменить ПИН-код пользователя, кастомизировать окно приветстви
- групповое развёртывание и удалённую настройку с рабочего места администратора
- полноценную альтернативу Microsoft Smart Card Logon на отечественных ОС на базе Linux
- защиту удалённых соединений (RDP)

***Сертификация** ФСТЭК России*

# Смарт-карт ридеры

Для работы со смарт-картами необходимы смарт-карт ридеры. "Аладдин" выпускает целую линейку ридеров семейства JCR:

- профессиональные ридеры Enterprise-класса, имеющие повышенн надёжность и ресурс, не царапающие поверхность смарт-карты:
  - в горизонтальном исполнении
    - JCR721 (для контактных карт)
    - JCR761 (с биометрическим сканером отпечатков пальцев)
  - в вертикальном исполнении
    - JCR731 (для контактных карт)
    - JCR781 (с биометрическим сканером отпечатков пальцев)
- **персональные компактные ридеры** для работы с электронными сервисами (ASE Drive)
- **OEM-модели** для встраивания в ПК и др. оборудование

***Импортозамещение:***
*любые импортные смарт-карты ридеры*

# Aladdin LiveOffice

## средство обеспечения безопасной дистанционной работы

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

### 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

### Позволяет

- в 5-7 раз экономить бюджет при организации дистанционной работы сотрудников и контрагентов
- автоматически выполнить все требования и политики безопасности
- полностью соответствовать требованиям ФСТЭК и ФСБ России по организации безопасной дистанционной работы
- использовать USB-устройство Aladdin LiveOffice как удалённое рабочее место (терминал) с предустановленным и преднастроенным ПО, функционирующим в замкнутой доверенной программно-аппаратной среде, вместо служебного ноутбука
- обеспечить централизованное управление с использованием JMS


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

# JAS

## высокопроизводительный сервер аутентификации Enterprise-класса

### Обеспечивает

- 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.
- усиленную и строгую аутентификацию пользователей
  - в инфраструктурах без использования PKI
  - в ОС на базе Linux, Windows
  - в сервисах и приложениях с использованием U2F-совместимых токенов, OTP, SMS, PUSH-уведомлений
- интеграцию с прикладным ПО на базе стандартных протоколов RADIUS, REST, WCF, ADFS, HTTP, SMPP
- высокую отказоустойчивость (Failover Cluster) и производительность – более 5,000 аутентификаций в секунду

### Позволяет

- использовать различные методы, способы, протоколы и средства аутентификации пользователей
  - практически любые имеющиеся или новые аппаратные USB-токены, OTP-токены, совместимые с RFC4226, RFC 6238, FIDO U2F
  - мобильные приложения Яндекс.Ключ, Google Authenticator, Aladdin 2FA, обеспечивающее безопасную передачу вектора инициализации, исключающую возможность повторного использования QR-кода и механизм PUSH-уведомлений
- вести мониторинг и аудит действий пользователей и администраторов с выгрузкой на сервер Syslog для интеграции с SIEM
- обеспечить учёт и централизованное управление жизненным циклом используемых средств (интегрирован с системой управления JMS)

***Импортозамещение:*** *любой аналогичный продукт*
***Сертификат:*** *ФСТЭК России*
***В Реестре отечественного ПО***

# Secret Disk

## защита данных на дисках

### Обеспечивает

- предотвращение утечки и несанкционированного доступа к ценной информации при утере, краже, изъятии, ремонте, неправильной утилизации компьютеров, серверов, дисков
- прозрачное шифрование данных
  - на ноутбуках, ПК, планшетах[1] 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)

### Позволяет

- шифровать
  - системный раздел[2], 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
- использовать для доступа к защищённой информации двухфакторную аутентификацию (в т.ч. до загрузки ОС)
- предоставлять доступ к зашифрованным данным другим пользователям
- защищать данные в резервных копиях, создаваемых с помощью сторонних приложений

### Версии Secret Disk

- **персональная** (единая лицензия для Linux и Windows)
- **серверная**
- **корпоративная** (Enterprise-версия) с централизованным управлением

***Импортозамещение:*** *Microsoft BitLocker, CheckPoint Endpoint Security и др.*

***Сертификаты:*** *ФСБ, ФСТЭК России, Минобороны*

***В Реестре отечественного ПО***

1. – Работающих под Windows, Linux
2. – Только для Windows



# Крипто БД

## защита баз данных, обезличивание персональных данных

### 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 персональных данных
- прозрачное селективное (выборочное) шифрование критически важных данных в СУБД с использование российских алгоритмов
- двухфакторную аутентификацию пользователей при доступе к данным в СУБД
- централизованное управление 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 (для систем, использующих банковские карты), информационных систем организаций КИИ
  - по моделям разделения доступа – дискретной и мандатной

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

### 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)
- вести мониторинг и аудит действий пользователей и администраторов с выгрузкой на сервер Syslog для интеграции с SIEM
- создавать защищённые информационные системы (ИС) с использованием сертифицированного СКЗИ
- получить некорректируемую юридически значимую доказательную базу для проведения расследований инцидентов информационной безопасности

- Существенно снизить риски утечки персональных данных и избежать административной, уголовной ответственности, оборотных штрафов

***Импортозамещение:*** *Встроенные в импортные СУБД зарубежные средства защиты на российские*

***Сертификаты:*** *ФСБ России до класса КС-3*

***В Реестре отечественного ПО***

# JaCarta SF/ГОСТ

## защищённый служебный флеш-накопитель для контролируемого переноса и отчуждения информации

### Обеспечивает

- безопасное хранение и перенос данных в зашифрованном виде
- 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)
- сокрытие наличия ценной информации на служебном флеш-накопителе
- возможность использования
  - в качестве средства идентификации и аутентификации пользователей в АПМДЗ (Соболь, Dallas Lock), в других СЗИ
  - в качестве средства ЭП (усиленной квалифицированной) с неизвлекаемым закрытым ключом в системах электронного документооборота (ЭДО)

