ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.72.075

АРХИТЕКТУРА СЕТЕВОЙ БЕЗОПАСНОСТИ ОКС-7

Р.А. Бельфер, доцент МТУСИ, к.т.н.; belfer-ra@mail.ru
Ю.Г. Горшков, доцент МГТУ им. Н.Э. Баумана, к.т.н.
М.Н. Даннави, аспирант МТУСИ

Ключевые слова: *архитектура сетевой безопасности, общеканальная сигнализация №7, сеть подвижной связи GSM, интеллектуальная сеть, угрозы «отказ в обслуживании».*

В стандарте ITU-T X.805 [1] изложены общие положения архитектуры сетевой безопасности инфокоммуникационных (ИК) сетей, состоящих из сетей связи и средств доступа пользователей к необходимой информации, ее хранению и обработке [2]. Данная работа посвящена разработке архитектуры сетевой безопасности конкретной системы общеканальной сигнализации ОКС-7, являющейся составной частью сетей связи общего пользования (ССОП) России — телефонной сети ТфОП/ISDN, сотовой сети связи стандарта GSM и интеллектуальной сети IN.

Общие положения архитектуры сетевой безопасности ОКС-7. При разработке архитектуры сетевой безопасности ОКС-7 исходим из общих положений международных стандартов по архитектуре сетевой безопасности инфокоммуникационных сетей X.805 [1] и информационной безопасности (ИБ) международных сетей связи E.408 [3], а также национального стандарта России по ИБ ССОП [4]. При разработке учитываются особенности ОКС-7 как составной части ССОП [5,6].

Архитектура сетевой безопасности ОКС-7 должна включать комплексное рассмотрение аспектов ИБ и отвечать на следующие вопросы:

1) какие способы обеспечения ИБ ОКС-7 от атак необходимы при реализации угроз безопасности?

2) какие типы оборудования ОКС-7 и на каких уровнях эталонной модели OSI нуждаются в обеспечении ИБ?

3) какие функции ОКС-7 нуждаются в обеспечении ИБ?

Требования к обеспечению сетевой безопасности ОКС-7, входящей в ССОП, исходят от:

- международных организаций и государственных органов, регламентирующих деятельность операторов связи при решении задач ИБ инфокоммуникационных сетей;
- операторов ССОП, обеспечивающих свои обязательства перед потребителями услуг связи в условиях конкуренции;
- пользователей или абонентов ССОП.

Способы обеспечения ИБ в ОКС-7. Приведем краткое описание способов обеспечения защиты от угроз ИБ в ОКС-7: управление доступом, аутентификация, неотказуемость, безопасность связи, целостность данных, готовность (доступность). Перечисленные способы обеспечивают защиту от основных угроз ИБ в ОКС-7, также как и приведенные в рекомендации X.805 способы обеспечения ИБ в ИК-сетях обеспечивают защиту от основных угроз.

Управление доступом защищает от несанкционированного использования эксплуатационным персоналом или устройствами сети сетевых ресурсов ОКС-7 (пунктов сигнализации). Эксплуатационный персонал подсистемы эксплуатации и технического обслуживания OAM (Operation, Administration Maintenance) подлежит защите от действий несанкционированных пользователей.

Аутентификация гарантирует подлинность участвующих в связи пунктов сигнализации ОКС-7.

Неотказуемость обеспечивает средства для предотвращения отрицания выполнения конкретных действий нарушителя, т. е. доказательство того, что данные должны быть отправлены и получены легитимными пунктами сигнализации. При этом гарантируется наличие данных, которые могут быть представлены третьей стороне для исследования их в качестве доказательства того, что события такого рода имели место.

Безопасность связи в ОКС-7 гарантирует, что сообщение предназначено для пункта сигнализации назначения, в который возможно направить трафик из данного пункта сигнализации отправителя. Оператор связи должен выбрать список разрешенных пунктов сигнализации получателя в соответствии с топологией сети и маршрутизацией.

Целостность данных. Уверенность в том, что сообщения между пунктами сигнализации ОКС-7 не были изменены, удалены, созданы или задержаны нарушителем.

Готовность (доступность). Гарантия того, что нет отказа санкционированному доступу к пункту сигнализации или звену сигнализации ОКС-7, хранимой информации в пунктах сигнализации (например, в таблицах маршрутизации).

