Обеспечение безопасной дистанционной работы сотрудников при использовании ими личных средств вычислительной техники с возможностью работы в ГИС, со служебной информацией (ДСП)

Aladdin LiveOffice

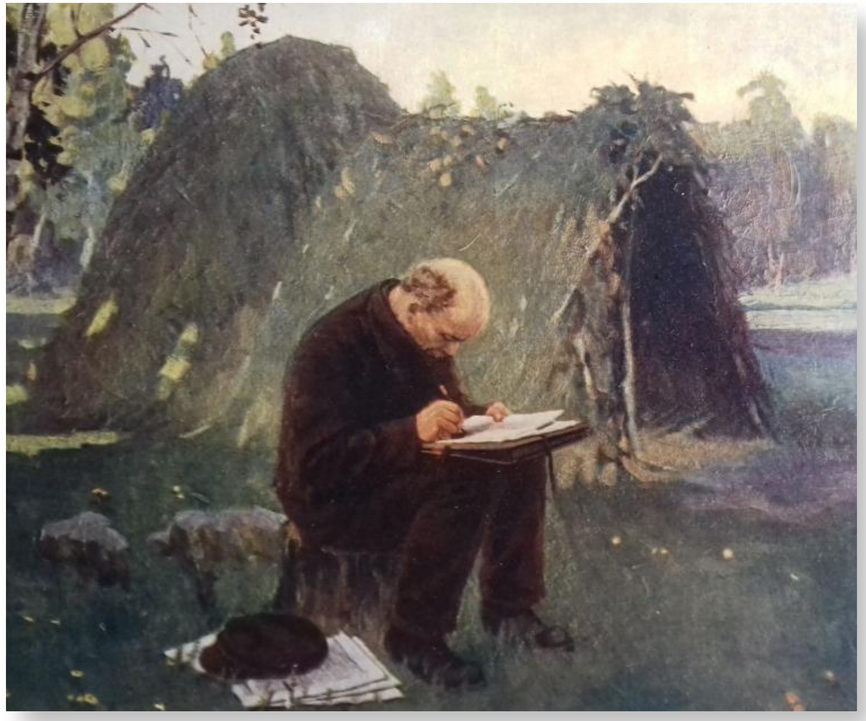
Сергей Груздев,
генеральный директор

Аладдин

Апрель 2023

Коронавирус, "удалёнка", LiveUSB

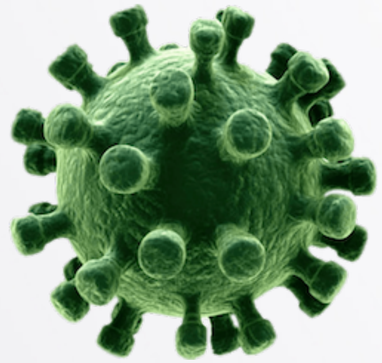
Всё это придумали не мы…



Мы попытались сделать техническое решение на базе технологии LiveUSB, обеспечивающее безопасную дистанционную работу сотрудников при использовании ими личных средств вычислительной техники

Новые вызовы

- **Коронавирус, грипп и др. -** люди болеют, есть большая потребность организовать безопасную работу сотрудников из дома, но средств на закупку второго комплекта вычислительной техники нет
- **Удалёнка -** за время пандемии к ней привыкли, для многих она стала нормой, однако проблемы с организацией действительно безопасной дистанционной работой (вне контролируемого периметра организации) остались
- **Инсайдер** (внутренний нарушитель) - после начала СВО проблема нелояльных, сочувствующих Украине и враждебно настроенных сотрудников существенно выросла, а вместе с ними - и недооценённые риски кражи чувствительной информации, несанкционированного доступа в ИС враждебно настроенных лиц с сильной мотивацией навредить



Аладдин

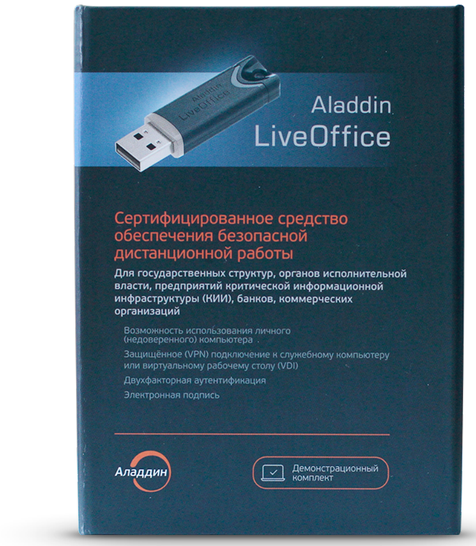
Новые требования к дистанционной работе

2021 год - легализация дистанционной работы

- **407-ФЗ**
  - Легализовал дистанционную (удалённую) работу
  - Определил обязанность работодателя **обеспечить работника** необходимым оборудованием, программно-техническими средствами и средствами защиты
    - **Служебный ноутбук** с набором средств защиты (дорого!)
    - **Специализированные средства** обеспечения дистанционной работы (дешевле в 5-10 раз)

