# Система сигнализации SS7 и ее уязвимость

М.А. Шнепс-Шнеппе

***Аннотация*—В условиях курса на импортозамещение в системах связи актуальным стал вопрос модернизации традиционных сетей коммутации каналов, где наиболее ценным нововведением последнего времени является система сигнализации SS7. В статье рассмотрены основы сигнализации SS7 и ее уязвимость на фиксированной и мобильной сети и уязвимость протокола SIGTRAN.**

***Ключевые слова*— сигнализация SS7; SIP; AS-SIP; уязвимость SS7; уязвимость SIGTRAN.**

## I. Введение

Перед связистами всего мира стоит одна и та же задача – как перейти от коммутации каналов к коммутации пакетов. Главным, заинтересованным «игроком» на этом поле смены парадигмы телекоммуникаций является индустрия: производители оборудования коммутации пакетов собираются заработать многие миллиарды долларов и платят журналистам многие миллионы за популяризацию новой парадигмы. Но жизнь вносит свои коррективы.

ОАО «Ростелеком» объявило курс на импортозамещение [1]. А еще недавно Ростелеком ратовал за «All-over-IP» и строил сети на импортном оборудовании. В новых экономико-политических условиях возникла дилемма: по какому пути далее идти – по «старому» пути коммутации каналов или по новому - к коммутации пакетов. Если действительно идти на строительство сетей связи собственными силами, то, на наш взгляд, следует вернуться к тому состоянию знаний, которые были достигнуты ранее – лет 20 назад и развивать их далее. В данном случае такой точкой отсчета условно можно назвать систему сигнализации ОКС-7 (по-английски SS7). В России отставание от передового мирового уровня, конечно, большое, особенно по технике коммутации пакетов, где требуется мощная микроэлектроника. Поэтому коммутация каналов на данный момент предпочтительнее. Но с системой SS7 тоже все не так просто. В последнее время в мире интенсивно распространяются суждения об уязвимости сигнализации SS7. Начнем с двух примеров.

Пример 1. 31 января 2014 г. Федеральная комиссия связи FCC издала документ о поддержке операторов, которые будут переходить от коммутации каналов (по технологии TDM) к IP протоколу [2]. Это связано со срывом сроков внедрения нового поколения экстренной службы NG9-1-1. Оказывается, операторы связи в США не спешат с переходом на IP технологии, опасаясь сбоев в сети, что непременно сопровождает нововведения. В частности, сбои появляются из-за ошибок в программном обеспечении, что может привести к крупным авариям на телефонных сетях.

Наиболее известен коллапс сети AT&T, который случился 15 января 1990 г. [3]. Тогда одновременно вышли из строя все 114 станций 4ESS сети AT&T. Устранить неполадки удалось только через 9 часов. Дело было в новой версии программного обеспечения, которую установили месяцем ранее на всех станциях 4ESS. Вкралась ошибка в работе системы SS7, которая проявилась при перегрузке одной из АТС и по принципу домино «вырубила» почти всю сеть AT&T. Были потеряны 65 млн. вызовов и нанесен трудно поправимый ущерб репутации компании. Другой подобный коллапс случился через полтора года – 26 июня 1991 г. в Балтиморе. На 6 часов остались без связи 5 млн. абонентов. Тоже из-за ошибки в программах SS7. Случались сбои и при внедрении услуг интеллектуальной сети: перенос номеров мобильной связи, внедрение Бесплатного вызова по коду 888 и другие. Коллапсы сетей связи страны приравняли к угрозам национальной безопасности, и в Конгрессе США провели расследование. Тем самым неявно был вынесен «приговор» системе SS7. В частности, в экстренной службе 911 отказались от применения сигнализации SS7 и услуг интеллектуальной сети и сохранили прежнюю систему многочастотной сигнализации MF.

Пример 2. В конце 2014 г. в Гамбурге прошел Chaos Communication Congress, прозванный конгрессом хакеров. Обсуждали уязвимость мобильных сетей и, в основном, уязвимость сигнализации SS7. Хотя эта проблема профессионалам была известна давно, популярной она стала недавно - после шпионских разоблачений Эдуарда Сноудена.

Далее мы рассматриваем основы сигнализации SS7 (раздел 2) и сигнализации SIP и AS-SIP (раздел 3). Затем обсуждаем уязвимость SS7 на фиксированной сети (раздел 4), на мобильной сети (раздел 5) и уязвимость протокола SIGTRAN (раздел 6).

