Техническое решение по обеспечению дистанционной работы в информационной системе с личных средств вычислительной техники пользователей

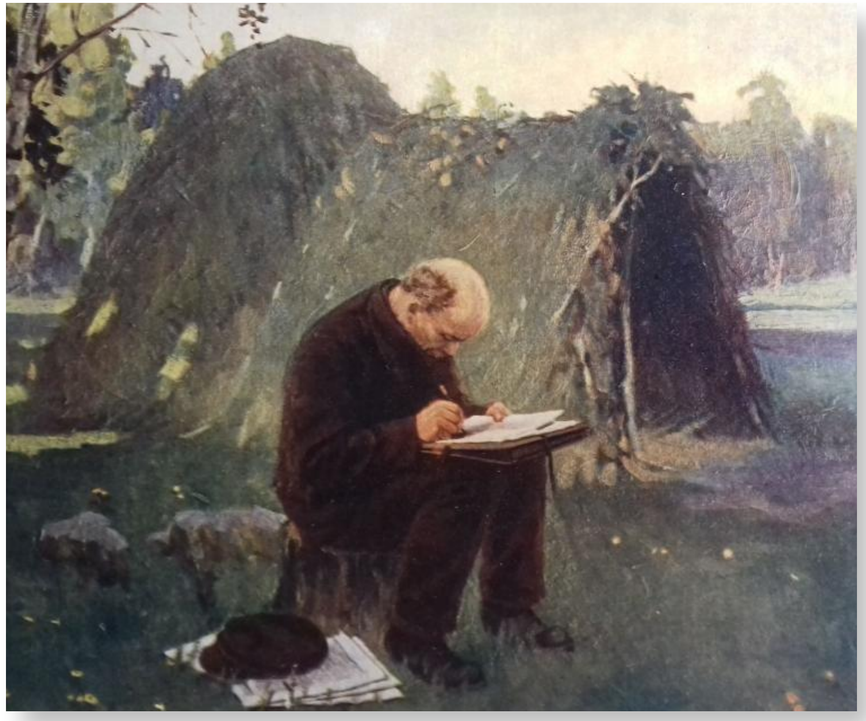
Aladdin LiveOffice

Сергей Груздев,
генеральный директор

Аладдин

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

Коронавирус навсегда изменил нашу жизнь

- Катализатор для многих процессов
  - Легализация дистанционной работы (сначала де-факто, сейчас 407-ФЗ)
    - Совместная работа с Регулятором по разработке новых Требований к средствам дистанционной работы

  ✓ **Очень полезный опыт**

  - Параллельно:
    - Разработка архитектуры решения (подход Secure by design)
    - Проработка технических решений (иногда тупиковых)
    - Интеграция с продуктами технологических партнёров (ОС, VPN, VDI)
    - Отработка различных кейсов и сценариев (с будущими Заказчиками)
    - Решение проблемы импортозамещения (в части отказа от использования проприетарного ПО и импортной элементной базы)
    - Создание Платформы для безопасного централизованного администрирования и управления жизненным циклом (включая удалённое администрирование СКЗИ, обновление "прошивки" устройства, встроенной ОС и установленных приложений, профилей, сертификатов, ключей)
    - Сертификация

  ✓ **Обычно это занимает 2.5 - 3 года, мы сделали это за 9 месяцев**

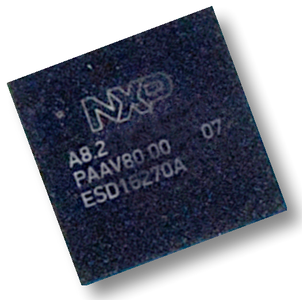
Техническое решение

- LiveOffice - это средство:
  - Для безопасной дистанционной работы
  - Для строгой и усиленной двухфакторной аутентификации пользователей
  - Для электронной подписи (УКЭП)
  - Для безопасного хранения и контролируемого использования служебной информации