- **Новые Требований ФСТЭК России к средствам дистанционной работы**
  - Утверждены Приказом ФСТЭК №32
  - Запланировано внесение изменений в "Меры защиты..." (Приказ №17 ФСТЭК) в части:
    - 2ФА (в соответствие с принятыми новыми ГОСТами по идентификации и аутентификации)
    - Дистанционной работы (новые требования + обязательное шифрование данных на дисках при выносе СВТ за пределы защищённого периметра организации)
- Выпущено первое сертифицированное решение для обеспечения безопасной дистанционной работы - **Aladdin LiveOffice**
  - Сертификат ФСТЭК России №4355 от 10.02.2021 г.

Aladdin LiveOffice - первое готовое сертифицированное решение



- Специализированное средство обеспечения безопасной дистанционной работы сотрудников органов исполнительной власти, государственных структур, предприятий КИИ, банков, коммерческих организаций при использовании ими личных средств вычислительной техники
- Разработано по поручению
  - Председателя Правительства РФ №ММ-П9-1861 от 16.03.2020 и зам. Председателя Правительства РФ №ДГ-П17-1987 от 18.03.2020 в целях принятия мер по распространению коронавирусной инфекции и переводу работников на дистанционный режим исполнения должностных обязанностей, обеспечивающий бесперебойное функционирование федеральных органов исполнительной власти и подведомственных организаций
  - Рабочей группы Минцифры, ФСТЭК и ФСБ России по организации удалённого рабочего места государственного служащего в рамках федерального проекта "Цифровое государственное управление" национальной программы "Цифровая экономика"
  - Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности (№3 от 26.10.2020), во исполнение ФЗ-407

✓ **Сертификат ФСТЭК России № 4355 от 10.02.2021**

Aladdin LiveOffice - что это такое

Специализированное
защищённое USB-устройство

- **Доверенная загрузка** компьютера с внешнего USB-носителя
- **Автоматическая настройка и подключение к шлюзу (VPN)**
- **RDP-соединение** со служебным СВТ или виртуальным рабочим столом (VDI)
- **Удалённый запуск и дистанционная работа с приложениями**, установленными на служебном СВТ
- *Защищённый носитель для хранения информации и переноса служебных документов*
- *Автономная работа со служебными документами*
- *Загрузка/выгрузка документов в/из ИС и/или сохранение их на защищённом разделе флеш-диска*

Полноценная **альтернатива** служебному ноутбуку с набором установленных средств защиты, обеспечивающих выполнение требований ФСТЭК России, но **сильно дешевле**

Aladdin LiveOffice - что это такое

Удаленный доступ к ИС

Средство 2ФА:
- Строгой (PKI)
- Усиленной

Средство ЭП (УКЭП)

Автономная работа со служебными документами (при плохом канале связи)

Защищённый носитель для хранения информации и переноса служебных документов

Защищённая ВКС (опция)

Защищённый обмен короткими сообщениями (опция)

Защита от фотографирования экрана / маркирование документов (опция)

