ЗИ

АКАДЕМИЯ
СОВРЕМЕННЫХ
ИНФОКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ

ЗИ **Защита информации**

ЗИ.1. Защита информации на корпоративных сетях VoIP
(количество частей – 1, число страниц -5)

ЗИ.1

Ключевые слова: *защита информации, информационная безопасность (ИБ), ИК-система, IP-телефония, корпоративная сеть, технология VoIP.*

Введение. Возможные угрозы в корпоративных инфокоммуникационных (ИК) системах требуют комплексных мер защиты, обеспечить которые могут решения на базе технологии VoIP. Это тем более актуально в свете формирования базовых требований, которым должно соответствовать мультисервисное оборудование с пакетной коммутацией, претендующее на получение статуса «телекоммуникационное оборудование российского происхождения» [1].

Общий подход к защите информации в сетях VoIP. При проектировании любой ИК-системы важно понимать, что ни одна из существующих технологий безопасности не в состоянии обеспечить абсолютную защиту от всех возможных угроз. Внутренняя политика и процедуры информационной безопасности (ИБ) в организации, вне зависимости от масштаба, нуждаются в тщательном анализе, который должен подтвердить, что лучшие решения по ИБ не только были внедрены, но и выполняются должным образом. Кроме того, структура и топология сетевой инфраструктуры, используемой для передачи трафика реального времени (как правило, системы IP-телефонии и видеосвязи), должны варьироваться в зависимости от типа угроз ИБ.

В настоящее время беспроводная инфраструктура корпоративной ИК-системы и точки подключения ее к сети Интернет представляют наиболее серьезную угрозу безопасности сети, и этому обстоятельству необходимо уделять особое внимание. Столь же тщательно следует относиться к угрозам безопасности, исходящим изнутри периметра информационной системы, тем более что инициировать их могут сами сотрудники организации или ее партнеры.

Соответствующие уровни сетевой безопасности необходимо рассматривать и реализовывать с учетом следующих факторов:

- тип и назначение сетевых ресурсов, которым необходимо обеспечить защиту;
- степень влияния угроз на бизнес-процессы организации;
- оценка предполагаемого уровня угрозы безопасности защищаемых ресурсов;
- экономическая эффективность внедряемых инструментов и технологий ИБ.

Таким образом, оценивая какое-то решение по информационной безопасности в ракурсе удобства его развертывания и стоимости, необходимо иметь в виду и последствия нарушения периметра ИБ.

Очевидно, что сегодня из множества форм общения наиболее широко представлен голосовой трафик. Естественно, крайне актуальной становится защита информации в такой подсистеме корпоративной ИК-инфраструктуры, базирующейся на коммутации пакетов, как система IP-телефонии (VoIP). Применение новой технологии VoIP в корпоративной сети, безусловно, несет ряд экономических и технологических преимуществ, но вместе с тем и новые угрозы безопасности для информационной системы организации.

Новые корпоративные системы IP-телефонии, как и системы предыдущего поколения, построенные на технологии коммутации каналов (TDM), нуждаются в подключении к сети связи общего пользования (ССОП). Это требует от них обеспечения защиты от всех видов угроз, свойственных TDM-системам, и в то же время адекватного ответа на новые типы угроз, характерных для сетей с передачей пакетов.

Угрозы ИБ могут быть позиционированы исходя из степени надежности и отказоустойчивости конкретной корпоративной ИК-системы, ее инфраструктуры, уязвимости стыков с внешними сетями, невнимательности и ошибок пользователей, преднамеренных атак хакеров и всякого рода «рассерженных» пользователей. Учитывая сложность решения задачи защиты всех видов информации в ИК-системе, в данной работе ограничимся рассмотрением вопросов защиты только системы IP-телефонии.

Необходимо учитывать, что корпоративная система IP-телефонии должна быть разработана и внедрена в соответствии с внутренними политиками безопасности, надежности и конфиденциальности.

Ключевые элементы информационной безопасности сетей IP-телефонии могут быть классифицированы следующим образом:

Конфиденциальность: необходимость защиты передаваемой информации (голос и данные) для предотвращения прослушивания или перехвата разговоров, внесения изменений в разговорный или сигнальный трафик, кражи паролей.

Целостность: обеспечение уверенности, что передаваемая информация (голос или данные) не подвергается изменениям со стороны неавторизованных пользователей, что запросы на выполнение определенных задач или функций (например, инициализация голосового вызова или измене-

Рис. 1

ние конфигурационных параметров) инициированы авторизованными пользователями или приложениями.

