

Персональный USB-токен с биометрической идентификацией пользователя по отпечаткам пальцев

- Для привилегированных пользователей, сотрудников на удалёнке, администраторов, ТОП-менеджеров
- Secure by design

НОВИНКА



JaCarta SecurBIO

Позволяет:

- Отказаться от использования паролей
- Существенно повысить уровень безопасности

Обеспечивает:

- Надёжную 2х и 3х-факторную аутентификацию пользователей
- Электронную подпись (УКЭП) для эл. документооборота
- Невозможность использования токена посторонними
- Поддержку PKI, работу с цифровыми сертификатами
- Работу с биометрией внутри защищённого устройства

Сертификат ФСБ №СФ/124-5060

Сертификат ФСТЭК - в процессе (УД-4, позже на УД-2 для гостайны)

В реестре радиоэлектронной продукции - №10598246





Назначение

SecurBIO-токен - это **новейший продукт** компании Аладдин.

Он предназначен для решения сразу нескольких важнейших проблем информационной безопасности.

> Обеспечивает

- **Усиленную и строгую многофакторную аутентификацию** пользователей в государственных и корпоративных информационных системах (ГИС, КИИ, АСУ ТП).
 - Невозможность входа в ИС от имени другого пользователя.
 - Неотказуемость от произведённых транзакций (доступ, ЭП).
- **Работу с электронной подписью** в системах эл. документооборота (ЭДО) с гарантией того, что воспользоваться таким устройством, выдавая себя за его владельца, посторонний не сможет.
- **Удобство** использования и **безопасность**.

> Гарантирует

- Однозначную идентификацию пользователя за счёт использования его уникальных биометрических характеристик - отпечатков пальцев.
- Невозможность несанкционированного использования устройства посторонними (внутренним или внешним нарушителем).
- Невозможность утечки и компрометации персональных биометрических данных.

> Соответствует

- Высочайшим требованиям безопасности, позволяющим использовать его в ИС с гостайной* до степени секретности "СС".

> Может использоваться:

- В ГИС до 1-го класса защищённости
- На предприятиях, ИТ-системы которых являются объектами КИИ
- На предприятиях ОПК и в структурах Министерства обороны РФ
- В корпоративных ИС и для обеспечения безопасности персональных данных до 1-го уровня защищённости
- Разработчиками СЗИ, СКЗИ, СЭД, ДБО, ОС и др.
- Производителями
 - Терминального оборудования (где важна надёжная 2ФА/3ФА**, нет клавиатуры и/или устройства отображения).

- Банкоматов (3ФА для сервисных инженеров).
- М2М/IIoT оборудования для КИИ, где невозможно или сложно использовать клавиатуру для ввода пароля администратора/пользователя.
- СКУД и пр.

> Рекомендуется к применению:

- При построении безопасной доверенной ИТ-инфраструктуры на базе PKI.
- При внедрении адаптивной МФА** в сегментированные ИС.
- Для обеспечения усиленной и строгой аутентификации нескольких групп привилегированных пользователей, когда важно однозначно идентифицировать их личность, прежде всего:
 - работающих дистанционно с удалённым доступом к сегментам ИС, в которых содержится и обрабатывается критически важная, конфиденциальная, служебная информация ограниченного распространения (в том числе с ограничительной пометкой ДСП).
 - администраторов, имеющих расширенные полномочия в ИС.
 - ТОП-менеджеров, VIP-пользователей ИС, имеющие расширенные права и полномочия в ИС, и являющиеся основной мишенью для злоумышленников.
- В проектах импортозамещения при миграции с MS Windows на отечественные ОС на базе Linux.

* - в планах по сертификации

** - 2х, 3х, многофакторная аутентификация





Возможности

> SecurBIO-токен имеет:

- **Встроенный** полупроводниковый емкостной сканер отпечатков пальцев
 - Это обеспечивает прямую передачу отпечатков в устройство, не допуская их попадания в компьютер или в ИС организации.
- **Встроенные алгоритмы** обработки биометрических данных - Match-On-Device
 - Все математические преобразования отпечатков пальцев в цифровые шаблоны, хранение, сравнение выполняются внутри устройства в его защищенной памяти и никогда не попадают наружу.
 - Алгоритмы преобразования и распознавания отпечатков пальцев - классические, а не новомодные нейросети (ИИ), обученные на неизвестных наборах данных во внешней среде.
- **Набор криптографических алгоритмов** с неизвлекаемым закрытым ключом, реализованных аппаратно
 - Для строгой 2ФА/3ФА.
 - Для ЭП (УКЭП).
- **Полную совместимость** с обычными USB-токенами JaCarta-2/3 PKI/ГОСТ
 - До верификации пользователя токен в системе не виден (не подключен), что резко снижает шансы на успешные атаки.
 - После успешной верификации пользователя (сравнения 1:1 предъявленного отпечатка пальца с хранимым в защищенной памяти устройства эталоном - цифровым шаблоном) SecurBIO-токен превращается в обычный USB-токен и полностью совместим с ним.
 - Вердикт "свой-чужой" от биометрической подсистемы не передается в ИС, а используется внутри устройства для его разблокирования (эквивалентного физическому подключению USB-токена к USB-порту) и передачи управления на подсистему аутентификации и ЭП.

