**На правах рукописи**

**ДАННАВИ Мохамад Насреддин**

# МЕТОД ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ ОТ УГРОЗ НАРУШЕНИЯ МАРШРУТИЗАЦИИ В ОБЩЕКАНАЛЬНОЙ СИГНАЛИЗАЦИИ СЕТИ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

**Специальность: 05.12.13 – Системы, сети и устройства телекоммуникаций**

**АВТОРЕФЕРАТ**
**диссертации на соискание ученой степени кандидата технических наук**

**Уфа – 2012**

Работа выполнена на кафедре телекоммуникационных систем ФГБОУ ВПО «Уфимский государственный авиационный технический университет» и в НПОУ ИЦ «Техника»

Научный руководитель — д-р техн. наук, доцент
**Виноградова Ирина Леонидовна**
каф. телекоммуникационных систем

Официальные оппоненты — д-р техн. наук, проф.
**Росляков Александр Владимирович**
каф. автоматической электросвязи
Поволжского государственного университета телекоммуникаций и информатики

канд. техн. наук
**Акульшин Виктор Николаевич**
Центр технической эксплуатации
ОАО «Башинформсвязь»

Ведущая организация – Башкирский государственный университет, г. Уфа

Защита диссертации состоится “ 27 ” апреля 2012 г. в 10 часов на заседании диссертационного совета Д-212.288.07 при Уфимском государственном авиационном техническом университете по адресу: 450000, г. Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке университета

Автореферат разослан “ 16 ” марта 2012 года.

Ученый секретарь
диссертационного совета
д-р. техн. наук, профессор — С. С. Валеев

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы**. Сеть общеканальной сигнализации (ОКС №7) является общемировой наложенной сетью передачи данных специального (служебного) назначения. Она обслуживает установление соединений, предоставление дополнительных услуг и межсетевое взаимодействие в большинстве существующих в настоящее время цифровых сетей связи общего пользования (ССОП): телефонной сети общего пользования (ТфОП), цифровой сети с интеграцией служб (ЦСИС), сетях подвижной сотовой связи (СПСС) и интеллектуальных сетях (ИС). Из-за угроз информационной безопасности, обусловленных атаками на сетевом уровне на пункты сигнализации, существует высокая вероятность отказа в обслуживании (DoS – Denial of Service), обусловленная нарушением маршрутизации сообщений в сети ОКС №7.

Вероятность реализации такой угрозы высока ввиду того, что злоумышленнику достаточно отправить на пункты сигнализации несложные нелегитимные сообщения сетевого уровня, управляющие командами системы ОКС №7, что и приведёт к выполнению функций обновления маршрутизации по желанию указанного злоумышленника. Важность анализа степени защищенности от угроз информационной безопасности вызвана тем, что последствием их реализации могут быть серьезные нарушения работы ССОП, составляющей которых является выход из рабочего состояния целых фрагментов сетей общего пользования. Это может иметь место, когда в пунктах сигнализации отсутствуют механизмы аутентификации сообщений обновления маршрутизации или эти механизмы несовместимы с собственными управляющими командами. Следует подчеркнуть также, что в настоящие время отсутствуют документы МСЭ-Т или ETSI по стандартизации для механизмов защиты от атак в системе ОКС №7.

Разработка методов анализа сетей ОКС №7, а также вопросы защищенности их от атак рассматривались в работах отечественных и зарубежных ученых: Г. П. Захарова, Б. С. Гольдштейна, К. Е. Самуйлова, Ю. Г. Горшкова, И. М. Ехриель, Р. А. Бельфера, Р. Д. Реле, j. Eloff, S. Muftic, A. Patel, P. Sanders, R. Colon. Тем не менее, остались нерешёнными вопросы, связанные с анализом качества отдельных механизмов информационной безопасности для ОКС №7 в ССОП и их влияния на работоспособность сети в целом.

В частности, эффективность метода оценки степени защищённости от угроз выражается в доле пользователей ССОП, которые защищены от последствий отказов (из-за атак категории DoS) в предоставлении им возможности установления соединений. Значение эффективности определяется конкретной ССОП и, в крайнем случае, может относиться ко всем пользователям (включая абонентов-роумеров других операторов связи) относительно местных, междугородных и международных соединений. Эффективность защищённости суще-

ственно зависит от наличия и принципа работы механизмов аутентификации сообщений. Предлагаемый в работе метод оценки и повышения защищенности от угроз нарушения маршрутизации является развитием разработанного ранее аппарата по оценке и повышения информационной безопасности отдельных механизмов аутентификации (криптография, аутентификация, анализ целостности данных, система контроля доступа и др.) с привлечением дополнительного анализа управляющих команд на смежных пунктах сигнализации.

**Цель работы:** исследование теоретических и практических вопросов, связанных с информационной безопасностью (ИБ) системы сигнализации ОКС №7; а также разработка методов повышения ИБ ССОП с использованием системы контроля доступа (механизмов аутентификации) служебных сообщений сетевого уровня.

**Задачи исследования.** Для достижения поставленной цели в работе сформулированы и решены следующие задачи:

1. Разработка классификации нарушений и модели последствий атак (категории DoS) нелегитимных сообщений на её основе для ОКС №7 и на параметры таблиц маршрутизации, позволяющей выявить нарушения сетевого уровня.
2. Разработка системы контроля доступа и определение степени защищенности от угроз нарушения маршрутизации в системе ОКС №7 для находящихся в эксплуатации сетей связи общего пользования.
3. Разработка метода количественной оценки механизмов аутентификации сообщений, учитывающего степень снижения ущерба в работе ССОП.
4. Разработка метода повышения ИБ за счёт использования свободных октетов в поле SIF, влияющих на установление соединения.
5. Разработка архитектуры сетевой безопасности для системы сигнализации ОКС №7, позволяющей выявлять нелегитимные сообщения раньше, чем запускается выполнение функций обновления маршрутизации.

