Аладдин

Средство обеспечения безопасной дистанционной работы из недоверенной среды

Aladdin LiveOffice

- Безопасная дистанционная работа из недоверенной среды (личные компьютеры, компьютеры подрядчиков)
- Двухфакторная аутентификация пользователя (2ФА) и электронная подпись (УКЭП, УНЭП)
- Загрузка встроенной доверенной ОС с USB-устройства: работа без установки ПО на компьютер пользователя
- Соответствие требованиям 32-го и 117-го Приказов ФСТЭК России
- Включён в реестры Минцифры и Минпромторга
- Сертифицирован ФСТЭК России

Электронная версия буклета

ДИСТАНЦИОННАЯ РАБОТА

Что важно знать

Дистанционная работа стала неотъемлемой частью деятельности многих организаций. Однако удалённый доступ к информационным системам (ИС) с личных или неконтролируемых компьютеров создаёт серьёзные риски:

- компьютеры пользователей могут быть заражены вредоносным ПО, содержать трояны или программы удалённого доступа;
- отсутствие централизованного администрирования таких устройств делает их уязвимым звеном;
- внутренние нарушения (намеренные или случайные) могут привести к утечке данных или заражению ИС.

Из-за использования небезопасно организованной удалёнки получили:

- массовый рост успешных атак на ИС;
- кражу чувствительной информации и персональных данных;
- блокирование работы сервисов, нарушение бизнес-процессов, разрушение ИТ-инфраструктуры (многие громкие инциденты до сих пор на слуху).

Каждая третья успешная атака совершается через подрядные организации — "слабое звено" в цепочке поставок (Supply Chain) — вендоров, интеграторов, аутсорсеров или разработчиков ПО, которые имеют удалённый доступ в сеть жертвы.

Основные причины успешных атак:

- небезопасно организованный удалённый доступ;
- недоверенная среда функционирования, из которой осуществлялся доступ в ИС организации.

Нормативные требования

К обеспечению безопасности дистанционной работы предъявляются специальные требования:

- Требования о защите информации в государственных информационных системах, иных ИС государственных органов и учреждений (117-й Приказ ФСТЭК России).
  Требования Приказа автоматически транслируются на все организации КИИ, ИСПДн и на их подрядчиков.
- Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах (Методический документ ФСТЭК России, утв. 12.04.2026).
- Требования о защите информации в государственных и иных информационных системах с использованием шифровальных (криптографических) средств (117-й Приказ ФСБ России).
- Требования по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах (32-й Приказ ФСТЭК России).
  При использовании сертифицированных средств, соответствующих данным требованиям, допускается работа из недоверенной среды.

Что понимается под недоверенной средой функционирования?

Это компьютеры, которые:

- Не администрируются владельцем ИС.
- Не входят в состав аттестованной ИС.
- Могут содержать в своём составе вирусы, специализированные трояны, предоставляющие удалённый доступ злоумышленникам.

К ним относятся:

- **Личные** компьютеры.
- Компьютеры подрядчиков.
- Компьютеры сотрудников **без комплекса средств защиты** для обеспечения безопасной дистанционной работы.

Важно: *Набор различных сертифицированных средств защиты (СДЗ, МСЭ, антивирус, VPN и пр.) не гарантирует безопасность дистанционной работы. Безопасность дистанционной работы обеспечивается применением специализированного сертифицированного средства.*

Сравнение подходов к организации безопасной удалённой работы

Проблема небезопасной удалённой работы заключается в том, что традиционные методы (VPN, антивирусы, двухфакторная аутентификация на уровне приложений) не обеспечивают защиту от главных рисков: работа из недоверенной среды, отсутствие контроля над конечным устройством, возможность утечки данных и заражения ИС. В таблице ниже показано, как различные подходы справляются с ключевыми угрозами.

