МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 621.391

ОЦЕНКА УРОВНЯ РИСКА БЕЗОПАСНОСТИ АТАКИ DOS-ФУНКЦИЙ МАРШРУТИЗАЦИИ СИСТЕМЫ СИГНАЛИЗАЦИИ ОКС-7 В СЕТИ GSM

В.А. Матвеев, **Р.А. Бельфер**, **Е.В. Глинская**

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: v.a.matveev@bmstu.ru; a.belfer@yandex.ru; glinskaya-iu8@rambler.ru

Выполнена оценка уровня риска безопасности атаки DoS-функций маршрутизации системы сигнализации общеканальной сигнализации ОКС-7 в сети GSM. Знание уровня риска угроз информационной безопасности позволяет при испытаниях и эксплуатации сети связи принимать решения по повышению информационной безопасности за счет усиления защиты от угроз, которым соответствует наиболее высокий уровень риска. Причиной актуальности поставленной задачи является недостаточная защищенность в ОКС-7 сети GSM существующих механизмов (брандмауэров) и разработка новых нестандартизированных механизмов защиты от атак нарушения маршрутизации. Показано, что системы сигнализации ОКС-7 и SIP с точки зрения поставленной задачи имеют много общего. Для системы SIP существуют разработанные методики для ранжирования угроз безопасности, которые положены в основу разработки методики ранжирования угроз DoS в ОКС-7. Предложены изменения для внесения в ранее разработанные методики оценки уровня угроз безопасности находящейся в эксплуатации системы сигнализации SIP мультимедийной сети нового поколения VoIP. При этом учтены специфика находящейся в эксплуатации ОКС-7, а также отсутствие возможности тестирования с имитацией угроз. Эти изменения относятся к расчетам уровня безопасности DoS-атак и ущерба при их реализации, которые являются исходными параметрами для расчета уровня риска безопасности. Сравнение трех предложенных методик ранжирования безопасности DoS-атак в ОКС-7 (на основе теории нечетких множеств, методов анализа иерархий AHP и анализа пар AHP) по достоверности результатов не представляется возможным из-за использования в них разных алгоритмов с разными характеристиками субъективных экспертных данных.

***Ключевые слова*:** общеканальная сигнализация № 7, подсистема передачи сообщений, подсистема управления соединениями сигнализации, GSM, угроза, отказ в обслуживании, пункт сигнализации.

ASSESSING THE SECURITY RISK OF ATTACKS DOS-ROUTING FUNCTIONS OF THE SIGNALING SYSTEM SS7 IN THE GSM NETWORK

V.A. Matveev, **R.A. Belfer**, **E.V. Glinskaya**

Bauman Moscow State Technical University, Moscow, Russian Federation
e-mail: v.a.matveev@bmstu.ru; a.belfer@yandex.ru; glinskaya-iu8@rambler.ru

The article describes the development of the methodology for assessing the security risk level of attacks of DoS routing functions of CCS7 signaling system in the GSM network. Awareness of the risk level of information security threats allows making

decisions which will improve the by means of information security during both communication network operation and its testing by means of increasing the protection against the threats, which risk level is the highest one. The problem is considered relevant because of the lack of necessary security mechanisms (firewalls) as well as the development of modern non-standardized mechanisms for protection against the attacks disturbing routing of CCS7 in the GSM network. It is shown that the signaling systems CCS7 and SIP have much in common in terms of this problem. For SIP system, there are some developed techniques for ranking the security threats, which seem to be the basis for the further development of the methodology of ranking DoS threats in CCS7. The authors propose some changes to be introduced into the previously developed methodology, which is used to assess the level of the security threats to SIP signaling system, being in service in the new generation VoIP multimedia network. Distinguishing features of the operating CCS7 are taken into account. It is also important to consider the lack of their testing with simulated threats. These changes relate to the calculation of the security levels of DoS attacks and possible damages during their implementation, which are the initial parameters for the calculation of the security risk level. It does not seem to be possible to compare these three proposed methods of ranging security of DoS attacks in CCS7 (based on the theory of fuzzy sets, the analytic hierarchy process, AHP, and analysis of AHP pairs) accoding to their result reliability due to using different algorithms with different characteristics of the subjective expert estimates.

***Keywords*:** common channel signaling No. 7, CCS7, message transfer part, MTP, signaling connection control part, SCCP, GSM, threat, denial of service, DoS, signaling point, signal point.