Здесь и далее под моделью нарушения понимается система управляющих команд сетевого уровня для служебной подсистемы ОКС№7.

**Методы исследования.** В работе использованы положения теории графов, случайных процессов и теории вероятности. Применены методы экспертных оценок, математического моделирования, в том числе компьютерного. Проведён вычислительный эксперимент с использованием результатов эксплуатации действующей телекоммуникационной системы.

**Объектом исследования:** система передачи, основанная на транспортной сети SDH с системой сигнализации ОКС№7.

**Предмет исследования:** теоретические, методические и практические вопросы повышения ИБ и эффективности функционирования протоколов системы сигнализации ОКС№7 на основе использования дополнительной системы аутентификации служебных сообщений.

**Научная новизна** работы заключается в следующем:

1. Разработана классификация и выполнено ранжирование отказов в обслуживании по установлению соединений для пользователей ССОП, отличающаяся тем, что привлечены результаты анализа угроз запуска функций обновления маршрутизации в ОКС №7 из-за нелегитимных сообщений.

2. Предложен алгоритм для определения степени защищенности от угроз нарушения маршрутизации в системе сигнализации ОКС №7 находящихся в эксплуатации ССОП. Показано, что наиболее чувствительными к последствиям угроз нарушениями маршрутизации являются участки смежных пунктов сигнализации разных уровней иерархии ССОП.

3. Разработан метод количественной оценки механизмов аутентификации сообщений, учитывающий степень снижения ущерба в работе ССОП, отличающийся тем, что оператору предоставляется возможность принимать решения по выбору механизмов аутентификации в целях повышения ИБ в ССОП.

4. Предложена архитектура сетевой безопасности системы сигнализации ОКС №7, основанная на положениях рекомендации X.805, отличающаяся тем, что учтены команды управления, обеспечивающих связь между оконечными пунктами. На основании этой архитектуры предложен и обоснован выбор модуля (включающего уровень и плоскость безопасности), обеспечивающего аппаратную реализацию механизма аутентификации сообщений.

**Практическая ценность** состоит в повышении ИБ и эффективности функционирования ССОП на основе применения разработанной системы рекомендаций по проведению анализа степени защищенности ОКС №7 в эксплуатируемых ССОП от атак (категории DoS), направленных на нарушение маршрутизации служебных сообщений. Предложен подход к повышению ИБ системы сигнализации ОКС №7, обеспечивающий снижение ущерба от отказов в ССОП, основанный на введении дополнительных механизмов аутентификации служебных сообщений.

**На защиту выносятся:**

1. Классификация нарушений ИБ и модель последствий атак (категории DoS) нелегитимных сообщений для системы сигнализации ОКС №7 на таблицы маршрутизации, основанная на полученных экспертным методом критериях оценки, позволяющие ранжировать чувствительные к отказу в обслуживании участки ССОП.

2. Вероятностный подход к моделированию параметров системы контроля доступа, основанный на использовании метода экспертных оценок, позволяющий повысить ИБ ССОП путём предотвращения несанкционированного доступа на пунктах сигнализации.

3. Метод количественной оценки степени защищенности работы ССОП с использованием механизмов аутентификации в ОКС №7, основанный на при-

менении интегральных параметров степени защищённости, позволяющий повысить ИБ ССОП путём снижения риска отказа в обслуживании по критерию установления/неустановления соединений.

4. Метод повышения ИБ, основанный на использовании свободных октетов в поле SIF, влияющих на установление соединения, позволяющий контролировать легитимность служебных сообщений ОКС №7.

5. Архитектура сетевой безопасности системы сигнализации ОКС №7, состоящая из уровней безопасности инфраструктуры и приложений, а также плоскости безопасности управления и плоскости безопасности транспортной сети, позволяющая определить типы оборудования и функции в ССОП, для которых необходимо применять мероприятия по защите ИБ.

**Апробация работы.** Основные положения диссертационной работы докладывались и обсуждались на ряде отраслевых и международных научно-технических конференциях, проводимых МТУСИ (2007-2008 г.г.), международной научно-технической конференции INTERMATIC-2008 (РАН, 2008 г.), на международном конгрессе «Безопасность информационных технологий» (МИФИ, 2009 г.), международной научно-технической конференции «Проблемы техники и технологии телекоммуникаций» (КГТУ, 2011 г.), а также на семинарах кафедр «Мультимедийные сети и услуги связи» МТУСИ и «Телекоммуникационные системы» УГАТУ.

**Публикации.** По материалам диссертации опубликовано семь печатных работ, из них – шесть в рецензируемых журналах, рекомендованных ВАК, пять докладов в сборниках трудов конференций, список которых приведен в конце автореферата.

**Структура и объем диссертации.** Диссертация состоит из введения, четырех глав, заключения, списка используемой литературы и приложения. Содержит 123 стр. машинописного текста, 21 рисунок, 3 таблицы, список используемой литературы из 45 наименований, приложения 1 стр.

Автор выражает свою искреннюю благодарность доценту кафедры ИУ-8 МГТУ им. Баумана, Бельфер Р. А. за оказанную помощь по выполнению работы.

## СОДЕРЖАНИЕ ДИССЕРТАЦИИ

**Во введении** обоснована актуальность темы исследования, определены цели и задачи диссертационной работы, показана научная новизна полученных результатов, практическая ценность работы, приведены основные положения, выносимые на защиту и сведения об апробации работы.

**В первой главе** на основе анализа положений системы безопасности ССОП (по рек. МСЭ-Т Х.805) представлена архитектура сетевой безопасности системы сигнализации ОКС №7, на базе которой и определено направление исследований параметров ИБ от атак типа «отказ в обслуживании» (категории

DoS). Архитектура сетевой безопасности в ОКС №7 предполагает комплексное рассмотрение таких аспектов ИБ, как:

- способы обеспечения ИБ от атак при их реализации;
- типы оборудования сигнализации с привязкой к уровням эталонной модели OSI, которые нуждаются в обеспечении ИБ;
- функции оборудования сигнализации, которые нуждаются в обеспечении ИБ.