Уровни безопасности ОКС-7. Приведенные выше способы обеспечения ИБ относятся к группе оборудования ОКС-7, которые в соответствии с общими положениями по архитектуре сетевой безопасности в рекомендации X.805 называются уровнями безопасности (Security Layers). Учитывая особенности конкретной технологии для ОКС-7, способы обеспечения ИБ рассматриваются относительно двух уровней безопасности: инфраструктуры (Infrastructure Security) и приложений (Application Security). Взаимосвязь уровней безопасности основана на иерархическом принципе. Уровень безопасности инфраструктуры обеспечивает уровень безопасности приложений.

Уровень безопасности инфраструктуры относится к устройствам ОКС-7: оконечным, промежуточным и транзитным пунктам сигнализации. Все приведенные выше способы обеспечения ИБ могут применяться ко всем уровням эталонной модели OSI уровня безопасности инфраструктуры ОКС-7.

Способы обеспечения ИБ ОКС-7 на уровне безопасности инфраструктуры предназначены для уменьшения уязвимости к атакам, соответствующим угрозам ИБ. Система ОКС-7 разработана с учетом ее согласования с эталонной моделью OSI и также построена по многоуровнему иерархическому принципу. Оборудование ОКС-7 разделено на четыре уровня, из которых не все идентичны уровням эталонной модели OSI. Способы обеспечения ИБ ОКС-7 на уровне безопасности инфраструктуры позволяют защитить уязвимость на всех уровнях ОКС-7. Оборудование трех уровней ОКС-7 всех типов пунктов сигнализации (оконечный, промежуточный, транзитный) подвержены атакам соответствующих угроз ИБ. К ним относятся:

- физический, канальный и сетевой уровни подсистемы передачи сообщений MTP (Message Transfer Part);
- сетевой уровень подсистемы управления соединением сигнализации SCCP (Signaling Connection Control Point).

На четвертом уровне ОКС-7 безопасности инфраструктуры угрозы ИБ воздействуют на различные подсистемы пользователей ОКС-7 и, соответственно, не на всех пунктах сигнализации. В общем виде можно выделить две группы пользователей ОКС-7. К первой относятся пользователи, для которых большинство функций связи определено выбором информационного канала в сети ТфОП/ISDN или GSM (на участке от мобильной станции коммуникации и шлюза к ТфОП). Такая подсистема ISUP (ISDN User Part) используется для межстанционной сетевой сигнализации. К другой группе относятся пользователи, для которых функции не определены выбором информационного канала. К подсистемам таких пользователей на ССОП относятся подсистемы:

- пользователей мобильной связи стандарта GSM(MAP, Mobile Application Part);
- пользователей интеллектуальной сети (INAP, Intelligent Network Application Part);
- настраиваемых приложений для усовершенствованной мобильной логики (CAMEL, Customizable Application for Mobile Enhanced Logic) [7];
- эксплуатации, технического обслуживания и административного управления OAM.

Приведенные выше подсистемы в ОКС-7 используют общую часть, которая позволяет обеспечить интерфейс с подсистемой SCCP. Для этих целей применяется прикладная подсистема возможностей транзакций (TCAP, Transaction Capabilities Application Part).

В ССОП стандарта GSM к подсистемам пользователей, не выполняющих функции выбора информационного канала, относится прикладная подсистема базовых станций (BSSAP, Base Station Subsystem Application Part). Подсистема BSSAP включает две прикладные подсистемы: управления базовыми станциями(BSSMAP, Base Station Subsystem Management Application Part) и прямой передачи (DTA, Direct Transfer Application Part).

Уровень безопасности приложений относится к оборудованию сетей связи ОП России (ТфОП/ISDN, GSM, IN), составной частью которых является оборудование ОКС-7. Оборудование ОКС-7 входит в: ТфОП/ISDN — коммуникационные станции местной сети связи, междугородной и международной сети; GSM — центр коммутации мобильной сети связи, домашний и гостевой, транзитный и локальный центры коммутации; IN — узлы коммутации услуг и управления услугами.

Плоскости безопасности ОКС-7. Приведенные выше способы обеспечения ИБ относятся к функциям ОКС-7, которые в соответствии с общими положениями по архитектуре сетевой безопасности в рекомендации X.805, называются плоскостями безопасности (Security Plane). Плоскости безопасности ОКС-7 делятся на плоскости безопасности управления и транспортной сети.