Угроза/Проблема	VPN + Антивирус + 2ФА [1]	Служебные ноутбуки с СЗИ	Aladdin LiveOffice
Защита от внутреннего нарушителя	Нет, сотрудник может скомпрометировать учётные данные	Частично, но физический доступ к ноутбуку есть	Устройство привязано к ПК, 2ФА, невозможность копирования
Защита от вредоносного ПО на клиенте	Антивирус не гарантирует защиту, трояны могут перехватывать данные	Контролируемая среда	Полная изоляция, загрузка с USB
Отсутствие следов работы на клиенте	Остаются кэши, файлы, история	Данные остаются на диске	Полное отсутствие следов
Предотвращение утечки данных (копирование, печать)	Нет, пользователь может сохранять и пересылать	Частично, требует дополнительных DLP-решений	Полный запрет, данные не покидают периметр
Работа с личного (недоверенного) ПК	Недопустимо (риск заражения, нет контроля)	Требуется выдача ноутбука	Да, безопасно
Сертификация ФСТЭК/ФСБ	Нет (как комплекс)	Только отдельные компоненты	Да, устройство сертифицировано целиком
Соответствие 117-му приказу ФСТЭК	Частично	Требуется дооснащение	Полное соответствие
Стоимость на одного сотрудника	Средняя (лицензии на ПО)	Высокая (ноутбук + ПО + обновления)	Низкая (USB-устройство)
Эксплуатационные расходы (поддержка, обновление, замена)	Средние (инциденты, вирусы)	Средние (ремонт, перепрошивка)	Низкие (обновление прошивки требуется крайне редко)

[1] *Набор отдельных средств*

Вывод: *только Aladdin LiveOffice комплексно решает проблему безопасной удалённой работы, позволяя использовать любые компьютеры без риска для ИС организации, при этом полностью соответствуя регуляторным требованиям и экономя бюджет.*

Как работает Aladdin LiveOffice

Aladdin LiveOffice — это специализированное средство для обеспечения безопасной дистанционной работы, сертифицированное ФСТЭК России.

Единственный в своём классе программно-аппаратный комплекс, который в одном USB-устройстве объединяет:

- Сертифицированное средство безопасной дистанционной работы (32-й приказ ФСТЭК России).
- Аппаратный токен с российской криптографией для 2ФА и ЭП.
- Защищённую операционную среду, загружаемую без установки на любой x86-ПК.
- Встроенное шифрованное хранилище для офлайн-работы.

USB-устройство представляет собой:

- Защищённый флеш-накопитель с несколькими разделами — открытыми и закрытыми, с аппаратным шифрованием служебных данных и для локальной работы с документами.
- Встроенный модуль безопасности (Secure Element), обеспечивающий:
  - аутентификацию пользователя (владельца устройства) до загрузки ОС;
  - аутентификацию и авторизацию используемого компьютера (для предотвращения использования устройства на других, не разрешённых компьютерах);
  - доверенную загрузку встроенной защищённой embedded OS на базе сертифицированной Linux (замкнутая доверенная среда функционирования);
  - аутентификацию (2ФА) пользователя при удалённом подключении;
  - электронную подпись (УКЭП, УНЭП);
  - безопасное обновление ОС и установленных приложений;
  - журналирование событий и инцидентов безопасности с возможностью их выгрузки во внешние системы (JMS, SIEM).

После загрузки с USB-устройства встроенной ОС автоматически устанавливается защищённое сетевое соединение (VPN), происходит 2ФА и подключение к рабочему столу пользовательского компьютера с доступом во все разрешённые сегменты ИС, с выходом в Интернет (с использованием средств защиты организации и при условии, что доступ разрешён).

