

МАТЕМАТИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ ЭКОНОМИКИ

УДК 621.395:004.1

Русев Е.

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ IP-ТЕЛЕФОНИИ ДЛЯ МАЛОГО И СРЕДНЕГО БИЗНЕСА: ПРЕИМУЩЕСТВА, НЕДОСТАТКИ, ПЕРСПЕКТИВЫ РАЗВИТИЯ

*Русев Евгений**; ФГБОУ ВО «Орловский государственный университет экономики и торговли»; РФ, 302028, г. Орел, ул. Октябрьская, д. 12; e-mail: ms.jeka@mail.ru

В статье рассмотрено применение технологии VoIP для малого и среднего бизнеса. Отмечены преимущества VoIP по сравнению с классическими АТС. Описаны основные протоколы, которые используются VoIP, их основные объекты и компоненты. Отдельное внимание уделено преимуществам использования VoIP для малого и среднего бизнеса в условиях снижения покупательской способности потребителей. Наряду с преимуществами указаны недостатки VoIP и сделаны выводы о перспективах развития технологии.

Ключевые слова: IP-телефония, VoIP, VoIP-протоколы, качество связи, коммуникация, каналы общения.

Rusev E.

IP-TELEPHONY TECHNOLOGY FOR SMALL AND MEDIUM-SIZED BUSINESS: ADVANTAGES, DISADVANTAGES AND DEVELOPMENT PROSPECTS

Rusev Eugene; Orel State University of Economics and Trade; 12 Oktyabrskaya Street, Orel 302028, Russian Federation; e-mail: ms.jeka@mail.ru

Use of VoIP technology for small and medium-sized business is considered in the article. VoIP advantages in comparison with classical automatic telephone exchanges are described. The basic protocols which VoIP uses are described and their basic objects and components are also considered. Special attention is paid to the advantages of VoIP use for small and medium-sized business under conditions of decrease in purchase ability of consumers. Along with the advantages VoIP disadvantages are considered and conclusions are made about the development prospects of the technology.

Keywords: IP-telephony, VoIP, VoIP protocols, communication quality, communication, communication channels.

Одной из основных задач IT-службы предприятия является обеспечение постоянной бесперебойной высококачественной коммуникации между ее сотрудниками. Так, официальным каналом общения на предприятии является почта как виртуальная, так и реальная для письменного общения и телефония для устного общения. В современных IT-инфраструктурах предприятий с каждым днем все реже можно встретить так называемые «legacy» (традиционные) АТС. Это в первую очередь объясняется тем, что современные технологии не стоят на месте, а применение самых передовых технологий становится все более доступным. В этой статье мы рассмотрим применение VoIP для малого и среднего бизнеса, достоинства и недостатки технологии, а также перспективы ее развития.

VoIP-технология (Voice over IP) – технология передачи голоса поверх протокола IP, иными словами IP-телефония – это и есть VoIP. Под IP-телефонией подразумевается набор

* Научный руководитель: Смагина Ирина Валерьевна, к.э.н., доцент; e-mail: irina-smag@yandex.ru

коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видеообщение по сети Интернет или любым другим IP-сетям. Протоколы обеспечивают регистрацию клиентского устройства (шлюз, терминал или IP-телефон) на сервере, вызов и/или переадресацию вызова, установление голосового или видеосоединения, передачу имени и/или номера абонента. Сигнал по каналу связи передаётся в цифровом виде и, как правило, перед передачей преобразовывается (сжимается) для того, чтобы удалить избыточность информации и снизить нагрузку на сеть передачи данных.

Говоря о технологии VoIP, необходимо рассмотреть основные протоколы, которые используются для реализации данной технологии. На данный момент существует несколько стандартизованных протоколов, на базе которых строятся системы IP-телефонии. Рассмотрим некоторые из них более подробно. Важным протоколом является протокол H.323.

К числу объектов стандарта H.323 относятся:

Терминал (Terminal) – конечное H.323-устройство пользователя. Может быть как аппаратным (телефонный аппарат), так и программным (приложение на компьютере). Терминалам могут назначаться один или несколько псевдонимов (номера телефонов, названия).

