

# Управляемый USB-over-IP-концентратор DistKontrolUSB от компании «ДистКонтрол» — незаменимый помощник в организации удаленного доступа в локальную сеть



В статье рассматриваются особенности, принцип работы, характеристики и преимущества управляемого USB-over-IP-концентратора DistKontrolUSB производства подмосковной компании «ДистКонтрол», обеспечивающего подключение USB-устройств, в том числе ключей различного типа, к компьютерной сети. Показана эффективность устройства и необходимость его применения при введении новых поправок к Федеральным законам № 63-ФЗ об электронной подписи и № 377-ФЗ об электронном документообороте.

Журнал «ИСУП», г. Москва

Электронный документооборот в России набирает популярность и в некоторых областях стал уже необходимым для исполнения. При этом значительно увеличивается количество организаций и документов, требующих использования ключей шифрования, включая электронную подпись (ЭП), стремительно растет и число работников, использующих такой способ аутентификации (идентификации, верификации) человека при оформлении документов самого разного вида и назначения. Вместе с тем все больше обостряются и проблемы, связанные с защитой ключей шифрования и исключением их потерь, обеспечением подключения все большего числа использующих их сотрудников к компьютерной сети, исключением несанкционированного доступа и т.д.

При решении этих проблем наиболее удачным является использование бизнес-модели USB over IP. Она известна достаточно давно — такая технология предусматривает подключение (проброс) всех USB-девайсов к одно-

му устройству (концентратору), а все допущенные специалисты работают с ними как с локальными. Применение такой бизнес-модели позволяет значительно упростить работу и снизить эксплуатационные расходы не только крупных объединений и предприятий, но и небольших организаций, и даже обычных пользователей. Например, с помощью технологии USB over IP появляется возможность пробросить аппаратный USB-ключ защиты ПО внутрь облачной платформы (или облака на базе VMware), что позволит использовать его так, будто он установлен на локальной машине, конечно, если это не будет вступать в противоречие с лицензионным соглашением.

Сегодня устройства USB over IP для организаций и компаний, использующих ключи шифрования, просто необходимы, поэтому спрос на них со стороны организаций и предприятий практически всех отраслей народного хозяйства России значительно вырос. Во многом это связано с новыми, действующими с 1 января 2022 года, тре-

бованиями государственных органов в отношении оформления и получения электронной подписи, сертификата квалифицированной электронной подписи (КЭП) и т. п.

В 2021–2022 годах вступили в силу поправки к Федеральному закону № 63-ФЗ «Об электронной подписи», появились соответствующие подзаконные акты и разъяснения по новым правилам получения и работы с КЭП в организациях, у индивидуальных предпринимателей и нотариусов.

В частности, с 1 января 2022 года функции по выпуску КЭП для юридических лиц индивидуальных предпринимателей и нотариусов возлагаются на Федеральную налоговую службу РФ. Теперь при обновлении КЭП или ее смене они должны обращаться в ФНС или аккредитованные ею удостоверяющие центры (АУЦ).

С 1 марта 2022 года работники смогут переходить на новые правила, предусматривающие использование для подписания документов не только электронной подписи физлица,

но и машиночитаемой доверенности (МЧД). Подчеркнем, что это будет электронная подпись именно физического лица без указания данных организации, в которой этот человек работает. С 1 января 2023 года требование перехода физических лиц на новые правила (ЭП и МЧД) становятся обязательными. Еще одно важное новшество: в отличие от КЭП руководителя организации, подпись работника будет без запрета на копирование или включение расширений.

Необходимо отметить, что повышению спроса на USB-концентраторы способствует еще один важный нормативный документ – Федеральный закон от 22 ноября 2021 г. № 377-ФЗ, который предусматривает возможность в рамках электронного документооборота (ЭДО) в том числе создавать, подписывать и хранить кадровые документы в электронном виде. Поэтому, несомненно, в локальных сетях компаний всех уровней, внедряющих электронный документооборот, появится потребность в приобретении этих устройств.

