УДК 621.392

АНАЛИЗ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ GSM ПРИ ВЫПОЛНЕНИИ ФУНКЦИЙ ЗАЩИТЫ ПРИВАТНОСТИ

Ю.Г. Горшков, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н.; y.gorshkov@rambler.ru
Р.А. Бельфер, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н.

Ключевые слова: *информационная безопасность, отказ в обслуживании (DoS), риски, регистрация, сигнализация, ОКС-7, угроза, приватность.*

Введение. Имеется довольно много причин для возникновения угроз вывода из рабочего состояния сетей связи в целых регионах страны, когда нарушается информационная безопасность (ИБ) системы сигнализации ОКС-7. Проблемам, ведущим к простоям сети ОКС-7, посвящается работа [1]. В работах [2–4] даются анализ и примеры возможных угроз ИБ, реализация которых злоумышленником может приводить к атаке DoS (Denial of Service – отказ в обслуживании) в системе сигнализации ОКС-7 сетей связи общего пользования (ССОП). Для этого достаточно отправить в смежные пункты сигнализации определенные нелегитимные сообщения подсистемы управления сетью сигнализации сетевого уровня ОКС-7, выполняющие функции обновления маршрутизации. В результате такой атаки выполнение функций маршрутизации ОКС-7 в ТфОП/ISDN, GSM, сети VoIP при конфигурации соединений абонентов ТфОП/ISDN через SIP-T будет нарушено [5].

В отличие от отечественных авторов [3–5] немецкий профессор Г. Руфа в своей книге [1] анализирует простои сети из-за угроз ИБ при создании перегрузок в сети, вызывающих потери этих же сообщений обновления маршрутизации подсистемы управления сетью сигнализации ОКС-7.

В данной статье анализируется риск ИБ сети GSM от атак DoS при определенной функции, выполняемой сетью. В качестве такой функции взята процедура информационной безопасности сети GSM – защита приватных данных местоположения абонента-роумера. Согласно Рекомендациям МСЭ-Т Е.408 [6], распространяющимся на требования к безопасности сетей электросвязи, характеристика риска ИБ определяется двумя показателями: вероятностью угрозы безопасности и последствием ее воздействия при атаке злоумышленника (реализации этой угрозы). Кроме того, ниже приводится сравнительный анализ этих показателей риска ИБ в результате указанной выше DoS-атаки в ОКС-7 при выполнении функции защиты приватных данных местоположения абонента-роумера мобильной станции (MS) и при отсутствии необходимости выполнения такой функции защиты. Рассмотрению подлежат процедуры защиты приватных данных местоположения MS абонента-роумера: при регистрации MS в гостевой сети и при вызове MS абонента-роумера из ТфОП/ISDN. Защита приватных данных местоположения не требуется при обслуживании MS, находящейся в домашней сети ее приписки.

Зависимость риска ИБ от места атаки DoS в иерархической структуре ОКС-7. Структура ОКС-7 Единой сети электросвязи России построена на многоуровневой иерархической структуре в составе ТфОП/ISDN и в составе сети оператора МТТ («Межрегиональный Транзит Телеком») [7]. Из примеров угроз DoS в ОКС-7 следует, что передача злоумышленником фиктивных сообщений обновления маршрутизации управления сетью сигнализации подсистемы передачи сообщений (Message Transfer Part, MTP) может привести к различным нарушениям при выполнении маршрутизации.

Наиболее уязвимыми с этой точки зрения являются участки сети ОКС-7 между пунктами сигнализации смежных уровней иерархии. Последствия атак DoS в ОКС-7 зависят от направления передаваемых злоумышленником сообщений. Передача таких сообщений подсистемы управления сетью сигнализации, как запрещение переноса трафика (Transfer Prohibited, TFP) от пункта сигнализации ОКС-7 верхнего уровня иерархии к пункту сигнализации смежного нижнего уровня, может приводить к прекращению обработки вызовов от абонентов, осуществляемой узлом нижнего уровня иерархии.

