УДК 621.392

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

ОЦЕНКА СНИЖЕНИЯ ПОСЛЕДСТВИЙ УГРОЗ НАРУШЕНИЯ МАРШРУТИЗАЦИИ В ОБЩЕКАНАЛЬНОЙ СИГНАЛИЗАЦИИ СЕТЕЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Предложен метод оценки снижения с помощью механизмов аутентификации ущерба работе сетей связи общего пользования, который может быть нанесен нарушением маршрутизации в ОКС-7.
E-mail: iu8@bmstu.ru

Ключевые слова: *информационная безопасность, сети связи общего пользования, общеканальная сигнализация № 7, угрозы нарушения маршрутизации.*

Фальсификация сообщений в сети связи общего пользования (ССОП) создает потенциальную возможность угрозы информационной безопасности (ИБ). Результатом таких угроз ИБ могут быть, например нарушения таблиц маршрутизации, что может приводить к серьезным последствиям в ССОП ТфОП/ISDN [1, 2] и IP-сетях [3, 4]. Для защиты от таких угроз ИБ в ССОП служит механизм аутентификации, который проверяет подлинность источника и целостность поступившего сообщения обновления маршрутизации. Такое сообщение поступает от соседнего коммутатора или маршрутизатора сети. Эти сообщения в сети общеканальной сигнализации № 7 (ОКС-7) ТфОП/ISDN относятся к сетевому уровню эталонной модели OSI, а в IP-сети — межсетевому или транспортному уровню IP эталонной модели TCP/IP.

Для защиты от угроз фальсификации маршрутизации могут быть использованы разные протоколы аутентификации. В IP-сети такие механизмы защиты специфицированы. При выполнении протокола маршрутизации на межсетевом уровне пользуются либо протоколом открытой аутентификации с помощью пароля (RFC-2453), либо протоколом аутентификации MD5 (RFC-2082), а при выполнении протокола маршрутизации на транспортном уровне – протоколом аутентификации MD5 (RFC-2385). В ОКС-7 при выполнении функций маршрутизации механизмы защиты ИБ не стандартизированы международными организациями стандартизации, а поэтому производители оборудования сети ТфОП/ISDN используют разные типы таких механизмов в ОКС-7. В одном пункте сигнализации может быть установлено несколько типов механизмов аутентификации в целях совместимости со смежными пунктами сигнализации тех или других производителей оборудования ОКС-7. Не исключено, что некоторые производители

оборудования ОКС-7 вообще не предусмотрели механизмов защиты. Это отмечено в работе [1]. В работе [5] указывается на серьезные последствия нарушения работы ССОП в результате реализации угроз нарушения маршрутизации ОКС-7.

В связи с этим остро стоит задача качественной оценки механизмов аутентификации для защиты от нарушения маршрутизации в ОКС-7 в целях сравнения разных механизмов и проведения технико-экономического обоснования выбора из них.

В настоящей работе при решении будем исходить из необходимости определения количественных оценок максимального ущерба, наносимого ССОП при реализации угроз нарушения маршрутизации ОКС-7 (т.е. в случае отсутствия механизмов аутентификации), а также степени обеспечения ИБ с помощью конкретного механизма защиты по снижению этого ущерба.

Как показано в работе [5], этот ущерб может отражаться такими последствиями, как отказ в установлении соединений одновременно большому числу пользователей сетей ТфОП/ISDN и GSM. Причиной атак, соответствующих таким угрозам, служит нелегитимное использование нарушителем разных функций сетевого уровня ОКС-7. Экономический ущерб в ССОП определяется в каждом конкретном пункте сигнализации сети ОКС-7, который подвержен воздействию угрозе от смежного с ним пункта сигнализации.

Большое число производителей оборудования ОКС-7 в ССОП может быть причиной использования нескольких типов механизмов аутентификации в оборудовании взаимодействующих сетей связи общего пользования ТфОП/ISDN, GSM, IN. В результате снижение экономического ущерба от угроз нарушения маршрутизации ОКС-7 требует технико-экономического обоснования выбора в смежных пунктах сигнализации совместимых механизмов аутентификации. Для этого требуется определить степень обеспечения ИБ механизмом аутентификации сообщений.