> SecurBIO-токен позволяет:

- Использовать **трёхфакторную аутентификацию** (3ФА) пользователей:
 - Фактор **биометрии** (отпечатки пальцев владельца устройства)

- Фактор **владения** (физическим устройством)
- Фактор **знания** (ПИН-код устройства). Фактор биометрии позволяет "привязать" устройство к человеку и быть уверенным в том, что
 - Доступ в ИС получает именно тот, кто владеет таким SecurBIO-токеном
 - Что транзакцию (вход в систему, подпись документа) осуществляет именно его владелец.
- **Отказаться от запоминаемого пароля** и использовать 2 фактора - биометрию и владение (2ФА).
- Использовать **ЭП как действительно собственноручную подпись**, с подтверждением волеизъявления конкретной личности, что существенно снижает риски мошенничества.
- **Работать без установки дополнительных драйверов** в ОС Windows, Linux (вкл. все российские ОС), macOS. 

При использовании SecurBIO-токена **владелец ИС не становится оператором персональных биометрических данных**, т.к. биометрические данные (отпечатки пальцев) не передаются в ИС, не хранятся и не обрабатываются в ИС.

Основные отличия от конкурирующих решений

Прямых аналогов SecurBIO-токену для корпоративного рынка PKI и ЭП пока нет. В основном производятся USB-токены с встроенным сканером отпечатков пальцев по стандарту FIDO Alliance и для Windows Hello:

- Нет роли Администратор
 - Пользователь сам регистрирует отпечатки пальцев, может добавлять, менять, удалять их.
- Для работы нужен сканер отпечатков пальцев, напрямую подключающийся к компьютеру
 - Снятые им отпечатки пальцев хранятся и обрабатываются в ОС на компьютере (возможна компрометация и утечка), при этом владелец ИС по российскому законодательству становится оператором персональных биометрических данных, со всеми вытекающими отсюда проблемами.

Имеющиеся на рынке аналоги не предназначены для использования в корпоративных ИС и в ГИС.



Основные преимущества

> Удобный дизайн и конструкция

- Оптимальный размер
 - Не больше брелка от машины
 - Не потеряется ни в сумке, ни в кармане.
- Легко подключается к любому компьютеру
 - Тип USB-разъёма в компьютере теперь не проблема, к нему устройство подключается гибким кабелем с разъёмами Type-C, Type-A, MicroUSB или MiniUSB.
- Имеет понятную индикацию
 - Световую
 - Вибро-отклик, говорящий о том, что уже можно убирать палец со сканера.
- Допускает сохранение до 10-ти цифровых шаблонов отпечатков пальцев.
- Автоматически повернёт и скорректирует изображение (отпечаток) пальца, приложенного к сканеру под углом
- Легко закрепляется на мониторе или в удобном месте на столе при постоянной работе в своём кабинете или дома.
- Имеет строгий дизайн, матовый корпус чёрного цвета.
 - Возможна дополнительная кастомизация в корпоративных цветах, нанесение логотипа (на заказ).