Шлюз (Gateway) – устройство, предназначенное для сопряжения разнородных сетей. Так, рекомендации ITU-T содержат информацию по сопряжению H.323-устройств с устройствами сетей ISDN, ATM и ТФОП.

Устройство управления конференциями (Multipoint Control Unit – MCU). Предназначено для ситуаций, когда необходимо организовать конференцию с числом участников более трех. Оно координирует передачу управляющей информации между участниками конференций.

Привратник (GateKeeper) – основной управляющий элемент сети H.323, координирующий и контролирующий работу всех ее устройств.

Другим важным протоколом является SIP-протокол, который представляет собой протокол для сигнализации и управления мультимедийными сеансами связи. Наиболее распространённые области применения в интернет-телефонии – для передачи голоса и осуществления видеозвонков, а также обмена мгновенными сообщениями по сетям IP (Internet Protocol). Он используется для создания, изменения и разрыва «сессий» между одним или несколькими участниками. Понятие «сессии» в протоколе SIP достаточно широкое. Под «сессией» могут подразумеваться не только телефонные звонки, но и передача данных, конференции, децентрализованные игры и т.д. SIP регламентирует только процедуру установки соединения между устройствами, поэтому обычно, наряду с SIP, используется протокол передачи информации. В случае IP-телефонии в качестве таких протоколов выступают RTP и SDP.

Рассмотрев принципы работы VoIP, определим основные причины перехода от традиционных АТС на IP-телефонию.

1. В рамках технологии VoIP телефонный звонок идет через интернет, а не через телефонную сеть, построенную оператором связи. Вы можете позвонить бесплатно сотруднику, который находится в другой стране, если он подключен к вашей IP – АТС (например, через программный телефон на его мобильном). Звонки на мобильные номера получаются также дешевле, поскольку большую часть пути до вызываемого абонента звонок идет через интернет, и только в конце переходит к поставщику телефонных услуг для терминирования звонка.

2. Пользователи традиционных АТС привыкли, что для проверки голосовой почты нужно набрать определенный номер, прослушать сообщение и удалить его. С VoIP-технологиями голосовое сообщение будет приходить вложением на ваш адрес электронной почты, причем есть возможность распознать его содержимое и прислать его в качестве текста.

3. Упрощение работы с факсами. В IP-телефонии факс будет приходить на адрес электронной почты с указанием того, кто его прислал, когда и во сколько. Такой функционал позволяет избежать лишних затрат на факсимильные аппараты.

4. Возможность использования сервисов самообслуживания, которая позволяет пользоваться умными IVR (Interactive Voice Response) – системами голосового меню, в котором

клиент сможет сам найти ответ на свой вопрос.

Рассмотрим преимущества использования VoIP-технологии для малого и среднего бизнеса. В условиях снижения покупательской способности и перенасыщенности рынка товарами и услугами каждая компания стремится минимизировать расходы с целью повышения маржинальности своего продукта. В таком разрезе применение IP-телефонии – идеальное решение, так как основное преимущество ее использования - это экономия. По данным многочисленных исследований, внедрение IP-телефонии позволяет уменьшить расходы на связь от 50 до 75%. Это обусловлено тем, что IP-телефония работает немного иначе, чем обычная старая телефонная связь. Компании не нужно приобретать огромное количество дополнительного оборудования, протягивать кабели, отводить отдельное помещение под громоздкую телефонную станцию и т.п. Так как мы говорим об использовании IP-телефонии для малого и среднего бизнеса, где штат образован относительно небольшим количеством людей, то для организации связи подойдет небольшой сервер, который может работать на обычном компьютере. В качестве станций можно использовать как стационарные телефоны, так и мобильные телефоны или даже программу на компьютере. Такое преимущество очень удобно: если появляется новый сотрудник, его можно оперативно подключить к общей сети.

Основные преимущества VoIP-технологии отражены на рисунке 1.



