электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 621.391

Анализ угроз информационной безопасности и последствия их реализации при сопряжении сети ТфОП/ISDN и IP

Никольский Т.В., *учащийся 11 класса*
лицей № 1553 им. В.И. Вернадского
115114, Россия, г. Москва, ул. Дербеневская, 13

Научный руководитель: Бельфер Р.А., доцент, к.т.н., с.н.с.
Россия, 105005, г. Москва, МГТУ им. Н.Э.Баумана,
bauman@bmstu.ru

Введение. Тема настоящей работы посвящена анализу угрозы (атаки) отказ в обслуживании DoS на сетевом уровне системы общеканальной сигнализации ОКС-7. Эта система относится к сетям связи нового поколения NGN при передаче речи и данных по сетям IP (Voice over IP – VoIP). В работе рассматривается возможный механизм защиты от них. Актуальность этой задачи в ОКС-7 вызвана: 1. Серьезными последствиями при реализации злоумышленником этой угрозы. На это указывают некоторые разработчики ОКС-7 (например фирмы “CISCO” [1]), специалисты международного союза электросвязи (ITU-T) по стандартизации этого оборудования [2].

2. Опыт эксплуатации сети ОКС-7 показывает отсутствие в действующих сетях связи защиты от некоторых из этих угроз. Анализу подлежат атаки DoS, которые реализуют угрозы информационной безопасности (ИБ), приводящие к нарушению маршрутизации в пунктах сигнализации системы ОКС-7. Целью работы является анализ алгоритма реализации злоумышленником этой угрозы DoS, рассмотрение ущерба при реализации одного из видов угрозы, принципы защиты от этой угрозы.

В разделе 1 приводится описание системы сигнализации стандарта SIP сети речи и данных нового поколения VoIP в качестве примера приводится участок системы SIP на действующей сети РФ. В разделе 2 рассматривается алгоритм реализации злоумышленником угрозы DoS в ОКС-7 в сети VoIP по протоколу системы сигнализации SIP. В разделе 3 рассматривается принцип защиты и оценка защищенности от угроз DoS в системе стандарта SIP сети речи и данных нового поколения VoIP.

Система сигнализации стандарта SIP сети речи и данных нового поколения VoIP и пример участка системы SIP на действующей сети РФ. IP-сеть основана на коммутации пакетов. В ней, как и в сети ТфОП, есть выделенная от транспортного потока сеть сигнализации. Среди нескольких созданных систем сигнализации для VoIP наиболее широко используются протокол Session Initiation Protocol (SIP) [3,4].

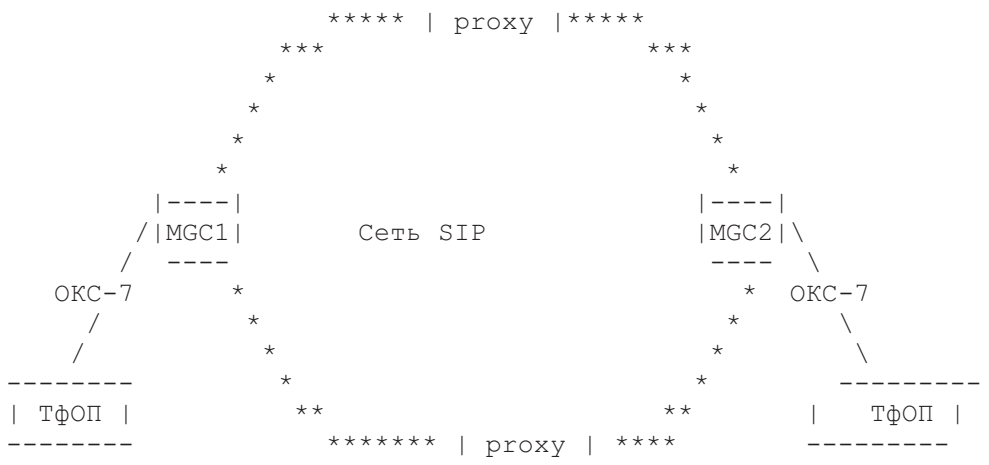

Рис. 1. Общая схема структуры связи абонентов ТфОП/ISDN через транзитную сеть SIP