> Усиленная защита от статике

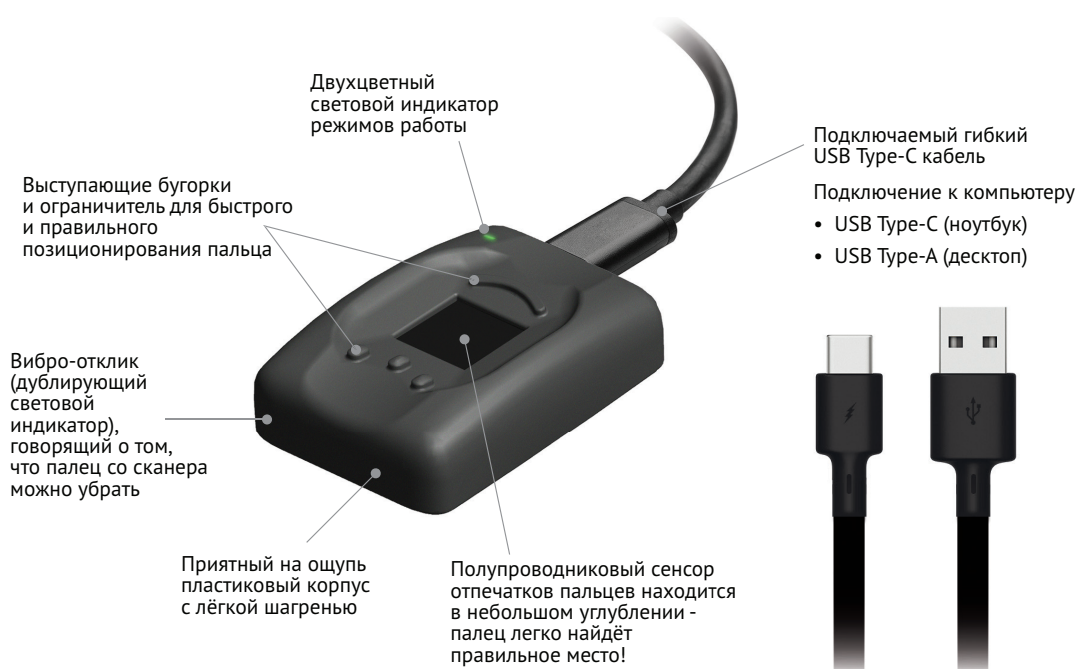
SecurBIO-токен имеет усиленную защиту от статике и для сканера, и для подключения по USB.

> Secure by design

При проектировании устройства во главу угла ставилась безопасность и невозможность компрометации персональных биометрических данных.

Для надёжной аутентификации и ЭП в устройстве на аппаратном уровне реализован набор криптографических алгоритмов с неизвлекаемым закрытым ключом.

- Для строгой 2ФА/3ФА рекомендуется использовать современный алгоритм ECDSA с длиной ключа 384 бита (заявленная стойкость $4 \cdot 10^{45}$), более быстрый и надёжный, чем RSA.
- Для ЭП (УКЭП) рекомендуется использовать российский криптографический алгоритм ГОСТ Р 34.10-2012 с длинами ключей 256 или 512 бит.