Знание уровня риска угроз информационной безопасности (ИБ) позволяет при проектировании, испытаниях и эксплуатации сети связи принимать решения по повышению ее ИБ за счет усиления защиты от угроз, которым соответствует наиболее высокий уровень риска. Во всех работах по определению уровня риска угрозы безопасности в сетях связи используются субъективные экспертные данные. От достоверности этих данных во многом зависит достоверность результатов ранжирования угроз безопасности. В работах [1, 2] выполнен анализ существующих методик ранжирования угроз безопасности, которые можно разделить на общие для технологий всех сетей связи или сетей определенной группы технологий и предназначенные для конкретных сетей связи. К конкретным сетям связи, для которых разработаны методики ранжирования угроз ИБ, относятся: мобильная сеть связи третьего поколения UMTS, беспроводная сеть стандарта IEEE 802.11, сети гибкого коммутатора (Softswitch) и др. Используя этот анализ разработали методики ранжирования угроз в другой технологии — системе сигнализации SIP (Session Initiation Protocol) сети связи нового поколения [1–4]. Настоящая работа посвящена разработке методики для системы сигнализации ОКС-7 в сети GSM.

С точки зрения поставленной задачи для методик ОКС-7 и SIP общее заключается в том, что они являются системами сигнализации находящихся в эксплуатации сетей связи общего пользования. Решение поставленной задачи построено на анализе необходимых изменений

методик ранжирования угроз в SIP в целях учета особенностей ОКС-7 и угроз в ней.

Это дает основание положить в основу разработки методики ранжирования DoS-угроз в ОКС-7 методики для угроз в системе SIP. В работах [1, 2] предложены три методики оценки уровня DoS-угроз и фрода находящейся в эксплуатации системы сигнализации SIP мультимедийной сети связи VoIP (Voice over IP) с использованием данных, полученных при тестировании с имитацией угроз. Две из них, кроме экспертных данных, используют математические аппараты — теорию нечетких множеств и нечеткой логики или методы анализа иерархий (Analytic Hierarchy Process – AHP) и анализа пар (Set Pairs Analysis — SPA). Третья методика построена на основе только экспертных данных.

Для методики на основе нечетких множеств и нечеткой логики, а также для методики на основе только экспертных данных при определении ранга угрозы характерно непосредственное использование количественных значений результатов тестирования (значений уровней безопасности угроз и ущерба при их реализации). В методике на основе методов AHP и SPA эти результаты тестирования с имитацией угроз учитываются косвенно по результатам опроса экспертов при составлении матрицы парных соединений и определении уровня потерь от каждой угрозы. Это может отрицательно отразиться на достоверности результатов ранжирования угроз безопасности.

Настоящая работа построена на анализе особенностей этой системы сигнализации и учета этих особенностей при разработке методики ранжирования угроз ИБ в ОКС-7 сети GSM. При этом следует обосновать выбор видов угроз, подлежащих ранжированию; провести анализ алгоритмов реализации этих угроз; определить уровни безопасности угроз и ущерба при их реализации. Прежде чем перейти к этим вопросам, рассмотрим архитектуры построения системы ОКС-7 в GSM.

Архитектура сети GSM. Для системы ОКС-7 в GSM характерен иерархический принцип архитектуры. В РФ эксплуатируются две архитектуры сетей GSM на базе системы сигнализации ОКС-7: федеральная сеть GSM ЗАО “Межрегиональный Транзит Телеком” (МТТ) [5, 6] и сеть GSM ЗАО “Ростелеком”, построенная на системе сигнализации ОКС-7 телефонной сети связи общего пользования (ТфОП)/ISDN (Integrated Services Digital Network). Последняя архитектура широко используется во многих странах мира [7–9].

На рис. 1 приведена упрощенная схема архитектуры федеральной сети GSM оператора связи МТТ, построенная на системе сигнализации ОКС-7 и представляющая собой иерархическую структуру. В каждом устройстве ОКС-7 выполняются функции сигнализации.

