Обеспечение защищенной связи в сетях связи специального назначения

Полегенько Анастасия Михайловна,
специалист
по защите информации
«Производство и разработка»
ЗАО «ТЕЛРОС»

Гончаров Сергей Александрович,
специалист
по защите информации
«Производство и разработка»
ЗАО «ТЕЛРОС»

Сети связи специального назначения (ССОН) предназначены для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка [1].

Необходимость интеграции различных видов услуг, таких как телефония, факсимильная связь, видеосвязь, передача данных, привела к развитию традиционных телефонных и появлению мультисервисных сетей связи.

Традиционные сети связи общего пользования (ССОП) строятся на основе технологии TDM (Time Division Multiplexing — временное мультиплексирование). На современном этапе развития телекоммуникаций цифровые TDM-УАТС (учрежденческая АТС) теряют свое доминирующее положение на рынке в связи с возможностями предоставления широкого набора услуг со стороны систем, основанных на принципах пакетной коммутации при передаче данных.

Пакетная коммутация, основанная на IP-технологии, реализуется в так называемых сетях следующего поколения NGN (Next Generation Network), которые предназначены для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортировки с включенной функцией QoS [2]. Основу сетей NGN, изначально сложившихся как NGN IPCC (International Packet Communication Consortium), составляют гибкие коммутаторы Softswitch и IP-АТС. NGN представляет собой модернизированную TDM-сеть с возможностью передачи IP-трафика, а также с дополнительными возможностями предоставления услуг для конечного пользователя. Схема перехода от ССОП к мультисервисной сети представлена на рис. 1.

В настоящий момент в NGN на смену архитектуре IPCC приходит TISPAN, ключевым элементом которой является IMS (IP Multimedia Subsystem). Основное отличие NGN TISPAN (IMS) от NGN IPCC заключается в гибкости и масштабируемости таких сетей. В них функции управления сеансами и маршрутизацией выполняет CSCF (Call Session Control Function), пришедший на смену Softswitch.

С одной стороны, сети NGN IPCC/TISPAN (IMS) предоставляют широкий набор дополнительных услуг (т. н. ДВО — дополнительные виды обслуживания), которые предоставляют возможности более эффективного управления сетью по сравнению с TDM-архитектурой. С другой стороны, такой спектр функциональных возможностей увеличивает число уязвимостей и порождает источники угроз информационной безопасности. Основные и дополнительные виды услуг в сетях с различной архитектурой представлены в таблице 1.

Учитывая характер передаваемой по каналам ССОН информации, вопрос использования защищенных средств коммутации является особо актуальным. Для того чтобы средство связи могло применяться в ССОН, оно должно удовлетворять требованиям ФСБ, ФСТЭК или Минобороны России, иметь соответствующие сертификаты и заключения.