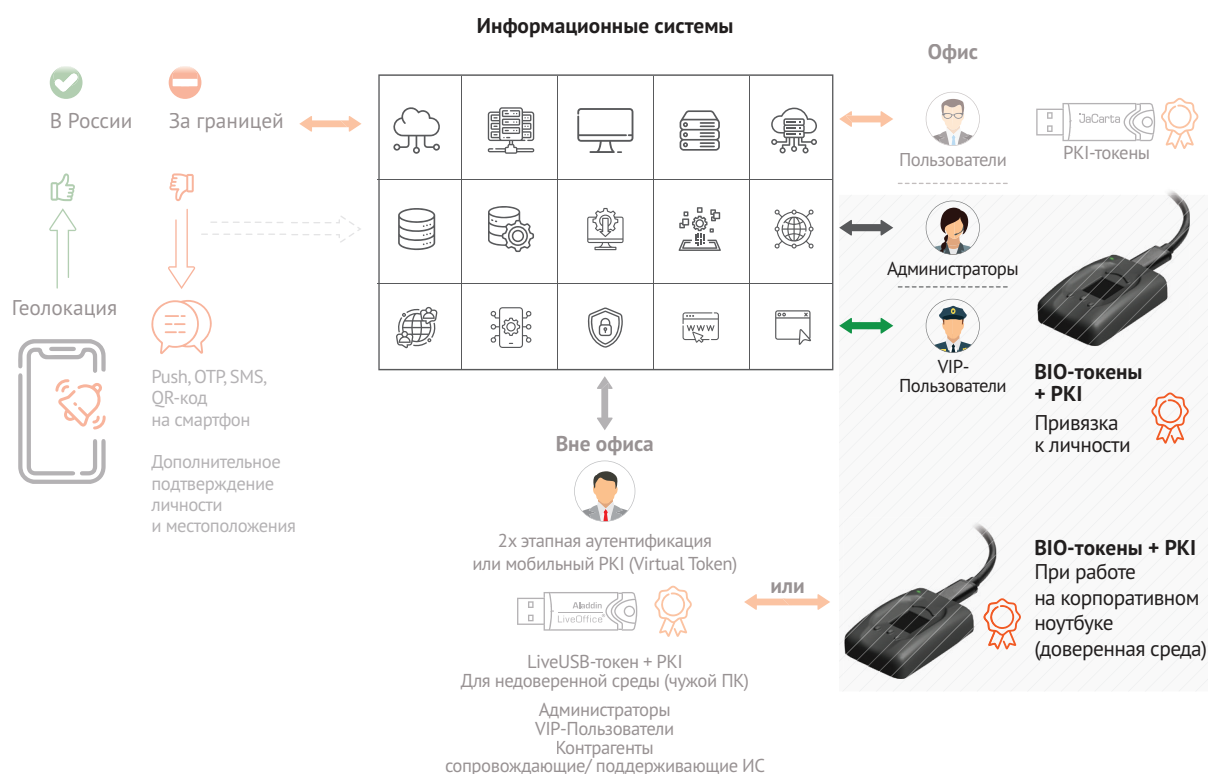


Адаптивная МФА

Для разных сред функционирования, условий работы, сегментов ИС должен быть определён разный набор факторов и дополнительных атрибутов (способов) для подтверждения идентификационных данных и их связи с личностью пользователя.

Больше рисков - больше дополнительных атрибутов и компенсационных мер.

Пример использования SecurBIO-токенов для адаптивной аутентификации.



Какое ПО необходимо/рекомендовано для работы

- **Aladdin SecurLogon** - для локальной и доменной аутентификации пользователей в ОС и службы каталогов Linux.
 - **Единая библиотека jсPKCS11-2** версии 2.11 или выше (реализует PKCS #11 v2.40).
 - **СКЗИ JaCarta-3**.
- > Для администраторов
- **Единый клиент JaCarta** - для администрирования токена и регистрации отпечатков пальцев (Windows, Linux).
 - **АРМ Администратора безопасности JaCarta** - для администрирования СКЗИ.
 - **Утилита импорта** содержимого PFX контейнеров, ключей ЭП и сертификатов ключей проверки ЭП.
 - **Aladdin Enterprise CA** - корпоративный Центр Сертификации для выпуска и обслуживания цифровых сертификатов для аутентификации пользователей.
 - **JMS (JaCarta Management System)** - корпоративная система централизованного управления жизненным циклом токенов, сертификатов, СЗИ и СКЗИ.



Техническая спецификация

Габаритные размеры (Д × Ш × В)	39.0×28.5×10.0 мм
Вес	10 г (без USB кабеля)
USB-интерфейс	• USB 2.0 Full-speed (12 Мбит/с), совместим с USB 1.1, 2.0, 3.0, 3.1 • Разъём USB на устройстве - USB Type-C
Потребляемый ток (при напряжении питания 5В ±0.25В)	не более 300 мА
Сенсор отпечатков пальцев	Активная емкостная КМОП-матрица • Разрешение - 508 dpi (точек на дюйм) • Размеры - 160 × 160 пикселей • Размеры активной области - 8 × 8 мм
Световые индикаторы работы	Зелёный - отображает готовность и работу устройства по шине USB Красный - отображает работу биометрической подсистемы
Тактильный индикатор	Виброотклик - возникает при положительном результате биометрической верификации - уведомление пользователю, что можно убирать палец со сканера, сканирование закончено
Готовность к работе после подключения питания и калибровки сканера	1,5 сек.
Среднее время сканирования пальца и создания шаблона (производится 1 раз при регистрации)	4,0 сек.
Среднее время сканирования пальца и проверки отпечатка	3,5 сек.
Среднее (типичное) время, затрачиваемое администратором на одного пользователя при регистрации 3х пальцев	0,5 минуты
Уникальный серийный номер	8 символов в формате HEX, лазерная гравировка, стойкая к истиранию
Реализованные криптографические алгоритмы	• Для PKI - RSA с длинами ключей 512, 768, 1024, 1280, 1536, 1984, 2048, 3072, 4096 бит - ECDSA с длинами ключей 112, 128, 160, 192, 224, 256, 384, 521 бит - DES с длиной ключа 56 бит - Triple-DES с длинами ключей 112, 168 бит - AES с длинами ключей 128, 192, 256 бит • Для ЭП (УКЭП), хэширования и шифрования данных - ГОСТ Р 34.10–2012, ГОСТ 34.10–2018 с длинами ключей подписи 256, 512 бит, с длинами ключей проверки подписи 512, 1024 бит - ГОСТ Р 34.11–2012 с длинами хэш-кода 256, 512 бит - ГОСТ 34.11–2018 с длинами хэш-кода 256, 512 бит - ГОСТ Р 34.12–2015 ("Магма", "Кузнечик"), ГОСТ 34.12–2018 - ГОСТ Р 34.11–2012, ГОСТ 34.11–2018 с длинами сообщений 256, 512 бит - ГОСТ Р 34.10–2012 - Р 50.1.115–2016 (RFC 8133/SESPAKE)
Программные интерфейсы	• PKCS #11 v2.40, совместим с российским профилем TC 26.2.001-2016 (Единая библиотека jсPKCS11-2) • APDU-команды (низкоуровневый интерфейс)
Климатическое исполнение	УХЛ4, группа 1.1 (для установки и работы в отапливаемых помещениях) • Соответствует требованиям ГОСТ РВ 20.39.304-98 (Аппаратура, приборы, устройства и оборудование военного назначения. Требования стойкости к внешним воздействующим факторам)
Нормальные (рекомендуемые) условия эксплуатации	• Температура: 20 ± 5 °С • Относительная влажность воздуха: 60 ± 15% • Атмосферное давление: от 84 до 107 кПа (630–800 мм рт. ст.)
Пыле- и влагозащищённость	IP33 (не рекомендуется использование устройства в пыльных и сырых помещениях с повышенной влажностью)
Электромагнитная безопасность	• Устройство не создает помех средствам вычислительной техники, а также устойчиво к различным помехам: - радиочастотным (диапазон частот от 80 до 1000 МГц) - электростатическому разряду (8 кВ для контактного разряда и 15 кВ для воздушного) - магнитному полю промышленной частоты (диапазон частот от 50 до 60 Гц).
Рекомендуемый срок полезного использования	3 года
Срок службы	5 лет
Время непрерывной работы	24 × 7 × 365
Сертификаты безопасности	ФСБ России - №СФ/124-5060 / ФСТЭК России - в процессе
Регистрационная запись в реестре радиоэлектронной продукции (ЕРРРП) по ПП-719	№10598245 (базовое исполнение) / №10598244 - 10598248 (различные варианты исполнений)
Сертификат СТ-1 (подтверждение российского производства)	№4043000044 (разработано и производится в России)
Возможность поставки в рамках госзакупок и гособоронзаказа по ПП-1875	Да