Рисунок 1 – Преимущества VoIP-технологии перед классическими АТС

Как уже говорилось ранее, основное и немаловажное преимущество IP-телефонии – это экономичность. Практически все компании работают со своими клиентами по телефону и вынуждены закладывать в бюджет средства на телефонную связь. Конечно, последнее время на рынке появляется огромное количество «выгодных» коммерческих предложений для корпоративных клиентов, но ни одно из них не сравнится с экономией от использования IP-телефонии.

Другим немаловажным преимуществом является качество связи. Использование современной телефонной системы позволит избежать проблем с качеством звука и даст уверенность, что никакой сбой не мешает работе.

IP-телефония позволит подстроиться под любую задачу для вашего бизнеса. Ее можно успешно интегрировать с используемой CRM и сразу получать в ней карточку клиента, управлять и принимать вызовы, хранить записи звонков и быть уверенным, что у вас не затеряется ни один клиент.

Еще одним скрытым, но важным преимуществом является уменьшение времени обработки звонка. Среднее время обработки звонка при использовании аналоговой телефонии – 1 минута 30 секунд, в то время как среднее время обработки звонка в IP-телефонии – 40 секунд. Такая существенная разница позволяет уменьшить «бесполезное время ожидания», что особенно важно в работе тех людей, которые регулярно совершают звонки (например, сотрудники call-центров).

Преимущества использования такой технологии очевидны, так как они напрямую связаны с затратами предприятия. Однако у каждой технологии есть свои недостатки, уязвимости и ограничения, и VoIP не исключение.

Одна из проблем – проблемы с NAT. NAT (от англ. Network Address Translation – «преобразование сетевых адресов») – это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Чтобы позволить устройству с приватным IPv4-адресом обращаться к устройствам и ресурсам за пределами локальной сети, приватный адрес сначала должен быть переведен на общедоступный публичный адрес. И вот как раз NAT переводит приватные адреса в общедоступные. Это позволяет устройству с частным адресом IPv4 обращаться к ресурсам за пределами его частной сети. NAT в сочетании с частными адресами IPv4 оказался полезным методом сохранения общедоступных IPv4-адресов. Один общедоступный IPv4-адрес может быть использован сотнями, даже тысячами устройств, каждый из которых имеет частный IPv4-адрес. NAT имеет дополнительное преимущество, заключающееся в добавлении степени конфиденциальности и безопасности в сеть, поскольку он скрывает внутренние IPv4-адреса из внешних сетей. Маршрутизаторы с поддержкой NAT могут быть настроены с одним или несколькими действительными общедоступными IPv4-адресами. Эти общедоступные адреса называются пулом NAT. Когда устройство из внутренней сети отправляет трафик из сети наружу, то маршрутизатор с поддержкой NAT переводит внутренний IPv4-адрес устройства на общедоступный адрес из пула NAT. Для внешних устройств весь трафик, входящий и исходящий из сети, выглядит имеющим общедоступный IPv4-адрес. Маршрутизатор NAT обычно работает на границе Stub-сети. Stub-сеть – это тупиковая сеть, которая имеет одно соединение с соседней сетью, один вход и выход из сети. Когда устройство внутри Stub-сети хочет связываться с устройством за пределами своей сети, пакет пересылается пограничному маршрутизатору, и он выполняет NAT-процесс, переводя внутренний частный адрес устройства на публичный, внешний, маршрутизируемый адрес. Сигнальные протоколы SIP и H.323 работают, обмениваясь сообщениями с сервером IP-телефонии. Пользователь, который совершает звонок, и пользователь, который принимает его, могут находиться в разных сетях за NATирующими устройствами. Несмотря на это, VoIP-трафик может дойти до сервера и пользователи услышат звонок, после того как параметры вызова будут полностью согласованы. Как только пользователь, принимающий звонок, поднимет трубку, в дело вступает медиапротокол RTP, который будет отправлять пакеты на внутренний адрес удаленного телефона (так как именно внутренний адрес будет указан в предшествующих SIP/H.323 заголовках), вместо того чтобы отправлять их на правильный NATируемый адрес. Но даже если RTP-пакеты будут отправляться на правильный NATируемый IP-адрес, большинство межсетевых экранов, особенно без соответствующей настройки, будут выкидывать такие пакеты. Поэтому, если принято решение о внедрении IP-телефонии и в компании есть удаленные сотрудники или филиалы, необходимо разбираться в теории NAT и правильно настраивать Firewall.