Доступность: обеспечение бесперебойного функционирования корпоративной системы IP-телефонии в условиях DoS-атак (Denial of Service – отказ в обслуживании), различных «червей», «вирусов» и т.п.

Основные функциональные части корпоративной системы IP-телефонии. Обеспечение информационной безопасности в системах IP-телефонии должно включать в себя рассмотрение вопросов безопасности множества интерфейсов сети (рис. 1).

Безопасность интерфейса с ССОП поддерживает взаимодействие с существующими аналоговыми и цифровыми системами и устройствами. Безопасность стыка с ССОП является неотъемлемой составляющей обеспечения безопасности корпоративных систем IP-телефонии (рис. 2).

При подключении любой сети связи к ССОП вероятность мошеннических действий становится реальной угрозой безопасности. Именно здесь осуществляются такие основные угрозы, как подмена пользователя и несанкционированный доступ к функциям корпоративной ИК-системы.

Процесс обработки сигнала при связи с ССОП может различаться в зависимости от архитектуры коммутационной системы. При обработке вызовов некоторые системы коммутации преобразуют TDM-сигнал с ССОП в пакеты (IP) до установления соединения, в то время как другие системы такого преобразования не выполняют. В последнем случае сигнал с ССОП замыкается на TDM-шине гибридной УПАТС, не задействуя при этом ядро пакетной коммутации, и тогда передаваемая с ССОП информация не представляет угрозы системе IP-телефонии. Однако при этом сохраняется угроза прослушивания разговоров.

Безопасность системы сигнализации. Угрозы, свойственные системе сигнализации, включают в себя нарушение нормальной работы системы связи (DoS), подмену пользователя, кражу кодов доступа (account codes) для преодоления ограничений, наложенных на пользователей ИК-систем, мошенничество при междугородной/международной связи.

Для снижения этой угрозы протокол сигнализации между устройством контроля вызовов и IP-телефоном или другим абонентским устройством, как правило, реализуется в виде проприетарного протокола или промышленного стандарта, например H.323 или SIP. Современные устройства контроля вызовов должны обеспечивать поддержку множества протоколов сигнализации (рис. 3).

Безопасность медиапотока (передаваемой в системе IP-телефонии голосовой и видеоинформации). Здесь следует выделить прослушивание (eavesdropping) и несанкционированную деятельность, приводящую к ухудшению качества связи. Нарушение конфиденциальности или качества может негативно влиять на целостность информации, а значит, на доверие бизнеса к выбранным решениям. Прослушивание и потеря информации в канале являются наиболее значимыми угрозами для данных голосового потока. Самой вероятной угрозой следует считать перехват информации (sniffing), передаваемой по сети Интернет и беспроводным каналам связи.

Голосовой трафик на сетях VoIP передается в виде пакетов непосредственно между взаимодействующими устройствами (телефонными аппаратами) (рис. 4).

Попытки прослушивания Ethernet-порта телефона путем непосредственного подсоединения к кабелю, мониторинга с помощью удаленных датчиков или перенаправления пакетов

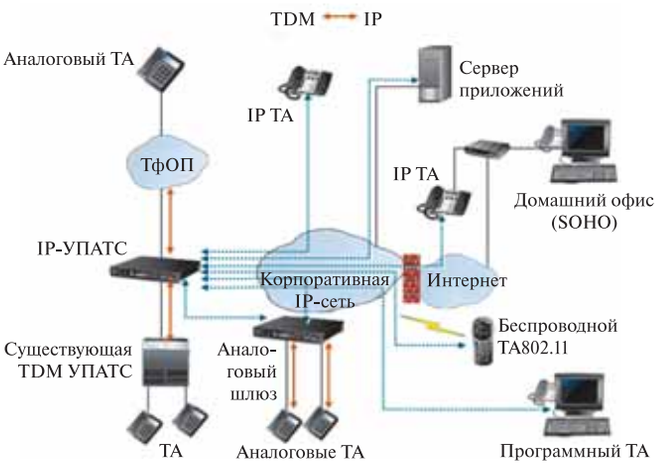

Рис. 2

Рис. 3

потока данных могут являться потенциальной угрозой ИБ – как и попытки повреждения пакетов потока данных, передаваемых по каналам сети связи.