Предъявляемые требования по безопасности к средствам АТС и системам

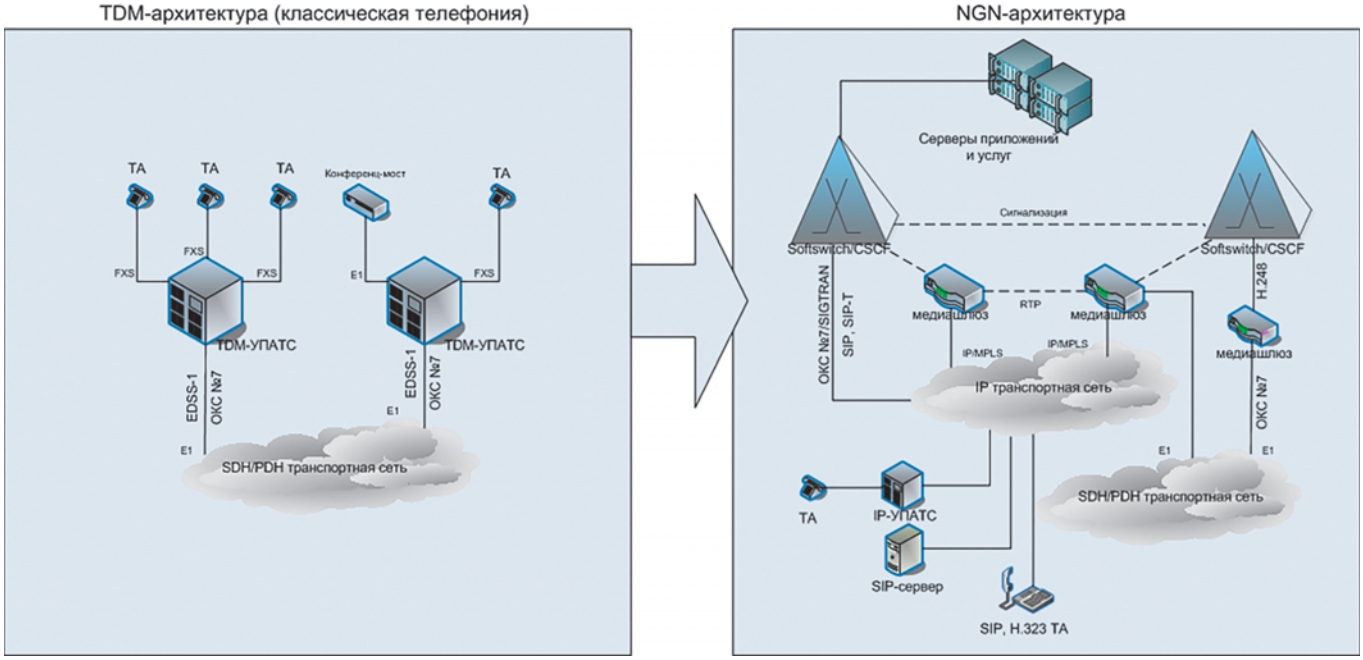

Рис. 1 Переход от TDM к NGN

Таблица 1. Список услуг, предоставляемых в различных сетях

№	Услуга / Тип сети	TDM	NGN	
			IPCC	TISPAN (IMS)
	Основные услуги			
1.	Аренда каналов	+	+	+
2.	Телефонная связь	+	+	+
3.	Передача факсимильных сообщений	+	+	+
4.	Обмен данными	+	+	+
	ДВО			
5.	Приоритетные вызовы	+	+	+
6.	Определение номера входящего вызова	+	+	+
7.	Блокировка/переадресация вызовов	+	+	+
8.	Наложенная сеть шифрованной связи (абонентское шифрование, группы)	+	+	+
9.	Доступ в сети, обрабатывающие информацию разных категорий, с одного устройства	+	+	+
10.	Голосовая/аудио/видео почта	*	+	+
11.	Информационно-справочные службы на базе IVR	*	+	+
12.	SIP-абоненты	–	+	+
13.	GUP Data Repository (хранение данных пользователя и доступ к ним с помощью RP интерфейса)	–	–	+
14.	Работа с любого места/терминала (AnyPlace)	–	–	+

Примечание: «+» — услуга присутствует в данном типе сетей;
«–» — услуга отсутствует в данном типе сетей;
«» — ограниченные возможности реализации услуги в данном типе сетей.*

Таблица 2. Основные проблемы сертификации некоторых ДВО

№	Услуга	Возможные проблемы сертификации
1.	Приоритетные вызовы	отсутствие исходных кодов ПО ПАТС
2.	Определение номера входящего вызова	отсутствие исходных кодов ПО ПАТС, а также угрозы, связанные с подменой аутентифицирующей информации (номера входящего вызова)
3.	Блокировка/переадресация вызовов	повышенные требования по защите от компьютерных атак (необходимость использования статической маршрутизации)
4.	Наложенная сеть шифрованной связи (абонентское шифрование)	нет сложностей при сертификации в случае использования сертифицированных ФСБ средств криптографической защиты при передаче сведений, составляющих гос. тайну
5.	Доступ в сети, обрабатывающие информацию разных категорий, с одного устройства	возникновение угроз, связанных с НСД (ошибки в маршрутизации для ИОД, подключение к каналам, передающим ИОД)
6.	Интеграция с компьютерными приложениями (КП)	а) для взаимодействия с КП необходима сертификация ПО АТС как ОС; б) разнообразие протоколов взаимодействия ДВО с КП, отсутствие открытых исходных кодов на КП; в) возникновение большого числа угроз информационной безопасности (компьютерные вирусы, уязвимости в ПО (НДВ) и др.)
7.	Видео/аудио связь (использование SIP-протокола)	а) разнообразие протоколов взаимодействия оконечных пользователей при установлении связи в режиме конференции; б) угрозы, связанные с передачей по сетям смешанного мультимедийного трафика (злоумышленная регистрация, срыв сессий, DoS-атаки и др.)