Общая схема структуры связи абонентов ТфОП/ISDN через транзитную сеть SIP (рис.1) включает участки ОКС-7 между граничными станциями ТфОП/ISDN и шлюзами сигнализации (Media Gateway Controller, MGC) MGC1 и MGC2. При этом используются сообщения всех четырех уровней системы ОКС-7. Шлюзы производят преобразование сигнальных сообщений протоколов ОКС-7 в сигнальные сообщения протокола SIP и наоборот. Шлюз MGC называют также Softswitch – преобразователем систем сигнализации. При установлении такого соединения система сигнализации ОКС-7 сети ТфОП России может включать пункты сигнализации, входящие в зоновые АМТС, АТС местных сетей связи.

На рис. 2 показана схема прохождения сообщений сигнализации при установлении и разъединении соединения между абонентами сетей ТфОП. На участке между ТфОП приведены сообщения подсистемы пользователя ISUP между последним пунктом

сигнализации ОКС-7 и шлюзом сигнализации MGC . На участке между шлюзами MGC приведены:

сообщения SIP – запросы

- INVITE (запрос на установление сеанса)
- ACK (подтверждение, что клиент агента пользователя UAC получил окончательный ответ на запрос INVITE)
- BYE (агент UA завершает установленный ранее сеанс)

и сообщения SIP – ответы.

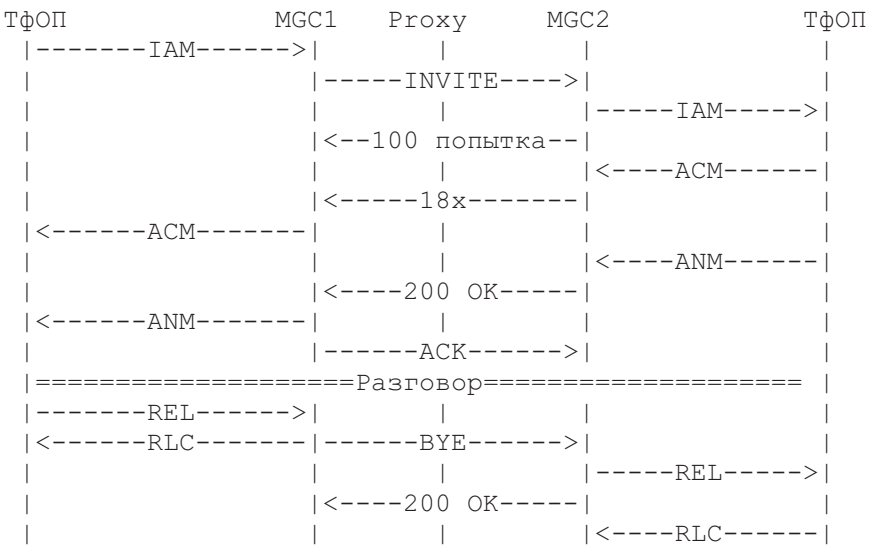

Рис. 2. Схема прохождения сообщений сигнализации при установлении и разъединении соединения между абонентами сетей ТфОП

Более детально принцип переноса сообщений протокола ОКС-7 по IP-сети показан на рис. 3, где приведен пример участка действующей сети РФ [5].