Плоскость безопасности управления относится к защите функций эксплуатации и технического обслуживания OAM. Примером таких функций в ОКС-7 является управление звеньями сигнализации (ЗС), которое может быть разделено на активизацию и деактивизацию ЗС (канала). Активизация — это процесс создания канала для передачи сообщений сетевого уровня MTP. Обслуживающий персонал выполняет этот процесс путем вызова команд из интерфейса OAM (для осуществления запроса об активизации канала). Когда канал отрегулирован на канальном уровне MTP и прошел тестирование, он объявляется доступным для переноса сигнального трафика.

Дезактивизация выводит канал из рабочего состояния, делая его недоступным для переноса сигнального трафика. Подобно активизации, этот процесс инициализируется обслуживающим персоналом с помощью вызова команд из интерфейса OAM. Нарушение ИБ ОКС-7 может быть осуществлено злоумышленником путем ложной активизации или дезактивизации канала.

Плоскость безопасности транспортной сети относится к защите всех четырех уровней ОКС-7 при воздействии намеренных угроз, имеющих злой умысел нелегитимного использования основных функций. Ниже приводятся краткое описание этих функций ОКС-7[6,8], а также общие положения по наибольшему ущербу в ССОП при реализации этих угроз.

1. Подсистема пользователя ISUP совместно с подсистемой передачи сообщений MTP обеспечивает соединение со стационарными абонентами ССОП. Нарушение ИБ ОКС-7 при нелегитимном воздействии на функцию ISUP приводит к отказу в установлении соединений, проходящих через пункт сигнализации, которому принадлежит эта подсистема пользователя.

2. Подсистема пользователя MAP обеспечивает взаимодействие компонентов мобильной сети GSM (мобильные центры коммутации, базовые станции, контроллеры базовых станций, домашний регистр, гостевой регистр и др.). Нарушение ИБ ОКС-7 при нелегитимном воздействии на функцию ISUP приводит к отказу в установлении соединений мобильным станциям, приписанных к этому оборудованию.

3. Подсистема пользователя MAP выполняет функцию отслеживания местоположения абонента, роуминга, доставки коротких текстовых сообщений SMS и др. Нарушение ИБ ОКС-7 при нелегитимном воздействии на эти функции GSM может привести к отказу в установлении соединений с абонентами-роумерами, передаче SMS.

4. Подсистема INAP выполняет функцию предоставления услуги пользователю путем обмена сообщениями между двумя узлами IN — между узлом коммутации SCP услуг SSP и узлом управления услугами. Рассмотрим выполнение этой функции на упрощенном примере предоставления услуги «Приплата» (PRM, Premium Rate). Все сообщения между SCP и SSP можно разделить на две группы [9]:

- пересчет кода и номера услуги в адрес абонента услуги;
- определение размера оплаты и распределение оплаты между оператором связи, поставщиком услуги и пользователем услуги.

Нарушение ИБ ОКС-7 при нелегитимном воздействии на эти функции может привести к отказу в предоставлении услуги IN, неправильном распределении оплаты за услугу.

5. Уровни MTP с первого по третий включают функции передачи информации от одного пункта сигнализации к другому [10].

Функционирование каналов передачи сообщений обеспечиваются комбинацией подсистем первого (MTP1) и второго (MTP2) уровней. Основные функции MTP2:

- обнаружение ошибок в сигнальных единицах;
- коррекция ошибок с помощью повторной передачи;
- мониторинг ошибок в ЗС;
- управление потоком в случае, когда переполняется буфер приема подсистемы MTP2.

Нарушение ИБ ОКС-7 при нелегитимном воздействии на эти функции может привести к отказу одного ЗС.

6. Подсистема сетевого уровня MTP3 выполняет функции обработки сообщений сигнализации. Эта функция произво-

дит маршрутизацию сообщений для соответствующих сетевых адресатов. Если принимающий узел не является пунктом назначения, то МТР3 выполняет функцию маршрутизации (т. е. узел является транзитным STP). Если же принимающий узел является пунктом назначения, то используется функция доставки принятых сообщений соответствующей подсистеме пользователя или функция управления сетью сигнализации.

Нарушение ИБ ОКС-7 при нелегитимном воздействии на эти функции может привести к отказу в предоставлении соединений и/или услуг одновременно для большого числа абонентов ССОП, обслуживаемых данным пунктом сигнализации.

7. Подсистема сетевого уровня МТР3 выполняет функции управления сетью сигнализации. Эти функции с помощью набора специальных сообщений и процедур производят обработку отказов в сети таким образом, чтобы информационные сообщения могли достичь своих адресатов (если это возможно). Данные процедуры координируют ресурсы ОКС-7, которые становятся доступными или недоступными.