Aladdin LiveOffice - где может использоваться

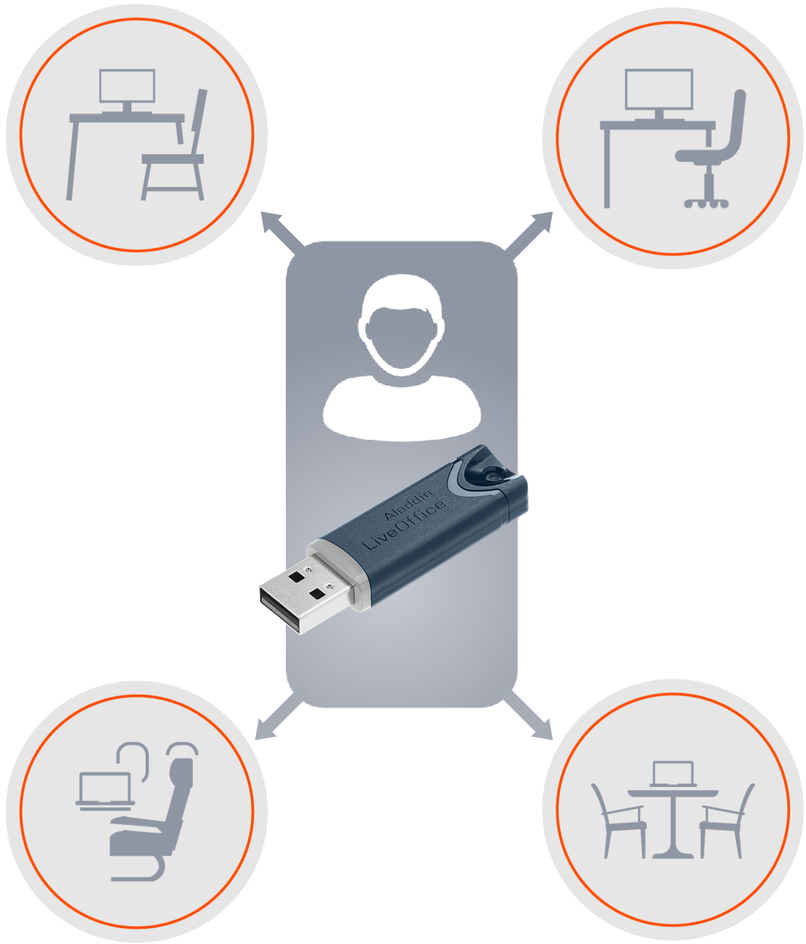
- В государственных информационных системах (ГИС) до 1-го класса защищённости включительно
- В информационных системах персональных данных (ИСПДн) до 1-й категории включительно
- В ИС значимых объектов критической информационной инфраструктуры (КИИ) до 1-ой категории включительно
- В АСУ ТП на критически важных объектах до 1-го класса защищённости включительно
- В медицинских (МИС), банковских (ИБС) и других ИС до 1-го класса защищённости включительно
- В информационных системах общего пользования II класса

Aladdin LiveOffice - смешанный режим работы

Дом (личное СВТ)

- **средство дистанционной работы**
- **средство 2ФА**
- **средство ЭП**
- *защищённый носитель*
- *защищённый ВКС*
- *обмен сообщениями (опция)*

Авторизованное личное СВТ1



Работа (служебное СВТ)

- **средство 2ФА**
- **средство ЭП**
- *защищённый носитель*

Командировка

- **средство дистанционной работы**
- **средство 2ФА**
- **средство ЭП**
- *защищённый носитель*
- *защищённый ВКС*
- *обмен сообщениями (опция)*

Авторизованное личное СВТ2

Дача, дорога

- **средство дистанционной работы**
- **средство 2ФА**
- **средство ЭП**
- *защищённый носитель*
- *защищённая ВКС*
- *обмен сообщениями (опция)*

Временная авторизация СВТ

Aladdin LiveOffice - для чего может использоваться

- Для организации дистанционного и/или смешанного режима работы
- Для юридически значимого электронного документооборота
- При реализации требований по защите информации от НСД для АС классов защищённости 1Г, 1Д, 2Б, 3Б
- При обработке информации, содержащей служебную тайну, информацию ограниченного распространения

Доступ ограничивается в соответствии с Конституцией РФ и Федеральными законами

- Все виды тайн (кроме гос. тайны)
- Все виды сведений (кроме составляющих гос. тайну)

Aladdin LiveOffice - с чем можно работать

Примеры

- налоговая тайна
- банковская тайна*
- врачебная тайна
- нотариальная тайна
- адвокатская тайна
- аудиторская тайна
- тайна страхования
- тайна связи
- тайна следствия и др.

- информация о новых решениях и технических знаниях (результаты интеллектуальной деятельности)
- информация о проектных решениях и иная конфиденциальная информация, которая стала известна органу исполнительной власти или организации, проводившим экспертизу проектной документации и (или) результатов инженерных изысканий в связи с проведением экспертизы
- информация, предоставляемая организациям (гражданам), осуществляющим производство и выпуск средств массовой информации
- инсайдерская информация
- информация, входящая в состав кредитной истории
- секрет производства (ноу-хау)
- сведения о должнике, просроченной задолженности и любые другие персональные данные должника
- информация о получателе социальных услуг

- информация, содержащаяся в профилях и индикаторах рисков, применяемых таможенными органами
- отдельные сведения при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд
- сведения, содержащиеся в индивидуальных лицевых счетах в системе обязательного пенсионного страхования
- информация о пенсионных счетах и др.