Безопасность системы управления. Инструменты управления, как правило, используются для конфигурирования, администрирования и мониторинга состояния системы, служб биллинга и пр. Интерфейсы управления могут подвергаться атакам с целью кражи личной информации пользователей (имени пользователя и пароля) или для организации разного рода атак, например DoS-атак. Наблюдение и прослушивание определенных портов иногда используется для получения различной информации (такой, например, как учет совершенных вызовов), которая может содержать в себе коды доступа к различным сервисам (выхода на сеть ССОП и т.д.), или информации о последних совершенных звонках. Также возможны случаи подмены приложений и злонамеренные системные изменения.

На рис. 5 показаны некоторые интерфейсы, представляющие потенциальную угрозу для системы управления в решении IP-телефонии.

Возможные решения по защите информации. Обеспечение целостности и контроля каждой из частей корпоративной ИК-системы гарантирует правильность и надежность функционирования системы IP-телефонии.

Современные корпоративные системы IP-телефонии, как правило, строятся на базе оборудования ведущих вендоров, таких как Cisco, Avaya, Mitel, Nokia Siemens Networks, Alcatel-Lucent и др. [2]. Ядром корпоративной системы IP-

телефонии является гибридная платформа (Mitel, Avaya, NEC и др.), которая позволяет создавать масштабируемую, полнофункциональную систему связи с числом пользователей от 30 до 60 тыс. (рис. 6).

Такие платформы, совмещающие возможности офисной IP-УПАТС с большим набором встроенных и интегрированных сторонних приложений, формируют основу для решений, которые принято называть унифицированными коммуникациями (Unified Communications, UC). На пользовательском уровне гибридной платформы происходит, во-первых, поддержка большого количества абонентских устройств: это фиксированные и беспроводные (Wi-Fi или IP-DECT) IP-телефоны, IP-устройства с веб-доступом, полнодуплексные IP-модули для аудиоконференцсвязи и др. Во-вторых, они способны поддерживать функционирование мощного пакета приложений с возможностью доработки (кастомизации) под нужды конкретных пользователей. Это реализуется посредством интерфейса программирования приложений (Application Programming Interfaces, API) и гарантирует совместную работу с использованием средств мультимедиа, управление взаимоотношениями с клиентами, единую систему сообщений и т.п. Правильно выбранная гибридная платформа делает возможной функционирование в сети оборудования разных производителей.

Отметим, что внедряемая платформа должна обеспечивать взаимодействие с существующей корпоративной системой связи, тем самым защищая ранее сделанные оператором инвестиции и позволяя добавлять новые сервисы IP-телефонии к рабочим группам, отделам и филиалам по мере надобности. Если архитектура такой платформы построена по принципу распределенных открытых систем (как программно, так и аппаратно), появляется возможность для внедрения и развертывания корпоративных систем IP-телефонии, которые наилучшим образом удовлетворяют потребностям организации, в том числе в области ИБ.

В настоящее время многоуровневую защиту корпоративных сетей поддерживают множество методов и решений: брандмауэры (Firewall), системы обнаружения (IDS) или предотвращения (IPS) вторжений, виртуальные частные сети (VPN), системы контроля доступа и т.п. Например, технология VPN может применяться в распределенных корпоративных сетях для защищенности информации, передаваемой между подразделениями организации по публичным каналам сети Интернет. Механизмы аутентификации и шифрования должны применяться в случае развертывания беспроводных сетей, например стандарта IEEE 802.11. Безопасность периметра корпоративной сети, а также ее стыка с сетью Интернет может быть достигнута путем внедрения брандмауэров – программных или программно-аппаратных комплексов с функциями обнаружения или предотвращения вторжений, фильтрации трафика, частичного ограничения или полного запрета определенных ресурсов и пр. Все это сегодня стандартные методы обеспечения безопасности корпоративных сетей любого масштаба.

Защита голосового и сигнального трафика. Первым рубежом при обеспечении информационной безопасности в ИК-системе должна служить физическая защита безопасности сети, т.е. защита инфраструктуры: коммутационных шкафов и стоек, активного сетевого оборудования (коммутаторов, маршрутизаторов и пр.), серверов, устройств контроля вызовов и т.д. Применение физической защиты осложняет злоумышленнику задачу прослушивания и перехвата данных, в том числе телефонных разговоров.