Интегральная характеристика обеспечения уровня ИБ механизма аутентификации. Для определения интегральной характеристики $R_{\text{sec}}(X)$ степени обеспечения ИБ механизмом аутентификации X используется метод, предложенный в международном проекте по архитектуре безопасности открытых распределенных систем [6], к которым относятся анализируемые ССОП:

$$R_{\text{sec}}(X) = \frac{\sum\limits_{i=1}^{N1} (K_i X_i Z)}{\sum\limits_{i=1}^{N1} K_i}, \qquad (1)$$

где i — конкретное требование ИБ к механизму аутентификации; $N1$ — общее число требований ИБ к механизму аутентификации; K_i и X_i — степени важности и выполнения требования i механизмом аутентификации соответственно.

Значение $X_i = 0$ означает, что требование ИБ механизмом аутентификации X не выполняется. Чем больше X_i, тем в большей степени требование ИБ выполняется механизмом аутентификации. Характеристики X_i и K_i в выражении (1) определяются экспертным методом. Значение Z определяет диапазон значений R_{sec}. Максимальное значение R_{sec} определяется произведением числа Z и максимального X_i, при котором K_i выполняется полностью. Далее в табл. 1 приведен упрощенный пример для иллюстрации определения интегральных значений $R_{sec}(X)$ рассматриваемых механизмов аутентификации **А**, **Б**, **В**, **Г**, **Д**, **Е**. Значения требований к информационной безопасности этих механизмов означают: $i = 1$ — обеспечение только подлинности источника сообщения обновления маршрутизации; $i = 2$ — обеспечение только целостности принятого сообщения обновления маршрутизации.

Кроме требований ИБ, имеющих конкретные характеристики X_i и K_i, предусмотрены так называемые критические требования, которые не имеют весовых значений и являются обязательными для выполнения. К таким требованиям относится наличие средств аудита, позволяющих записывать подробную информацию о сообщениях обновления маршрутизации; системы извещений, позволяющей в реальном масштабе времени указывать на признаки атак, вызванных фальсификацией сообщений обновления маршрутизации.

Данные расчета $R_{sec}(X)$, приведенные в табл. 1, иллюстрируют применение предлагаемого метода. С этой же целью выбраны и приведены параметры K_i и X_i. Диапазон значений R_{sec} принят равным 100 (произведение $Z = 10$ и максимального значения $X_i = 10$). Далее приведен список анализируемых механизмов аутентификации, из которых только механизм **А** используется для защиты от нарушения маршрутизации в IP-сетях, а остальные выполняют защиту других функций ССОП.

А. Подлинность источника и целостности сообщения обновления маршрутизации с помощью кода аутентичности MD5 (Message Authentication Code). В IP-сетях такая аутентификация реализуется с помощью односторонней функции хеширования (по протоколу MD5) сообщения обновления маршрутизации вместе с общим секретным значением (ключом) соседнего маршрутизатора [3].

Б. Механизм аутентификации аналогичен приведенному механизму **А** за исключением того, что используется функция хеширования по протоколу HMAC [7, 8].

В. Механизм аутентификации аналогичен приведенному механизму **А** за исключением того, что для вычисления MAC используется не функция хеширования, а алгоритм симметричного шифрования DES. Такой алгоритм формирования MAC принят национальным бюро стандартов США [7, 8].

Г. Механизм аутентификации аналогичен приведенному механизму **В** за исключением того, что для вычисления MAC используется алгоритм симметричного шифрования другого алгоритма (KASUMI). Такой алгоритм формирования MAC принят в сотовой сети подвижной связи третьего поколения UMTS [8].

Д. Подлинность источника и целостность сообщения обновления маршрутизации реализуется с помощью симметричного шифрования хеш-кода (профиля) сообщения [8].

Е. Подлинность источника и целостность сообщения обновления маршрутизации реализуется с помощью шифрования с открытым ключом [8].

Таблица 1

Значения интегральных характеристик обеспечения ИБ механизмов аутентификации

Требование i	K_i	X_i					
		А	**Б**	**В**	**Г**	**Д**	**Е**
1	1	1	1	1	1	1	1
2	10	1	3	3	5	7	10
R_{sec}		10,0	28,2	28,2	46,4	64,5	91,8

Как видно из табл. 1 наименьшее значение $R_{\text{sec}}(X)$ имеет механизм **А**, а наибольший — механизм **Е**. Механизмы **Б** и **В** имеют одинаковое значение $R_{sec}(X)$.

Технико-экономическая эффективность механизма аутентификации в ОКС-7. Интегральная характеристика механизма аутентификации в пунктах сигнализации ОКС-7 должна учитывать степень снижения ущерба ССОП в результате защиты от угроз нарушения маршрутизации. При этом учитываются многие факторы и в том числе значение интегральной характеристики уровня обеспечения ИБ этим механизмом аутентификации.

