УДК 621.391

Р. А. Бельфер, Ю. Г. Горшков,
М. Н. Даннави

ПОСЛЕДСТВИЯ НАРУШЕНИЯ МАРШРУТИЗАЦИИ ОБЩЕКАНАЛЬНОЙ СИГНАЛИЗАЦИИ НА ФУНКЦИОНИРОВАНИЕ СЕТЕЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Проанализированы последствия реализации угроз нарушения маршрутизации в общеканальной сигнализации. Показано, что наиболее чувствительными к атакам, соответствующим этим угрозам информационной безопасности, являются участки между пунктами сигнализации разных уровней иерархии сетей связи.

Ключевые слова: *телефонная сеть связи общего пользования, отказ в обслуживании, угроза, интеллектуальная сеть, общеканальная система сигнализации.*

Во многих работах по информационной безопасности общеканальной сигнализации ОКС-7 отмечается ее уязвимость по отношению к угрозам нарушения маршрутизации, приводящим к ущербу работе сетей связи общего пользования (ССОП) [1–4]. Как отмечено в работе [1], в ОКС-7 не предусмотрены механизмы аутентификации для защиты от угроз атак типа “отказ в обслуживании” (Denial of Service (DoS)).

Настоящая статья посвящена анализу потенциальных последствий ущерба, нанесенного работе ССОП (ТфОП / ISDN, GSM, и интеллектуальных сетей связи IN), и реализации угроз нарушения маршрутизации ОКС-7.

Факторы, влияющие на последствия атак DoS в общеканальной сигнализации ОКС-7. Для реализации таких угроз нарушителем используются функции подсистем MTP и SCCP сетевого уровня ОКС-7. Уровень ущерба, нанесенного работе ССОП атаками DoS, определяется теми функциями MTP и SCCP, которые нелегитимно использует нарушитель на различных участках смежных пунктов сигнализации Signaling Point (SP) ОКС-7. Поэтому последствия нарушения работы ССОП зависят от топологии этих сетей: уровней иерархического построения, схем резервирования и взаимодействия.

Учитывая сложную топологию ССОП [5, 6], последствия атак DoS на ССОП (ТфОП/ISDN, GSM и интеллектуальную сеть связи IN) рассмотрим на упрощенной гипотетической схеме сети ОКС-7, приведенной на рис. 1 (для упрощения на рисунке показан пучок звеньев сигнализации). Здесь представлены оконечные и промежуточные пункты сигнализации (соответственно SEP и SP) двух сетей местного уровня (A и B) и участка междугородного уровня. В скобках указаны узлы коммутации, в которые входят пункты SP: SEP (в АТС), SP (в узле

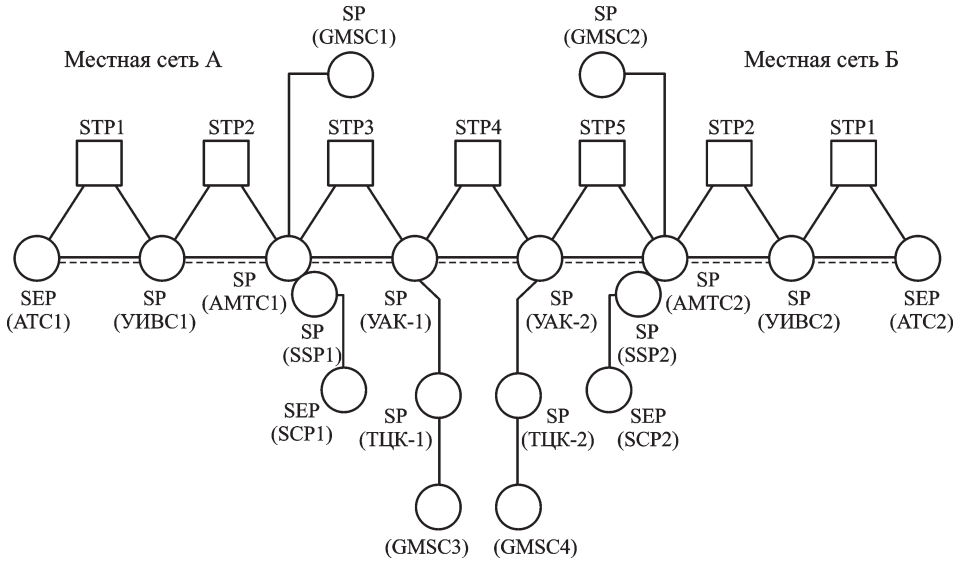

Рис. 1. Гипотетическая схема сети ОКС-7:
сплошные линии — пучок звеньев сигнализации, штриховая — речевой сигнал

исходящей и входящей связи (УИВС)), SP (в узле автоматической коммутации (УАК-1)), SP (в УАК-2). На участках местного и международного уровня предусмотрены альтернативные пути — через транзитные пункты сигнализации STP.

К смежным пунктам сигнализации SP (в AMTC) подключены: SP (в GMSC), т.е. шлюз мобильной станции коммутации MSC; SP (в SSP), т.е. узел управления коммутацией интеллектуальной сети; SP (в УАК).

