Aladdin LiveOffice

- средство обеспечения безопасной дистанционной работы сотрудников с использованием ими личных средств вычислительной техники

Для гос. структур и коммерческих компаний

КОНФИДЕНЦИАЛЬНО

Актуальность решения для удалённой работы

- Эпидемия коронавируса, карантин, режим домашней изоляции показал **неготовность** федеральных структур, органов исполнительной власти, государственных организаций к организации полноценной и эффективной удалённой работы своих сотрудников
- Причины
  - В стране нет столько денег, чтобы для работы на "удалёнке" обеспечить каждого сотрудника госструктур служебным ноутбуком и набором средств защиты для него
  - Действующие требования регуляторов запрещают удалённое подключение и работу с государственным информационным системам (ГИС)
- Поручения Правительства РФ (№ММ-П9-1861, №ДГ-П17-1987 от 16 и 18.03.2020)
  - Для противодействия распространению коронавирусной инфекции **обеспечить** работу сотрудников органов исполнительной власти и гос. организаций в удалённом режиме с использованием **личных** средств вычислительной техники с предоставлением им **удалённого доступа** к ГИС

Актуальность решения для удалённой работы

- Отпадает ли необходимость в работе "на удалёнке" в связи с отменой ограничений, с возвращением страны к нормальной жизни?
  - Нет. Вирус никуда не делся, он лишь временно отступил.
  - Иммунитет приобрело не более 10% населения страны (а для победы над ним необходимо минимум 70%), впереди осень, зима... Возможны новые вспышки заболеваний и новый карантин
  - Многие коммерческие организации смогли организовать эффективную работу "на удалёнке", и КПД у многих существенно вырос
- Возможность работы "на удалёнке" для многих федеральных структур, органов исполнительной власти и гос. структур остаётся как никогда актуальной и востребованной

Идея решения

- Для удалённой работы сотрудники могут использовать свои личные персональные компьютеры (ПК)
  - Любые ПК на базе архитектуры x86 (вкл. Mac)
  - Для работы необходимо
    - Свободный USB-порт
    - Возможность выбора в BIOS/UEFI источника или приоритета загрузки ОС
    - Специализированное защищённое аппаратное USB-устройство **Aladdin LiveOffice** с предварительно настроенным Администратором профилем доступа
    - Загрузить ПК с подключенного USB-устройства
    - Ввести правильный ПИН-код устройства
  - После этого автоматически устанавливаются защищённое VPN и RDP-соединения
  - Пользователь получает удалённый доступ к рабочему столу своего служебного ПК или терминальному (виртуальному) приложению, может пользоваться всем набором установленного ПО с привычным ему интерфейсом и настройками, получает доступ в ГИС
  - Используемый личный ПК должен быть авторизован, удалённый доступ в ГИС с неавторизованных ПК не допускается

Идея решения

- Пользователи смогут
  - Безопасно дистанционно работать
    - с ГИС до 1-го класса защищённости включительно
    - с ИСПДн до 1-го уровня защищённости персональных данных
  - Работать с информацией ограниченного распространения (с грифом "Для служебного пользования")
    - Сохранить результаты работы или необходимую информацию на скрытый защищённый раздел своего USB-устройства Aladdin LiveOffice
  - Использовать несколько имеющихся у них ПК (например, домашний ПК, ноутбук, ПК на даче)
    - Перед началом работы на новом ПК Пользователь должен его авторизовать (послать запрос Администратору и получить от него код авторизации)
- Пользователи не смогут
  - Скопировать обрабатываемую информацию на локальные, съёмные диски, флеш-накопители и на другие устройства
  - Загрузить какой-либо файл (возможно, зараженный) на свой служебный ПК или в ГИС
  - Распечатать обрабатываемую информацию на подключенный локальный или сетевой принтер

Архитектура решения и состав

Основа решения

- Технология Live USB
  - Загрузка **доверенной ОС** (Live ОС) **со специального USB-устройства** на недоверенном личном ПК
  - **Фиксированный** набор предустановленных приложений
  - **Настройки** для автоматического подключения делаются Администратором заранее, изменить их или установить дополнительное приложение Пользователь не сможет
  - Во время работы Live ОС установленные на этом ПК в "домашней" ОС приложения, подключенные периферийные устройства (диски, принтеры и пр.) будут **недоступны**