Обозначим интегральную характеристику технико-экономической эффективности механизма аутентификации X как $R_{fh}(X)$, где f — пункт сигнализации ОКС-7, в который поступает фальсифицированное сообщение обновления маршрутизации из смежного пункта сиг-

нализации h, и запишем

$$R_{fh}(X) = \frac{\sum\limits_{w=1}^{N2} C_{fh}(W) X_{fh}(W) Z}{\sum\limits_{w=1}^{N2} C_{fh}(W)}. \qquad (2)$$

В формуле (2) интегральной технико-экономической эффективности механизма аутентификации приняты следующие обозначения ее экономической эффективности по снижению ущерба в ССОП.

Показатель W означает вид ущерба ССОП от реализации угрозы фальсификации маршрутной информации в ОКС-7, который выражается в отказе установления соединений одновременно большому числу пользователей ССОП. Анализу подлежат следующие виды наибольшего ущерба работе ССОП: $W = 1$ — отказ в установлении соединений между абонентами ТфОП/ISDN; $W = 2$ — отказ в установлении соединений между мобильными станциями (MS) сети GSM; $W = 3$ — отказ в установлении соединений между абонентами ТфОП/ISDN и мобильными станциями GSM; $W = 4$ — отказ в установлении только тех соединений между абонентами ТфОП/ISDN, которым требуется предоставление услуг интеллектуальной сети. $N2$ — общее число принятых видов ущерба ССОП, т.е. $N2 = 4$.

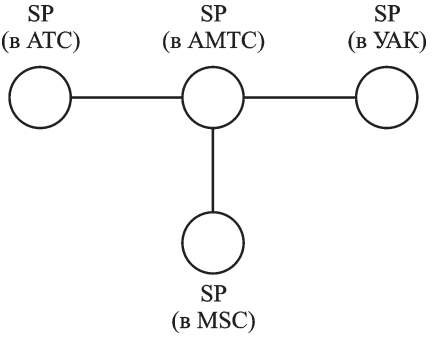
Показатель $C_{fh}(W)$ в формуле (2) означает максимальное значение конкретного вида ущерба W ССОП при реализации угрозы фальсификации маршрутной информации ОКС-7 в случае отсутствия механизма аутентификации в пункте сигнализации f при поступлении этих нелегитимных сообщений из пункта сигнализации h.

Показатель $X_{fh}(W)$ в формуле (2) означает степень снижения максимального ущерба $C_{fh}(W)$ механизмом аутентификации X, установленном в пунктах сигнализации f и h. Значение $X_{fh}(W)$ определяется экспертным путем с учетом значения $R_{sec}(X)$, вычисленного по формуле (1).

Оба показателя ($C_{fh}(W)$ и $X_{fh}(W)$) зависят от топологии ССОП (принадлежности их определенной сети связи ОП ТфОП/ISDN, GSM, IN); структуры резервирования путей маршрутизации и звеньев сигнализации; пунктов сигнализации ОКС-7, подключенных к пункту сигнализации h, кроме пункта сигнализации f; конкретных функций сетевого уровня ОКС-7, используемых нарушителем для нелегитимного обновления таблиц маршрутизации; числа фальсифицированных сообщений обновления маршрутизации, отправляемых нарушителем при использовании одной функции сетевого уровня ОКС-7.

Чтобы полностью оценить экономическую эффективность механизмов аутентификации в ОКС-7 во всем оборудовании ССОП,

нужно выполнить практически нереализуемую задачу вычисления значения $R_{fh}(W)$ для всех смежных пунктов сигнализации в ССОП. Это так же нереально, как невозможно учесть все виды угроз в ОКС-7 сетей связи. Поэтому перед специалистами стоит задача определения показателей $C_{fh}(W)$ и $X_{fh}(W)$ в отношении наиболее уязвимых участков смежных пунктов сигнализации для воздействия угроз нарушения маршрутизации ОКС-7 с точки зрения нанесения наибольшего ущерба ССОП. Такими являются, например, участки смежных пунктов сигнализации между разными уровнями иерархического построения ТфОП/ISDN, GSM.



Упрощенная гипотетическая схема фрагмента сети ОКС-7

Для нелегитимного обновления таблиц маршрутизации ОКС-7 нарушители могут использовать следующие функции сетевого уровня (передачей нелегитимных сообщений) [1]: “запрет передачи” (сообщение TFP); “недоступность подсистемы пользователя” (сообщение UPU); “перегрузка” пучка звеньев сигнализации (сообщение TFC); “ограничение передачи” (сообщение TFR); “переключение звена сигнализации” (сообщение COO, ECO); “запрет доступа” (сообщение SSP); “подсистема перегружена” (сообщение SSC) и др.