Сегодня на уровне лучших зарубежных производителей устройств USB over IP на российском рынке работает практически одно предприятие – это созданное в 2011 году ООО «ДистКонтрол», разработчик и изготовитель современного высокотехнологического оборудования передачи данных, в том числе для организации удаленной работы. Продуктовая линейка компании включает: управляемые концентраторы и хабы USB over IP, системы мониторинга несущих конструкций (СМИК), систему «Фотоэксперт» (оборудование для

фотоконтроля), а также оборудование для систем «умный дом» и интернета вещей (IoT) серии «Циркон».

Основной функцией управляемого USB-over-IP-концентратора DistKontrolUSB (рис. 1) является подключение к компьютерной сети токенов электронной защиты (типа Token, ruToken, ESMART Token, JaCarta, LT и др.), токенов с электронной цифровой подписью и ключей для:

- ▶ программных продуктов ФНС;
- ▶ единых государственных реестров (ЕГР) юридических лиц и индивидуальных предпринимателей;
- ▶ единой платформы 1С для автоматизации деятельности организации (бухгалтерского, кадрового, управленческого, финансового и других видов учета);
- ▶ клиент-банков;
- ▶ электронных торговых площадок и т. д.

При этом концентратор дает возможность всем ее пользователям удаленно управлять физическим подключением USB-девайсов к своему компьютеру (ноутбуку, планшету, телефону). Кроме того, устройство предусматривает и возможность подключения самой разнообразной периферийной техники – сканеров, принтеров, МФУ, сенсоров и т. д.

Концентратор DistKontrolUSB работает на аппаратном уровне – он пробрасывает в сеть не подключенные USB-устройства, а именно порты (рис. 2). Очевидно, что аппаратные решения предоставления USB по локальной сети в несколько раз стабильнее программных решений. Поэтому на уровне пользователя аппаратные решения в этом случае выглядят так,

как будто данный конкретный USB-накопитель вставили в порт компьютера напрямую.

Для подключения к серверу с USB-устройством и эмуляции (имитации работы одной системы средствами другой без потери функциональных возможностей и искажений результатов) устройства на компьютере используется клиентская программа DistKontrolUSB Client, которая способна работать и как обычное приложение, и в качестве службы (сервиса). Запуск пользователя как службы дает возможность применять устройства без требования входа клиента в систему, при этом пользователь будет работать в фоновом режиме непрерывно.

Управляемый USB-over-IP-концентратор DistKontrolUSB обладает несколькими степенями защиты. Прежде всего, это авторизация при подключении USB-устройств с использованием персональных логина и пароля. Кроме того, в концентратор заложена функция ограничения доступа по IP-адресу через брандмауэр, осуществляющий контроль и фильтрацию входящего/исходящего трафика, – входить в сеть можно только с IP-адреса, закрепленного за конкретным сотрудником. Также в брандмауэре оговорены права пользователя на отводимые порты. Особо отметим, что это единственное решение на рынке, позволяющее помимо назначения прав на использование USB-устройств осуществлять и визуальное скрывание USB-устройств для пользователей, которым оно не назначено.

Физическое включение и выключение USB-устройств осуществляется удаленно. Функция отключения пользователя по времени позволяет делегировать отдельным работникам права на порты для того, чтобы они могли самостоятельно управлять питанием.

Дополнительно для регистрации несанкционированного доступа используется системный журнал программы управления концентратором, в котором хранится вся информация по подключениям/отключениям как портов концентратора, так и любого из используемых USB-устройств. В журнале также регистрируется вся информация о неправильных попытках ввода логина, пароля и IP-адресов, с которых осуществлялись эти попытки. В устройстве предусмотрен мони-



Рис. 1. USB-over-IP-концентратор DistKontrolUSB

торинг эксплуатации концентратора с сообщениями информации о его состоянии по e-mail.