Исходя из особенностей функций ОКС №7 в ССОП, определена архитектура безопасности системы сигнализации ОКС №7, включающая два уровня безопасности: уровень безопасности инфраструктуры и уровень безопасности приложений, а также две плоскости безопасности: плоскость безопасности управления и плоскость безопасности транспортной сети. Учитывая особенности технологии ОКС №7, способы обеспечения ИБ рассматриваются относительно двух уровней безопасности: уровня безопасности инфраструктуры (Infrastructure Security) и уровня безопасности приложений (Application Security). Взаимосвязь уровней безопасности основана на иерархическом принципе. Уровень безопасности инфраструктуры обеспечивает уровень безопасности приложений.

Уровень безопасности инфраструктуры реализован на основе таких устройств ОКС №7, как: оконечное, промежуточное и транзитное оборудование на пунктах сигнализации. Приведены способы обеспечения ИБ, которые могут применяться ко всем уровням эталонной модели OSI. Способы обеспечения ИБ в системе ОКС №7 на уровне безопасности инфраструктуры предназначены для уменьшения уязвимости к атакам, соответствующим угрозам ИБ.

Уровень безопасности приложений относится к оборудованию сетей связи ССОП, составной частью которых является оборудование системы сигнализации ОКС №7. В ТфОП/ЦСИС оборудование ОКС №7 входит составляющей частью в коммуникационные станции местной сети связи, междугородной и международной сети. В СПСС стандарта GSM оборудование системы сигнализации входит в центр коммутации мобильной сети связи MSC, в «домашний» HLR и «гостевой» регистры VLR, транзитные и локальные центры коммутации. В ИС оборудование системы сигнализации входят в узел коммутации услуг SSP и в узел управления услугами SCP. В результате чего следствием нарушения ИБ в системе сигнализации является нарушение ИБ в целом ССОП.

Плоскость безопасности управления относится к защите функций эксплуатации, подсистемы технического обслуживания и администрирования OMAP (Operation, Maintenance and Administration Part). Примером таких функций является управление звеньями сигнализации, которое может быть разделено на процесс активизации и деактивизации звена (канала) сигнализации.

Дезактивизация выводит канал из рабочего состояния, делая его недоступным для переноса сигнального трафика. Подобно активизации, этот процесс инициализируется обслуживающим персоналом. Плоскость безопасности

транспортной сети относится к защите всех четырёх уровней ОКС №7 при воздействии намеренного нелегитимного использования основных функций.

Отказ звена сигнализации или пункта сигнализации (ПС) может повлечь недоступность проходящих через него маршрутов сигнализации к ПС назначения, что в свою очередь может вызвать изменение таблицы маршрутизации и в других ПС. Такие последствия атак в системе ОКС №7 послужили основанием принятия решения по постановке задачи диссертационной работы. Все это показывает, что число возможных вариантов атак в системе сигнализации настолько большое, что нет необходимости да и возможности в анализе их всех.

Поэтому практическую целесообразность представляет анализ таких атак в ОКС №7, которые воздействуют на наиболее чувствительные (с точки зрения нанесения большого ущерба) участки ССОП. В результате анализа определен такой тип угроз, относящихся к уровню безопасности инфраструктуры и плоскости безопасности транспортной сети, что и определило постановку задач, подлежащих исследованию в диссертационной работе.

**Во второй главе** предложен метод анализа последствий атак (категории DoS) в системе сигнализации ОКС №7 ССОП. Анализируются результаты нелегитимного использования нарушителем тех функций подсистем MTP-3 и SCCP сетевого уровня в ОКС №7, которые приводят к наиболее характерным серьезным последствиям нарушения работы ССОП. Анализ проведён на обобщённой схеме сети системы сигнализации, рис. 1, и позволил разработать основные рекомендации по проведению аналогичных исследований на реальных сетях ТфОП/ЦСИС, СПСС стандарта GSM и ИС, с входящими в них ПС в системе сигнализации ОКС №7.