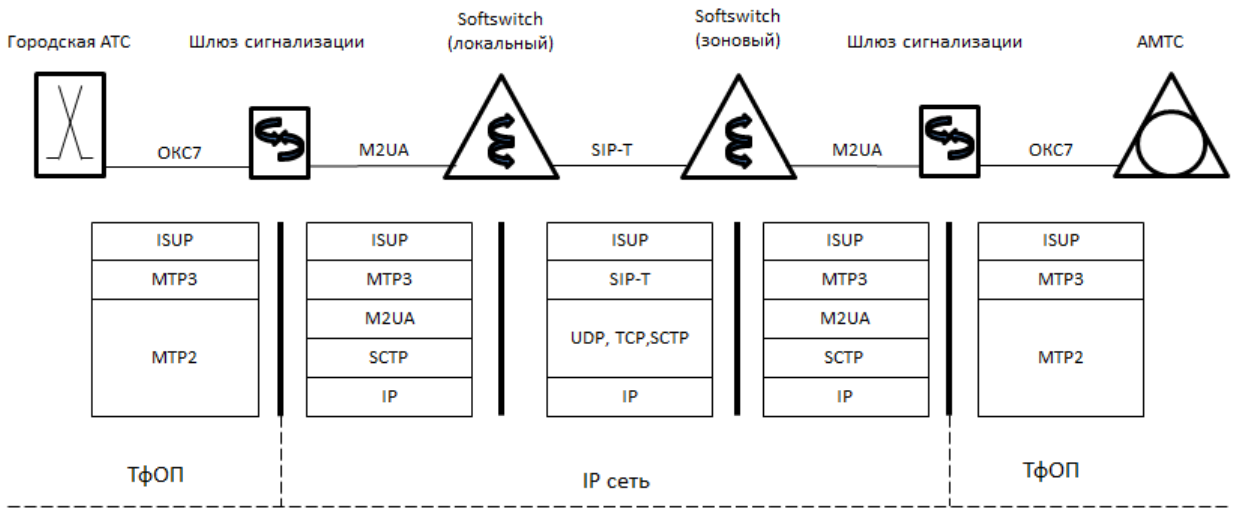

Рис. 3. Пример участка действующей сети РФ

Интерфейс IP-сети с внешней сетью ОКС-7 обеспечивают шлюзы сигнализации. На рисунке представлен вариант, когда на Softswitch мы имеем стандартные приложения (такие, например, как ISUP) и стандартный протокол MTP3. При этом у Softswitch есть собственный код пункта сигнализации и, являясь полноправным пунктом сигнализации сети ОКС-7, принимает и передает сообщения ОКС-7, в том числе и сообщения эксплуатационного управления сетью сигнализации. Однако на Softswitch отсутствует MTP2 [6].

В приведенном сценарии удаленный доступ к услугам протокола MTP2, который расположен на шлюзе сигнализации, через IP-сеть к протоколу MTP3 на Softswitch обеспечивает протокол M2UA группы SIGTRAN. Для транспортировки сообщений MTP3 по IP-сети группой SIGTRAN выбран протокол SCTP (RFC 2960), обладающий рядом существенных преимуществ по сравнению с другими транспортными протоколами. В частности, SCTP обеспечивает подтверждаемую, достоверную, свободную от ошибок и не дублируемую передачу пользовательских данных, наделен функциями эксплуатационного управления трактом передачи, имеет механизмы исключения перегрузок, противодействия лавинам сообщений и нелегальным проникновениям в систему, вызывающим перегрузки.

Алгоритм реализации злоумышленником угрозы DoS в ОКС-7 системы сигнализации SIP. В настоящем разделе рассматривается один из алгоритмов реализации злоумышленником угрозы DoS в ОКС-7 системы сигнализации SIP – нарушение таблицы маршрутизации ОКС-7 с помощью сообщений вынужденной маршрутизации TFP (Transfer Prohibited) [7].

