



Aladdin LiveOffice:

безопасное рабочее место 1C, Termidesk, RDP

text: Андрей Виноградов

Как максимально безопасно организовать удаленное рабочее место с доступом к серверу с конфиденциальными данными? А если требуется еще и использовать различные ноутбуки или десктопы, причем не только свои? Компания «Аладдин» предложила остроумное решение: Aladdin LiveOffice — специализированное USB-устройство, предназначенное для организации территориально распределенных рабочих мест с высочайшим уровнем доверия. По сути, это загрузочная флешка (для простоты так и будем называть устройство далее) с образом операционной системы, которая превращает любой подходящий компьютер в защищенный тонкий клиент. При этом пользователь не может вносить изменения в накопитель, а обновления образа устанавливает только администратор. Мы решили буквально вставить устройство в USB-порт и посмотреть, как это работает на практике — вместе с 1C, RDP и Termidesk.



Что внутри

Aladdin LiveOffice внешне выглядит как обычный USB-накопитель, однако, по сути, это специализированное защищенное устройство, разработанное на платформе, которая изначально создавалась для защищенных носителей силовых структур.

На нем размещен неизменяемый для пользователя образ LiveOS на базе сертифицированной Astra Linux SE «Воронеж» или РЕД ОС, встроенные средства доверенной загрузки, VPN-клиент и заранее определенный набор прикладных клиентов. Решение сертифицировано ФСТЭК России (сертификат № 4355), а также имеет сертификаты ФСТЭК России на средство аутентификации и ФСБ России на средство электронной подписи и СКЗИ — то есть перед нами не самодельная сборка энтузиастов, а полноценный продукт с прикладной сертификацией, который можно официально использовать в ГИС, ИСПДн, значимых объектах КИИ и других защищенных информационных системах.

Отдельно стоит отметить, что «личная» флешка пользователя — не единственный элемент решения. У администратора есть свое похожее устройство, отличающееся по цвету корпуса, между которым и пользовательскими носителями выстроена криптографическая связь. Другой администратор, даже располагая точно такой же флешкой, не сможет вмешаться в чужую инфраструктуру — приятная деталь с точки зрения разделения полномочий внутри крупной организации.

Как это выглядит для пользователя: процесс тестирования

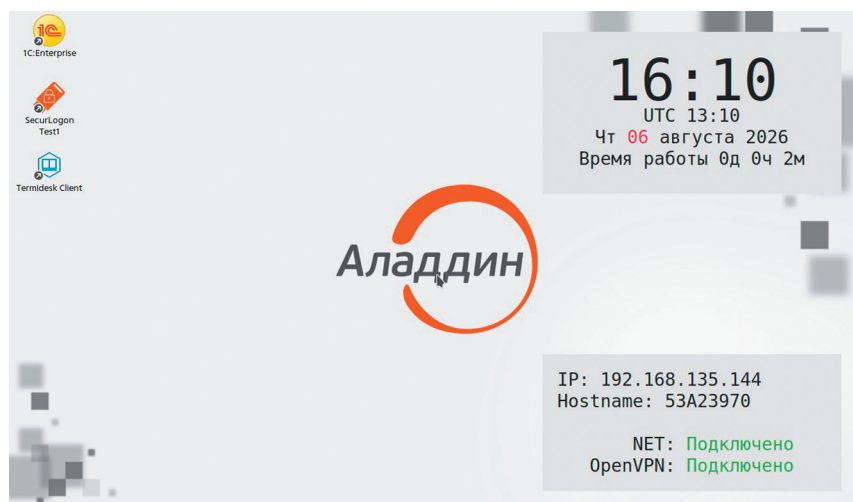
Первое, что хочется отметить, — процедура запуска действительно простая, «без танцев с бубном», которых я, признаться, подсознательно ожидал от защищенного решения такого уровня.

Вставляем Aladdin LiveOffice в свободный USB-порт компьютера (замечу, интерфейс здесь USB 2.0, о чем ниже). Включаем или перезагружаем компьютер, и на этапе POST нажимаем клавишу вызова меню загрузки — F12, F9, F8 или другую, в зависимости от конкретного BIOS/UEFI. Администратор выдает сотруднику короткую инструкцию под конкретную модель техники, так что угадывать клавишу самому не придется.

В появившемся меню выбора источника загрузки выделяем пункт Aladdin LiveOffice — компьютер передает управление уже не установленной на нем Windows или Linux, а встроенному в носитель средству доверенной загрузки.