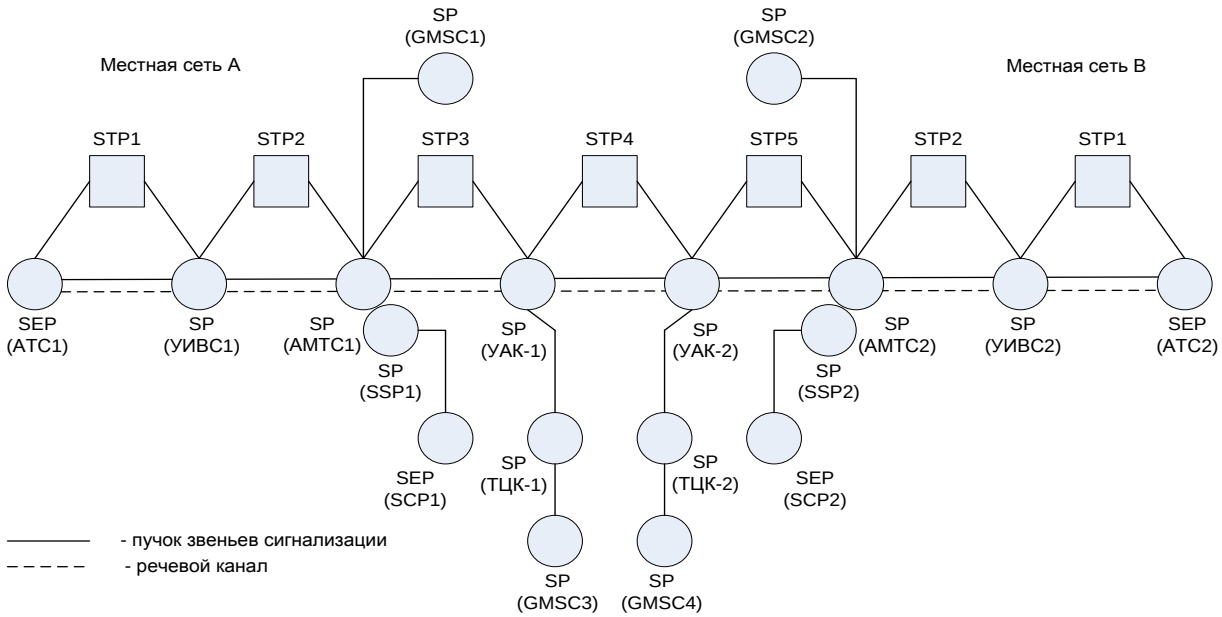


Рисунок 1 – Обобщённая схема служебной подсистемы ОКС №7

На рис. 1 представлены ПС двух местных сетей (А и В) и междугородного участка. В скобках указаны узлы коммутации, в которые входят следующие ПС: SEP (в АТС), SP (в УИВС), SP (в АМТС), SP1 (в УАК-1), SP2 (в УАК-2).

На участках местной и междугородной сетей предусмотрены альтернативные пути сигнализации через STP. Предусмотрено подключение к фиксированной сети связи абонентов мобильной сети. Показано подключение промежуточного пункта SP в шлюзе мобильного центра коммутации GMSC к АМТС. Мобильный центр коммутации MSC, обслуживающий мобильные станции, подключен к GMSC.

Пункт сигнализации SP1 в УАК-1 взаимодействует с SP в ТЦК-1, а SP-2 в УАК-2 с SP в ТЦК-2; SP в ТЦК-1 соединен по системе ОКС №7 с SP в GMSC-1, а SP в ТЦК-2 с SP в GMSC-2. Мобильные станции, обслуживаемые мобильными центрами коммутации MSC-1 и MSC-2, соответственно через шлюзы GMSC-1 и GMSC-2 могут устанавливать соединения через ТЦК-1 и ТЦК-2.

В приведенной обобщённой схеме для представления пользователям услуг интеллектуальной сети показаны взаимодействующие по системе ОКС №7 ПС в узле коммутации услуг SSP и SEP узла управления услугами SCP. Узел SSP установлен непосредственно на АМТС. Следует отметить, что SSP может быть выделенным от АМТС и взаимодействовать с ней по системе ОКС №7. Описание атак приводится по группам, классифицированным в соответствии с типами нелегитимных сообщений сигнализации.

Анализируются последствия угроз ИБ ОКС №7, реализация которых приводит к «отказу в обслуживании» ССОП. Рассмотрению подлежат результаты нелегитимного использования нарушителем следующих функций сетевого уровня МТР-3 в системе сигнализации ОКС №7:

– вынужденная ремаршрутизация;
– управление потоком сигнального трафика подсистемы МТР3;
– управляемая маршрутизация;
– управляемый и ограниченный перенос;
– перезапуск МТР и перевод трафика на резервное звено сигнализации;
– восстановление трафика на исходное звено сигнализации;
– функция уровня SCCP «запрет доступа»; и
– функция уровня SCCP «подсистема перегружена».

При анализе ущерба от атак в системе сигнализации конкретной эксплуатируемой ССОП следует учитывать:

– возможность создания нарушителем нелегитимного сообщения обновления маршрутизации, или имитации трансляции такого сообщения от смежного ПС;
– схему резервирования при взаимодействии узлов коммутации разных уровней иерархии ССОП;

– схему сопряжения ССОП ТфОП/ЦСИС, СПС стандарта GSM и интеллектуальных сетей между собой;

– возможность создания нарушителем одного или нескольких нелегитимных сообщений в пункте сигнализации ОКС №7;

– возможность частичного нанесения ущерба, выраженного в повышении вероятности нелегитимной перегрузки в сети ОП или снижении коэффициента готовности пучков маршрутов.

В выводах по главе отмечается необходимость разработки метода оценки степени защищенности от угроз нарушения маршрутизации в системе ОКС №7 на ССОП.

**В третьей главе** разработан метод оценки механизма аутентификации в системе сигнализации ОКС №7 в ССОП. При выполнении функций маршрутизации в ОКС №7 механизмы аутентификации не сертифицированы международными организациями стандартизации, а поэтому производителями оборудования ССОП могут быть использованы разные типы таких механизмов. В одном ПС может быть установлено несколько типов механизмов аутентификации с целью совместимости со смежными ПС тех же или других производителей оборудования. Не исключено, что некоторые производители оборудования вообще не предусматривают механизмов защиты. В связи с этим стоит задача качественной оценки механизмов аутентификации для защиты от нарушения маршрутизации в системе сигнализации для того, чтобы сравнить различные механизмы и провести обоснованный выбор из них.

Предлагаемый метод оценки предусматривает расчет интегральной характеристики оценки эффективности механизма аутентификации, предусматривающий экспертный метод оценки некоторых характеристик. В указанном методе учитываются две интегральные характеристики механизма безопасности:

– интегральная характеристика уровня (или степени) обеспечения информационной безопасности от атак;

– интегральная характеристика экономической эффективности безопасности, которая относится к стоимостным показателям механизма защиты, и определяется сложностью его реализации.

Для иллюстрации предлагаемого метода приводится расчетный пример.

В качестве механизмов аутентификации в примере выбраны стандартизированные механизмы (А, Б, В, Г, Д, Е), используемые для защиты от других видов атак в сетях СПСС, ТфОП/ЦСИС и др. Обозначим интегральную характеристику уровня обеспечения ИБ механизмом аутентификации X через $R_{\text{sec}}(X)$:

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

где: i – номер требования ИБ к механизму аутентификации; N1 – общее число требований ИБ к механизму аутентификации; Ki – степень важности выполнения требования i-м механизмом аутентификации; Xi – степень выполнения требования i механизмом аутентификации.