Два пункта сигнализации SP (в УАК) соединены друг с другом и каждый из них соединен с транзитным центром коммутации (ТЦК) сети GSM [6]. К основным функциям сетевого уровня ОКС-7, нелегитимное использование которых злоумышленником представляет угрозу нарушения маршрутизации, относятся следующие функции MTP [1]: запрет передачи (сообщение TFP); недоступность подсистемы пользователя (сообщение UPU); перегрузка пучка звеньев сигнализации (сообщение TFC); ограничение передачи (сообщение TFR); переключение звена сигнализации (сообщения COO, ECO), а также функции SCCP: запрет доступа (сообщение SSP), подсистема перегружена (сообщение SSC) и др.

Далее приведены примеры последствий реализации угроз нарушения маршрутизации сети ОКС-7 (см. рис. 1) при использовании злоумышленником функции MTP “запрет передачи” (сообщение TFP), т.е. недоступности определенного пункта сигнализации.

Пример 1. Нарушитель создает в пункте SP (AMTC1) нелегитимное сообщение TFP о недоступности пунктов сигнализации SP (в УИВС1) и STP2. Эти сообщения передаются нарушителем из SP (AMTC1) в пункты SP (УАК-1) и STP3. Последствием такой атаки DoS является отказ всем входящим вызовам от пользователей ТфОП/ISDN

и GSM в установлении соединений с абонентами всех АТС, подключенными к УИВС1. При этом сохраняется возможность установления соединений внутри местной сети ТфОП/ISDN, а также между абонентами и мобильными станциями, обслуживаемыми мобильными станциями MSC через GMSC1.

Если нарушитель предпринимает такие же нелегитимные действия в отношении остальных УИВС местной сети, то аналогичные последствия будут относиться к абонентам остальных АТС местной сети А. Приведенный пример последствий относится к конфигурации, при которой зоновая АМТС1 соединена с одним УАК-1.

В действительности на сетях ТфОП/ISDN России и других стран (Германии, США и т.д.) в целях резервирования зоновая АМТС соединена с двумя УАК [1]. Для упрощения на рис. 1 это не показано. Поэтому приведенные последствия имеют место, когда указанные нелегитимные сообщения TFP направляются нарушителем одновременно в оба узла УАК.

Пример 2. Нарушитель создает в пункте SP (АМТС1) нелегитимные сообщения TFP о недоступности обоих пунктов SP (УАК), к которым подключен SP (АМТС1). Эти сообщения передаются в любой пункт SP (УИВС) или одновременно во все пункты местной сети А. Последствия такой атаки аналогичны предыдущим последствиям, приведенным в примере, за исключением того, что отказ относится к исходящим вызовам установления соединения от абонентов АТС местной сети А.

Пример 3. Нарушитель создает в пункте SP (АМТС1) нелегитимное сообщение о недоступности пункта SP (GMSC1).

1. Это сообщение передается в пункт SP (УИВС1). Последствием такой угрозы является отказ в установлении соединений абонентов всех АТС местной сети А, подключенных к УИВС1 с мобильными станциями, обслуживаемыми шлюзом GMSC1.

2. Это сообщение TFP передается в пункты SP (УАК-1) и STP-3. Последствием такой угрозы является отказ всем абонентам ТфОП/ISDN (кроме абонентов местной сети А), а также всем мобильным станциям (кроме обслуживаемых шлюзом GSM1) в установлении соединений с мобильными станциями, обслуживаемыми шлюзом GMSC1.

Пример 4. Нарушитель создает в пункте сигнализации SP (АМТС1) нелегитимное сообщение TFP о недоступности пункта SP (SSP1).

1) Это сообщение TFP передается в пункт SP (УИВС1). Последствием такой угрозы является отказ в установлении соединений абонентов всех АТС местной сети А, подключенных к узлу УИВС1 и требующих предоставления услуг платформой интеллектуальной сети с узлом управления услугами SCP1.

2) Это сообщение TFP передается в пункты SP (УАК-1) и STP-3. Последствиями такой угрозы являются отказы от исходящих вызовов,

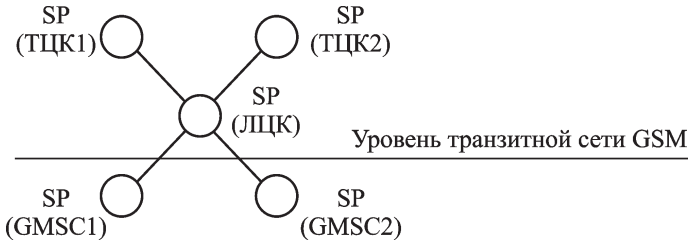

Рис. 2. Фрагмент сети ОКС-7

поступающих от всех абонентов ТфОП/ISDN (кроме абонентов местной сети А), по установлению соединений с требованием предоставления услуг платформой интеллектуальной сети с SCP1; от всех мобильных станций, устанавливающих соединения с требованием предоставления услуг платформой интеллектуальной сети с SCP1.