Последствия такой атаки могут быть самыми разными. Например, злоумышленник из зоновой АМТС может передать хотя бы в одну из АМТС зоны два нелегитимных сообщения TFP о недоступности пункта сигнализации этой зоновой АМТС с двумя соединенными с ней пунктами сигнализации узлов автоматической коммутации (УАК). В результате пользователям этой АМТС зоны невозможно предоставить установление междугородных и международных соединений по исходящим от них вызовам. Передача этих сообщений от пункта сигнализации нижнего уровня иерархии к пункту сигнализации смежного верхнего уровня может приводить к прекращению выполнения функций по установлению соединений для входящих вызовов, обрабатываемых узлом нижнего уровня иерархии.

Если сообщения TFP о недоступности пункта сигнализации АМТС зоны от пункта сигнализации зоновой АМТС будут переданы в пункты сигнализации двух соединенных с ней УАК, прекращается предоставление установления междугородных и международных соединений по входящим вызовам ко всем пользователям этой АМТС зоны.

Приведем особенности информационной безопасности сетей GSM при выполнении функций защиты приватности.

Риск ИБ при атаке DoS в ОКС-7 на процедуру регистрации мобильной станции абонента-роумера. Рассмотрим возможности защиты приватных данных местоположения при регистрации MS абонента-роумера в гостевой сети и при вызове абонента-роумера из ТфОП/ISDN. Покажем, что следствием DoS-атаки ОКС-7 может стать отказ в регистрации мобильной станции в гостевой сети, а это в свою очередь приводит к одновременному отказу гостевым абонентам в установлении как исходящих, так и входящих вызовов.

Для аутентификации пользователя и шифрования/дешифрования речи на радиоучастке сетевое устройство абонента-роумера должно знать ключ абонента-роумера пользователя, который связан с международным идентификатором абонента (International Mobile Subscriber Identity, IMSI). Этот уникальный идентификатор абонента в сети GSM записан в SIM-карту. Передача ключа и международного идентификатора IMSI на радиоучастке сети недопустима. Использование при аутентификации пользователя IMSI накладывает

требование скрыть его для защиты от незаконного получения приватных данных, к которым относится местоположение мобильной станции абонента-роумера.

В стандарте Альянса 3GPP [8] приведен формат IMSI, включающий идентификатор страны постоянного места жительства абонента, идентификатор сети мобильного GSM-оператора, идентификационный номер мобильной станции конкретного абонента мобильной связи. Перехват IMSI на радиоучастке позволяет нарушителю обнаружить личность пользователя, передающего сообщение. Для того чтобы можно было вызывать MS, оказавшуюся в гостевой сети, или чтобы эта MS могла установить исходящее соединение, необходимо выполнить процедуру регистрации. В SIM-карте мобильной станции содержится идентификатор области местоположения мобильного абонента (Local Area Identity, LAI). Процедура регистрации (обновление местоположения MS) начинается после включения питания мобильной станции. При этом MS посылает на базовую станцию запрос на проведение регистрации. Запрос содержит идентификатор области местоположения MS (LAI) и временной идентификатор мобильной станции TMSI (Temporary Mobile Subscriber Identity), значение которого уникально для каждой MS.

Код TMSI также описан в стандарте [8]. Параметр TMSI используется вместо IMSI из соображений приватности местоположения абонента, чтобы предотвратить его перехват злоумышленником. С помощью кода TMSI в широковещательном режиме выполняется процедура определения абонента в сети. Запрос попадает в MSC (Mobile service Switching Center – коммутирующий центр услуг мобильной связи) и в VLR (Visitors Location Register – временную базу данных абонентов, которые находятся в зоне действия определенного MSC) через базовую станцию и контроллер базовой станции. При поступлении MS абонента-роумера в новую гостевую сеть в VLR не будет TMSI пользователя, запрашивающего регистрацию. В этом случае производится декодирование LAI, полученного от мобильной станции. LAI вместе с TMSI определяет VLR, которая ранее обслуживала данную MS. С помощью сообщений подсистемы мобильных приложений (Mobile Application Part, MAP) ОКС-7 устанавливается соединение текущего VLR с предыдущим.

В свою очередь VLR передает по протоколу MAP текущей VLR параметры пользователя: идентификатор IMSI, коды RAND, SRES, ключ шифрования и др. Полученные данные позволяют произвести в новой зоне обслуживания абонента-роумера аутентификацию мобильной станции, а также шифрование данных [9]. После успешного завершения этой процедуры с помощью сообщений MAP производится смена параметров местоположения LAI и временного идентификатора местоположения TMSI.