Здесь у пользователя запрашивается пароль (ПИН-код) устройства. Кстати, до момента авторизации можно посмотреть список уже зарегистрированных для этого носителя компьютеров — удобная функция для самопроверки, если, например, вы не уверены, что именно этот ноутбук уже привязан к вашей флешке.

При первом использовании появляется дополнительный шаг — авторизация самого компьютера. Устройство считывает так называемый отпечаток



машины — набор параметров процессора, платформы и диска — и выдает на экран код компьютера, состоящий из десяти цифр. Пользователь сообщает этот код администратору (по телефону, почте, мессенджеру — не важно, канал не критичен к безопасности, поскольку сама схема построена на криптографии HOTP), в ответ получает код авторизации, вводит его, и с этого момента конкретный компьютер становится доверенным для данного носителя. Приятно, что весь обмен происходит еще до появления сети, то есть до того, как поднялся Wi-Fi или Ethernet, и теоретический злоумышленник просто не успевает вмешаться в процесс.

После успешной авторизации начинается собственно загрузка Astra Linux в режиме LiveCD. Здесь я должен быть откровенным: происходит это не мгновенно. USB 2.0 плюс особенности загрузки Linux с несколькими переключениями графического режима дают в сумме заметную паузу с чередой черных экранов — было бы обманом утверждать, что все происходит за пять секунд. Но для рабочего сценария «один раз загрузился утром и работаешь весь день» это не критично.

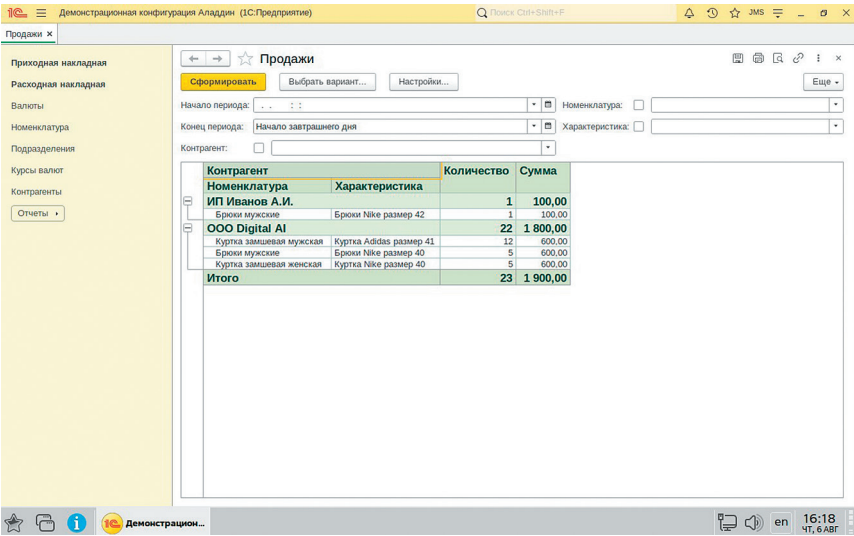
Дождавшись рабочего стола, мы увидели предельно лаконичный интерфейс в стиле киоска: никаких терминалов, файловых менеджеров и лишних на-

строек — только необходимый минимум для конфигурации сети, экрана и звука, плюс сразу видны иконки предустановленных клиентов. Справа расположены два виджета — часы и текущий сетевой адрес самого носителя в инфраструктуре, что удобно с точки зрения журналирования и техподдержки. Настроили сетевое подключение (в нашем случае — проводное, но поддерживается и Wi-Fi), и VPN-клиент автоматически поднял защищенный туннель до инфраструктуры организации.

Работа с 1С

Представим ситуацию, когда компания находится в одном городе, а база 1С — на сервере в другом, и сотрудникам нужен защищенный канал для оформления заказов, работы с документами и отчетностью без риска, что данные окажутся на локальном диске случайного компьютера.

Запустили клиент 1С прямо с рабочего стола Aladdin LiveOffice. Клиент, что скрывать, загружается не молниеносно — это особенность самой 1С, а не носителя. Подключились к тестовой базе, сформировали отчет по продажам, полистали справочники — с точки зрения пользователя процесс практически не отличается от привычной работы в офисе: те же меню, те же формы, та же логика.