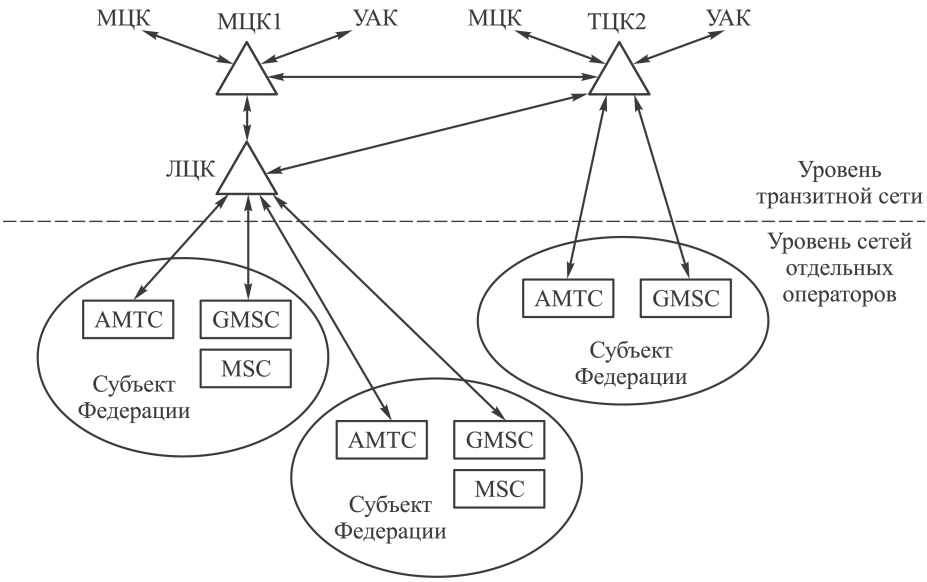

Рис. 1. Архитектура федеральной сети GSM

Первый уровень включает в себя мобильные центры коммутации (Mobile Switching Center — MSC), шлюз мобильного центра коммутации (Gate MSC — GMSC).

Взаимодействие сети GSM со стационарной сетью ТфОП/ISDN осуществляется через GMSC, к которому подключены мобильные центры коммутации. Второй уровень иерархии GSM – транзитная сеть, представляющая собой транзитные центры коммутации (ТЦК), выполняющие для мобильных абонентов те же функции, что и узел автоматической коммутации (УАК) для ТфОП/ISDN. Все ТЦК соединены между собой по полносвязной схеме. Показано взаимодействие ТЦК с международным центром коммутации (МЦК), УАК сети ТфОП/ISDN. При взаимодействии федеральной сети GSM с фиксированной сетью ТфОП на междугородном уровне возможны соединения мобильной станции с телефонным аппаратом (ТА) фиксированной сети ТфОП: MS–MSC–GMSC–ТЦК–УАК–АМТС–АТС–ТА. Кроме ТЦК уровень транзитной сети может включать в себя локальные центры коммутации (ЛЦК), которые являются промежуточным уровнем иерархии федеральной сети GSM. Локальные центры коммутации (узлы доступа к транзитной сети) соединяются не менее чем с двумя ТЦК. В этом случае взаимодействие мобильной станции и стационарного телефонного абонента при междугородней связи осуществляется по схеме: MS–MSC–GMSC–ЛЦК–ТЦК–УАК–АМТС–АТС–ТА.

Взаимодействие мобильной станции при международной связи осуществляется через МЦК по схеме: MS–MSC–GMSC–ЛЦК–ТЦК–УАК–МЦК(страны) — МЦК (другой страны) — и далее, через устройства, которые определяются архитектурой сети GSM в этой стране.

На рис. 2 приведена архитектура системы ОКС-7 сети ТфОП/ISDN, обеспечивающая сигнализацию в сети GSM. Эта схема не соответствует конкретной сети, хотя выполняет достаточную детализацию поставленной в настоящей работе задачи.

На рис. 2 показаны узлы коммутации всех уровней (местный, междугородний и международный) сети ТфОП/ISDN операторов связи страны и МЦК оператора связи взаимодействующей страны. В каждом узле коммутации показан соответствующий пункт сигнализации: SEP (Signaling End Point) – оконечный пункт сигнализации; SP (Signaling Point) — промежуточный пункт сигнализации; STP (Signaling Transfer Point) — транзитный пункт сигнализации.