Полный список тайн и служебных сведений включён в Формуляр к продукту

* *Согласовано с Банком России*

Aladdin LiveOffice позволяет

- Использовать **личный** компьютер
  - **Как обычно** – для поиска информации в Интернете, обучения, игр, просмотра фильмов и пр.
    - При этом он загружается без подключения USB-устройства
    - Что-либо устанавливать или перенастраивать не требуется
  - **Для дистанционной или автономной работы** с возможностью обработки документов ограниченного распространения (ДСП)
    - Компьютер загружается с подключённым USB-устройством
    - Работает под управлением сертифицированной ОС с фиксированным набором приложений
    - Обеспечивается **замкнутая доверенная среда и защищённый канал** передачи данных в ИС организации

Aladdin LiveOffice позволяет

- Использовать **служебный** компьютер
  - USB-устройство будет выполнять функции привычного USB-токена
    - для двухфакторной аутентификации (2ФА) при входе в ИС
    - для электронной подписи в СЭД, ДБО, в различных электронных сервисах и Web-порталах
    - *в качестве защищённой USB-флешки для хранения, переноса, контролируемого распространения и использования служебной информации*

Aladdin LiveOffice позволяет

- Использовать устройство Aladdin LiveOffice для работы ТОЛЬКО на **авторизованных** компьютерах
  - Например, на личном домашнем и служебном компьютере
- При удалённом подключении к ИС организации **отказаться от использования запоминаемых паролей**, вводимых пользователями вручную

✓ **Это существенно повысит безопасность**

  - Если пользователь не знает свой пароль, то и не сможет его дискредитировать, используя в соцсетях и в других электронных сервисах

- Использовать надёжную **двухфакторую** аутентификацию (2ФА) пользователей:
  - **Строгую** (рекомендуется) – при наличии развёрнутой инфраструктуры открытых ключей (**PKI**) с помощью цифрового сертификата доступа и неизвлекаемого закрытого ключа
  - **Усиленную** – при отсутствии развёрнутой инфраструктуры открытых ключей - с помощью сложного автоматически сгенерированного пароля длиной 32 символа
    - Такой пароль **не известен** Пользователю и не может быть им использован при работе с другими электронными сервисами

Aladdin LiveOffice позволяет

- Владельцам крупных ГИС (информ. ресурсов, баз данных и пр.) организовать **безопасную работу своих контрагентов**, не являющихся сотрудниками организации
- Проблемы и риски при работе с контрагентами
  - Заставить внешних контрагентов (не являющихся своими сотрудниками) выполнять все требований безопасности* при дистанционной работе с ГИС практически невозможно
    - Нельзя проконтролировать
    - Выполнить все Требования сложно и очень дорого
  - При дистанционной работе с ГИС вне контролируемой среды контрагенты могут
    - Оставлять себе копии всех вносимых и получаемых данных из ГИС (например, оформляемые полисы, персональные данные клиентов и пр.)

      Эти данные могут попасть в обогащённые хакерские базы взломанных ресурсов (пример - Collection #2-5) - там будет лишь небольшая выборка данных, но вызванный резонанс нанесёт организации непоправимый ущерб
    - Загрузить в ИС вирус или трояна и парализовать работу организации или электронного сервиса (умышленно или неумышленно, при невыполнении хоть одного требования безопасности)

✓ **Aladdin LiveOffice в качестве защищённого терминала обеспечивает работу контрагентов в преднастроенной, замкнутой доверенной среде, все процессы (обработка документов, их хранение) производятся в среде организации, скопировать документы, загрузить в систему вирус или троян контрагент не сможет**

✓ **Такое решение в 5-10 раз дешевле, чем аттестованный по требованиям безопасности компьютер, удобнее и безопаснее**

* согласно требованиям и 17-му Приказу ФСТЭК "Меры защиты..."

Aladdin LiveOffice запрещает

- Использовать устройство на чужом (неавторизованном) компьютере
- Скопировать информацию на другие диски или устройства с функцией хранения информации
- Распечатать обрабатываемую служебную информацию на локальный или сетевой принтер
- Загрузить с внешнего носителя или из Интернет любой файл* и передать его в ИС организации
- Напрямую выйти в Интернет
- Получить доступ к данным при его краже или утере

* возможно зараженный

Aladdin LiveOffice - преимущества

✓ **Существенная экономия бюджета на организацию дистанционной работы**

✓ **Безопаснее, чем служебный ноутбук**

Служебный ноутбук

Стоимость: 7 : 1

Специализированное средство LiveOffice

Необходимо установить сертифицированные средства защиты и программное обеспечение:

- Средство доверенной загрузки
- ОС
- Антивирус
- Средство 2ФА (USB-токен, S/C)
- Средство идентификации и авторизации СВТ
- VPN
- Средство прозрачного шифрования дисков
- Межсетевой экран
- Средства мониторинга и контроля удалённого доступа

Необходимо обеспечить их совместимость

Все необходимое для работы уже на борту

Используется личное СВТ (организация на платит за него)