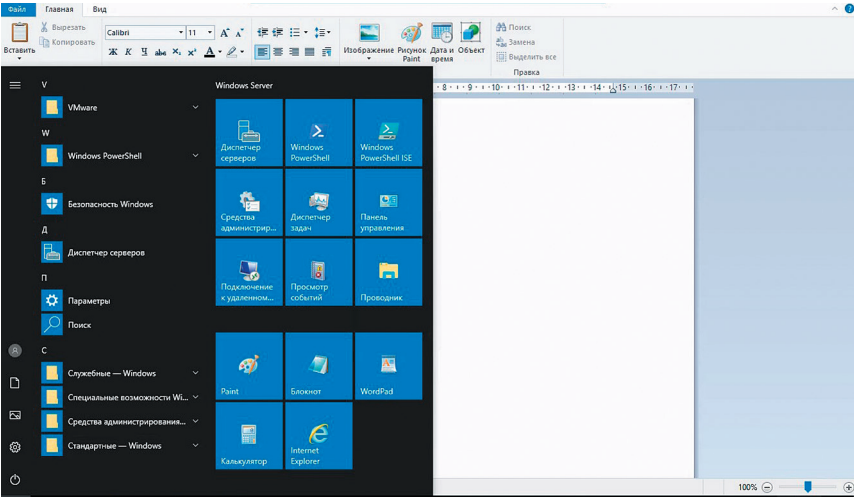
При этом важно понимать: сама база, документы и отчеты физически находятся на сервере организации, а не на флешке и не на диске компьютера, с которого мы подключались. Завершили сессию, выключили компьютер — никаких временных файлов, кэшей 1С или следов работы на локальном диске не осталось.

С точки зрения ИБ это принципиально иная модель по сравнению с обычным ноутбуком, где вся база и вложенные документы могут быть локально скопированы, экспортированы или просто забыты в кэше. Здесь пользователь

получает не полноценную копию системы, а контролируемое окно в нее.

Отдельно хочу остановиться на работе с Termidesk — это принципиально значимая часть тестирования, поскольку речь идет об отечественной VDI-платформе, актуальность которой сейчас растёт вместе с общим переходом на импортонезависимую инфраструктуру.

В отличие от RDP, который является просто протоколом подключения к конкретной машине, Termidesk — полноценная система виртуализации рабочих столов с собственным брокером соединений, аналог западных VDI Horizon



или Citrix, но уже адаптированный под российские реалии и способный работать в связке с отечественными гипервизорами.

Важная деталь: при работе через Termidesk конфигурирование доступа к конкретным удаленным ресурсам выполняется уже не на уровне носителя Aladdin LiveOffice, а на уровне сервера Termidesk, то есть администратор VDI-платформы сам решает, какому сотруднику назначить одну виртуальную машину, а какому — несколько. В рамках тестирования мы подключились через клиент «Термидеска» к виртуальной машине на базе Astra Linux. Подключение прошло стабильно, задержек и артефактов изображения не заметили, что для терминального режима является ключевым показателем.

Очень порадовало, что список поддерживаемых VDI-решений не ограничивается одним Termidesk — сюда также входят VDI Horizon и Citrix, что дает организациям возможность выбрать привычную им платформу без необходимости полной перестройки инфраструктуры под требования конкретного тонкого клиента.

RDP и другие сценарии

Помимо 1С и Termidesk, мы протестировали и стандартное RDP-подключение — к тестовой Windows-машине. Здесь предусмотрено два варианта аутентификации: с сохранением пароля на смарт-карте устройства либо строгая двухфакторная аутентификация по сертификату, когда пользователю достаточно ввести ПИН-код смарт-карты, а сам пароль от домена он попросту не знает и не может использовать где-либо еще.

Подключение прошло штатно, встроенный в Astra Linux клиент FreeRDP оказался вполне стабильным. По собственному опыту и опыту разработчиков, для комфортной работы в терминальном режиме на один экран в Full HD достаточно канала около 1 Мбит/с — цифра не выглядит пугающей даже для не самого быстрого мобильного Интернета в дороге.

Что решение запрещает и почему это правильно

В базовой конфигурации Aladdin LiveOffice не дает подключить внешние накопители, печатать документы на локальном или сетевом принтере, произвольно скачивать файлы из Интернета или передавать их в корпоративную систему. Обычного веб-серфинга тоже нет: браузер может быть добавлен по запросу заказчика, но по умолчанию лишние приложения из образа исключены. На первый взгляд это выглядит как избыточная строгость, но на практике логика понятна: чем меньше возможностей у пользователя вне контролируемого сценария, тем меньше поверхность атаки и тем проще администратору быть уверенным в конфигурации каждого выданного носителя.