## II. Основы сигнализации SS7

Разработанная в конце 70-х гг. система сигнализации №7 (Signaling System 7, SS7) играет важную роль в процессе конвергенции сетей. Она была создана для

Статья получена 9 апреля 2015. Шнепс-Шнеппе М.А., главный научный сотрудник ЦНИИС (email: sneps@mail.ru)

передачи управляющих сигналов в режиме коммутации пакетов отдельно от основной сети (out-of-band signaling). Ранее в телефонных сетях передача речи и сигналов управления происходила по одному каналу (inband signaling). Система SS7 является крупнейшим достоянием телекоммуникационных сетей.

Внедрение SS7 дает операторам телефонных сетей возможность гибко формировать новые услуги на базе уже существующего оборудования. Система сигнализации обеспечивает высокую скорость установления соединения и передачи данных (без потерь и дублирования), переключение трафика на альтернативные маршруты в случае отказов, удобную для обработки структуру сообщений, трансляцию номеров абонентов.

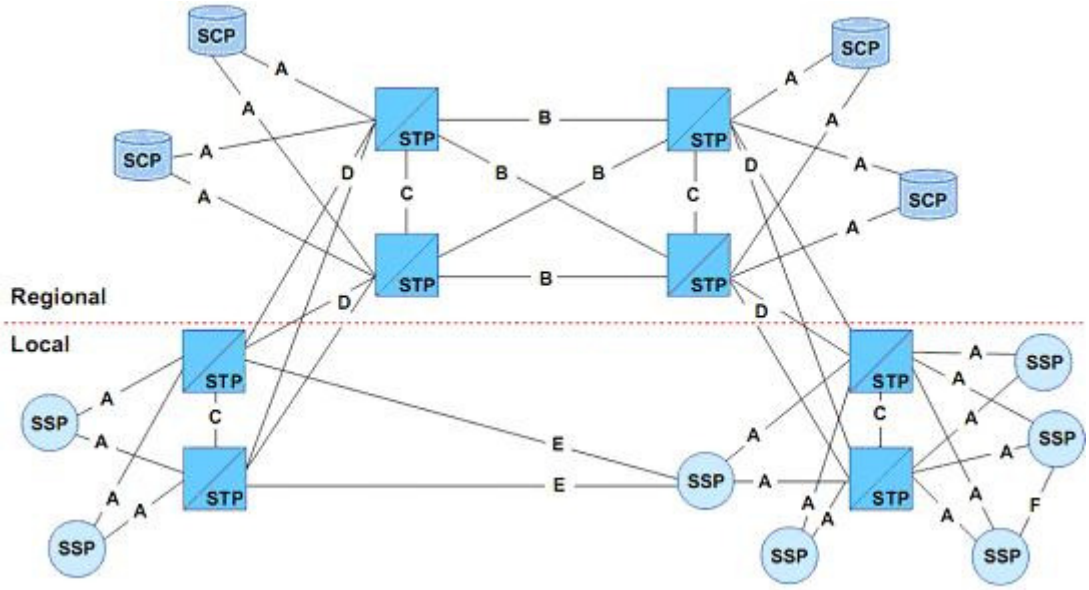



Рис. 1 Упрощенное представление сети SS7

Рисунок 1 показывает основные блоки сети SS7: пять типов звеньев сети SS7 (A, B, C, D и C) и три типа узлов интеллектуальной сети (SSP, STP и SCP). Интеллектуальная сеть IN (Intelligent Network) строится как дополнительный уровень сети оператора связи. Услуги IN обеспечиваются пунктами управления услугами (Service Control Point, SCP) и пунктами коммутации услуг (Service Switching Point, SSP). Обмен сообщениями SS7 происходит через транзитные пункты передачи сигнальных сообщений (Signal Transfer Point, STP). Это — коммутаторы пакетов сети SS7, осуществляющие их коммутацию и маршрутизацию.

Интеллектуальные функции (переадресация вызова, идентификация абонента и др.) реализуются пунктами SCP. Собственно «интеллект» SCP — это алгоритмы реализации услуг и наборы различных баз данных. Узел SSP распознает вызовы из сети общего пользования и передает их для обработки в SCP. SCP содержит центральную базу данных для обслуживаемого региона; SCP в ответ на запрос передает в SSP информацию как обработать вызов, который SSP затем осуществляет под управлением SCP.