Атаки DoS в ОКС-7 сети GSM. Дифференцированный подход к ранжированию отдельно по каждому типу угроз безопасности имеет преимущества в отношении получения более достоверных результатов. В методиках для SIP рассматриваются угрозы фрода и DoS-атаки. Система ОКС-7 в сети GSM подвержена разным видам угроз безопасности. Например, в работе [10] анализируются угрозы нарушения приватных данных пользователя и механизмы защиты от них. При решении выбора вида угроз для методики ранжирования исходим из ожидаемого наиболее высокого риска безопасности. В работах [7, 9,

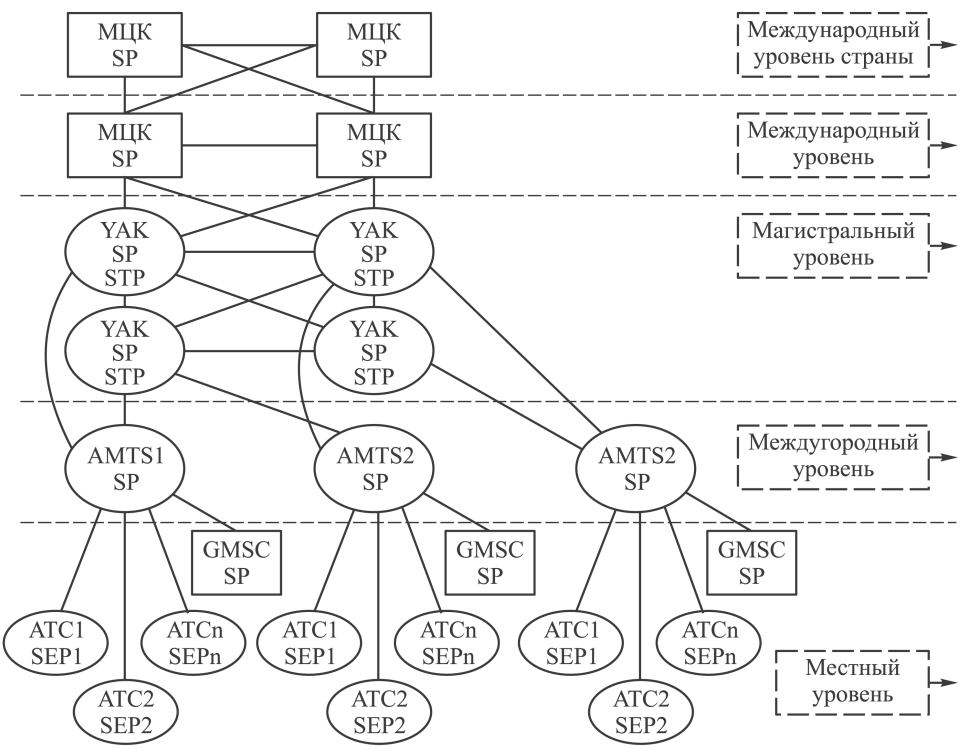

Рис. 2. Архитектура системы ОКС-7 сети ТфОП/ISDN, обеспечивающая сигнализацию в сети GSM

11, 12] показано, что такими угрозами ИБ являются нелегитимные сообщения ОКС-7 функций маршрутизации подсистемы передачи сообщений MTP (Message Transfer Part) и подсистемы управления соединениями сигнализации SCCP (Signaling Connection Control Part). Источником этих сообщений может быть легитимный соседний пункт сигнализации или нелегитимный пункт сигнализации.

К сообщениям MTP относятся: запрещение переноса трафика TFP (Transfer Prohibited), разрешение переноса TFA (Transfer Allowed), перегрузка пучка звеньев сигнализации TFC (Transfer Control), ограничение передачи TFR (Transfer Restricted); перевод трафика на резервное звено сигнализации COO (Changeover Order), подтверждение перевода трафика на резервное звено сигнализации COA (Changeover Acknowledgement), аварийный перевод трафика на резервное звено сигнализации ECO (Emergency Changeover Order), подтверждение аварийного перевода трафика на резервное звено сигнализации ECA (Emergency Changeover Aknowiegement) и др.

К сообщениям SCCP относятся: запрет доступа SSP (Subsystem Prohibited); подсистема перегружена SSC (Subsystem Congested) и др.

Недостаточная защищенность от DoS-атак в ОКС-7 с помощью брандмауэров явилась причиной разработки новых механизмов для защиты от таких атак [13–15]. Актуальность разработки методики оценки риска DoS-атак вызвана необходимостью проведения работ по повышению ИБ находящейся в эксплуатации ОКС-7 сети GSM.