Отказ ЗС одного пункта сигнализации или отказ пункта сигнализации может повлечь недоступность проходящих через него маршрутов сигнализации к пункту сигнализации назначения, что в свою очередь может вызвать изменение таблицы маршрутизации и в других пунктах сигнализации ОКС-7.

Управление сетью сигнализации подразделяется на выполнение функций управления информационными потоками (УИП) и управления маршрутами (УМ). Функция УИП обеспечивает трансляцию информационных потоков сигнализации, которые представляют собой сообщения подсистемы ISUP и подсистем пользователей через SCCP (MAP,INAP и др.). Функция УИП состоит в перемещении информации к адресату в случае повреждений или перегрузок в ОКС-7 с наименьшими возможными потерями. Функция УМ обеспечивает обмен информацией между пунктами сигнализации для коррекции таблиц маршрутизации. Как только происходит событие, влияющее на доступность маршрутов, функция УМ посылает сообщения оповещения остальным пунктам сигнализации об изменении маршрутизации.

Нарушение ИБ ОКС-7 при отправлении ложных сообщений УМ создает нелегитимную коррекцию таблицы маршрутизации. В результате система УИП направляет в пункты сигнализации нелегитимные сообщения коррекции информационных потоков.

8. Функция УМ с помощью специальных сообщений МТР3 обеспечивает выполнение функций УИП при полной или ограниченной доступности сигнальных маршрутов.

Нарушение ИБ ОКС-7 при отправлении ложных сообщений УИП создает нелегитимную недоступность или нелегитимную доступность сигнальных маршрутов.

Результатом нарушений ИБ ОКС-7 при выполнении функций УМ и УИП может быть отказ в обслуживании одновременно большого числа пользователей ССОП (ТфОП/ ISDN, GSM, IN), являющихся абонентами двух и более оконечных узлов сетей ТфОП/ ISDN и GSM. Все это приводит к существенному нарушению функционирования ССОП, составной частью которых является ОКС-7.

9. Подсистема управления соединением SCCP расположена в стеке уровней ОКС-7 над подсистемой МТР и обеспечивает дополнительные функции сетевого уровня в части управления прикладными системами (в сетях GSM, IN и др.). Подсистема SCCP вместе с подсистемой МТР3 соответствует третьему (сетевому) уровню ОКС-7 и при этом дает возможность передавать информацию, несвязанную с информационным каналом.

Подсистема SCCP выполняет следующие функции [11]:

- дополнительную маршрутизацию (кроме той, которая обеспечивается подсистемой МТР3), используя номера подсистем SSN (Subsystem Number) и глобальные заголовки (Global Title). Эта функция называется управлением маршрутизацией SCCP;
- отслеживание состояния подсистемы, которые могут работать с SCCP-функциями (отслеживание состояния удаленного SCCP-пункта, а также локальных подсистем пользователя). Эта функция называется управлением подсистемой SCCP. С помощью специальных сообщений она передает состояние удаленного SCCP-пункта, а также локальных подсистем (состояние доступности или недоступности, перегрузки). Программы маршрутизации управления подсистемой SCCP отправляют сообщения остальным узлам для информирования их об отказе.

Нарушение ИБ ОКС-7 в результате передачи ложных сообщений управления подсистемой SCCP может привести к нелегитимному отказу в обслуживании SCCP, подсистем (MAP,INAP, OMAP), локальных подсистем (центр коммутации мобильной сети GSM, домашний и гостевой регистры GSM и др.). Все это может привести к отказу в обслуживании в ССОП.

Угрозы ИБ типа «отказ в обслуживании». Как отмечено в [12], диапазон угроз ИБ в сетях связи настольно широк, что создание их полной классификации вызывает затруднения. Определим тип угроз ОКС-7, которые оказывают набольшее воздействие на ИБ ССОП.

Для ОКС-7 характерна высокая степень централизации ее функций. Этим объясняется высокое требование к коэффициенту неготовности пучка сигнальных маршрутов, представляющих совокупность всех маршрутов между исходящим и входящими пунктами сигнализации. Коэффициент неготовности пучка маршрутов согласно требованиям, изложенным в рекомендации Q.706 [13], не должен быть выше $1{,}9 \cdot 10^{-5}$ (т. е. 10 мин. неготовности в течение 1 года). Неготовность пучка маршрутов определяется согласно рекомендации Q.706 неготовностью различных элементов сети сигнализации (звеньев и пунктов), а также структурой данной сети.