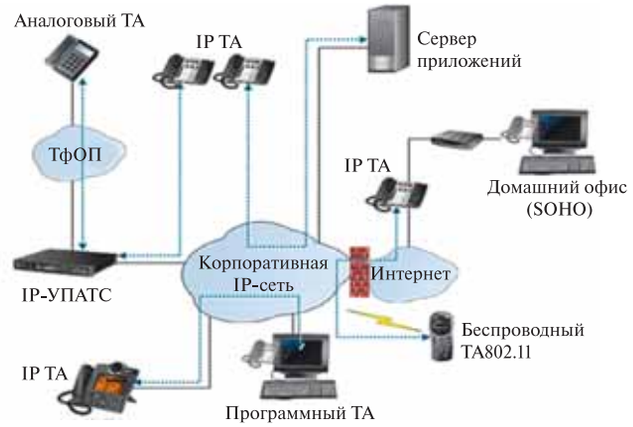

Рис. 4

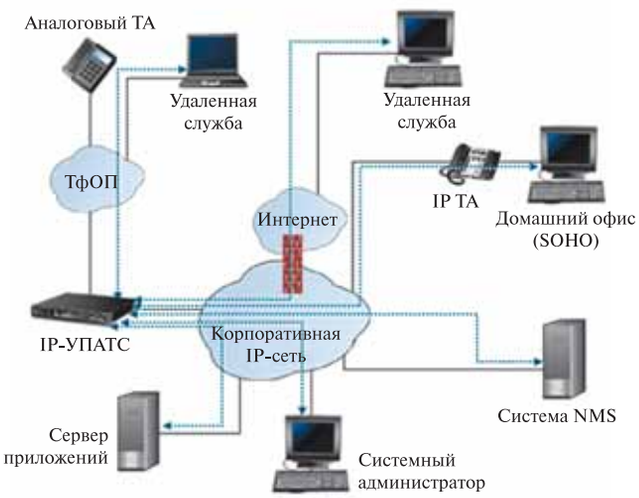

Рис. 5

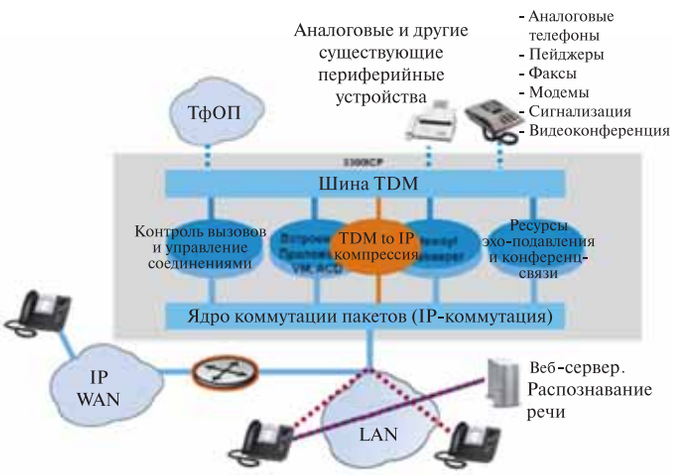

Рис. 6

Для обеспечения конфиденциальности контроля вызовов и сигнализации в системах IP-телефонии в качестве базового оборудования (ядро системы, телефонные аппараты, программное обеспечение) должно использоваться оборудование, в котором защита сигнализации основывается на известных промышленных стандартах и протоколах, например AES и SRTP. Для достижения желаемого уровня безопасности в состав решения можно включить аутентификацию на базе стандарта 802.1X (для настольных устройств), а также поддержку Extensible Authentication Protocol (EAP), исполь-

зующего EAP-MD5 при запросах сервера RADIUS. Реализуя данную процедуру, пользователи проходят аутентификацию, вводя логин и пароль.

При достижении критерия «доступность» ИК-системы, в частности подсистемы IP-телефонии, возникает задача ее защиты от вирусных атак и другого вредоносного ПО. При этом целесообразно применять платформу, использующую встроенную специализированную операционную систему (ОС), например VxWorks. Такая ОС имеет ограниченную по сравнению с ОС общего назначения (Windows, Linux, Unix) функциональность, поэтому меньше подвержена влиянию вредоносного ПО. Дело в том, что указанные ОС общего назначения включают в себя в качестве базового функционала такие службы, как служба веб-сервера, служба печати и т.п. Применяемые повсеместно, они представляют собой легкую добычу для атак вирусов, червей и др.

В специализированной ОС весь необходимый функционал дорабатывается производителем с учетом конкретных нужд клиента. Это означает, что каждая ее реализация отличается от другой. На практике это приводит к тому, что злоумышленнику крайне трудно создать вредоносное ПО, направленное на поражение данной конкретной версии специализированной ОС.