управления АТС содержат ряд ограничений по использованию дополнительных возможностей оборудования, требования по защите от НСД и сигнализации при его наступлении, регистрации событий (журналированию), контролю доступа и управлению. Для получения сертификата (заключения) ФСБ России должен быть проведен комплекс исследований и испытаний, который осуществляется только испытательными лабораториями, аккредитованными в системе сертификации ФСБ России.

Из состава оборудования средств АТС должны быть исключены несертифицированные функции и недекларированные СОРМ, а сертификация каждого ДВО — отдельная сложная задача. Основные проблемы сертификации ДВО средств АТС приведены в таблице 2.

Таким образом, сертификация IP АТС, в том числе представленных на сегодняшний день на рынке, является достаточно сложной задачей в силу указанных выше требований по безопасности.

IP-АТС Т76-С производства ЗАО «ТЕЛРОС» — единственная на сегодняшний день IP-АТС, имеющая заключение Центра защиты информации и специальной связи ФСБ России, которая предназначена для обработки информации, содержащей сведения, составляющие государственную тайну. В представленной АТС отсутствуют многие ДВО, что связано с необходимостью исключения возможных каналов утечки информации и соответствия предъявляемым требованиям.

IP-АТС Т76-С предоставляет услуги закрытой телефонной связи и передачи данных по каналам, защищенным внешним СКЗИ. АТС обладает следующими основными техническими характеристиками:

- интерфейсы FXS, FXO, E1 (G. 703) с сигнализацией EDSS-1, 2 интерфейса Ethernet 1000 Base-T;
- протоколы IP-телефонии SIP, IAX2;
- линейные алгоритмы сжатия, кодеки G. 711, G. 726, G. 729, GSM;
- подавление пауз и эхоподавление при передаче голосового трафика;
- поддержка не менее 40 одновременных разговоров.

В IP-АТС Т76-С встроен аппаратно-программный модуль доверенной загрузки (АПМДЗ), предназначенный для защиты IP-АТС Т76-С от НСД. Кроме этого, комплекс ПО реализует функции межсетевого экранирования и создания виртуальных туннелей.

Таким образом, вопрос обеспечения защищенной связи в ССОН на сегодняшний день является достаточно актуальным, требует развития рынка телекоммуникационных средств (в особенности отечественной индустрии средств связи), которые должны отвечать повышенным требованиям к функциональности и информационной безопасности.

Источники:

1. Федеральный закон от 07.07.2003 №126-ФЗ «О связи».
2. Рекомендации МСЭ-Т.
3. Бакланов И. Г. NGN: принципы построения и организации [Текст]. — М.: Эко-Трендз, 2007. — 400 с.
4. Гольдштейн Б. С., Соколов Н. А., Яновский Г. Г. Сети связи: Учебник для ВУЗов [Текст]. — СПб.: БХВ-Санкт-Петербург, 2010. — 400с.
5. Журнал «Технологии и средства связи», №6, 2013 [Электронный ресурс]. — URL: http://www.tssonline.ru/articles2/fix-op/ osobennosti-setey-novogo-pokoleniya-%28ngn%29.-chast-1.-next-generation-network-%28ngn%29-peculiarities.-part-1.
6. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN [Электронный ресурс] — URL: http://static1.ozone.ru/multimedia/book_file/1009558472. pdf.