Целью процедуры вынужденного изменения маршрутизации (ремаршрутизации) является восстановление способности переноса сигнальных сообщений между двумя смежными пунктами в направлении к определенному пункту назначения. Процедура управляемой маршрутизации применяется, когда сигнальный маршрут в направлении определенного пункта назначения вновь оказывается доступным (например, после устранения отказов в удаленных элементах сети сигнализации), и становится возможной процедура обратного перевода трафика с резервного на нормальный сигнальный маршрут. Пример указанных процедур приведен на рис. 4

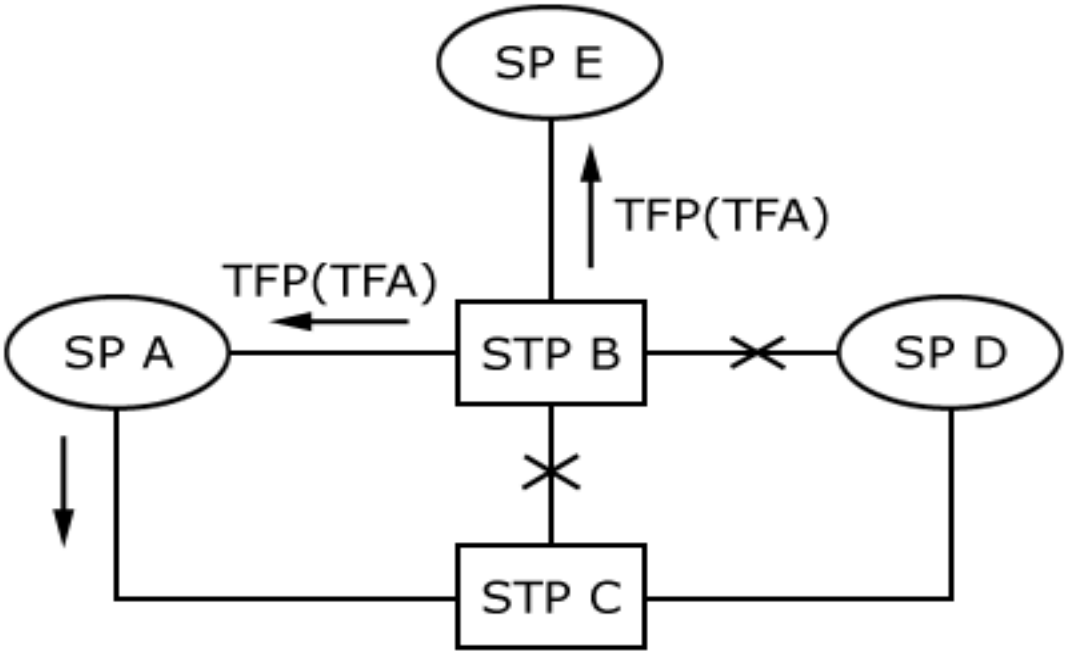

Рис. 4. Процедура вынужденной ремаршрутизации и управляемой ремаршрутизации

Процедура вынужденной ремаршрутизации инициируется в пункте SP A при приеме сообщения TFP о запрещении переноса со стороны смежного транзитного пункта сигнализации STP B. Это сообщение указывает на невозможность доставки MSU к пункту назначения SP D из-за отказа звеньев сигнализации SP D-STP B и SP D-STP C.

В пункте сигнализации, получившем сообщение TFP, выполняется следующая последовательность действий:

- останавливается перенос сигнального трафика по недоступному сигнальному маршруту (SP A-STP B-SP D), после чего в буфере ЗС сохраняется часть не переданного трафика;
- определяется резервный сигнальный маршрут (SP A-STP C-SP D);

- перенос сигнального трафика восстанавливается, начиная с содержимого буфера ЗС, по пучку ЗС, относящемуся к резервному сигнальному маршруту. Формат сообщения TFP включает поле адреса пункта назначения, к которому относится это сообщение (в данном случае адрес SP D).

Анализируем ущерб при реализации этой угрозы. Злоумышленник, решил нанести удар по ТфОП и тем самым вывести ее из строя. Он подключается к АМТС и посылает нелегитимные сообщения TFP о недоступности SP1 (УАК-1) и STP3. Эти сообщения передаются в SP (УИВС1). Последствием такой угрозы является отказ исходящих вызовов установления соединений абонентов всех АТС местной сети А, подключенных к УИВС1 с абонентами ТфОП/ISDN других местных сетей. На рисунке 5 приведен пример невозможности установлении исходящих вызовов соединения от абонентов по системе SIP.