Экономия бюджета в 5-10 раз

или

За те же деньги можно обеспечить средствами дистанционной работы 5-10 сотрудников

Поверхность для атаки здесь существенно меньше, информация хранится и обрабатывается на рабочем ПК, на устройстве не хранится

Aladdin LiveOffice - преимущества

- **Безопаснее**
  - Поверхность атаки меньше, чем у служебного ноутбука, где вся информация хранится и обрабатывается на нём
  - Риски утечки и компрометации служебной информации будут существенно ниже
- Возможность встраивания решения в существующую инфраструктуру с минимальными её изменениями
- Возможность кастомизации решения с учётом используемых платформ и средств
- Сохранение всех привычек и навыков работы
  - При дистанционной работе пользователи работают в привычной им среде, с набором привычных приложений
  - Все документы находятся в привычных местах

  ✓ **Всё как при работе в офисе**
- Использование однократной сквозной аутентификации (Single Sign-On)
  - Пароль вводится пользователем один раз
- Продолжение работы после прерывания с того же места
  - Например, если пользователь прервал редактирование документа при работе в офисе, а затем продолжил из дома

Как это работает

Как это работает

- Если заранее всё настроено
  - Подключить токен к USB-порту компьютера
  - Включить компьютер
  - При загрузке нажать F12 (F9, F8… или др. согласно типу BIOS/UEFI компьютера - даём в инструкции)
  - В меню выбрать источник загрузки: **Aladdin LiveOffice**
  - Ввести **Пароль пользователя** устройства (ПИН-код)
  - Дождаться подключения к своему удалённому служебному компьютеру или виртуальному рабочему столу (VDI) и начать работу

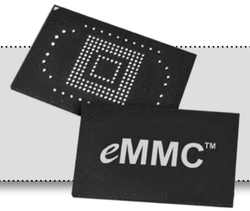
Как это работает

- **При первом использовании:**
  - Подключить токен к USB-порту компьютера
  - Загрузить компьютер с подключенным токеном
  - При загрузке нажать F12 (F9, F8… или др. согласно типу BIOS/UEFI)
  - В меню выбрать источник загрузки: Aladdin LiveOffice
  - Ввести ПИН-код USB-токена
    - Авторизовать свой личный компьютер (у Администратора)
    - Ввести код авторизации компьютера
    - Настроить сетевое подключение (Ethernet, WiFi)
    - Кликнуть по иконке "Удалённое подключение" и дождаться подключения к своему удалённому служебному компьютеру или виртуальному рабочему столу (VDI)
  - Начать работу

Компоненты решения

- как обеспечивается безопасность

Архитектура и компоненты решения



Разделы флеш-памяти специализированного USB-накопителя

- **Доверенный загрузчик (АПМДЗ)**
- Модуль аутентификации пользователя до загрузки LiveOS
- Модуль SSO (Single Sign On)
- Модуль идентификации и авторизации ПК
- Модуль безопасного обновления "прошивки" и образов дисков

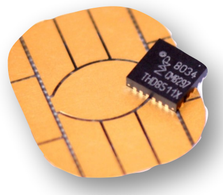
Read Only

- **Подключаемый раздел - LiveOS**
- Фиксированный набор предустановленных и преднастроенных приложений:
  - VPN-клиент (сертифицированный)
  - RDP/VDI-клиент
  - Набор офисных приложений
- Клиент/API для работы с ЭП
- Клиент системы централизованного управления

Read Only

- **Скрытый зашифрованный системный раздел** для настроек и профилей пользователя
- Журнал событий безопасности

- Скрытый зашифрованный раздел для данных пользователя (опция)

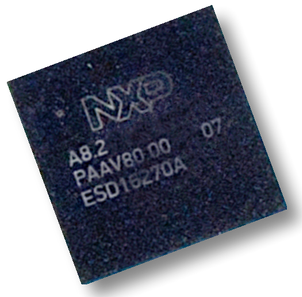


Secure Element на базе защищённого смарт-карточного чипа

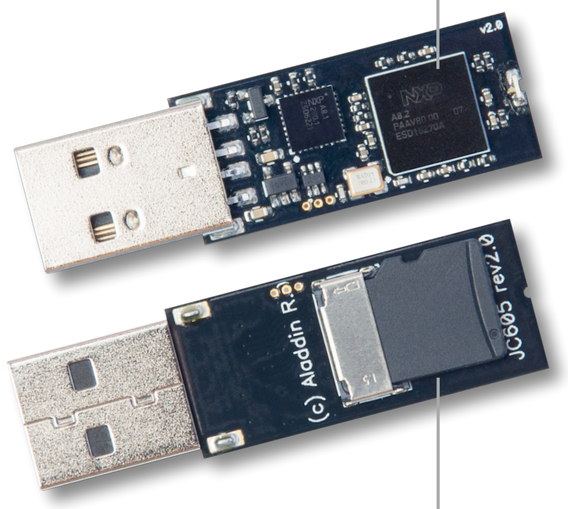
Сертифицированное средство:
- ЭП
- 2ФА

Защищённое хранилище криптографических ключей, сертификатов

Как обеспечивается безопасность



ASIC A8.2



Карта памяти (upgradable)