Приведенный в формуле (2) показатель максимального ущерба $C_{fh}(W)$ определяется экспертным путем с учетом доли нелегитимного использования каждой из этих функции.

Передача нелегитимного сообщения TFP функции “запрет передачи” относится к одной из тех, реализация которых может привести к наибольшему ущербу ССОП.

Приведем пример для определения технико-экономической эффективности механизмов аутентификации $R_{fh}(X)$ для упрощения гипотетической схемы фрагмента сети ОКС-7 (рисунок).

На рисунке показаны участки смежных пунктов сигнализации Signaling Point (SP) в узлах автоматической коммутации АТС, АМТС, УАК, MSC — центр мобильной коммутации в GSM [1].

В каждом из этих SP могут быть установлены механизмы аутентификации X, приведенные ранее.

Данные расчета $R_{fh}(X)$, приведенные в табл. 2, представлены для иллюстрации применения предлагаемого метода.

Рассмотрим участок смежных SP (в АМТС) — SP (в АТС). Нарушитель создает в SP (АМТС), т.е. пункте h, два нелегитимных сообщения

"запрет передачи" TFP в SP (в УАК) и в SP (в MSC). Оба эти сообщения отправляет в SP (в АТС), т.е. пункт f. Ограничимся анализом действий только этих нелегитимных сообщений.

Ущерб ССОП при их приеме выражается отказом в установлении соединений между абонентами ТфОП/ISDN ($W = 1$) и между абонентами ТфОП/ISDN и мобильными станциями GSM ($W = 3$).

Максимальное значение ущерба $C_{fh}(W)$ при $W = 1$ в этом случае выражается в отказе исходящим вызовам абонентов всех АТС, подключенных к АМТС, в установлении междугородных и международных соединений.

Максимальное значение ущерба $C_{fh}(W)$ при $W = 3$ в этом случае выражается в невозможности исходящим вызовам от абонентов АТС установить соединения с мобильными станциями, обслуживаемыми MSC.

Результаты расчета $R_{fh}(X)$ приведены в табл. 2 при условии, что все механизмы аутентификации предусмотрены во всех пунктах сигнализации ОКС-7. При определении значений X_{fh} экспертами должны учитываться характеристики уровня обеспечения ИБ механизмом аутентификации $R_{\text{sec}}(X)$, приведенным в табл. 1.

Таблица 2

Значения показателей технико-экономической эффективности механизмов аутентификации

Показатель W	$C_{fh}(W)$*	X_{fh}					
		А	**Б**	**В**	**Г**	**Д**	**Е**
1	10	3	4	4	5	9	10
2	0						
3	10	3	4	4	5	9	10
4	0						
$R_{fh}(X)$		15	20	20	25	45	50

*Приведенные значения $C_{fh}(W)$ для $W = 1$ и $W = 3$ — одинаковые для одного и того же механизма аутентификации, так как в примере рассматривается защита от одной угрозы нарушения таблицы маршрутизации с помощью сообщения "запрет передачи" TFP.

Из табл. 2 следует, что для приведенного примера смежных пунктов сигнализации наибольшая экономическая эффективность имеет место при использовании предусмотренных в пунктах сигнализации механизмов аутентификации **Е** ($R_{\text{fh}}(X) = 50$), использующих криптографию с открытым ключом.

При отсутствии механизмов аутентификации в смежных пунктах сигнализации недостаточно показателя интегральной характеристики технико-экономической эффективности механизма аутентификации

$R_{fh}(X)$. В этом случае необходимо учитывать дополнительно стоимостные показатели самого механизма аутентификации и сложность его реализации в пункте сигнализации. Это значение $R_{cost}(X)$ определяется согласно методу в международном проекте [6] по формуле

$$R_{cost}(X) = \frac{\sum\limits_{i=1}^{N1}(K_i X_i Z_i) + \sum\limits_{j=1}^{N3} K_j X_j Z_j}{\sum\limits_{i=1}^{N1} K_i + \sum\limits_{j=1}^{N3} C_j}, \qquad (3)$$

где K_i, X_i, Z, $N1$ — показатели, используемые для определения $R_{sec}(X)$ по формуле (1); j — технический показатель механизма аутентификации, позволяющий оценить его стоимость или сложность установления в пункте сигнализации ОКС-7 (при отсутствии в нем); $N3$ — общее число показателей j в анализируемых механизмах аутентификации; C_j — максимальная экономическая эффективность при отсутствии затрат на показатель j механизма аутентификации; X_j — степень выполнения C_j в механизме аутентификации; чем выше значение Y_j, тем меньше разность между C_j и Y_j.