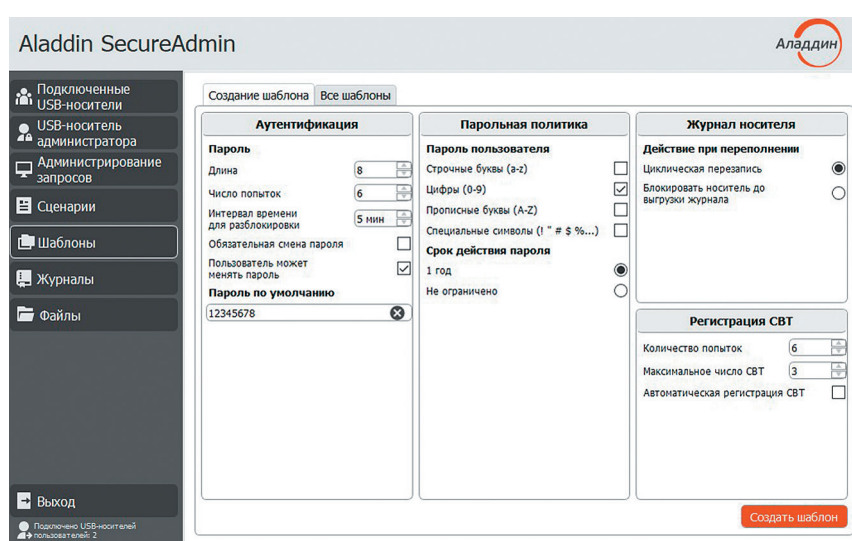
При этом гибкость сохраняется: если у заказчика есть реальная бизнес-потребность — печать документов, специфический браузер для работы с порталом, ВКС-клиент для совещаний — вендор идет навстречу и предоставляет отдельный образ с включенным функционалом. Управление при этом остается полностью на стороне ИТ-службы клиента.

Администрирование без выделенного сервера

Вся эта конструкция управляется через программу Aladdin SecureAdmin, которая работает локально и не требует развертывания отдельного сервера. Администратор создает ключи инициализации носителей, задает политики паролей, регистрирует разрешенные компьютеры, загружает пользовательские профили, VPN-контейнеры и приложения.

Поддерживаются групповые операции сразу над несколькими устройствами, ролевое разделение полномочий между администраторами разных подразделений, ведение журналов безопасности.

Отдельно порадовала возможность удаленной помощи пользователю через безопасный проброс носителя по сети к рабочему месту администратора —



сценарий особенно ценен, когда сотрудник и специалист поддержки физически разнесены на тысячи километров.

Впечатления

Признаться, когда читаешь сухое описание на сайте — со всеми этими СКЗИ, сертификатами ФСТЭК и терминами про доверенную загрузку — складывается впечатление некой сложной, тяжелойесной технологии для избранных. На практике все оказалось приземленнее и понятнее. Обычный пользователь просто вставляет флешку, вводит пароль и через некоторое время оказывается в привычной рабочей среде — будь то 1С или другая корпоративная система. Подключение при этом работает гладко и через Termidesk, и через обычный RDP. Вся сложность и вся защита остаются на уровне архитектуры, невидимой для конечного сотрудника.

Отдельного упоминания заслуживает продуманность мелких деталей: привязка носителя к конкретному компьютеру, дистанционная регистрация нового устройства взамен вышедшего из строя, отсутствие локальных следов работы после завершения сессии, разделение ролей администраторов. Каждая из этих деталей закрывает вполне реальный, а не гипотетический риск.

В итоге Aladdin LiveOffice оставляет хорошее впечатление как инструмент для удаленной работы с корпоративными приложениями, в протестированном нами сценарии — непосредственно с 1С. Решение сочетает удобство с эффективным использованием удаленной инфраструктуры: сотруднику не требуется отдельный настроенный рабочий компьютер, а подключение к корпоративной системе можно организовать из различных мест.

В первую очередь решение можно рекомендовать компаниям, сотрудники которых регулярно используют 1С удаленно, в командировках или с разных рабочих мест, но при этом организация хочет сохранить контроль над корпоративной инфраструктурой и данными, соответствовать требованиям регуляторов (сертифицированы все программные компоненты между пользователем и целевым сервисом) и получить комплексное решение от вендоров, давно и успешно реализующих совместные проекты. Особенно актуален Aladdin LiveOffice для компаний, которым важно быстро организовать защищенный доступ к корпоративным системам без необходимости оснащать каждого сотрудника отдельным служебным ноутбуком. **P**