Другим примером высоких требований к надежности ОКС-7 является норма к коэффициенту неготовности транзитного центра коммутации (ТЦК) транзитной федеральной сотовой сети GSM России. Основная часть оборудования ТЦК составляет ОКС-7. Коэффициент неготовности ТЦК не должен быть выше $5 \cdot 10^{-5}$ по отказам 2-го типа (прерывание и невозможность восстановления всех связей или потеря 50% коммуникационной емкости в течение более 2 мин.) [14].

Необходимо подчеркнуть, что нормы неготовности пучка маршрутов и отдельного оборудования рассматриваются с учетом только аппаратно-программных отказов. Воздействие атак, соответствующих угрозам ИБ, при этом не рассматривалось. В то же время приведенные выше примеры нарушения ИБ некоторых функций ОКС-7 показывают, что характеристики последствий воздействия угроз ИБ могут быть более серьезными, чем, например, прекращение функционирования конкретного пучка маршрутов.

В первую очередь это относится к использованию нарушителем передачи нелегитимных сообщений обновления маршрутизации на сетевом уровне ОКС-7. Результатом может стать одновременный отказ не одного, а нескольких пучков маршрутизации. В конечном счете это может отразиться на выводе из работы целого фрагмента ССОП. Такой тип угрозы часто называют «отказ в обслуживании» (DoS, Denial of Service).

Как показано в [15] на примере IN и подвижной сети связи третьего поколения UMTS, одной из основных характеристик угроз ИБ является результат последствия воздействия угрозы. Для угрозы DoS ОКС-7 это отражается на нарушении функционирования сетей связи ОП, т. е. последствия угроз DoS ОКС-7 относятся к отказу в обслуживании одновременно большого числа пользователей ССОП: ТфОП/ISDN и GSM. Таким образом, потенциальный ущерб от угроз DoS ОКС-7 выражается в отказе пользователям ССОП установления соединений или предоставления услуг IN.

Выводы. В результате нелегитимного использования функций ОКС-7 угрозы ИБ типа «отказ в обслуживании» (DoS) могут быть причиной нанесения значительного ущерба путем прекращением выполнения функций ССОП (ТфОП/ISDN, GSM, IN). Этот ущерб выражается в отказе установления соединении между пользователями и/или в предоставлении услуг IN и может относиться одновременно к большому числу абонентов ССОП. Причиной таких последствий могут стать ложные сообщения обновления таблиц маршрутизации ОКС-7, отправляемые нарушителем.

ЛИТЕРАТУРА

1. ITU-T Recommendation X.805. Security architecture for System providing end-to-end communication, 2003.
2. **Москвитин В.Д.** От взаимосвязанной сети связи к Единой сети электросвязи России // Вестник связи. — 2003. — №8.
3. ITU-T Recommendation E.408. Telecommunication Network Security Requirement, 2004.
4. ГОСТ Р 524.48—2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. — М.: Стандартинформ, 2006.
5. **Росляков А.В.** ОКС-7 архитектура, протоколы, применение. — М.: Эко-Трендз, 2008.
6. **Драйберг Ли, Хьюит В.** Система сигнализации №7 (SS7/ОКС7), протоколы, структуры и применение. — М.: Вильямс, 2007.
7. **Заболотный И.** МТТ берет интеллектом // Сети и системы связи. — 2008. — №6.
8. **Боккер П.** ISDN. Цифровая сеть с интеграцией служб. Понятия, методы, системы. — М.: Радио и связь, 1991.
9. **Лихтиндер Б.Я., Кузякина М.А., Росляков А.В., Фомичев С.М.** Интеллектуальные сети связи. — М.: Эко-Трендз, 2000.
10. ITU-T Recommendation Q.704: Specifications of Signaling System №7. Message transfer part. Signaling network function and messages, 1996.
11. ITU-T Recommendation Q.714: Specifications of Signaling System №7. Signaling Connection Control Part Procedures, 2001.
12. **Уинстром М.** Организация защиты сетей Cisco. — М.: Вильямс, 2005.
13. ITU-T Recommendation Q.706: Specifications of Signaling System №7. Message transfer part signaling performance, 1993.
14. **Мардер Н.С.** Электросвязь в Российской Федерации / Уч. пособие. — М.: ИРИАС, 2004.
15. **Бельфер Р.А.** Классификация угроз информационной безопасности сетей связи ВСС России (ISDN, IN, UMTS) и методы их количественной оценки // Электросвязь. — 2002. — №7.

Получено 2.03.09