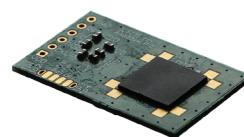
Модельный ряд

> Персональный SecurBIO-токен

- **JaCarta SecurBIO PKI** - для PKI-проектов
- **JaCarta SecurBIO ЭП** - для систем электронного документооборота с использованием ЭП (УКЭП).

> OEM-модуль JaCarta SecurBIO для встраивания в оборудование

SecurBIO-токен может поставляться в бескорпусном исполнении для встраивания в различное терминальное, бортовое оборудование, СКУД и пр.



Другие продукты с поддержкой биометрии

> Смарт-карт ридеры с поддержкой биометрии

Aladdin SecurBIO Reader - семейство профессиональных смарт-карт ридеров Enterprise-класса с встроенным прижимным полупроводниковым сканером отпечатков пальцев.

- **JCR761** - смарт-карт ридер с горизонтальной загрузкой смарт-карты
- **JCR781** - смарт-карт ридер с вертикальной загрузкой смарт-карты.

Рекомендуется

- Для организации сменной работы пользователей за одним рабочим местом
- Для использования одной смарт-карты (с RFID) для доступа на объект/в помещения, для интеграции с СКУД.



> Смарт-карты с поддержкой биометрии

- **JaCarta PKI/SC** - смарт-карта с поддержкой PKI и BIO
- **JaCarta-2 PKI/ГОСТ/SC** - смарт-карта с поддержкой PKI, ЭП и BIO.



О компании

Аладдин – ведущий российский вендор – разработчик и производитель

- ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры предприятий и защиты её главных информационных активов
- средств аутентификации и электронной подписи для обеспечения информационной безопасности и защиты данных.

Компания работает на рынке с апреля 1995 г.

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”.

Компания получила статус системно-значимых компаний-разработчиков и поставщиков средств ИБ, деятельность компании приравнена к предприятиям ОПК, выпускающих продукцию оборонного назначения.

Продукты компании по направлениям

- Информационная безопасность, корпоративный PKI
- Многофакторная аутентификация, обеспечение безопасного доступа к информационным ресурсам предприятия
- Средства обеспечения безопасной дистанционной работы пользователей при использовании ими недоверенных средств вычислительной техники (например, личных)
- Средства электронной подписи
- Защита данных (на дисках, съёмных носителях, в базах данных)
- Доверенная загрузка.

+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

© 1995-2025, АО "Аладдин Р.Д." Все права защищены.



<https://t.me/aladdinrd>
<https://vk.com/aladdinrd>