- Использовали существующую аппаратную платформу ("быстрый старт")
  - Защищённый машинный носитель информации (ЗМНИ) JaCarta SF/ГОСТ
  - Был разработан для МО РФ (ГОСТ РВ 0015-002-2012)
  - Сертифицирован для работы с гос. тайной с грифом секретности "СС"
- Безопасная архитектура и реализация
  - Заказной (**ASIC**) микроконтроллер на базе ARM-процессора
  - **Secure Element** на базе смарт-карточного чипа (сертифицированная российская криптография, неизвлекаемые ключи), неклонируемость и защита от взлома
  - "Изолирование" карты памяти, загрузка и контроль прошивки встроенного контроллера
  - APDU-Firewall, работа только по "белым спискам" команд
  - Доверенный загрузчик
  - Собственная встроенная ОС для микроконтроллера
  - Аппаратное шифрование защищённых разделов флеш-памяти
  - Возможность удалённого безопасного обновления ("прошивка" зашифрована и подписана ЭП на ключе устройства)
  - Безопасный обмен с ПО на хосте (защита команд и данных)
- Внедрили технология разработки безопасного ПО (ГОСТ Р 56939-2016), автоматизированного тестирования и поиска уязвимостей
  - Степень покрытия автотестами - 93%, тестирование - на симуляторах
  - Качество самих тестов проверяется с помощью мутационного тестирования

Как обеспечивается безопасность

Личный компьютер

Все задачи выполняются на служебном ПК или на VM, на личный ПК передаются лишь отрисованные "картинки"

Служебный компьютер

- **Remmina RDP Client**

Протестировано:

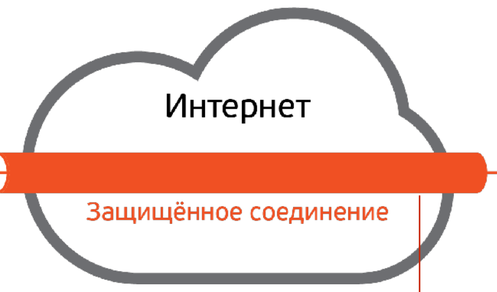
- Citrix Workspace App
- VMware Horizon client

VPN client

- **ViPNet**

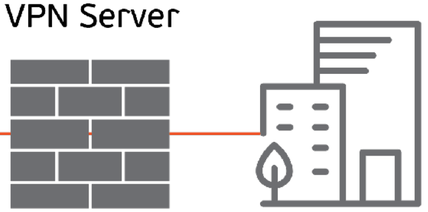
Протестировано:

- ЗАСТАВА
- Континент-АП
- КриптоПро NGate (исп. 5)
- Cisco AnyConnect
- OpenConnect
- OpenVPN и др.



Внутри VPN используется протокол RDP

VPN Server



- RDP
- VDI

Российские VDI:

- "Брест"
- *"Скала-Р" (в работе)*

Как выглядит экран при использовании маркирования?

Справочный центр

Содержание

- Обновления безопасности и методические указания
- Astra Linux Red-Book
- Операционная Система Общего Назначения Орёл
- Операционная Система Специального Назначения Смоленск
- Операционная Система Специального Назначения Ленинград
- Программный Комплекс Средств Виртуализации "Брест"
- Средства криптографической защиты информации (СКЗИ)
- Про Astra Linux в Интернете
- Обучение по Astra Linux
- Таблица вариантов исполнения ОС СН «Astra Linux Special Edition».
- Таблица вариантов исполнения ОС ОН "Astra Linux Common Edition"
- Общедоступные информационные ресурсы Astra Linux
- Архив

Операционные системы Astra Linux

Обновления безопасности
для Astra Linux Special Edition Смоленск 1.6
для Astra Linux Special Edition Смоленск 1.5
для Astra Linux Special Edition Ленинград 8.1

Замечания и предложения
по содержанию Справочного центра

Операционные системы Astra Linux Common Edition и Astra Linux Special Edition разработаны коллективом открытого акционерного общества «Научно-производственное объединение Русские базовые информационные технологии» и основаны на свободном программном обеспечении.