Уровень безопасности DoS-атаки. Согласно стандарту Международного союза электросвязи (ITU-T) E.408 [16] количественная оценка угрозы ИБ в сети связи, выраженная риском ИБ, определяется двумя характеристиками: вероятностью реализации угрозы и последствиями при реализации этой угрозы (т.е. ущербом). В методиках оценки уровня риска безопасности угроз SIP используются эти характеристики. Под вероятностью реализации угрозы принимается уровень безопасности угрозы. Методики ранжирования DoS-атак в ОКС-7 также используют экспертные данные уровней безопасности DoS-атак и уровни ущерба при реализации атаки. Параметрами для оценки уровня безопасности DoS-атаки в ОКС-7 сети GSM являются: уровень противодействия угрозе (степень защищенности механизма ИБ) и уровень качества фиксации угрозы с помощью мониторинга.

Покажем в качестве примера следующие значения критериев уровней противодействия угрозе: 0 — существует эффективный метод противодействия угрозе (его эффективность не зависит от параметров конфигурации инструментов безопасности сети); 1 — существует эффективный метод противодействия угрозе (его эффективность зависит от параметров конфигурации инструментов безопасности сети); 2 — не существует эффективного метода противодействия угрозе.

Получение таких данных в методиках для находящейся в эксплуатации SIP построено на проведении тестирования с имитацией угроз [17]. В находящейся в эксплуатации системе ОКС-7 сети GSM такое тестирование не представляется возможным. Значения уровня противодействия угрозе по принятым параметрам могут быть получены экспертами на базе знаний находящейся в эксплуатации сети и сведений, полученных производителями и поставщиками оборудования.

Примем для примера в качестве критериев уровни качества фиксации угрозы с помощью мониторинга следующие значения: 0 — при появлении признаков реализации угрозы система мониторинга автоматически формирует аварийный сигнал; 1 — угроза фиксируется в журналах регистрации и может быть обнаружена в результате их анализа администратором; 2 — факт реализации угрозы не фиксируется.

На основании состава значений каждого из этих критериев экспертным методом проводится оценка уровня угрозы. Примем в качестве примера следующие значения уровня DoS-угрозы в ОКС-7: 0 — очень низкий, 1 — низкий, 2 — ниже среднего, 5 — средний, 6 — выше среднего, 7 — высокий, 8 — очень высокий. Методика уровня риска безопасности угроз с использованием теории нечетких множеств и нечеткой логики в системе ОКС-7 (так же, как и в SIP) предусматривает вычисление риска угрозы ИБ на основании значений в диапазоне [0–1] уровней безопасности и уровней ущерба при реализации угроз. Значение уровня безопасности DoS-атаки в этом диапазоне отражает вероятность реализации этой угрозы. Остальные две методики (на методах AHP, SPA и на основе только экспертных данных) не требуют такого преобразования. Полученные значения уровней угроз преобразуются экспертным методом в значения этого диапазона. Пример шкалы такого преобразования приведен ниже.

Пример шкалы преобразования уровня угрозы

Уровень безопасности DoS	0	1	2	3	4	5	6	7	8
Преобразованное значение уровня безопасности атаки DoS	0,05	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,95

Уровни ущерба при реализации DoS-атаки. В качестве оценки уровня ущерба при реализации DoS-атаки в ОКС-7 сети GSM примем уровень потерь операторов и уровень потерь пользователя при прекращении выполнения функций установления соединения. Эти данные составляются квалифицированными экспертами на основе опыта эксплуатации (включая данные мониторинга системы). При этом важно учесть, какому уровню иерархии сети ОКС-7 принадлежит это сообщение. Рассмотрим несколько примеров ущерба в сетях GSM на каждой из приведенных архитектур (см. рис. 1 и 2) в результате передачи

нелегитимных сообщений TFP подсистемы MTP или нелегитимных сообщений запрет доступа SSP подсистемы SCCP.

Архитектура на рис. 1. 1. Ущерб от передачи этих нелегитимных сообщений из пункта сигнализации шлюза GMSC в пункт сигнализации ЛЦК приводит к прекращению выполнения функций по установлению входящих вызовов с мобильными станциями субъекта федерации.

2. Ущерб от передачи этих нелегитимных сообщений из пункта сигнализации ЛЦК в пункте сигнализации GMSC приводит к прекращению выполнения функций по установлению исходящих вызовов с мобильных станций субъекта федерации.