Важно: *все процессы обработки данных происходят внутри контролируемого периметра организации. Данные не передаются на клиентское устройство — пользователь видит лишь отрисованные "картинки" экрана, а система получает только сведения о нажатиях клавиш и движениях мыши. Никаких следов работы (файлов, кэша, истории) на компьютере пользователя не остаётся.*

Aladdin LiveOffice предотвращает

- Использование устройства на неавторизованном компьютере
- Копирование информации на другие диски или устройства хранения
- Печать служебной информации на локальные или сетевые принтеры
- Загрузку файлов с внешних носителей или из Интернета
- Прямой выход в Интернет (только через защищённый шлюз организации)
- Доступ к данным при утере или краже устройства (привязка к авторизованному компьютеру и двухфакторная защита)

Позволяет

- Использовать USB-устройство вместо служебного ноутбука.
- Более чем на порядок сэкономить бюджет на приобретение или обновление устаревшего парка компьютеров.
- Полностью выполнить требования 117-го Приказа ФСТЭК России по обеспечению безопасной дистанционной работы:
  - собственных сотрудников;
  - сотрудников подрядных организаций.
- Работать в смешанном режиме:
  - офис/удалённо (дом, дача, командировка);
  - офлайн/онлайн.
- Сохранять конфиденциальные документы и результаты работы на встроенном защищённом флеш-накопителе.
- Использовать USB-устройство:
  - как обычный USB-токен для 2ФА при входе в компьютер, в сеть, на портал, в ИС;
  - как средство ЭП в системах юридически значимого документооборота (в системах ДБО, сдачи эл. отчётности, эл. торгов и пр.).
- Использовать личный или чужой компьютер для работы, при этом:
  - на него ничего не устанавливается;
  - перенастройка не требуется;
  - следов работы (и документов) не остаётся.
- Сохранить все привычки и навыки работы пользователей:
  - работа производится в привычной среде — все процессы происходят на их физических или виртуальных рабочих местах;
  - все документы находятся на своих привычных местах — всё как при работе в офисе.
- Быстро встроиться в существующую инфраструктуру с минимальными изменениями:
  - использовать существующие VPN-шлюзы и имеющиеся лицензии;
  - подключиться к развёрнутой инфраструктуре VDI или к служебным компьютерам пользователей по RDP-протоколу.
- Самостоятельно конфигурировать, добавлять, менять функциональность устройства, устанавливая "на борт" нужные приложения, например:
  - VPN для зарубежных отделений и филиалов;
  - 1С-приложения для дистанционной работы бухгалтеров, HR-службы и пр.;
  - обеспечить безопасное дистанционное администрирование устройств;
  - централизованно управлять жизненным циклом устройств и цифровыми сертификатами для доступа в ИС и ЭП.

Обеспечивает

- Полноценную дистанционную работу с любого недоверенного компьютера, например, с личного компьютера сотрудника:
  - в ГИС, КИИ, АСУ ТП, МИС, ИБС и др. до 1-го класса защищённости;
  - в ИСПДн до 1-го уровня защищённости персональных данных;
  - возможность обработки персональных данных, коммерческой, служебной тайны (ДСП):
  - 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 свою учётную запись, пароль, параметры удалённого подключения;
  - загрузить в ИС троян или вирус-шифровальщик.
- Возможность оперативного подключения к ИС с любого доступного компьютера для привилегированных пользователей:
  - руководства организации;
  - администраторов.