Последствия такой DoS-атаки, когда злоумышленник отправляет нелегитимные сообщения обновления маршрутизации для тех абонентов-роумеров гостевой сети, мобильные станции которых не смогли выполнить процедуру регистрации, выражаются в отказе установления входящих и исходящих соединений. Это может иметь место при прекращении функционирования маршрута ОКС-7 между VLR, которая ранее обслуживала данную MS абонента-роумера, и текущей VLR. При большом удалении их друг от друга по сети ОКС-7 и при пересечении нескольких уровней иерархии показатель риска, выраженный вероятностью атаки DoS, выше для MS абонентов-роумеров. Другой показатель риска (последствие атаки) при отказе в регистрации MS и отказе принятия на обслуживание гостевой сетью для абонентов-роумеров хуже, чем при отказе на установление или прием вызовов. Для абонентов-роумеров гостевой сети, MS которых выполнили процедуру регистрации, последствия такой атаки DoS аналогичны последствиям при отказе установления исходящих соединений (входящих от них вызовов) абонентов – мобильных пользователей GSM, находящихся в зоне обслуживания приписки MS. Для выполнивших процедуру регистрации MS абонентов-роумеров имеет место дополнительный риск ИБ при установлении входящих к ним вызовов. Этому посвящен следующий раздел.

Риск ИБ при атаке DoS в ОКС-7 на процедуру вызова мобильной станции абонента-роумера из ТфОП/ISDN. Процедура вызова MS абонента-роумера из ТфОП/ISDN по сравнению с процедурой вызова MS, находящейся на обслуживании в домашней сети, требует обмена дополнительными сообщениями прикладного уровня ОКС-7. Это вызвано необходимостью переадресации в гостевую сеть с выполнением защиты приватных данных местоположения MS абонента-роумера. При этом между домашней сетью приписки MS и обслуживающей сетью MS абонента-роумера может быть транзитная сеть ОКС-7 с большим числом промежуточных пунктов сигнализации с несколькими уровнями иерархии. Это увеличивает риск ИБ при атаках DoS в ОКС-7 на процедуру вызова мобильной станции абонента-роумера из ТфОП/ISDN.

Приведем сообщения по обеспечению защиты приватных данных местоположения MS абонента-роумера и покажем, между какими конечными пунктами сигнализации и по какому протоколу прикладного уровня ОКС-7 они передаются.

При установлении вызова MS абонента-роумера из ТфОП/ISDN вызывающий абонент через ТфОП/ISDN отправляет начальное адресное сообщение IAM подсистемы ISUP ОКС-7. В адресную часть этого сообщения входит международный номер ISDN вызываемой мобильной станции (Mobile Station International ISDN Number, MSISDN), определенный стандартом ITU-T E.164. Этот номер используется вызывающей стороной, чтобы установить соединение с вызываемой стороной. Он связан с модулем SIM, принадлежащим пользователю, и является его мобильным абонентским номером. MSISDN состоит из кода страны, национального кода адресата (адреса сетевого поставщика услуг и регистра HLR) и номера абонента. Сеть ТфОП/ISDN через ОКС-7 транслирует это сообщение шлюзу GMSC, который на основании MSISDN определяет регистр HLR домашней сети GSM. Подсистема MAP отправляет маршрутную информацию от GMSC в HLR для определения вызываемой мобильной станции MS. Это сообщение ОКС-7 MAP содержит в качестве одного из параметров идентификатор IMSI. В регистре HLR имеется информация о местоположении вызываемой MS (указан адрес регистра VLR).

Рассмотрим пример, когда вызываемая станция MS находится в гостевой сети. Следующее сообщение (1) подсистемы MAP «Запрос номера» MSRN из HLR домашней сети в VLR гостевой сети запрашивает роуминговый номер вызываемой мобильной станции MSRN (Mobile Station Roaming Number). Использование MSRN вызвано необходимостью скрыть местоположение абонента (это приватная информация) [10]. Регистр VLR назначает номер MSRN из пула свободных номеров. Данный номер временный, действует только до окончания установления соединения и определяется на основании международного идентификатора мобильного абонента IMSI.