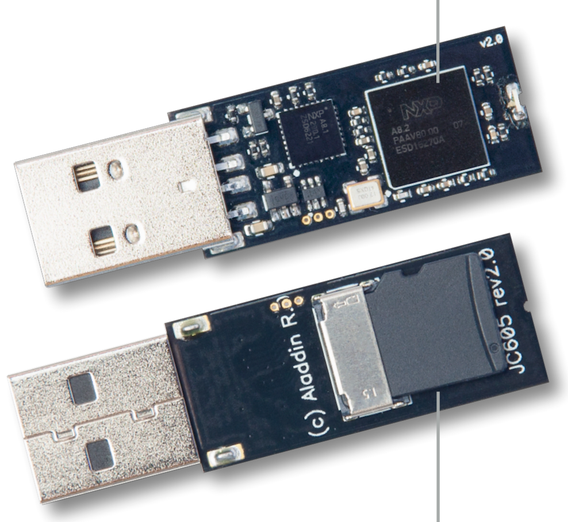
Основа решения - технология LiveUSB

- Использование **личного** (недоверенного) компьютера
  - Запуск модуля доверенной загрузки (Профиль защиты)
    - Аутентификация пользователя (до загрузки ОС)
    - Идентификация компьютера (Авторизация)
    - Проверка целостности ("прошивки" устройства, образа LiveOS, служебных настроек, данных пользователя)
    - Монтирование скрытых защищённых разделов флеш-накопителя (LiveOS, служебные настройки, журнал событий ИБ, данные пользователя)
  - Загрузка компьютера с внешнего USB-накопителя (LiveUSB)
    - Сертифицированный Linux
    - Сертифицированный VPN (защищённое соединение со шлюзом организации)
    - RDP-клиент для соединения со служебным компьютером или с виртуальным рабочим столом (VDI) с подключением к ИС
    - Набор офисных приложений для работы с документами в режиме офлайн

Как обеспечивается безопасность



ASIC A8.2

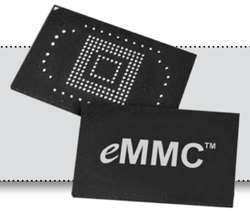


Карта памяти
(upgradable)

- 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 со степенью 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)

    ✓ **Взламывать украденное устройство и пытаться извлечь из него информацию бесполезно - ключи шифрования в нём не хранятся**
- Внедрили технология разработки безопасного ПО (ГОСТ Р 56939-2016), автоматизированного тестирования и поиска уязвимостей
  - Степень покрытия автотестами - 95%, тестирование - на симуляторах
  - Качество самих тестов проверяется с помощью мутационного тестирования

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

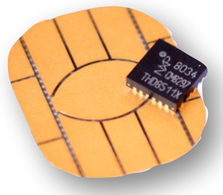
Read Only

- **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**



Secure Element на базе защищённого смарт-карточного чипа

Сертифицированное средство:
- ЭП
- 2ФА

Защищённое хранилище криптографических ключей, сертификатов

Как это работает

Если заранее всё настроено:

1. **Подключить** токен к USB-порту компьютера
2. **Загрузить** (или перезагрузить) компьютер
3. При загрузке **нажать F12** (F9, F8… или др. согласно типу BIOS/UEFI компьютера)
4. В меню **выбрать источник загрузки**: Aladdin LiveOffice
5. **Ввести ПИН-код** устройства
6. Дождаться подключения к своему удалённому служебному компьютеру или виртуальному рабочему столу (VDI) и начать работу
7. Рабочие документы можно сохранить на защищённый зашифрованный раздел USB-диска и работать с ними офлайн, экономя трафик

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

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:

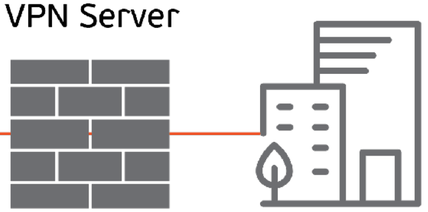
- Citrix Workspace App
- VMware Horizon client

VPN client

Интернет

Защищённое соединение

VPN Server



- RDP
- VDI

VDI "Брест"

- **ViPNet**

Протестировано:

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

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 (АПМДЗ)
  - 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

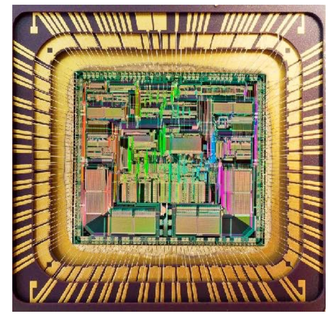
✓ **Контролируемый доступ и контролируемое распространение информации**

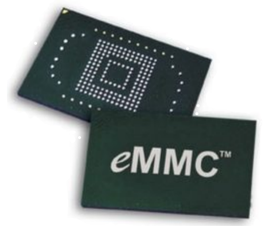
Технологические вызовы

- "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
    - ✓ **Это очень важно - ведь никто не научился выпускать ПО без ошибок и уязвимостей, мы не исключение**
  - 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 - *в планах на 2021 г.*
      - Процессоры Intel Core 10-го и 11-го поколения (из-за отсутствия драйверов для Linux) - *задача перехода на новые ядра сертифицированного Linux - в планах*