На рис. 2 дан стек протоколов SS7. В проводных сетях интеллектуальные услуги предоставляются по протоколу INAP (Intelligent Network Application Part). В мобильных сетях соответственно — это беспроводная интеллектуальная сеть (Wireless Intelligent Network, WIN) и протокол CAP. Там же показан протокол MAP – основной протокол предоставления вызовов в мобильной сети GSM.

Стек протоколов ОКС-7 восходит к модели OSI. Нижние три уровня MTP (Message Transfer Part) совпадают с уровнями OSI: 1 (физический), 2 (канальный) и 3 (сетевой). MTP описывает транспортные протоколы, включая сетевые интерфейсы, обмен данными, обработка сообщений и маршрутизация их на верхний уровень. SCCP обеспечивает адресацию и маршрутизацию сообщений и сервис управления для приложений. TCAP используется для создания запросов к базе данных и является связующим протоколом с интеллектуальными сетями (INAP), мобильными службами (MAP) и т.д.

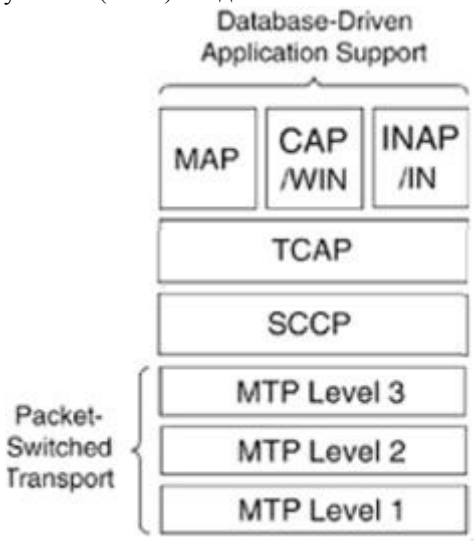



Рис. 2. Стек протоколов SS7

Состав сигнального сообщение SS7 иллюстрирует рис. 3. Работа сети SS7 регламентируется множеством таймеров – их более 40. Часть из них дана в таблице 1.

Набор таймеров SS7 несколько разнится в версиях стандартов от ANSI, ETSI и ITU-T. Рис. 4 иллюстрирует применение таймеров в алгоритме установления соединения.

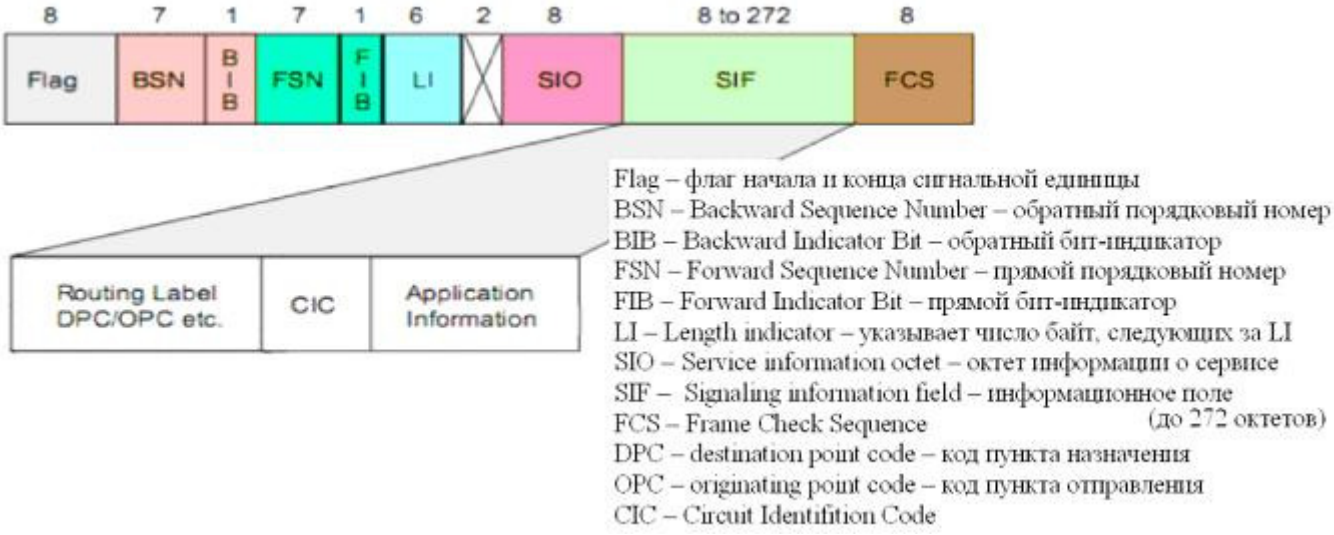



Рис. 3. Сигнальное сообщение SS7 (MSU, Message Signal Unit).