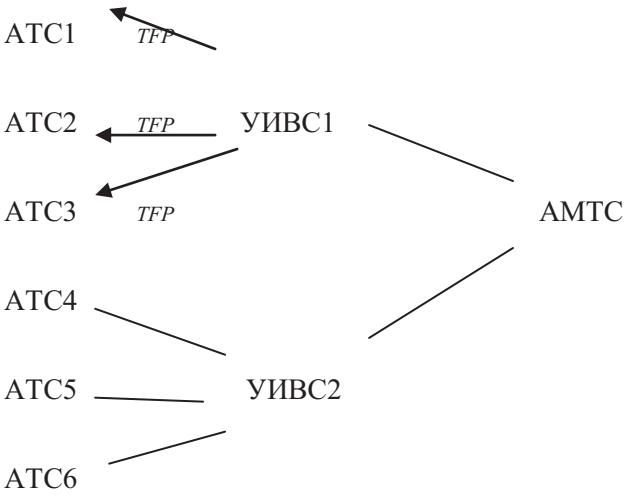

Рис. 5. Пример угрозы DoS в сети ССОП (невозможность установления исходящих вызовов)

Или наоборот он посылает нелегитимные сообщения TFP о недоступности SP (УИВС1) и STP2. Эти сообщения передаются в SP (УАК-1) и STP3. Последствием такой угрозы является отказ входящим вызовам установления соединений всех абонентов ТфОП/ISDN с абонентами зоновой сети АМТС1 (рис. 6).

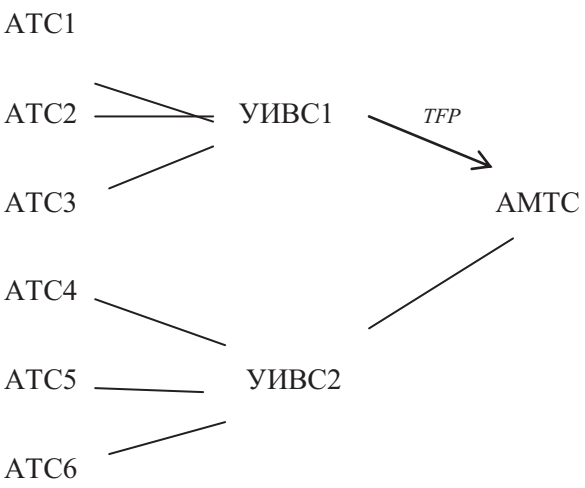

Рис. 6. Пример угрозы DoS в сети ССОП (невозможность установления входящих вызовов)

Результатом действий злоумышленника является то, что будет невозможность установления для исходящей абонента любой АТС, а входящей зависит от недоступности конкретных АТС.

Но злоумышленник может отправить эти сообщения так, что альтернатвного пути не будет. В таком случае как уже говорилось выше часть сети просто выйдет из строя. Данный пример приведен для нелегитимных сообщений TFP, но отказы DoS могут быть и от других сообщений управления сетью ОКС-7 (сообщения перегрузки, недоступность пользовательского уровня и др.).

Принцип оценки защищенности от угроз DoS стандарта SIP сети речи и данных нового поколения VoIP. В IP-сети при выполнении протокола маршрутизации RIP или OSPF может быть использован либо протокол открытой аутентификации MD5 (RFC-2453), либо протокол аутентификации MD5 (RFC-2082), а при выполнении протокола маршрутизации BGP протокол аутентификации MD5 (RFC-2385) [8]. Как было отмечено выше в системе ОКС-7 защита от такого атак отсутствует. Этот недостаток может быть устранен с помощью разных механизмов аутентификации: MD5, аутентификация с помощью ЭЦП, механизм аутентификации источника сообщений по протоколу ОКЛИК-ОТЗЫВ, использующий шифрование с общим ключом; механизм аутентификации сообщений с помощью кода аутентичности сообщения MAC, использующий шифрование с общим ключом без дешифрования; механизм аутентификации сообщений по протоколу HMAC без использования шифрования [8,9].