Следующие два примера приведены для расширенного (по сравнению со схемой, приведенной на рис. 1) фрагмента сети ОКС-7 (рис. 2). Здесь показано взаимодействие локального центра коммутации (ЛЦК) уровня транзитной сети [5] с двумя транзитными центрами коммутации (ТЦК1 и ТЦК2), с шлюзом GMSC и зоновой АМТС.

Пример 5. Нарушитель создает в пункте SP (ЛЦК) нелегитимные сообщения TFP о недоступности пунктов SP (ТЦК1 и ТЦК2). Эти сообщения передаются в пункты SP (АМТС) и SP (GMSC). Последствием такой атаки DoS является отказ вызовам на установление соединений через уровень транзитной сети GSM, исходящим от абонентов всех АТС зоны обслуживания АМТС и от мобильных станций, обслуживаемых станциями коммутации MSC через GMSC.

Пример 6. Нарушитель создает в пункте SP (ЛЦК) нелегитимное сообщение TFP о недоступности пунктов SP (АМТС). Это сообщение передается в пункты SP (GMSC). Последствием такой атаки DoS является отказ исходящим вызовам в установлении соединений через уровень транзитной сети GSM от абонентов АТС зоны обслуживания АМТС с мобильными станциями, которые обслуживаются мобильными станциями коммутации через GMSC.

Результаты анализа последствий реализации угроз нарушения маршрутизации ОКС-7. Реализация таких угроз может привести к отказу большому числу пользователей ССОП в установлении соединений между абонентами ТфОП/ISDN между мобильными станциями сети GSM, а также между абонентами ТфОП/ISDN и мобильными станциями GSM. Это относится как к соединениям без предоставления услуг интеллектуальной сети, так и с предоставлением таких услуг.

Степень нанесения ущерба работе ССОП от атак DoS в ОКС-7 зависит от нелегитимно используемых функций подсистем MTP и SCCP участков смежных пунктов сигнализации, подверженных действию нарушителя. Такие участки различных уровней иерархии сетей связи являются наиболее чувствительными к атакам DoS.

Результаты настоящей работы могут быть использованы при решении задач информационной безопасности действующих ССОП ТфОП/ISDN, GSM и IN. К таким задачам следует отнести анализ уязвимых мест для реализации угроз DoS MTP и SCCP ОКС-7, приводящей к значительному ущербу функционирования сетей ОП, а также тестирования защищенности от этих угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Д р а й б е р г Л., Х ь ю и т т Д. Система сигнализации № 7 (SS7/ОКС-7). Протоколы, структура и применение. – М.: Вильямс, 2007.
2. Л у к а ц к и й А. Безопасность Softswitch или плач Ярославны в эпоху NGN // Мобильные системы. – 2006. – № 5.
3. Б е л ь ф е р Р. А., Г о р ш к о в Ю. Г., Д а н н а в и М. Н. Архитектура сетевой безопасности ОКС-7 // Электросвязь. – 2009. – № 4.
4. Б е л ь ф е р Р. А., Г о р ш к о в Ю. Г. Система сигнализации ОКС-7. Требования к QoS и организации программного обеспечения сетевого уровня: Учеб. пособие. – М.: Изд-во МТУСИ, 2007.
5. А д ж е м о в А. С., К у ч е р я в ы й А. Е. Система сигнализации ОКС № 7 // Радио и связь. – 2002.
6. А н т о н я н А. Б. Новая редакция генеральной схемы создания и развития федеральной сети подвижной радиотелефонной связи общего пользования России стандарта GSM // Электросвязь. – 2003. – № 1.

Статья поступила в редакцию 15.01.2008

Рувим Абрамович Бельфер родился в 1937 г. Окончил Московский электротехнический институт связи в 1960 г. Канд. техн. наук, доцент кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор более 60 научных работ в области сетей передачи данных и информационной безопасности в системах и сетях связи.

R.A. Bel’fer (b. 1937) graduated from the Moscow Electric Engineering Institute for Communication in 1960. Ph. D. (Eng.), assoc. professor of “Information Security” department of the Bauman Moscow State Technical University. Author of more than 60 publications in the field of data transfer networks and data security in communication systems and networks.

Юрий Георгиевич Горшков родился в 1945 г. Окончил Новосибирский электротехнический институт связи в 1969 г. Канд. техн. наук, доцент кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор более 40 научных работ в области информационной безопасности и разработки защищенных систем связи.

Yu.G. Gorshkov (b. 1945) graduated from the Novosibirsk Electric Engineering Institute for Communication in 1969. Ph. D. (Eng.), assoc. professor of “Information Security” department of the Bauman Moscow State Technical University. Author of more than 40 publications in the field of data security and development of secured communication systems.

Мохамад Насреддин Даннави родился в 1981 г. Окончил Московский технический университет связи и информатики (МТУСИ) в 2006 г. Аспирант кафедры “Мультимедийные сети и услуги связи” МТУСИ. Автор ряда научных работ в области информационной безопасности в системах и сетях связи.

M.N. Dannavi (b. 1981) graduated from the Moscow Technical University for Communication and Information Technology in 2006. Post-graduate of “Multimedia Networks and Communication Services” department of the Moscow Technical University for Communication and Information Technology. Author of some publications in the field of data security in communication systems and networks.