3. Ущерб от передачи таких нелегитимных сообщений одновременно из пунктов сигнализации ТЦК1 и ТЦК2 в пункт сигнализации ЛЦК приводит к прекращению выполнения функций по установлению входящих вызовов с мобильными станциями двух субъектов федерации.

Архитектура на рис. 2. 1. Ущерб от передачи этих нелегитимных сообщений одновременно из двух пунктов сигнализации МЦК другой страны в пункты сигнализации обоих МЦК приводит к прекращению выполнения функций по установлению исходящих международных вызовов в другую страну со всех мобильных станций. Аналогичный ущерб имеет место от передачи этих сообщений из пунктов сигнализации двух УАК в пункты сигнализации обеих МЦК страны.

2. Ущерб от передачи этих нелегитимных сообщений одновременно из двух пунктов сигнализации обоих МЦК страны в пункты сигнализации МЦК другой страны приводит к прекращению выполнения функций по установлению исходящих международных вызовов в другую страну со всех мобильных станций. Аналогичный ущерб имеет место от передачи этих нелегитимных сообщений из пунктов сигнализации обоих МЦК страны в пункты сигнализации двух УАК.

Значения экспертов для конкретных DoS-атак оцениваются по принятой шкале уровней ущерба оператора и шкале уровней ущерба пользователя, как это принято в методике для SIP. Примем в качестве примера следующие значения уровня ущерба оператора: 0 — очень низкий, 1 — низкий, 2 — ниже среднего, 5 — средний, 6 — выше среднего, 7 — высокий, 8 — очень высокий, 9 — недопустимый. Аналогично назначаются значения уровней ущерба пользователя. В методике ранжировании DoS-атак только на основе теории нечетких множеств и нечеткой логики на основании уровней ущерба оператора и пользователя экспертами составляется общее значение ущерба от конкретной атаки, которое переводится в диапазон [0–1].

Выводы. Оценка уровня риска безопасности DoS-атак вызвана необходимостью проведения работ по повышению ИБ находящейся в

эксплуатации ОКС-7 сети GSM. Актуальность этой задачи определяется недостаточной защищенностью существующих механизмов (брандмауэров) и разработкой новых усовершенствованных механизмов защиты от атак нарушения маршрутизации. Предложены изменения в разработанные ранее методики оценки уровня угроз безопасности для находящейся в эксплуатации системы сигнализации SIP мультимедийной сети нового поколения VoIP. Эти изменения относятся к расчетам уровней безопасности DoS-атак и ущерба при их реализации, которые являются исходными параметрами при расчете уровня риска безопасности.

Сравнение методик по достоверности результатов ранжирования угроз безопасности не представляется возможным из-за использования в них разных алгоритмов с разными характеристиками субъективных экспертных данных. Две из предложенных методик (на основе нечетких множеств и нечеткой логики и на основе только экспертных данных) используются непосредственно при определении ранга безопасности DoS-атак. В методике на основе методов AHP и SPA эти значения учитываются косвенным образом на промежуточном этапе расчета, что может отрицательно отразиться на достоверности результатов ранжирования угроз безопасности.

ЛИТЕРАТУРА

1. *Матвеев В.А.*, *Морозов А.М.*, *Бельфер Р.А.* Оценка уровня риска угрозы безопасности фрода в сети VoIP по протоколу SIP // Электросвязь. 2014. № 6. С. 35–38.
2. *Матвеев В.А.*, *Морозов А.М.*, *Бельфер Р.А.* Методика ранжирования угроз фрода и DoS в системе SIP, основанная на методах анализа иерархий и анализа пар // Электросвязь. 2014. № 8. С. 25–27.
3. *Матвеев В.А.*, *Бельфер Р.А.*, *Калюжный А.М.*, *Морозов А.М.* Анализ зависимости уровня риска информационной безопасности сетей связи от экспертных данных при расчетах с использованием модели нечетких множеств // Вопросы кибербезопасности. 2014. № 2. С. 33–39.
4. *Матвеев В.А.*, *Бельфер Р.А.*, *Калюжный Д.А.*, *Морозов А.М.* Анализ зависимости уровня риска угроз безопасности фрода сети NGN от экспериментальных данных при расчетах с использованием методов анализа иерархий и анализа пар // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2014. № 6. С. 84–95.
5. *Антонян А.Б.* Новая редакция генеральной схемы создания и развития федеральной сети подвижной радиотелефонной связи общего пользования России стандарта GSM // Электросвязь. 2013. № 1. С. 17–21.
6. *Мардер Н.С.* Электросвязь в Российской Федерации. М.: ИРИАС, 2004. 96 с.
7. *Драйберг Ли*, *Хьюит В.* Система сигнализации № 7 (SS7/ОКС-7), протоколы, структура и применение. М.: Вильямс, 2006. 750 с.
8. *Росляков А.В.* ОКС № 7. Архитектура, протоколы, применение. М.: Эко-Трендз, 2008. 320 с.
9. *Даннави М.Н.* Метод повышения защищенности от угроз нарушения маршрутизации в общеканальной сигнализации сети связи общего пользования. Дисс. . . . канд. техн. наук. Уфимский государственный авиационный технический университет, 2012.