Значение Xi = 0 означает, что требование ИБ механизмом аутентификации X не выполняется. Чем больше Xi, тем в большей степени требование ИБ выполняется механизмом аутентификации. Характеристики Xi и Ki в (1) определяются экспертным методом. Значение Z определяет диапазон значений Rsec(X). Максимальное значение Rsec(X) определяется произведением числа Z на максимальное Xi, при котором Ki выполняется полностью. Ниже, в табл. 1 приведена иллюстрации определения интегральных значений Rsec рассматриваемых механизмов аутентификации. Значения коэффициентов ИБ следующие:

i = 1: обеспечение только подлинности источника сообщения обновления маршрутизации;

i = 2: обеспечение только целостности принятого сообщения обновления маршрутизации.

Кроме требований ИБ, имеющих характеристики Xi и Ki, предусмотрены так называемые критические требования, которые не имеют весовых значений и являются обязательными для выполнений. К таким требованиям относятся:

– средства аудита, которые позволяют записывать полную информацию о сообщениях обновления маршрутизации;

– система извещений, позволяющая в реальном масштабе времени указывать о признаках атак, вызванных фальсификацией сообщений обновления маршрутизации.

Расчетные значения $R_{\text{sec}}(X)$ в табл. 1 представлены для иллюстрации предлагаемого метода выбора механизма аутентификации из числа анализируемых. С этой же целью выбраны и приведенные параметры Ki и Xi. Диапазон значений Rsec принят равным 100 (произведение Z = 10 на максимальное значение Xi = 10).

Таблица 1 – Значения интегральных характеристик ИБ механизмов аутентификации

| Требование i | Ki | Xi | | | | | |
|---|---|---|---|---|---|---|---|
| | | А | Б | В | Г | Д | Е |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 10 | 1 | 3 | 3 | 5 | 7 | 10 |
| Rsec(X) | | 10,0 | 28,2 | 28,2 | 46,4 | 64,5 | 91,8 |

Смысл механизмов аутентификации (А, Б, В, Г, Д, Е) состоит в следующем:

А – подлинность источника и целостность 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 ключом соседнего маршрутизатора.

Б – механизм аутентификации аналогичен вышеприведенному А, за исключением того, что используется функция хеширования по протоколу HMAC.

В – механизм аутентификации аналогичен механизму А за исключением того, что для вычисления MAC используется не функция хеширования, а алгоритм симметричного шифрования DES[1].

Г – механизм аутентификации аналогичен механизму В за исключением того, что для вычисления MAC используется алгоритм симметричного шифрования KASUMI, используемый в сотовой сети подвижной связи UMTS.

Д – подлинность источника и целостность сообщения обновления маршрутизации реализуется с помощью симметричного шифрования хеш-кода (профиля) сообщения.

Е – подлинность источника и целостность сообщения обновления маршрутизации реализуется с помощью шифрования с открытым ключом.

Как видно из табл. 1, наименьшее значение $R_{\text{sec}}(X)$ характеризуется механизмом хеширования (А), а наибольшее – механизмом, использующим шифрование с открытым ключом (Е); Б и В имеют одинаковое значение $R_{\text{sec}}(X)$.

Обозначим интегральную характеристику эффективности механизма аутентификации X через $R_{fh}(X)$, где f – ПС системы сигнализации, в который поступает фальсифицированное сообщение обновления маршрутизации из смежного пункта сигнализации h:

$$R_{fh}(X) = \frac{\sum_{w=1}^{N3} C_{fh}(W) \cdot X_{fh}(W) \cdot Z}{\sum_{w=1}^{N3} C_{fh}(W)}. \qquad (2)$$

В (2) для интегральной эффективности механизма аутентификации приняты следующие обозначения (определяющие её эффективность по снижению ущерба в ССОП): показатель W означает вид ущерба ССОП от реализации угрозы фальсификации маршрутной информации в ОКС №7, который в общем виде выражается в отказе установления соединений одновременно большому числу пользователей. Ограничимся для примера следующими значениями W:

W = 1: отказ в установлении соединений между абонентами ТфОП/ЦСИС;

W = 2: отказ в установлении соединений между мобильными станциями (MS) сети СПС стандарта GSM;

W = 3: отказ в установлении соединений между абонентами ТфОП/ЦСИС и мобильными станциями СПС стандарта GSM;

[1] Принятым национальным бюро стандартов США.

W = 4: отказ в установлении только тех соединений между абонентами ТфОП/ЦСИС, которым требуется предоставление услуг ИС; и

NЗ – общее число принятых видов ущерба ССОП, т.е. в примере NЗ = 4.

Показатель $C_{fh}(W)$ в (2) означает максимальное значение конкретного вида ущерба W ССОП при реализации атаки фальсификации маршрутной информации ОКС №7 в случае отсутствия механизма аутентификации в ПСf при поступлении этих нелегитимных сообщений из ПСh. $C_{fh}(W)$ отражает важность требований к механизму аутентификации по снижению ущерба W.

Показатель $X_{fh}(W)$ в (2) означает степень снижения максимального ущерба $C_{fh}(W)$ механизмом аутентификации X. Показатели $C_{fh}(W)$ и $X_{fh}(W)$ зависят от:

– топологии ССОП (принадлежности к определенной сети связи ОП ТфОП/ЦСИС, СПС стандарта GSM, ИС). Значение Z определяет диапазон значений $R_{fh}(X)$. Максимальное значение $R_{fh}(X)$ определяется произведением Z на максимальное значение $X_{fh}(W)$, при котором снижение ущерба $C_{fh}(W)$ выполняется полностью;

– структуры резервирования путей маршрутизации и звеньев сигнализации;

– пунктов сигнализации ОКС №7, подключенных к ПСh, кроме ПСf и др.;

– конкретных функций сетевого уровня в системе ОКС №7, используемых нарушителем для нелегитимного обновления таблиц маршрутизации;

– числа фальсифицированных сообщений обновления маршрутизации, отправляемых нарушителем при использовании одной функции сетевого уровня в системе сигнализации ОКС №7.