Использование специализированных ОС также позволяет снизить угрозы DoS-атак. Тем не менее множество DoS-атак направляется против стека протоколов TCP/IP, поэтому их целью являются любые устройства в сети, функционирующие на базе протокола IP.

Поскольку система IP-телефонии является составной частью корпоративной ИК-системы, защита от DoS-атак должна обеспечиваться правильной сетевой политикой безопасности в целом. В качестве эффективных мер защиты от DoS-атак можно назвать внедрение механизма виртуальных частных вычислительных сетей (VLAN), организацию систем DMZ, использование брандмауэра, IPS, политику разделения серверов и т.п. Данные механизмы совместно со специализированной ОС позволяют на логическом уровне разделить сеть передачи данных и сеть передачи голосовой информации и таким образом защитить систему IP-телефонии от вышеуказанных атак.

Не менее острой в корпоративных системах IP-телефонии остается проблема предотвращения мошенничества и злоупотреблений. Очень наглядно это проявляется в попытках бесплатных звонков неавторизованных пользователей. Рассмотрим более подробно, как осуществляется аутентификация и каким образом пользователь (или группа пользователей) может получить запрет на различные виды связи (например, исходящую или междугородную).

Для того чтобы защитить пользователей от мошенничества и злоупотреблений, система IP-телефонии должна быть основана на решениях, включающих функции управления доступом на абонентскую и линейную части, например класс обслуживания (Class of Service, CoS), класс запрета (Class of Restriction, CoR) и запрет на соединение (Interconnect Restrict). Таким образом, администратор системы заранее задает разрешенные пути соединения, запреты на набор номера и доступные функции. CoR позволяет запретить определенным пользователям доступ к набору определенных исходящих номеров или направлений связи (Call Barring). Подобные ограничения, записанные для каждого номера или линии (транка), могут составить, таким образом, план запрета для каждого класса. Пользователь, желающий обойти эти ограничения, должен досконально изучить проприетарные методы сигнализации, которые, как отмечалось выше, используются в системах IP-телефонии.

Введение механизма специальных кодов (Account Code) предоставляет дополнительные возможности для управления доступом и использования услуг, которые обычно недоступны. Кроме того, для предотвращения подключения к системе IP-телефонии неавторизованного пользователя после регистрации абонентского устройства следует установить соответствие между MAC-адресом, IP-адресом, добавочным номером (Ext) и регистрационным номером (PIN). Это соотношение (MAC/IP/Ext/PIN) должно быть действующим, чтобы система разрешила соединение.

Для предотвращения несанкционированного доступа к системе управления (как правило, осуществляется через веб-браузер), а именно для защиты личных данных (имя пользователя и пароль) от перехвата и последующего неправомерного использования, служит протокол SSL. Чтобы усилить защиту, необходимо изменять пароль по умолчанию. Кроме того, система должна поддерживать несколько уровней доступа к своим ресурсам: уровень системного администратора, уровень группового администрирования, пользовательский уровень. Следует предусмотреть ограничение одновременно подключенных пользователей всех уровней доступа, а также временной лимит сессий подключения. Пользователи должны иметь авторизованный доступ к ограниченному числу элементов управления системой, для того чтобы устанавливать некоторые из параметров своих индивидуальных абонентских устройств (например, IP-телефонов), таких как кнопки быстрого набора, различные функциональные клавиши и т.п.

Практически все современные системы связи поддерживают удаленный доступ, что также является потенциальной угрозой нарушения безопасности. Безопасность такого доступа обеспечивается использованием для контроля вызовов проприетарных протоколов сигнализации, усиленных SSL-шифрованием, а также промышленного стандарта SRTP.

Безопасность корпоративной ИК-системы требует соблюдения главного правила: любые функции и методы доступа к ним, которые в данный момент времени пользователю не требуются, должны быть деактивированы.

Заключение. Рассмотренные выше аспекты лишь частично решают задачу обеспечения безопасности корпоративных систем IP-телефонии. На практике следует рассматривать всю инфраструктуру корпоративной сети, вне зависимости от степени ее защищенности, как враждебный мир, который может нарушить ее работу. Именно такой строгий и консервативный подход гарантирует максимальный уровень защищенности.

ЛИТЕРАТУРА

1. Распоряжение Правительства РФ от 31.05.2010 № 858-р «О разработке и утверждении значений параметров, методики определения значений параметров и порядка присвоения телекоммуникационному оборудованию, произведенному на территории Российской Федерации, статуса телекоммуникационного оборудования российского происхождения».
2. Vendor Landscape: IP Telephony //Info-Tech Research Group. – 2011.