10. *Горшков Ю.Г.*, *Бельфер Р.А.* Анализ риска информационной безопасности сетей GSM при выполнении функций защиты приватности // Электросвязь. 2012. № 3. С. 26–28.
11. *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. 95–100.
12. *Бельфер Р.А.*, *Горшков Ю.Г.*, *Даннави М.Н.* Оценка снижения последствий угроз нарушения маршрутизации в общеканальной сигнализации сетей связи общего пользования // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2009. № 4. С. 75–80.
13. *Sengar H.*, *Wijesekera D.*, *Jajodia S.* Authentication and Integrity in telecommunication Signaling Network. Engineering of Computer-Based Systems. 12th IEEE International Conference and Workshops. P. 163–170.
14. *Yucun Yang* 1, *Weiwei He* 2, *Suili Feng* 1. Security Analysis and Amendment of 3G Core Network Based on MTPsec. IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008. P. 519–523.
15. *Sengar H.*, *Wijesekera D.*, *Jajodia S.*, "MTPSec: customizable secure MTP3 tunnels in the SS7 network". Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International.
16. *ITU-T Recommendation* E.408. Telecommunication Network Security Requirement, 2004.
17. *Матвеев В.А.*, *Морозов А.М.* Анализ результатов испытаний действующей сети нового поколения NGN на уязвимость к атакам DoS // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2013. № 3. С. 43–57.

REFERENCES

[1] Matveev V.A., Morozov A.M., Bel'fer R.A. Assessing the Risk Level of Security Threat of Fraud in the Voip Network via SIP. *Elektrosvyaz'* [Telecommunications], 2014, no. 6, pp. 35–38 (in Russ.).

[2] Matveev V.A., Morozov A.M., Bel'fer R.A. Methods of Ranging Fraud and DoS Threats in the SIP, Based on the Hierarchy Analytic Methods and Pair Analysis. *Elektrosvyaz*' [Telecommunications], 2014, no. 8, pp. 25–27 (in Russ.).

[3] Matveev V.A., Bel'fer R.A., Kalyuzhnyy A.M., Morozov A.M. Analysis of Dependence of Risk Level of Safety of Communication Networks on Expert Data during Calculations with the Use of a Model of the Illegible Sets. *Voprosy kiberbezopasnosti* [Cybersecurity], 2014, no. 2, pp. 33–39 (in Russ.).

[4] Matveev V.A., Bel'fer R.A., Kalyuzhnyy D.A., Morozov A.M. Dependence Analysis of Threat Risk Level of Fraud Security Within NGN Using Experimantal Data During Calculation by Analytic Hierarchy Process and Set Pairs Analysis. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2014, no. 6, pp. 84–95 (in Russ.).

[5] Antonyan A.B. The New Version of the General Scheme of Creation and Development of a Russian Federal Public Mobile Radio Telephone Communication GSM. *Elektrosvyaz*' [Telecommunications], 2013, no. 1, pp. 17–21 (in Russ.).

[6] Marder N.S. Elektrosvyaz' v Rossiyskoy Federatsii [Telecommunications in the Russian Federation]. Moscow, IRIAS Publ., 2004. 96 p.

[7] Dryburgh L. Hewett J. Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. Front Cover. Cisco Press, 2005. Computers. 696 p.

[8] Roslyakov A.V. OKS No. 7. Arkhitektura, protokoly, primenenie [Architecture, Protocols, Applications]. Moscow, Eko-Trendz Publ., 2008. 320 p.