MSRN включает гостевой код страны, текущий центр коммутации MSC, номер абонента и др. Регистр VLR пере-

сылает присвоенный в сообщении (2) MAP временный номер MSRN в HLR домашней сети. Далее MSRN пересылается в шлюз GMSC (3). Шлюз GMSC отправляет сообщение (4) на установление соединения IAM подсистемы ISUP в текущий MSC. В адресной части IAM содержится полученный номер MSRN, включающий адрес MSC.

Теперь, когда входящий вызов достиг нужного MSC, определяется идентификатор IMSI и дальнейшие процедуры протокола MAP ОКС-7 не требуются. Номер MSRN возвращается в пул для использования при дальнейших вызовах.

Начиная с этого этапа за все дальнейшие шаги в роуминговой сети отвечает центр MSC – до тех пор, пока регистр VLR не посылает MSC сигнал об установлении соединения с мобильной станцией. При успешном вызове абонента-роумера обслуживающий центр отправляет сообщение «Ответ» (ANM) подсистемы ISUP в шлюз GMSC (5) и далее назад – коммутатору вызывающей стороны в сети ТфОП/ISDN.

Приведенные участки сети ОКС-7 являются дополнительными и предназначены в основном для обеспечения приватности местоположения при вызове MS абонента-роумера. На трех участках передаются сообщения подсистемы пользователя MAP (три сообщения: два между HLR и VLR, одно между HLR и GMSC) и на двух – сообщения пользователя ISUP (два сообщения – между GMSC и MSC). Здесь HLR находится в сети приписки MS, а VLR и MSC – в обслуживаемой гостевой сети. При отсутствии функции обеспечения защиты приватности местоположения не требовалось бы и использовать большинство этих дополнительных участков ОКС-7. Расширение области сети ОКС-7, задействованной для выполнения функции защиты приватности, повышает риск ИБ.

Риск ИБ (как по показателям вероятности, так и по последствиям указанных атак DoS) при вызове MS абонентов-роумеров тем выше, чем больше удалены друг от друга указанные устройства сети ОКС-7 и чем больше пунктов сигнализации смежных уровней иерархии пересекаются.

Выводы. Качественные показатели риска информационной безопасности от воздействия DoS-атак (отказ в обслуживании) в ОКС-7 зависят от выполняемых функций в сети GSM. В статье показана зависимость обоих показателей риска ИБ (вероятности и последствий указанных атак DoS) в ходе выполнения функции защиты приватных данных местоположения мобильной станции абонента-роумера при ее регистрации и вызове.

ЛИТЕРАТУРА

1. **Rufa G.** Developments in Telecommunications. With a Focus on SS7 Network Reliability //Springer, 2009.
2. **Драйберг Ли, Хьюит В.** Система сигнализации № 7 (SS7/ОКС-7), протоколы, структура и применение. – М.: Вильямс, 2006.
3. **Бельфер Р.А., Горшков Ю.Г.** Система сигнализации ОКС-7. Требования к QoS и организация программного обеспечения сетевого уровня. – М.: Информсвязьиздат, 2007.
4. **Бельфер Р.А., Горшков Ю.Г., Даннави М.Н.** Оценка снижения последствий угроз нарушений маршрутизации в общеканальной сигнализации сетей связи общего пользования // Вестник МГТУ им. Н.Э. Баумана, Сер. «Приборостроение». – 2009. – № 4.
5. **Бельфер Р.А., Морозов А.М.** Информационная безопасность сети связи для соединений абонентов ТфОП/ISDN через SIP-T // Электросвязь. – 2012. – № 3. – С. 15.
6. ITU-T Recommendation E.408. Telecommunication Network Security Requirement, 2004.
7. **Мардер Н.С.** Электросвязь в Российской Федерации /Учеб. пособие. – М.: ИРИАС, 2004.
8. 3GPP TS 23.003. Technical Specification Group Core Network; Numbering, addressing and identification, 2006.
9. **Веселовский К.** Системы подвижной радиосвязи. – М.: Горячая линия, 2006.
10. GSM 03.03. Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification, 1996.

Получено 29.02.12