Полная оценка эффективности всех механизмов аутентификации в системе ОКС №7 для всех видов оборудования ССОП представляет практически нереализуемую задачу вычисления значения $R_{fh}(X)$ для всех смежных пунктов сигнализации в ССОП. Кроме того, невозможно учесть все виды атак в системе ОКС №7. Поэтому ставится задача определения показателей $C_{fh}(W)$ и $X_{fh}(W)$ в отношении наиболее уязвимых мест для атак нарушения маршрутизации в системе ОКС №7 с точки зрения нанесения наибольшего ущерба ССОП.

При отсутствии механизмов аутентификации в смежных пунктах сигнализации недостаточно показателя интегральной характеристики эффективности механизма аутентификации $R_{fh}(X)$. В этом случае необходимо учитывать дополнительно стоимостные показатели самого механизма аутентификации и сложность его реализации в ПС Rcost(X):

$$R_{cost}(X) = \frac{\sum_{i=1}^{N1}(K_i X_i Z) + \sum_{j=1}^{N2} K_j X_j Z}{\sum_{i=1}^{N1} K_i + \sum_{j=1}^{N2} C_j}, \quad (3)$$

где Ki, Xi, Z, N1 – показатели, используемые для определения Rsec(X) по (1); j – технический показатель механизма аутентификации, позволяющий оценить его стоимость или сложность установления в ПС; N2 – общее число показателей j в анализируемых механизмах аутентификации; Cj – максимальная величина экономической эффективности при отсутствии затрат на показатель j механизма аутентификации; Xj – степень выполнения Cj в механизме аутентификации. Чем выше значение Xj, тем меньше разница между Cj и Xj.

В табл. 2 для иллюстрации приведены результаты расчета стоимостных показателей анализируемых механизмов аутентификации.

Таблица 2 – Значения стоимостных характеристик механизмов аутентификации

| Показатель j | Cj | Xj | | | | | |
|---|---|---|---|---|---|---|---|
| | | 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 |
| Rcost(X) | | 52,6 | 58,0 | 54,8 | 56,8 | 55,16 | 80,6 |

Значение Z определяет диапазон Rcost(X). Максимальное значение Rcost(X) определяется произведением Z на максимальное значение Xj, при котором Cj выполняется полностью. Во всех примерах, приведенных в табл. 1 и 2, принято Z=10. Чем выше значение Rcost(X), тем больше затрат требуется на реализацию механизма безопасности (в данном случае механизма аутентификации). Из табл. 2 видно, что механизм D, например, значительно экономичнее механизме E (Rcost(D)= 55,16, а Rcost(E)= 80,6), но значительно уступает по характеристике обеспечения ИБ в табл. 1 (Rsec(D)= 64,5, Rsec(E)= 91,8).

В результате разработанный аналитический метод оценки механизма аутентификации в ОКС №7 позволяет сравнить различные механизмы защиты от угроз нарушения маршрутизации.

**В четвертой главе** разработаны рекомендации по организации системы проведения работ по оценке степени защищенности находящихся в эксплуатации ССОП от атак нарушения маршрутизации системы ОКС №7. На рис.2 приведена упрощенная схема системы сигнализации анализируемой ССОП республики Ливан, включающая ТфОП/ЦСИС, СПСС и ИС.

Для ТфОП/ЦСИС показаны такие уровни, как: местный, междугородный и международный анализируемой ССОП, а также международные уровни двух других взаимодействующих с ним стран. Сеть СПС стандарта GSM представ-

ляет одноуровневую структуру. Каждая из трех АМТС соединена с двумя (из четырех полносвязных УАК), а к одной из АМТС подключен шлюз мобильных станций коммутации GMSC, и выделенный узел коммутации услуг SSP ИС.

Для того, чтобы оценить степень защищенности находящихся в эксплуатации ССОП от таких атак (категории DoS) в системе ОКС №7 следует последовательно для каждого из наиболее чувствительных участков смежных пунктов сигнализации (с точки зрения последствий ущерба для работы ССОП) последовательно решить ряд задач: определить степень максимального ущерба для работы ССОП (при отсутствии механизмов аутентификации в ПС). Определить по результатам тестирования[2] совместность механизмов аутентификации в ПС ОКС №7 (либо их отсутствие).