Важно, что потери сотрудниками ключей при использовании DistKontrolUSB исключаются, поскольку само устройство не покидает офисного помещения. Используется в концентраторе и сквозное SSL-шифрование (*от англ. Secure Sockets Layer* – уровень защищенных сокетов), позволяющее кодировать информацию с целью более безопасного обмена данными.

Для включения и отключения портов управляемого концентратора USB over IP (подключенных к нему USB-устройств) можно использовать: веб-интерфейс; планировщик задач и назначенных заданий; утилиту управления концентратором (скриптами из командной строки или своего приложения); клиентское приложение (работающее в графическом режиме или в виде службы), а также API (скриптами из командной строки или своего приложения).

Концентратор DistKontrolUSB предусматривает ограничение USB-портов по току, а также схему выключения при перегреве. Реализация этих функций обеспечивает защиту нагрузки от нештатных ситуаций. В случае перегрева выход блокируется вплоть до устранения неисправности, удаление нагрузки перезагрузит USB-вход. Кроме того, чтобы минимизировать броски пускового тока в ситуациях с высокой емкостной нагрузкой, в устройство заложена схема плавного запуска USB-портов. Также концентратор обеспечивает минимальный ток нагрузки на один порт (0,5 А) при ограничении тока, потребляемого нагрузкой (величина предельного тока нагрузки – 0,9 А).

К концентратору одновременно может быть подключено любое количество компьютеров. Использование одного USB-устройства одновременно несколькими хостами не допускает протокол USB. То есть в одну единицу времени одним портом может пользоваться один компьютер, при этом пользоваться концентратором может неограниченное количество компьютеров. Ограничения заложены в самом протоколе (спецификации) USB.



Рис. 2. Концентратор DistKontrolUSB с подключенными портами

Возможность подключения управляемого концентратора USB over IP к нескольким USB-хостам одновременно создает условия для продолжения использования USB-устройств в кластерных системах. При этом следует отметить, что концентратор DistKontrolUSB тестировался совместно с платформами виртуализации сервера VMware и Microsoft Hyper-V.

Концентратор может устанавливаться в стойку стандартных размеров – 1, 2 или 4 юнита в зависимости от количества портов.

Управляемые USB-over-IP-концентраторы DistKontrolUSB имеют сертификаты соответствия требованиям стандартов ГОСТ Р и ЕАС, а также пожарной безопасности. Устройство внесено в Единый реестр уведомлений Центра по лицензированию, сертификации и защите государственной тайны ФСБ России. Кроме того, важным для клиентов компании «ДистКонтрол» элементом является наличие сертификатов совместимости драйвера DistKontrolUSB client с операционными системами общего и специального назначения Astra Linux Common Edition.

Основное преимущество управляемых USB-over-IP-концентраторов производства ООО «ДистКонтрол» – цена, которая при таких же характе-

ристиках гораздо ниже, чем у зарубежных аналогов. Особенно это заметно при пересчете стоимости изделия на один порт.

Уровень разработки устройства DistKontrolUSB, его технических и эксплуатационных характеристик, качества изготовления подтверждает список пользователей продукции компании. В него входят крупнейшие государственные структуры, банки, научные центры, промышленные объединения и предприятия самых разных отраслей России: Федеральная налоговая служба РФ, ГК «Агентство по страхованию вкладов», Пенсионный фонд РФ, ПАО Сбербанк, ПАО ВТБ, АО «Тинькофф Банк», ПАО «Газпром», ПАО «Транснефть», ПАО «Татнефть», ПАО «Промсвязьбанк», АО «Яндекс Банк», ООО «Эвотор», АО «Корпорация «Глория Джинс», ПАО «МТС», ПАО «Мегафон», ЗАО «КОНСУЛЬТАНТ ПЛЮС», АО «ПФ «СКБ Контур», АО «Шереметьево-Карго» и др.

Следует отметить и тот факт, что продукция ООО «ДистКонтрол» стала ярким примером успешного импортозамещения, что очень важно в условиях развязанных западными странами санкционных войн.

Журнал «ИСУП», г. Москва