Astra Linux Common Edition предназначена для автоматизации коммерческих предприятий и органов государственного управления.

Astra Linux Special Edition предназначена для применения в автоматизированных системах в защищенном исполнении, обрабатывающих информацию ограниченного распространения, включая государственную тайну до степени секретности "особой важности".

На сайте представлена подробная информация о разработанных операционных системах семейства Astra Linux, а также техническая документация для пользователей операционных систем и разработчиков программного обеспечения. Кроме того, предоставлена возможность скачать дистрибутивы и исходные тексты операционной системы Astra Linux Common Edition, а также задать интересующие вопросы разработчикам.

Мы будем признательны Вам за вопросы и предложения, которые позволят совершенствовать наши изделия в Ваших интересах и адаптировать их под решаемые Вами задачи!

Репозитория открытого доступа в сети Интернет для операционной системы Astra Linux Special Edition нет. Операционная система распространяется посредством DVD-дисков.

Информацию о сетевых репозиториях операционной системы Astra Linux Common Edition Вы можете получить на нашем сайте.

Драйверы для операционных систем Astra Linux

Недавно обновлено

- Параметры модуля ядра Parsec, задаваемые в файле /boot/boot.conf
  прокомментировано около 3 ч. назад
- Параметры модуля ядра Parsec, задаваемые в файле /boot/boot.conf
  обновлено около 4 ч. назад • изменения
- Параметры модуля ядра Parsec, задаваемые в файле /boot/boot.conf
  прокомментировано около 4 ч. назад
- Обновление Astra Linux SE с компакт-дисков
  обновлено около 10 ч. назад • изменения
- Инструкция по использованию ALP-образа Astra Linux SE
  обновлено ноя 08, 2020 • изменения
- Samba + FreeIPA аутентификация пользователей Samba в Kerberos
  обновлено ноя 06, 2020 • изменения
- Samba
  обновлено ноя 03, 2020 • изменения
- Установка и настройка x2go
  обновлено окт 30, 2020 • изменения
- Драйверы видеокарт NVidia
  обновлено окт 27, 2020 • изменения

Технологические вызовы

при реализации новых требований

Аладдин

Технологические вызовы

"Электронный замок" - должен:

- Быть выполнен в форм-факторе USB-токена (необходимо совместить "личинку" замка и "ключ")
- Соответствовать требованиям Профиля защиты к средствам доверенной загрузки уровня платы расширения 4 класса защиты (СДЗ)
- Выполнять аутентификацию пользователя **до** загрузки ОС
- Передавать в ОС аутентификационные данные пользователя (SSO)
- Разрешать работу **только** на авторизованных компьютерах (и иметь встроенные механизмы авторизации)
- Быстро проверять целостность "прошивки" и защищённых разделов
- Управлять монтированием и работать со скрытыми защищёнными разделами
    - Подключать их после аутентификации пользователя и только на авторизованных компьютерах

✓ **Контролируемый доступ и контролируемое распространение информации**

Технологические вызовы

"Электронный замок" - должен:

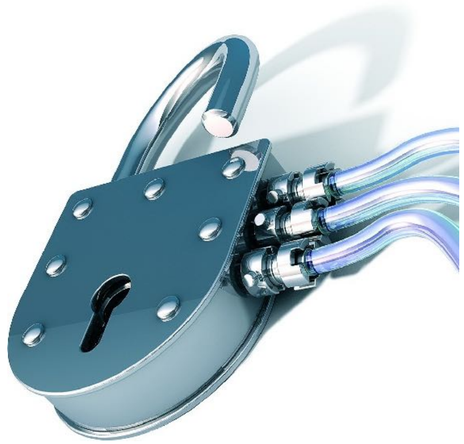
- Работать со всеми USB-контроллерами (2.0, 3.0, 3.1, 3.2) и USB-хабами на низком уровне (до загрузки ОС)

✓ **Столкнулись с ошибками реализации новых спецификаций USB 3.1, 3.2 в контроллерах, пришлось с нуля писать весь USB-стек**

- Иметь **механизм безопасного дистанционного обновления**:
  - "прошивки" устройства, образа ОС и приложений, профилей и настроек
- Работать на всех возможных моделях компьютеров, находящихся в личном пользовании

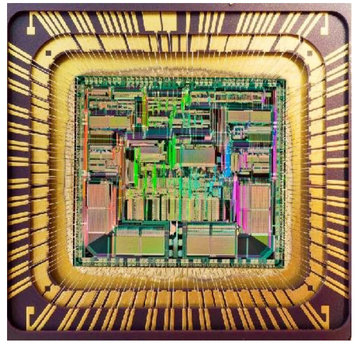
✓ **Пока смогли решить не все проблемы**