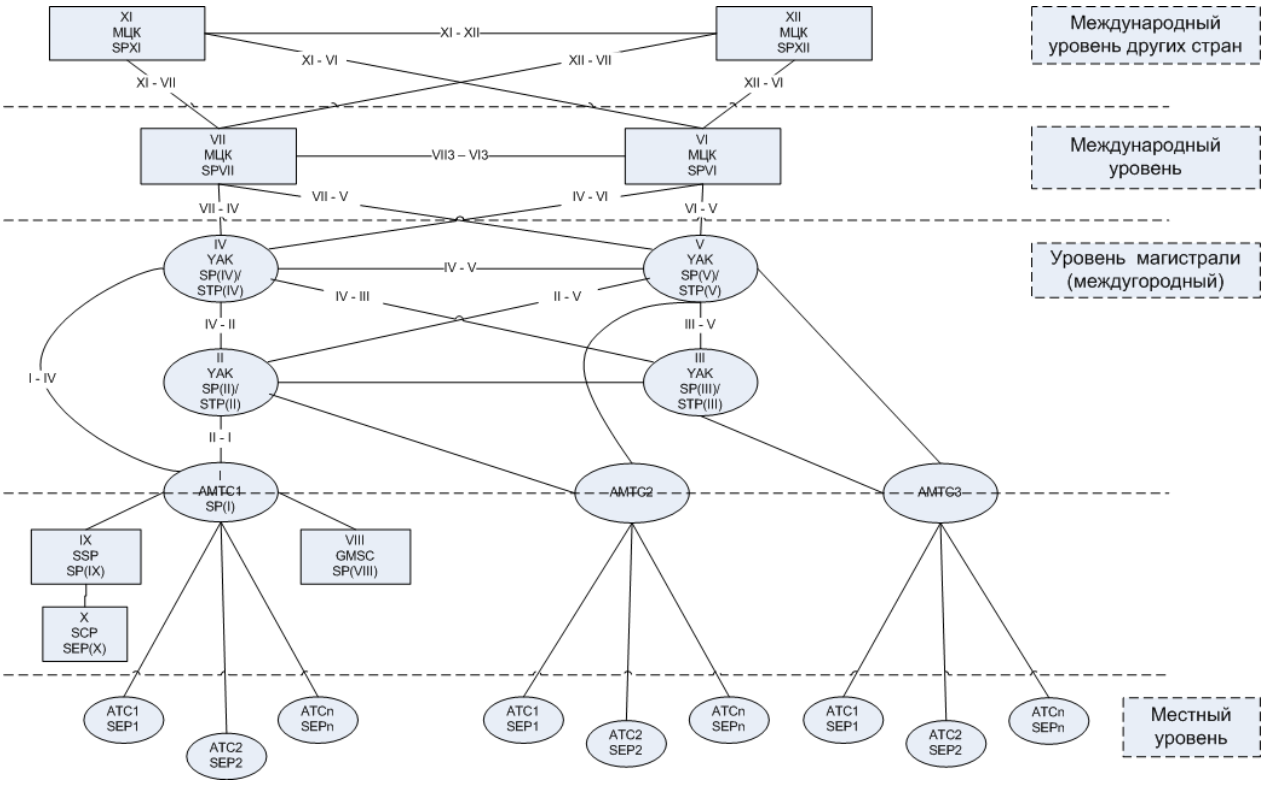


Рисунок 2 - Упрощенная схема ОКС №7 сети связи общего пользования

Алгоритмы обеспечения ИБ в сетях связи (подобно приведенным выше протоколам аутентификации) являются частью функций объектов сети. В то же время в существующих спецификациях по тестированию таких систем как ОКС №7, алгоритмы механизмов аутентификации не специфицированы, поэтому не подлежат в документах ITU-T тестированию на соответствие. В связи с этим для проведения тестирования совместимости механизмов аутентификации в ОКС №7 необходимо

[2] Международными организациями по стандартизации ITU-T, ETSI, 3GPP и др. уделяется большое внимание тестированию функциональности объектов сети. Разработаны рекомендации по базовым вопросам тестирования (стандарт ITU-T Q.3900), а также по тестированию некоторых конкретных технологий связи (например, стандарты Q.781 – Q.787 по тестированию ОКС №7). Тестирование предусматривается как в части проверки алгоритмов на соответствие спецификациям, так и в части совместимости алгоритмов разных производителей оборудования.

проведение научно-исследовательских работ, в частности, определить эффективность механизмов аутентификации при их совместимости можно по формуле (3). В случае низкой защищенности от угроз необходимо разработать предложения по использованию других механизмов аутентификации. В случае несовместимости механизмов или их отсутствия на участке смежных ПС необходимо разработать предложения по доработке ОКС №7 в части установки совместимых механизмов аутентификации с необходимой степенью защищенности.

Тестированию подлежат механизмы защиты от несанкционированных сообщений обновления маршрутизации, которые содержат нелегитимные адреса ПС ОКС №7. Такие сообщения могут направляться злоумышленником из шлюза (STP) одной национальной сети в шлюз другой национальной сети. В качестве механизма защиты используется «просеивание» поступающих сигнальных единиц MSU и обычно не применяется для внутрисетевых MSU. Процедуры отсева выполняются подсистемами сетевого уровня MTP и SCCP.

Для приведенной на рис.2 схемы ОКС №7 анализируемых ССОП наиболее чувствительным с точки зрения ущерба от нарушения маршрутизации являются следующие участки смежных ПС:

– на международном уровне между ПС в международных центрах коммутации МЦК анализируемой ССОП и МЦК соседних стран;

– на междугородном уровне между АМТС и двумя соединенными с ней УАК;

– между АМТС и подключенными к ней GMSC, SSP, АТС.

Предложен метод выбора механизмов аутентификации в ПС ОКС №7 по результатам тестирования на совместимость механизмов защиты в действующих сетях ССОП. Ущерб ССОП при реализации угроз, приводящих к нелегитимному изменению таблиц маршрутизации, может быть нанесен в случаях:

– при действии нарушителя со стороны ПС в МЦК соседних стран (т.е. в МЦК XI и МЦК XII);

– при действиях нарушителя со стороны ПС анализируемой сети (т.е. МЦК VI и МЦК VII).

В каждом из этих случаев подлежат анализу следующие сообщения сетевого уровня:

– запрет передачи (TFP);

– недоступность подсистемы пользователя (UPU);

– перегрузка пучка звеньев сигнализации (TFC);

– ограничение передачи (TFR);

– запрет доступа (SSP);

– подсистема SCCP перегружена (SSC).

**В заключении** изложены основные результаты диссертационной работы.

**В приложении** представлены документы, подтверждающие применение результатов работы на корпоративной сети передачи данных предприятия НПОУ ИЦ «Техника», г. Уфа и в учебном процессе Уфимского государственного авиационного технического университета при проведении лабораторных и практических работ по направлению «Телекоммуникации», а также материалы, поясняющие методику расчёта анализа ущерба ССОП на междугороднем и местном уровнях.

## ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ

1. Предложена расширенная классификация нарушений ИБ и выполнен анализ модели нарушений, которые в отличие от традиционных средств информационной безопасности предполагают анализ функций обновления маршрутизации в ОКС №7, позволяющие сделать вывод о наиболее опасных активных угрозах технологической безопасности (класс 1.3) и прямых активных угрозах эксплуатационной безопасности (класс 2.1.3), а также наиболее значимых угрозах по степени влияния на функционирование ССОП.