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
    - ✓ **Планируется портирование решения на отечественный IoT-микроконтроллер 1892ВМ268 - Cortex M33 с технологией TrustZone (совм. с "ЭЛВИС") и запуск производства в РФ модулей флеш-памяти**
      - Это даст увеличение скорости работы с зашифрованными разделами **до 24 МБ/с** (макс. скорость USB 2.0)





- 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
  - Сразу сделали версии и для Windows, и для Linux (до УД-2)
  - Отработали технологию сборки проектов под разные ОС из единых исходников

Технологические вызовы

- 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)

Aladdin LiveOffice

Разработано по поручению Председателя Правительства РФ №ММ-П9-1861 от 16.03.2020 и зам. Председателя Правительства РФ №ДГ-П17-1987 18.03.2020 для противодействия распространению коронавирусной инфекции и обеспечения работы сотрудников органов исполнительной власти и гос. организаций в удалённом режиме с использованием личных средств вычислительной техники с предоставлением им удалённого доступа к государственным информационным системам.

Aladdin LiveOffice

Назначение

- Организация безопасной дистанционной работы сотрудников при использовании ими личных (или доступных для использования) средств вычислительной техники
- Обеспечение безопасного удалённого доступа к рабочему столу своего физического служебного компьютера или виртуального (при наличии развёрнутой инфраструктуры VDI) с возможностью подключения и дистанционной работы

- в государственных информационных системах (ГИС) до 1-го класса защищённости включительно
- в информационных системах персональных данных (ИСПДн) до 1-й категории включительно
- в информационных системах значимых объектов критической информационной инфраструктуры (КИИ) до 1-ой категории включительно
- в автоматизированных системах управления производственными и технологическими процессами (АСУ ТП) на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1-го класса защищённости включительно
- в медицинских (МИС), банковских (ИБС) и других информационных системах (ИС) до 1-го класса защищённости включительно
- в информационных системах общего пользования II класса

Aladdin LiveOffice

Возможности

- Aladdin LiveOffice может использоваться:
  - для организации **дистанционного** и/или **смешанного** режима работы, когда сотрудник часть времени работает на "удалёнке" (с использованием личного компьютера), а часть – в офисе (с использованием служебного компьютера, тогда LiveOffice используется как обычный USB-токен для 2ФА, ЭП и "защищённая флешка")
  - для юридически значимого электронного документооборота
  - при реализации требований по защите информации от несанкционированного доступа для автоматизированных систем (АС) классов защищённости 1Г, 1Д, 2Б, 3Б
  - при обработке информации, содержащей сведения конфиденциального характера, связанные с профессиональной деятельностью (служебная тайна, служебная информация ограниченного распространения), доступ к которой ограничен в соответствии с Конституцией РФ и Федеральными законами
    - налоговая, банковская, врачебная, нотариальная, адвокатская, аудиторская тайна
    - тайна страхования, связи, следствия и др.
    - секреты производства (ноу-хау), сведения о должнике, профили и индикаторы рисков (таможня), информация о пенсионных счетах, кредитные истории, результаты проверок, экспертиз и пр.

✓ **В режиме дистанционной работы**

✓ **В автономном режиме (офлайн), например, при плохом канале связи**

✓ **В смешанном режиме - офис (служебный компьютер) / дом (личный компьютер)**

Не позволяет:

- Использовать устройство на чужом (неавторизованном) компьютере - все его функции и пользовательские данные будут недоступны, даже при вводе правильного пароля доступа
- Скопировать или сохранить обрабатываемую информацию на локальные, съёмные диски, флеш-накопители и на другие устройства с функцией хранения информации
- Распечатать служебную информацию на локальном или сетевом принтере
- Загрузить на свой компьютер какой-либо файл (возможно, заражённый) с внешнего носителя или из сети Интернет и передать его в ИС организации
- Выйти в сеть Интернет при дистанционной работе напрямую со своего личного компьютера (сеть будет доступна только через служебный компьютер, и работа в сети защищена используемыми в организации средствами защиты)
- Получить доступ к служебным или пользовательским данным, сохранённым в памяти устройства, а также использовать устройство для удалённого доступа в ИС организации в случае его утери или кражи

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 ✗

Техническое решение по обеспечению дистанционной работы в информационной системе с личных средств вычислительной техники пользователей

Будь собой в электронном мире!

Аладдин

Сергей Груздев
s.gruzdev@aladdin.ru
+7 (985) 762-2855
www.aladdin-rd.ru