*Таблица 1. Таймеры MTP3 по стандарту ITU-T.*

| Timer | Use | Range |
|---|---|---|
| T1 | Delay to avoid missequencing on changeover | 500 (800)–1200 ms |
| T2 | Waiting for changeover acknowledgment | 700 (1400)–2000 ms |
| T3 | Time-controlled diversion delay—avoid missequencing on changeback | 500 (800)–1200 ms |
| T4 | Waiting for changeback acknowledgment (first attempt) | 500 (800)–1200 ms |
| T5 | Waiting for changeback acknowledgment (second attempt) | 500 (800)–1200 ms |
| T6 | Delay to avoid message missequencing on controlled rerouting | 500 (800)–1200 ms |
| T7 | Waiting for signaling data link connection acknowledgment | 1–2 s |
| T8 | Transfer prohibited inhibition timer | 800–1200 ms |
| T9 | Not used | Not used |
| T10 | Waiting to repeat signaling route-set test message | 30–60 s |
| T11 | Transfer restricted timer | 30–90 s |
| T12 | Waiting for uninhibit acknowledgment | 800–1500 ms |
| T13 | Waiting for force uninhibit | 800–1500 ms |
| T14 | Waiting for inhibition acknowledgment | 2–3 s |
| T15 | Waiting to start signaling route-set congestion test | 2–3 s |
| T16 | Waiting for route-set congestion status update | 1.4–2 s |
| T17 | Delay to avoid oscillation of initial alignment failure and link restart | 800–1500 ms |

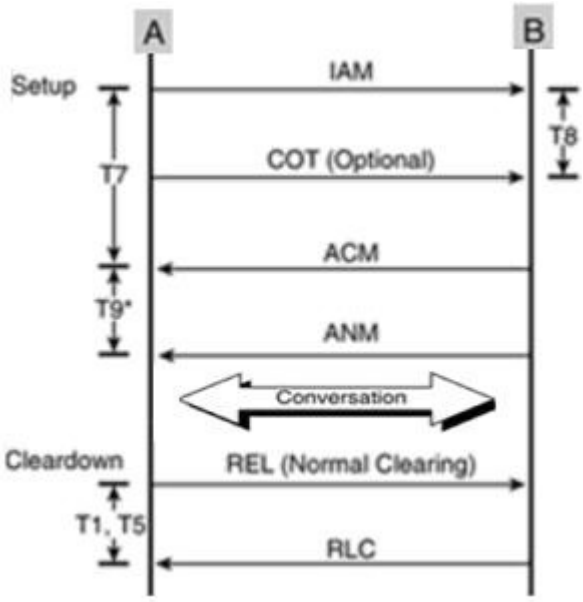
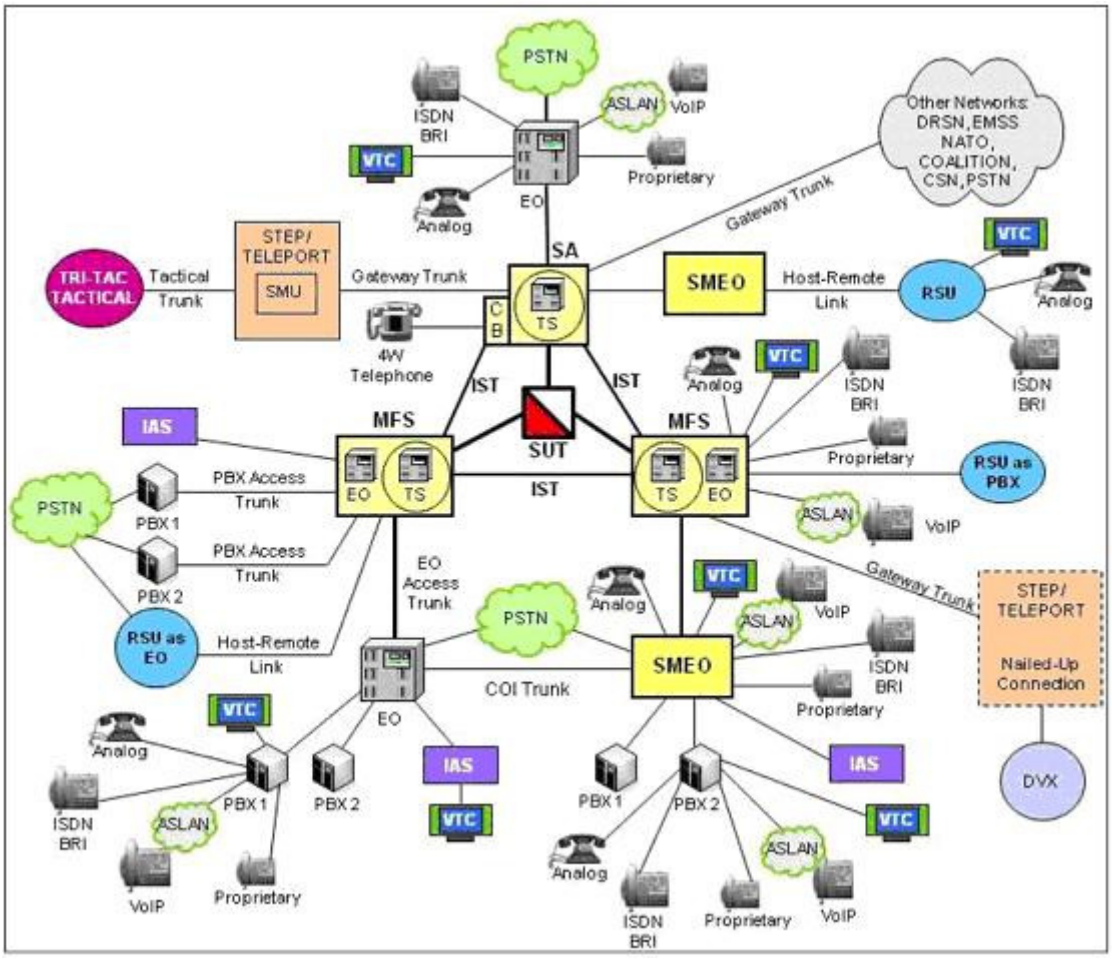