Другая проблема – возможные сложности с качеством связи. Сети с коммутацией каналов (ТФОП) гарантируют отличное качество передаваемой аудиоинформации, поскольку не делят среду передачи с другими сервисами. IP-телефония, как правило, пересекается с другим пользовательским трафиком, таким как почта и интернет. Поэтому, чтобы достичь такого же хорошего качества голоса при использовании IP-телефонии, зачастую приходится правильно настраивать приоритизацию трафика или даже обновлять имеющуюся инфраструктуру.

Еще одним негативным аспектом является отсутствие возможности определения местоположения звонящего. В случае с сетями с коммутацией каналов информация о местоположении абонента записывается всего раз при непосредственном предоставлении абоненту сервиса и изменяется только в том случае, если он перемещается, при этом номер за ним сохраняется. В случае с сетями подвижной сотовой связи информация о местоположении абонента может быть определена при помощи метода триангуляции по имеющимся координатам базовых станций (мобильных вышек) или при помощи GPS-координат, которые сообщает мобильный телефон абонента. В сетях VoIP нет простого способа определения местоположения звонящего, чем очень часто пользуются мошенники, вымогатели и другие сомнительные личности. Кто-то может подумать, что это и хорошо: зачем кому-то давать возможность узнать Ваше местоположение? Но подумайте о безопасности своей и своих сотрудников. В случае звонка на номер экстренных служб в чрезвычайной ситуации, они также не смогут определить где находится звонящий, а это может стоить кому-то жизни.

Рассмотрев преимуществ и недостатки, необходимо поговорить о перспективах развития технологии. Как и в любой информационной системе, здесь речь идет в первую очередь об улучшении безопасности. Если раньше, выбирая, на чём строить офисную телефонию, заказчиков больше всего волновали вопросы стоимости и надёжности, то в связи с нынешним положением вопросы защиты и безопасности всё чаще начинают преобладать. Хотя IP-телефония имеет массу преимуществ по сравнению с системами традиционной телефонии, её намного легче взломать. В случае с традиционной системой PSTN злоумышленник должен получить физический доступ к среде передачи или системам, которые задействованы в обмене голосовой информацией. IP-телефония – это, прежде всего, сеть с коммутацией пакетов, которые передаются наряду с другими корпоративными сервисами: интернетом, почтой и другими. Если эта сеть недостаточно защищена, то злоумышленнику даже не обязательно находиться в одной стране с системой IP-телефонии, чтобы получить доступ к критичным данным, украсть их или модифицировать.

Вот почему необходимо обеспечивать многоуровневую защиту систем корпоративной IP-телефонии. Недостаточно просто поставить стойкий пароль к интерфейсу управления. Это должен быть чёткий набор определённых мер, применяемых в комплексе, – межсетевое экранирование, антивирусная защита, регулярные обновления программного обеспечения, шифрование передаваемых данных и другое.

Отдельно следует уделить внимание повышению осведомлённости своих сотрудников об атаках из разряда социальной инженерии. Одним из наиболее распространённых векторов атаки данного типа на сегодняшний день является «фишинг». Суть его заключается в том, что злоумышленник рассылает письма с вредоносными вложениями в надежде на то, что человек откроет это вложение и тем самым загрузит его на свой компьютер. Защититься от таких атак можно сразу на нескольких уровнях:

1. Межсетевой экран, на котором адрес отправителя фишинговых писем должен быть заблокирован. Автоматизировать процесс получения актуального списка адресов активных отправителей для блокировки на МСЭ можно с помощью решений Threat Intelligence. Существуют как платные решения от таких компаний, как Anomali, ThreatConnect или EclecticIQ, так и бесплатные OpenSource, например, YETI и MISP.

2. Решение для защиты почтового сервера, которое проверяет все письма на предмет подозрительных вложений, адреса отправителя, блокирует спам. Примерами таких решений является Kaspersky Security для почтовых серверов, AVG Email Server Edition для ME, McAfee Security for Email Servers. Кстати, в этом случае также можно автоматизировать процесс блокировки с помощью решений TI.