Выполнение требований ФСТЭК России

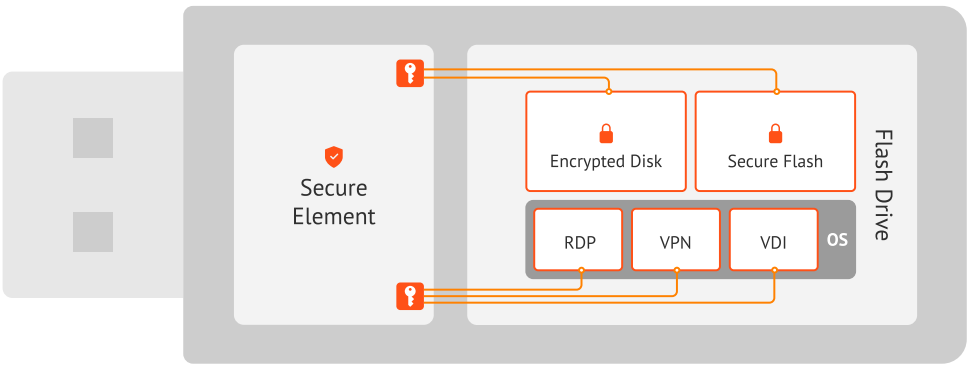
Область требований 117-го Приказа	Что требует ФСТЭК России	Что даёт Aladdin LiveOffice (ALO)	Как помогает выполнить Приказ
Идентификация и аутентификация	Усиленная/строгая аутентификация пользователей ГИС/ИС, отказ от паролей, особенно при удалённом доступе	Сертифицированное средство с функциями идентификации и аутентификации, поддерживающее работу с аппаратными токенами/ сертификатами в рамках корпоративного PKI	Реализует строгую аутентификацию по сертификатам и аппаратным ключам, снижает риски компрометации паролей и выполняет требования к уровню доверия аутентификации пользователей ГИС/ИС
Управление доступом	Реализация технического разграничения доступа, учёт ролей, прав, среды доступа (внутренний/удалённый пользователь)	Механизмы управления доступом к системам и ресурсам через политики ALO, в том числе в зависимости от типа пользователя и сценария удалённого доступа	Позволяет настроить, какие пользователи, с каких устройств и к каким ресурсам допускаются, что помогает выполнить требования по разграничению прав и контролю удалённого доступа
Регистрация событий безопасности и мониторинг	Регистрация событий, журналирование аутентификации, доступа, административных операций; использование логов для оценки КЗИ и расследования инцидентов	Встроенные функции регистрации событий безопасности; журналы, интегрируемые с SIEM/ мониторингом	Обеспечивает необходимый объём событий для мониторинга и оценки показателя КЗИ, а также доказательную базу при проверках и инцидентах в ГИС/ИС
Безопасный удалённый доступ	Использование сертифицированных средств для удалённого доступа из недоверенной среды, защита канала связи СКЗИ, приравнивание удалённого пользователя к внутреннему	Средство безопасной дистанционной работы, сертифицированное ФСТЭК России; обеспечивает защищённый доступ пользователей к системам и приложениям.	Даёт техническую платформу для удалённого доступа в соответствии с требованиями 117-го Приказа ФСТЭК России: защищённый канал, контроль среды, строгая аутентификация и регистрация действий пользователей.
Строгая аутентификация и SSO в корпоративной среде	Требование поддержки строгой аутентификации по сертификатам и единого входа (SSO) во все приложения, а не только в ОС	Встраивается в экосистему Aladdin (PKI, JaCarta, SecurLogon, JC-WebClient), обеспечивая сквозной сценарий "токен + сертификат → доступ в домен и приложения".	Позволяет обеспечить единый, контролируемый механизм аутентификации и SSO, соответствующий уровню доверия и требованиям ФСТЭК России к защите доступа к ГИС/ИС и прикладным системам.
Уровень доверия к средствам защиты	Использование сертифицированных средств защиты с заданным уровнем доверия для ГИС/ИС соответствующих классов	Сертификат ФСТЭК России по 4-му уровню доверия для ALO как ПО со встроенной СЗИ НСД.	Делает ALO формально допустимым для применения в составе системы защиты по 117-му Приказу ФСТЭК России, позволяя закрывать ряд технических мер по идентификации, доступу и регистрации событий.