Состав

- Специализированное защищённое USB-устройство - "три в одном":
  - **Защищённый флеш-накопитель**
    - Для загрузки Live ОС
    - Для безопасного хранения служебной информации (недоступной для чтения и изменения) - пользовательских профилей настроек (сетевого подключения и пр.)
    - Для безопасного хранения и транспортировки рабочих документов
  - Средство строгой/усиленной двухфакторной аутентификации (**2ФА**)
  - Средство усиленной квалифицированной электронной подписи (**УКЭП**) с неизвлекаемым закрытым ключом
- Live ОС
  - Сертифицированная ОС Linux с фиксированным набором приложений
- VPN
  - Сертифицированный ФСБ России
  - RDP-клиент (внутри VPN-соединения)

Архитектура решения и состав

- USB-устройство
  - За основу решения был взят **защищённый служебный флеш-накопитель** JaCarta SF/ГОСТ
    - Разработан и сертифицирован компанией "Аладдин" для контролируемого распространения и хранения информации, включая гос. тайну со степенью секретности "Совершенно секретно"
  - Изменена логика работы и подключения скрытых защищённых дисков
  - Добавлены новые возможности
    - **Строгая** и/или **усиленная двухфакторная аутентификация** Пользователей с использованием развёрнутой в организации инфраструктуры открытых ключей (**PKI**) или без неё при подключении к удалённому рабочему столу своего служебного ПК и в ГИС
    - **Аутентификация** сделана так, **чтобы Пользователи не знали и не вводили пароль вручную**, и, следовательно, не смогли бы использовать этот же пароль при работе с другими электронными сервисами (в соц. сетях, при заказе пиццы и пр.), а следовательно
      - **Пользователи не смогут дискредитировать свою учётную запись и не смогут подвергнуть организацию (ГИС) риску в случае перехвата пароля, взлома или утечки учётных данных внешнего эл. сервиса**
    - Загрузка Live ОС, монтирование защищённых скрытых дисков, подключение к удалённому рабочему столу или VDI, работа с ГИС - только **после аутентификации** Пользователя и **только на авторизованных ПК**
      - **При попытке несанкционированного использования устройства его функции и данных будут недоступны**

Технические подробности

- USB-устройство
  - **Возможность работы как с обычным USB-токеном для 2ФА и ЭП** на своём служебном ПК или на личном из-под домашней ОС (Windows, Linux, macOS)
  - **Централизованное дистанционное безопасное администрирование** - обновление пользовательских профилей, настроек и параметров удалённого подключения, цифровых сертификатов, ключей, "прошивки" устройства, Live ОС, приложений (VPN-клиентов для совместимости с существующей инфраструктурой организации), добавление новых функций и возможностей и т.п.
  - **PIN-код Пользователя заранее не устанавливается** - это сделано для того, что Пользователи никогда не использовали устройства с PIN-кодом, установленным по-умолчанию, а задавали его самостоятельно в соответствии с политикой безопасности при первом использовании своего устройства
  - **Возможность автоматического разблокирования устройства** без обращения к Администратору если превышено количество попыток ввода неправильного PIN-кода
  - **Журнал событий безопасности** - ведётся самими устройством, хранится на скрытом системном разделе, доступ к которому имеет только Администратор и система централизованного управления (на чтение и стирание)
  - Устройство соответствует требованиям ГОСТ РВ 20.39.304-98 (Аппаратура, приборы, устройства и оборудование военного назначения. Требования стойкости к внешним воздействующим факторам)

Технические подробности

- Сертификация
  - На соответствие новым Требованиям ФСТЭК России к средствам обеспечения безопасной дистанционной работы, по Требованиям безопасности информационной по 4 классу защиты, а также требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий по 4-му уровню доверия
  - По линии ФСБ РФ как средство СКЗИ
    - В процессе
  - Live ОС в составе продукта:
    - Сертифицированная операционная система (соответствие требованиям профиля защиты ИТ.ОС.А4.ПЗ)
  - Сертификат соответствия требованиям Технического регламента Таможенного союза ТР ТС 020/2011 "Электромагнитная совместимость технических средств"

- Технические подробности
  - Срок полезного использования – 3 года, гарантийный срок – 1 год
  - Срок хранения записанных во флэш-память данных – не менее 10 лет
  - Страна происхождения (разработки и производства) - РФ

Средство обеспечения безопасной работы сотрудников на "удалёнке"

- В следующей версии планируется добавить
  - ВидеоКонференцСвязь (**ВКС**) с возможностью обсуждения, демонстрации и загрузки документов ограниченного распространения (**ДСП**)
  - **Live-версию офисного пакета** для работы с документами (в том числе в автономном режиме без удалённого подключения)
  - **Возможность подключения к разным ГИС** с автоматическим выбором нужной VPN
  - **Возможность дистанционного обновления** встроенной ОС ("прошивки"), Live ОС и необходимого ПО для ранее купленного USB-устройства JaCarta Remote Access

Мои контакты
Сергей Груздев

Будь собой в электронном мире!

Аладдин

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