Данный раздел посвящен принципу сравнительного анализа защищенности этих

механизмов аутентификации. Используем математическую модель, предложенную для сравнения механизмов защиты от угроз информационной безопасности авторами международного проекта, финансируемого Европейской комиссией по сетям связи (материалы проекта опубликованы в открытой печати [10]).

Сравнение производится по показателю *R*:

$$R = \frac{\sum_{i=1}^{N} k_i \times x_i \times 5}{\sum_{i=1}^{N} k_i}$$

Здесь под k_i понимается степень важности требования заказчика по характеристике *i*. Чем больше k_i, тем важнее *i*-е требование (k_i = 1, 2, 3). Выбор характеристик k_i зависит от функций конкретной сети и определяется на этапе согласования технических требований. Для рассматриваемого примера сравнительного анализа защищенности от угроз несанкционированного доступа примем следующие требования степени важности по защите от угроз несанкционированного доступа k_i:

k_1 – защита от формирования нелегитимных сообщений и передача их по полученному злоумышленником адресу оконечного пункта;

k_2 – защита от перехвата сообщений с целью его уничтожения;

k_3 – защита от изменения информационной части сообщений.

Значение x_i показывает степень выполнения этого требования. В указанном отчете x_i = 0 – требование совсем не выполняется, x_i = 1 – выполняется частично, x_i = 2 – требование полностью удовлетворено. При выбранных в формуле возможных k_i , x_i и коэффициенте 5 диапазон *R* может принимать значения между 0 и 10. Значения k_i , x_i определяем методом экспертных оценок. Приведенные значения k_i ,x_i для возможных механизмов аутентификации рассматриваются для получения результатов Rsec и Rcos .

Выводы. Результаты настоящей работы могут быть использованы при введении в эксплуатацию новых систем операторами связи РФ при продолжении исследования рассматриваемой проблемы обеспечении ИБ системы общеканальной сигнализации ОКС-7 в сети VoIP по протоколу сигнализации SIP.

Список литературы

1. Драйберг Ли, Хьюит В. Система сигнализации №7 (SS7/ОКС7), протоколы, структура и применение. М.: Вильямс, 2006. 752 с.
2. Дэвидсон Д. Основы передачи голосовых данных по сетям IP. 2-изд. М.:Вильямс, 2007. 400 с.

3. Гольдштейн Б.С., Зарубин А.А., Саморезов В.В. Протокол SIP: справочник. СПб.: БХВ-Санкт-Петербург, 2005. 455 с.
4. Бельфер Р.А., Морозов А.М. Информационная безопасность сети связи для абонентов ТфОП/ISDN через SIP-T // Электросвязь. № 3. 2012. С. 20-25.
5. Бельфер Р.А. Сети и системы связи (технологии, безопасность): учеб. пособие. М.: МГТУ им. Н.Э. Баумана, 2012. 740 с.
6. Бельфер Р.А., Горшков Ю.Г., Даннави М.Н. Последствия нарушений маршрутизации общеканальной сигнализации на функционирование сетей связи общего пользования // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2009. № 3. С. 90-95.
7. Бельфер. Р.А., Горшков Ю.Г., Даннави М.Н. Алгоритмы аутентификации в сетях общего пользования России // Электросвязь. № 8. 2008. С. 12-17.
8. Даннави М.Н. Метод повышения защищенности от угроз нарушения маршрутизации в общеканальной сигнализации сети связи общего пользования: автореф. дис. канд. техн. наук. Уфа, 2012. 16 с.