В табл. 3 приведены результаты расчета стоимостных показателей анализируемых механизмов аутентификации при следующих показателях: $j = 1, 2, 3$ и 4 — отсутствие затрат на использование шифрования с открытым ключом, с общим ключом, хеширования сообщения и отсутствие затрат на генерацию ключей.

Как следует из работы [6], чем выше значение $R_{cost}(X)$, тем выше экономическая эффективность этого механизма безопасности (в данном случае механизма аутентификации).

Таблица 3

Значения стоимостных характеристик механизмов аутентификации

Показатель j	C_j	X_j					
		А	**Б**	**В**	**Г**	**Д**	**Е**
1	10	10	10	10	10	10	10
2	7	7	7	5	3	0	7
3	2	1	0	2	2	0	0
4	1	0	0	0	0	0	0
$R_{cost}(X)$		51,6	58	54,8	50,3	27,9	48,4

Как видно из табл. 2 и 3, несмотря на то что механизмы ИБ **А**, **Б**, **В**, **Г** выше по стоимостным показателям их реализации $R_{cost}(X)$, технико-экономическая эффективность при их использовании для приведенного примера $R_{fh}(X)$ значительно ниже, чем при защите от угроз

нарушения маршрутизации ОКС-7 с помощью механизмов аутентификации **Е** и **Д**.

Выводы. 1. Разработанный аналитический метод технико-экономической оценки механизма аутентификации в ОКС-7 позволяет сравнить различные механизмы защиты от угроз нарушения маршрутизации в ОКС-7 по снижению ущерба ССОП.

2. Предложены показатели отражающие ущерб ССОП от воздействия угроз, которые выражаются в одновременном отказе установления соединений абонентам ТфОП/ISDN, мобильным станциям GSM (с предоставлением и без предоставления услуг IN).

3. В качестве угроз нарушения маршрутизации в ОКС-7, реализация которых приводит к нарушению работы ССОП, анализу подлежат нелегитимные действия нарушителя по фальсификации сообщений, использующих функции сетевого уровня ОКС-7.

4. Ущерб сетям связи общего пользования от реализации угроз маршрутизации ОКС-7 может быть нанесен нарушителем на многих участках смежных пунктов сигнализации сети ОКС-7. Последствия этих угроз ОКС-7 требуют анализа технико-экономической эффективности механизмов аутентификации в первую очередь на наиболее уязвимых из этих участков смежных пунктов сигнализации. При этом следует учитывать использование нарушителем тех функций сетевого уровня ОКС-7, нелегитимные сообщения которых приводят к наибольшему ущербу ССОП.

5. Предложенный метод расчета может быть использован для оценки и, при необходимости, доработки находящейся в эксплуатации ССОП сети ОКС-7 с целью обеспечения необходимой ИБ от угроз нарушения маршрутизации.

Предложенный метод оценки снижения последствий угроз нарушения маршрутизации начали использовать в текущем году при анализе информационной безопасности сетей связи общего пользования одной из зарубежных стран. Операторы сетей связи общего пользования одной из зарубежных стран совместно с министерством связи этой страны на основе предложенного метода приступили к анализу последствий угроз в результате нарушения маршрутизации в ОКС-7.

СПИСОК ЛИТЕРАТУРЫ

1. Драйберг Л и, Хьюитт Джефф. Система сигнализации № 7 (SS7/ОКС-7). Протоколы, структура и применение. – М.: Вильямс, 2006.
2. Бельфер Р. А., Горшков Ю. Г. Система сигнализации ОКС-7. Требования к QoS и организация программного обеспечения сетевого уровня: Учеб. пособие / МТУСИ – М.: Инсвязьиздат, 2007.
3. Уинстром М. Организация защиты сетей Cisco. – М.: Вильямс, 2005.

4. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник – СПб.: Питер, 2002.
5. Бельфер Р. А., Горшков Ю. Г., Даннави М. Н. Архитектура сетевой безопасности ОКС-7 // Электросвязь. – 2009. – № 4.
6. Muftic S. et. al. Security architecture for open distributed systems. John Willey & Sons Ltd, 1993.
7. Столингс В. Основы защиты сетей. Приложения и структуры. – М.: Вильямс, 2002.
8. Бельфер Р. А., Горшков Ю. Г., Даннави М. Н. Алгоритмы аутентификации в сетях общего пользования России // Электросвязь. – 2008. – № 8.

Статья поступила в редакцию 18.11.2008

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.