[9] Dannavi M.N. Metod povysheniya zashchishchennosti ot ugroz narusheniya marshrutizatsii v obshchekanal'noy signalizatsii seti svyazi obshchego pol'zovaniya. Diss. kand. tekhn. nauk [A Method for Increasing Protection against Threats to Disrupt Routing in Common Channel Signaling in Public-Service Communications Network. Cand. tech. sci. diss.]. Ufa State Aviation Technical University, 2012.
[10] Gorshkov Yu.G., Bel'fer R.A. GSM Network Information Security Risk Analysis during Performing the Functions of Privacy Protection. *Elektrosvyaz*' [Telecommunications], 2012, no. 3, pp. 26–28 (in Russ.).
[11] Bel'fer R.A., Gorshkov Yu.G., Dannavi M.N. Consequences of Violation of Routing of Channel Common Signalization for Functioning of Networks of General-Purpose Communication. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2009, no. 3, pp. 95–100 (in Russ.).
[12] Bel'fer R.A., Gorshkov Yu.G., Dannavi M.N. Estimation of Reducing Consequences of Threats of Routing Violation in Shared Channel Signaling of Public Telecommunications. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2009, no. 4, pp. 75–80 (in Russ.).
[13] Sengar H., Wijesekera D., Jajodia S. Authentication and Integrity in telecommunication Signaling Network. Engineering of Computer-Based Systems, *12th IEEE International Conference and Workshops*, pp. 163–170.
[14] Yucun Yang 1, Weiwei He 2, Suili Feng 1. Security Analysis and Amendment of 3G Core Network Based on MTPsec, *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, 2008, pp. 519–523.
[15] Sengar H., Wijesekera D., Jajodia S. "MTPSec: customizable secure MTP3 tunnels in the SS7 network". *Parallel and Distributed Processing Symposium*, 2005. *Proceedings*. *19th IEEE International*.
[16] ITU-T Recommendation E.408. Telecommunication Network Security Requirement, 2004.
[17] Matveev V.A., Morozov A.M. Analyzing results of tests of the functioning new generation network for vulnerability to DoS attacks. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2013, no. 3, pp. 43–57 (in Russ.).

Статья поступила в редакцию 25.03.2015

Матвеев Валерий Александрович — д-р техн. наук, профессор, зав. кафедрой "Информационная безопасность" МГТУ им. Н.Э. Баумана, руководитель НУК факультета ИУ МГТУ им. Н.Э. Баумана. Автор более 200 научных работ и 25 патентов в области приборостроения и высокотемпературной сверхпроводимости.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Matveev V.A. — D.Sc. (Eng.), Professor of Engineering, Head of the Department of Information Security, Head of the Research and Educational Complex, Department of Informatics and Control Systems, Bauman Moscow State Technical University, author of over 200 research publications and 25 patents in the fields of instrument engineering and high temperature superconductivity.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.

Бельфер Рувим Абрамович — канд. техн. наук, доцент кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана. Автор более 100 научных работ в области информационных технологий.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Belfer R.A. — Ph.D. (Eng.), Associate Professor of Engineering, Department of Information Security, Bauman Moscow State Technical University, author of over 100 research publications in the field of data security in telecommunication networks.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.

Глинская Елена Вячеславовна — старший преподаватель кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана. Автор более 10 научных работ в области управления информационной безопасностью.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Glinskaya E.V. — Senior Lecturer, Department of Information Security, Bauman Moscow State Technical University, author of over 10 research publications in the field of information security management.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.

Просьба ссылаться на эту статью следующим образом:

Матвеев В.А., Бельфер Р.А., Глинская Е.В. Оценка уровня риска безопасности атаки DOS-функций маршрутизации системы сигнализации ОКС-7 в сети GSM // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2015. № 4. С. 127–138.

Please cite this article in English as:

Matveev V.A., Belfer R.A., Glinskaya E.V. Assessing the security risk of attacks DOS-routing functions of the signaling system SS7 in the GSM network. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2015, no. 4, pp. 127–138.

Издательство МГТУ им. Н.Э. Баумана

Сдано в набор 15.06.2015 Подписано в печать 25.07.2015
Формат 70 × 108/16 Усл.-печ. л. 12,08 Уч.-изд. л. 12,91
Заказ
Отпечатано в типографии МГТУ им. Н.Э. Баумана