### Позволяет

- обрабатывать и защищать служебную тайну, информацию ограниченного распространения (ДСП), гостайну со степенью секретности "Совершенно секретно"
- реализовать контроль отчуждения (переноса) информации со съёмных машинных носителей и на них
- настроить политику безопасности
  - доступ к данным не смогут получить ни администраторы (ни при локальном, ни при сетевом подключении), ни системные процессы – backup, антивирус и др.
  - установить разные уровни административных полномочий для Главного администратора и Администратора, выполняющего оперативные задачи по заданным политикам и шаблонам
- вести мониторинг и аудит действий пользователей и администраторов с выгрузкой на сервер Syslog для интеграции с SIEM
- выполнить требования законодательства РФ и Регуляторов к съёмным носителям информации
  - приказов ФСТЭК России №17, 21, 25, 31, требований профилей защиты средств контроля отчуждения (переноса) информации со съёмных машинных носителей
  - Минобороны России к ЗМНИ (защищённым машинным носителям информации)
  - СТР, СТО БР ИББС, 152-ФЗ "О персональных данных", 187-ФЗ "О безопасности КИИ"

***Сертификаты**: Минобороны, ФСТЭК России для работы со служебной информацией ограниченного распространения (ДСП) и с гостайной со степенью секретности "Совершенно секретно"*
** – в процессе сертификации (новая версия JaCarta-2 SF)*

# SecurCD

## защита данных на оптических дисках

### Обеспечивает

- безопасную адресную передачу чувствительной информации на оптических дисках CD/DVD/BR в зашифрованном виде
- блокирование работы встроенных в ОС и специализированных программ чтения/записи данных на оптические диски типа Nero, UltraISO и др. для исключения возможности записи и передачи данных в открытом (незашифрованном) виде
- чтение данных только получателем при наличии закрытого ключа
- защиту данных от внешних[1] и внутренних нарушителей

### Позволяет

- обрабатывать и защищать информацию ограниченного распространения, гостайну со степенью секретности "Совершенно секретно"
- вести мониторинг и аудит действий пользователей и администраторов с выгрузкой на сервер Syslog для интеграции с SIEM
- самостоятельно генерировать ключевые пары
- обмениваться открытыми ключами с контрагентами
- хранить закрытые ключи в защищённом служебном флеш-накопителе JaCarta SF/ГОСТ и/или в защищённом на пароле файл-контейнере
- работать совместно с защищённым служебным флеш-накопителем JaCarta SF/ГОСТ как плагин, расширяющим его функциональность, так и без него

***Сертификат:** Минобороны России для работы с гостайной со степенью секретности "Совершенно секретно"*

1. – Только для конфиденциальной информации

# JaCarta FlashDiode

## однонаправленный флеш-накопитель для безопасного переноса информации в закрытый контур

### Обеспечивает

- безопасный перенос данных из открытого контура информационной системы в закрытый, где производится обработка
  - **информации ограниченного доступа** (например, ГИС, МИС, КИИ, АСУ ТП, ИСПДн)
  - **гостайны** со степенью секретности до "Совершенно Секретно"
- невозможность скрытого несанкционированного копирования и переноса информации (её утечки) из закрытого контура (реализовано архитектурно на аппаратном уровне)
- возможность записи на флеш-накопитель только аутентифицированным пользователем и только на авторизованных для этого компьютерах
- аудит действий пользователей и администраторов

### Позволяет

- отказаться от использования однократно записываемых оптических дисков (CD-R) и перейти на более удобные и привычные многократно записываемые специализированные флеш-накопители
- удешевить стоимость владения автоматизированной системы (АС)
  - не требуется утилизация носителей после использования в закрытом контуре
  - не нужны приводы для работы с оптическими дисками и соответствующие средства контроля и защиты
  - не нужны специализированные дорогостоящие однонаправленные USB-шлюзы для использования съёмных дисковых накопителей
  - упрощаются процедуры переноса информации в закрытый контур (без необходимости переаттестации АС)
  - экономится время сотрудников и администраторов
- работать в виртуальных средах (в открытом контуре)
- безопасно обновлять базы сигнатур для антивирусов, системное, прикладное и встроенное ПО ("прошивки" различных устройств), базы данных и пр.

***Сертификаты:*** *Минобороны России (для работы с гостайной со степенью секретности «Совершенно секретно»), на сертификации в ФСТЭК России*

# JMS

## корпоративная система централизованного управления

### 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)

### 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

### Включает

- высокопроизводительный сервер аутентификации Enterprise-класса — JAS (опционально)

***Импортозамещение:*** *любого импортного аналога*

***Сертификаты:*** *ФСТЭК России, Минобороны России (для работы с гостайной до "Совершенно секретно")*

***В Реестре отечественного ПО***

# 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.

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 России, 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 России, 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 и др.)
  - Выпущены учебные пособия "Аутентификация – теория и практика", «Идентификация и аутентификация в цифровом мире» и др.
  - 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, Secure Element
- Биометрическая идентификация и аутентификация по отпечаткам пальцев (Match On Card/Device)
- PKI для Linux и российских ОС, включая Центр выпуска и обслуживания сертификатов (Enterprise Certificate Authority)
- 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

Аладдин

+7 (495) 223 00 01
www.aladdin.ru
aladdin@aladdin.ru
129226, Москва, ул. Докукина, 16с1

Аладдин — ведущий российский вендор-разработчик и производитель ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры



https://t.me/aladdinrd
https://vk.com/aladdin

ККБ-BKL-20240212-v16.3-RU