ОБЛАЧНЫЙ СЕРВИС ВКС

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гороховик В.А., Тарасовец В.В.

Лагутин А.Е. – к.т.н.

Бизнес будет всегда стремиться к тому, чтобы увеличить скорость принятия решений и качество внутренних и внешних корпоративных коммуникаций. Сегодня особенно актуально при этом достичь ещё и максимальной экономии средств. Наиболее проверенный и эффективный способ сократить расходы – использовать видеоконференцсвязь (ВКС) вместо командировок для проведения совещаний и рабочих встреч. Многие компании строят собственную ВКС-инфраструктуру. Однако есть еще один способ, который позволяет избежать капитальных затрат на ее (инфраструктуру) создание или модернизацию, получив при этом требуемый для поддержания бизнес-процессов сервис. Это видеоконференцсвязь как услуга из облака.

Круг компаний, которым нужна видеоконференцсвязь, очень широк: промышленность, ТЭК, финансовой сектор, ритейл. Главные условия – наличие удаленных офисов и потребности в общении с сотрудниками, подрядчиками, партнерами не только на уровне директивных писем и отчетов. Любые совещания, переговоры, обучающие семинары могут проводиться с минимальным вложением средств. Благодаря ВКС исключаются расходы на авиа и ж/д билеты, на гостиницы и командировочные.

Сервис ВКС из облака позволяет участвовать не только в конференциях, но и пользоваться единым списком контактов, обмениваться мгновенными текстовыми сообщениями, совместно работать над документами, осуществлять запись видеосеансов.

Особенности подключения

Для подключения облачной видеоконференцсвязи не нужно ничего, кроме конечного оборудования в переговорных комнатах. Если у заказчика нет такого оборудования, его можно взять в аренду.

Принять участие в сеансе видеосвязи можно также и с мобильных устройств посредством программного клиента. Точно так же, как пользователи работают с облачной почтой или мессенджерами, они могут подключаться к ВКС со своих планшетов, телефонов или ноутбуков[1].

Структурная схема облачной видеоконференции представлена на рисунке 1.

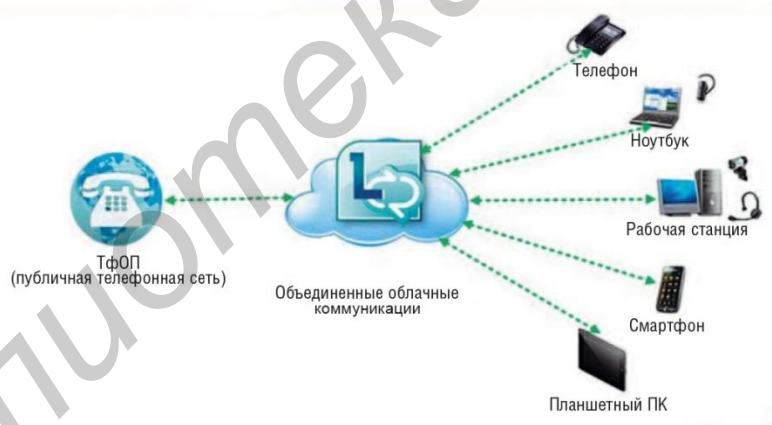

Рисунок 1 – Структурная схема облачной видеоконференции

Внешние участники, компании которых не имеют собственной ВКС-инфраструктуры, подключаются через web-браузер или систему унифицированных коммуникаций Skype for Business (Microsoft Lync).

Одним из главных преимуществ облачной услуги ВКС является возможность не вкладываться в закупки дорогостоящего оборудования для проведения видеосеансов. Вместо этого заказчик по подписке получает сервис, уже развернутый в ЦОДе системного интегратора.

Управление и оптимизация

Облачной ВКС просто управлять и возможно быстро масштабировать по запросу, например, когда требуется провести расширенную встречу. И неважно, что такое может быть нечасто, а обычная нагрузка – совещание на 5–10 человек. Когда компания создает такую технологически гибкую ВКС на базе собственной инфраструктуры (иными словами обеспечивает на постоянной основе возможность проведения сеансов видеоконференцсвязи на 50–100 человек) техническое обслуживание и модернизация обходятся достаточно дорого[2].

Кроме того, с помощью облачной ВКС компания-заказчик может оптимизировать расходы на ИТ-персонал. Инфраструктуру на стороне системного интегратора нет необходимости администрировать, держать для этого отдельных сотрудников или давать дополнительную нагрузку на существующих. Для заказчика все происходит автоматически: пользователи звонят на номера общей конференции и включаются в нее. Но по желанию заказчика инструменты управления услугой могут быть предоставлены его ИТ-службе.

Безопасность передачи данных заказчиков при использовании услуги ВКС, как правило, обеспечивается на нескольких уровнях. В рамках первого уровня защита подключения к конференции осуществляется при помощи паролей (PIN-кодов) и управления списком участников заказчиком, в рамках второго – посредством подключения выделенного канала связи и специальных средств шифрования трафика, доступно опционально[2].

Записи переговоров заказчиков хранятся в дата-центре, который надежно защищен от сетевых угроз, будь то DDoS-атаки, попытки несанкционированного доступа или сетевое сканирование. Для этого применяются различные средства защиты: системы обнаружения и предотвращения вторжений (IDS/IPS), системы предотвращения DDoS-атак и пр.

Список использованных источников:

1. Polycom [Электронный ресурс]. – Режим доступа : http://www.polycom.com.ru.

2. Интернет-издание о высоких технологиях [Электронный ресурс]. – Режим доступа : http://www.cnews.ru.