2. Разработана модель последствий атак (категории DoS) на процесс маршрутизации в ОКС №7, приводящих к выводу из рабочего состояния фрагментов ССОП, основанная на полученных экспертным методом критериях оценки, позволяющая ранжировать чувствительные к отказу в обслуживании участки ССОП и разрабатывать рекомендации по проведению анализа реальной информационной защищённости эксплуатируемых ССОП. Показано, что наибольший ущерб от таких атак производится нелегитимными сообщениями, созданными в пунктах сигнализации смежных уровней иерархии ССОП.

3. Предложен вероятностный подход к моделированию параметров систем контроля доступа, основанный на использовании метода экспертных оценок с привлечением статистических данных как из эксплуатации, так и полученных в результате ускоренных испытаний, позволяющий рассчитать количественные показатели ИБ, связанные с возможностью несанкционированного доступа к ресурсам и средствами контроля ОКС №7, и разработать мероприятия повышения ИБ ССОП на основе определения пути изменения указанных количественных показателей. Предложенный подход позволяет со значительной степенью достоверности (0,97) формализовать процесс функционирования системы контроля доступа ОКС №7 с точки зрения обеспечения ИБ ССОП.

4. Разработан метод количественной оценки степени защищенности работы ССОП, основанный на использовании предложенных механизмов аутентификации в ОКС №7 и интегральных параметров степени защищённости в отношении снижения риска отказа в обслуживании по установлению соединений, позволяющий выполнять оценку интегральной защищённости работы ССОП и на её основе вырабатывать мероприятия по снижению указанного риска отказа, повышая тем самым ИБ сети связи.

5. Предложен метод повышения ИБ, основанный на использовании свободных октетов в поле SIF, влияющих на установление соединения, позволяющий контролировать легитимность служебных сообщений ОКС №7 и тем самым обеспечивает их фильтрацию.

6. Разработана архитектура сетевой безопасности ОКС №7, учитывающая типы оборудования и функции системы сигнализации (уровни и плоскости безопасности), позволяющая определить аппаратные и программные модули ССОП, для которых необходимо применять мероприятия по защите ИБ. На основании

данной архитектуры предложен и обоснован выбор модуля, обеспечивающего аппаратную реализацию механизма аутентификации сообщений.

## ОСНОВНЫЕ ПУБЛИКАЦИИ

### *В рецензируемых журналах из списка ВАК*

1. Бельфер Р. А., Горшков Ю. Г., Даннави М. Н. Алгоритмы аутентификации в сетях связи общего пользования России // Электросвязь, – № 8, 2008. – С. 12 – 17.

2. Бельфер Р. А., Горшков Ю. Г., Даннави М. Н. Архитектура сетевой безопасности ОКС №7 // Электросвязь, – № 4, 2009. – С. 12 – 15.

3. 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: научн. журн. Бауманск. гос. техн. ун-та. Сер. «Приборостроение». 2009, № 3. – С. 95 – 100.

4. Бельфер Р. А., Горшков Ю. Г., Даннави М. Н. Оценка последствий угроз нарушения маршрутизации в общеканальной сигнализации сетей связи общего пользования // Вестник МГТУ им. Н.Э. Баумана: научн. журн. Бауманск. гос. техн. ун-та. Сер. «Приборостроение». 2009, № 4. – С. 75 – 80.

5. Даннави М. Н. Последствия воздействия некоторых несанкционированных сообщений ОКС №7 на сети связи общего пользования // Телекоммуникации и транспорт, – № 1, 2009. – С. 42 – 44.

6. Виноградова И. Л., Даннави М. Н. Требования к системе транспортировки сообщений общей канальной сигнализации по защите информации // Вестник УГАТУ: научн. журн. Уфимск. гос. авиац. техн. ун-та. 2011, № 5 (Т. 45). – С. 66 –72.

### *В других изданиях*

7. Бельфер Р.А., Даннави М. Н. Принцип согласования SLA между несколькими поставщиками услуг связи // Технологии информационного общества: Сб. докл. Московской отраслевой научн.-техн. конф. –М.: Инсвязьиздат, 2007, –с.40–43.

8. Бельфер Р. А., Даннави М. Н. Показатели качества обслуживания пользователей // Технологии информационного общества: Сб. докл. Московской отраслевой научн.-техн. конф. – М.: Инсвязьиздат, 2007, – с. 61 – 64.

9. Бельфер Р. А., Горшков Ю. Г., Даннави М. Н. Виды угроз информационной безопасности в сетях связи общего пользования // Труды МТУСИ, 2008, Т. II, – С. 101 – 103.

10. Даннави М. Н. Информационная безопасность в сетях связи общего пользования // INTERMATIC-2008: Сб. докл. Восьмой международной научн.-техн. конф. – Москва, РАН, 2008, – с. 324 – 327.

11. Даннави М. Н. Анализ угроз информационной безопасности (DoS) в сетях связи общего пользования // Безопасность информационных технологий: Сб. докл. Восьмой международной научн.-техн. конф. – Москва, МИФИ, 2009, – с. 100 – 102.

12. Султанов А.Х., Виноградова И.Л., Даннави М.Н. Задача обоснования требований к системе транспортировке сообщений общей канальной сигнализации ОКС №7 по защите информации // Проблемы техники и технологии телекоммуникаций: Сб. докл. Двеннадцатой международной научн.-техн. конф. – Казань, КГТУ, 2011, – с. 491 – 493.

ДАННАВИ Мохамад Насреддин

# МЕТОД ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ ОТ УГРОЗ НАРУШЕНИЯ МАРШРУТИЗАЦИИ В ОБЩЕЙ КАНАЛЬНОЙ СИГНАЛИЗАЦИИ СЕТИ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Специальность: 05.12.13 – Системы, сети и устройства телекоммуникаций

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать 12.03.2012. Формат 60×84 1/16.
Бумага обёрточная. Печать плоская. Гарнитура Таймс.
Усл.печ.л. 1,0. Уч.-изд.л. 0,9.
Тираж 100 экз. Заказ № 618

ФГБОУ ВПО Уфимский государственный авиационный технический университет
Центр оперативной полиграфии УГАТУ
450000, Уфа-Центр, К.Маркса, 12