- Некоторые компьютеры (BIOS/UEFI) не имеют механизма (возможности) загрузки с внешнего носителя (но их не очень много)
- Apple Mac - научились запускать Linux, надо писать драйверы для "родных" мышек, клавиатур, Touchpad'ов - *было в планах, но отказались после начала СВО*

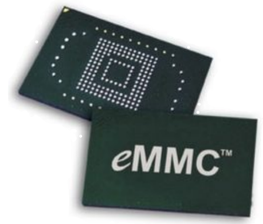


Технологические вызовы

- Необходимость "**быстрой**" реализации российских алгоритмов шифрования на относительно слабых микроконтроллерах
  - Практически достигли технического порога скорости
  - Требуется использование специализированного крипто-акселератора
- Использование отечественной элементной базы
  - Требования по импортозамещению, повышению уровня доверия



  - ✓ **Портировали решение на отечественный IoT-микроконтроллер 1892ВМ268 - Cortex M33 с технологией TrustZone (совм. с "ЭЛВИС")**
    - Это дало увеличение скорости работы с зашифрованными разделами **до ~20 МБ/с** (макс. скорость USB 2.0), но **поставки чипов заблокированы**
  - ✓ **Используем модули флеш-памяти российского производства**



- Безопасное дистанционное администрирование
  - Обычно для этого используется АРМ Администратора Безопасности, но по требованиям безопасности его НЕЛЬЗЯ подключать к сети Интернет
  - ✓ **Пришлось решать и эту задачу, ведь все пользователи на "удалёнке"**
- Централизованное управление и обновление - поддержали в JMS
  - Сразу делаем версии и для Windows, и для Linux

Технологический вызов

Отказ от использования пользовательских паролей (запоминаемых и вводимых вручную) при удалённой аутентификации

✓ **ПРОБЛЕМА:**

- Если пользователь выучит свой сложный (правильный) пароль для удалённого подключения к ИС организации, то рано или поздно он обязательно использует его в соцсетях, при заказе пиццы и пр.
- Такие ресурсы часто взламывают, а взломанные аккаунты попадают в обогащённые базы данных, из которых можно выудить нужные данные и попробовать подключиться к ИС от имени такого пользователя, и об этом не сразу узнают…
  - Это приведёт к утечкам и дискредитации служебной информации

- В решении для удалённого подключения используется **только двухфакторная аутентификация** (2ФА) пользователей
  - **СТРОГАЯ**, с использованием цифровых сертификатов - если в организации развёрнута инфраструктура открытых ключей (PKI)
  - **УСИЛЕННАЯ**, с использованием сложного сгенерированного 32-х символьного пароля, который автоматически подставляется в систему так, чтобы пользователь его не знал, не мог использовать и дискредитировать

✓ **Вызов:**

- Для Linux пришлось с нуля разрабатывать эти технологии (SecurLogon)
- Для Linux на рабочем компьютере пришлось сделать весь PKI-стек

Для тех, кому не нужна сертификация

- Делаем коммерческую версию (CE) с настройками под существующую ИТ-инфраструктуру
- Больше возможностей для настройки и манёвра
- Дешевле (почти половина стоимости сертифицированного решения - это сертифицированная ОС и VPN)

Соответствие новым Требованиям к средствам дистанционной работы

Защищённое специализированное USB-устройство, соответствующее Требованиям к средствам дистанционной работы	✓
Аутентификация пользователя ДО загрузки LiveOS	✓
2ФА в LiveOS и на удалённом служебном ПК с однократным вводом ПИН-кода по технологии SSO, отказ от использования пользователями запоминаемых паролей	✓
Возможность работы ТОЛЬКО на авторизованных ПК (<3)	✓
Использование сертифицированных LiveOS и VPN	✓
Возможность сохранения рабочих документов (в т.ч. ДСП), настроек и профилей пользователя на аппаратно зашифрованных разделах USB флеш-диска	✓
Возможность безопасного удалённого (централизованного) обновления "прошивки" USB-устройства, образов ОС, настроек	✓
Возможность безопасного **удалённого** администрирования USB-устройства (СКЗИ, СЗИ, LiveOS, VPN, VDI)	✓
Централизованное управление жизненным циклом, автоматизация рутинных операций	✓
Возможность работы с ЭП (УКЭП) в системах ЭДО	✓

Остерегайтесь подражателей - уже появились!
Это глубоко интегрированное, а не интеграционное аппаратно-программное решение ✗

Заказывайте тестовый демо-комплект

Обеспечение безопасной дистанционной работы сотрудников организации в ГИС с имеющихся недоверенных (личных) средств вычислительной техники

Будь собой в электронном мире!

Аладдин