3. Антивирусное ПО для защиты конечных устройств, которое заблокирует опасное вложение, если всё-таки вредонос сможет пролезть через МСЭ и почтовый сервер. Для этого подойдёт Kaspersky Endpoint Security, Norton, Trend Micro и другие.

Отдельное внимание стоит уделить безопасности облачных систем. Сейчас уже слож-

но обозначить чёткие границы офисной сети. С распространением облачных решений, распределённых сетей VPN и всеобщей виртуализации корпоративная сеть уже перестала иметь чёткую географическую привязку.

Аналогично обстоят дела и в сфере VoIP. Каждый крупный провайдер IP-телефонии имеет в своем наборе услуг облачную АТС, которая настраивается в считанные минуты и способна обеспечить телефонией компанию любого размера и неважно, где территориально она расположена. Облачная или виртуальная АТС – это очень удобное решение, которое привлекает заказчиков тем, что не надо держать лишние сервера в здании и обслуживать их. Вместо этого можно просто арендовать необходимые серверные мощности или сервис телефонии. Однако с точки зрения информационной безопасности, облачные АТС – это идеальная цель для хакерских атак, потому что, как правило, аккаунты для доступа к настройкам АТС находятся в открытом доступе. Если владелец аккаунта не озаботится созданием стойкого пароля, то он рискует оплатить немаленький счёт за телефонные разговоры злоумышленника или предоставить доступ к записям разговоров своих сотрудников. В этой связи при выборе провайдера следует также проверить, обеспечивает ли он дополнительные мероприятия по защите целостности и конфиденциальности данных, используется шифрование при подключении к аккаунту с настройками облачной АТС, шифруются ли данные при их транспортировке.

Другим, наиболее распространённым методом защиты корпоративной инфраструктуры является организация защищённой сети VPN, когда подключение извне осуществляется по зашифрованному каналу, а данные внутри сети передаются в незашифрованном виде. Это относится и к голосовому трафику. Однако тенденции развития информационных технологий указывают на то, что в недалёком будущем голосовая информация также будет подвергаться шифрованию. Большинство VoIP-вендоров уже давно имплементируют в своих решениях поддержку таких протоколов, как SIP/TLS, SRTP, ZRTP и др., стимулируя пользователей применять ещё один уровень защиты. Например, большинство IP-телефонов и решений видеоконференцсвязи от компании Cisco, а также системы CUCM, CUBE, Cisco SBC, UCCS и др. поддерживают TLS 1.2 и SRTP. Самое распространённое Open Source решение IP-АТС Asterisk имеет поддержку защищённых протоколов передачи медиатрафика начиная с версии 1.8. В программной Windows-based АТС 3CX версии V15 поддержка SRTP включена по умолчанию.

VoIP-решения зачастую очень тесно интегрируются с другими корпоративными системами, такими как CRM, ERP, CMS, не говоря уже о таких каналах бизнес-коммуникаций, как e-mail, обмен мгновенными сообщениями (чат) и социальные сети, формируя в совокупности концепцию UC (Unified Communications). Потенциальные преимущества, которые несёт данная концепция, очень привлекательны, но вместе с тем создаётся множество точек, уязвимых к возможному взлому. Недостаточный уровень защиты одной из них может быть угрозой всей корпоративной сети. Поэтому разработчики, несомненно, будут усиливать безопасность каналов интеграции данных систем.

Можно также ожидать интеграцию систем корпоративной телефонии в такие средства защиты, как DLP (средства защиты от утечек), адаптации метрик VoIP в SIEM-системах (система управления информацией и событиями безопасности), а также появление унифицированных репутационных баз (Threat Intelligence) со списками потенциально опасных номеров или других индикаторов компрометации, относящихся к VoIP, которые будут автоматически блокироваться имеющимися средствами защиты.