Состав демо-комплекта

В состав демонстрационного комплекта Aladdin LiveOffice входят:

- Специализированные USB-устройства (2 шт.) с предустановленным программным обеспечением
- Эксплуатационная документация

Архитектурные особенности



Техническая спецификация

Критерий	Характеристики
Сертификация	Сертификат ФСТЭК России №4355 Сертификаты ФСБ России №СФ/124-4641, СФ/124-5060 (на СКЗИ в составе продукта)
В Реестре ПАКов (Минцифры)	№20648
В Реестре отечественного ПО	№4300, 4301
В Реестре радиоэлектронной промышленности Минпромторга (ПП-878, ПП-719)	№10495358, 10495359, 10495360
Возможность поставки в рамках госзакупок и ОЗ (по ПП-1875, 44-ФЗ, 223-ФЗ, ПП-325)	Да
Выполнение требований 117-го и 32-го Приказов ФСТЭК России	п.30а, б, в, г, д, з, и, 34д, е, з, к, 37, 40, 41, 42, 46, 48, 49, 51, 58, 63а, б, в, и, к, 70, 71 - удалённый доступ из недоверенной среды, защита конечных устройств, работа с ДСП, строгая/усиленная аутентификация пользователей в соответствие с требованиями ГОСТ Р 58833-2020, ГОСТ Р 70262.1-2022, ГОСТ Р 70262.2-2025, защита канала передачи данных.
Выполняет требования ФСБ к СКЗИ	Соответствует требованиям ▸ 63-ФЗ и Приказа ФСБ России № 796 к средствам ЭП. ▸ 117-го Приказа ФСБ России - п.1, 3, 6 (Шифрование данных на носителях вне контролируемой зоны, защита канала передачи данных с помощью сертифицированного СКЗИ).
Поддерживаемые аппаратные платформы	На базе x86 (Intel, AMD) с возможностью загрузки системы с внешнего USB-накопителя ▸ Установленная на компьютере ОС не важна.
Поддерживаемые криптографические алгоритмы	Строгая аутентификация и поддержка PKI реализованы аппаратно с использованием зарубежных криптографических алгоритмов: ▸ RSA: аппаратная генерация ключей длиной 1024, 2048, 4096 бит. ▸ AES: длины ключей 128, 192, 256 бит. ▸ DES: длина ключа 56 бит. ▸ 3DES: длины ключей 112 и 168 бит. ▸ SHA-1, SHA-224, SHA-256, SHA-384, SHA-512: вычисление значения хеш-функции. ▸ криптография на эллиптических кривых ECC (ECDSA, ECDH). ЭП реализована аппаратно с использованием российских криптографических алгоритмов: ▸ ГОСТ Р 34.10-2012/ГОСТ 34.10-2018 (256 и 512 бит): генерация ключевых пар, формирование и проверка электронной подписи. ▸ ГОСТ Р 34.11-2012/ГОСТ 34.11-2018 (256 и 512 бит): вычисление значения хеш-функции. ▸ ГОСТ Р 34.12-2015/ГОСТ 34.12-2018, ГОСТ Р 34.13-2015/ГОСТ 34.13-2018 (Магма, Кузнечик): генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ).
Поддерживаемые ОС на компьютерах, к которым осуществляется подключение	▸ Microsoft Windows 7 и выше. ▸ Семейство GNU/Linux, включая все актуальные российские ОС (требуется установка ПО Aladdin SecurLogon).

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. (31 год).

Многие продукты, решения и технологии компании стали лидерами в своих сегментах, во многих крупных организациях и Федеральных структурах — стандартом де-факто.

Компания имеет все необходимые лицензии ФСТЭК России, ФСБ России 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 14 национальных стандартов по идентификации и аутентификации.
  - Выпущено учебное пособие "Аутентификация — теория и практика".
  - Защищена докторская диссертация.
- Доверенная загрузка и "стерилизация" импортных ARM-процессоров с TrustZone.
- Разработка встраиваемых (embedded) Secure OS и криптографии для микроконтроллеров, 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.
- Аутентификация и электронная подпись для Secure Element (SE), USB-токенов, смарт-карт, IIoT-устройств, Web-порталов и электронных сервисов.

Аладдин

+7 (495) 223 00 01
aladdin@aladdin.ru
Москва, ул. Докукина, 16с1
www.aladdin.ru
t.me/aladdinrd
vk.com/aladdin