Список источников:

1. IP-телефония [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki/IP-телефония>.
2. Атаки на VoIP: кому это выгодно? [Электронный ресурс]. – Режим доступа: <https://wiki.merionet.ru/ip-telephoniya/67/ataki-na-voip-komu-eto-vygodno/>.
3. Взаимодействие клиентов SIP [Электронный ресурс]. – Режим доступа: <https://habr.com/post/188352/>.

4. Гольдштейн Б.С, Пинчук А.В., Суховицкий А.Л. IP-телефония. – М.: Радио и связь, 2001. – 336 с.
5. Защита VoIP сетей [Электронный ресурс]. – Режим доступа: <https://habr.com/company/audiocodes/blog/270739/>.
6. Гольдштейн А.Б. Основы IP-телефонии [Электронный ресурс]. – Режим доступа: <http://iks.sut.ru/lectures/agold/>.
7. Мегеллен Д.В., Мадсен Л., Джаред С. Asterisk: будущее телефонии. - Пер. с англ. – СПб: Символ-Плюс, 2009. – 656 с.
8. Основы IP-телефонии, базовые принципы, термины и протоколы [Электронный ресурс]. – Режим доступа: <https://habr.com/post/183152/>.
9. Райт А. IP-телефония – немного теории, немного практики, немного экономики // Компас. – 2002. – №3. – с. 14-15.
10. Дмитриев Е.Е. Сокращение расходов организации путем внедрения инновационных информационных технологий // Научные записки ОрелГИЭТ. – 2016. – № 3 (15). – С. 149-156.
11. Матрохина К.В. Разработка средств защиты информации в системах корпоративной мобильной VOIP связи // Образование и наука без границ: социально-гуманитарные науки. – 2017. – № 7. – С. 13-16.

УДК 657.6:004.1

Сергеева И.И., Перелыгина Т.В.

УНИВЕРСАЛЬНЫЙ ОТЧЕТ КАК ИНСТРУМЕНТ РАСШИРЕНИЯ АНАЛИТИЧЕСКИХ МЕХАНИЗМОВ ЛИНЕЙКИ ПРОГРАММ 1С

Сергеева Инна Ивановна, кандидат экономических наук, доцент, ФГБОУ ВО «Орловский государственный университет экономики и торговли»; РФ, 302028, г. Орел, ул. Октябрьская, д. 12; e-mail: inchiksergeeva@yandex.ru

Перелыгина Татьяна Владимировна; ФГБОУ ВО «Орловский государственный университет экономики и торговли»; РФ, 302028, г. Орел, Октябрьская ул., д. 12; e-mail: ttl83@mail.ru

Основной целью любой информационной системы предприятия является сбор информации для последующего анализа и определения на его основе управленческого воздействия на бизнес-процессы предприятия. Для реализации данной цели разработчики программных продуктов линейки 1С предусмотрели широкий спектр аналитических инструментов. В их число входят, в том числе, стандартные и универсальные отчеты. Они очень гибки в настройках и доступны любому пользователю в режиме «1С:Предприятие».

Стандартные отчеты можно сформировать по системным настройкам или разработать собственный вариант отчета, задать для любого из них отборы, сортировки, группировки, оформление и расшифровки данных, а также сохранить неограниченное количество вариантов любого отчета с различными наборами настроек и выводимых данных. Для повседневного учета этого достаточно.

Инструмент «Универсальный отчет» позволяет конечному пользователю реализовать собственную аналитическую логику и дает возможность более глубокого анализа данных (например, для сравнения записей в документе и в регистрах, на основании которых он заполняется) либо для создания собственного отчета. Он помогает получать информацию, недоступную в стандартных отчетных формах, поскольку строится на основании данных списков, справочников, документов, задач, бизнес-процессов, планов видов расчета и их табличных частей, регистров накопления, регистров сведений, регистров расчета, регистров бухгалтерии и их виртуальных таблиц.

Вариантов применения «Универсального отчета» очень много, например, предложенная авторами данной статьи проверка корректности расчета среднего заработка – ключевого показателя при расчете больничного листа, отпускных, командировочных и других выплат. В каждом случае средний заработок считается по-разному и регулируется при этом законодательством РФ, поэтому степень ответственности и значимость расчета этого показателя очень высока. Стандартными