Рис. 4. Применение таймеров в алгоритме установления ISDN соединения

Мы кратко изложили суть системы SS7, дали представление о ее сложности, о перипетиях при ее внедрении. В целом эти перипетии уже позади. За 30 лет эксплуатации сетей SS7 инженеры научились обеспечивать надежную их работу. И вот ныне наступают времена перехода к технологии коммутации пакетов, перехода от сигнализации SS7 к сигнализации SIP. Эта дилемма стоит и перед Ростелеком. И, естественно, возникает вопрос: каким путем идти? На наш взгляд, стоит понаблюдать за развитием сети DSN

(Defence Switched Network) МО США, наиболее сложной ведомственной сети в мире. В настоящее время центральным звеном сети DSN является сеть SS7 (рис. 5), но уже начался переход на протокол SIP, точнее, на его защищенную версию AS-SIP. Этот протокол намного сложнее SS7, значит, и внедрять его будет намного больше. Стоит ли Ростелекому спешить с программой «All-over-IP»?




| | | | |
|---|---|---|---|
| 4W | 4-Wire | NATO | North Atlantic Treaty Organization |
| ASLAN | Assured Services Local Area Network | PBX | Private Branch Exchange |
| BRI | Basic Rate Interface | PBX 1 | Private Branch Exchange 1 |
| CB | ChannelBanic | PBX 2 | Private Branch Exchange 2 |
| COI | Community of Interest | PSTN | Public Switched Telephone Network |
| CSN | Canadian Switch Network | RSU | Remote Switching Unit |
| DRSN | Defense Red Switch Network | SA | Standalone |
| DSN | Defense Switched Network | SMEO | Small End Office |
| DVX | Deployable Voice Exchange | SMU | Switched Multiplex Unit |
| EMSS | Enhanced Mobile Satellite System | STEP | Standardized Tactical Entry Point |
| EO | End Office | SUT | System Under Test |
| IAS | Integrated Access Switch | Tri-Tac | Tri-Service Tactical Communications Program |
| ISDN | Integrated Services Digital Network | TS | Tandem Switch |
| IST | Interswitch Trunk | VoIP | Voice over Internet Protocol |
| MFS | Multifunction Switch | VTC | Video Teleconferencing |

Рис. 5. Архитектура DSN (Defence Switched Network) [4].

В центре схемы на рис. 5 размещен блок SUT (System Under Test), это сеть SS7, по которой устанавливаются все соединения на оборонной сети DSN. На сети военного назначения непрерывно появляется все новое оконечное оборудование, в значительной мере это IP средства, а сеть SS7 сохраняет свое центральное место. Устройства подключаются по любым протоколам: 4W – 4х проводной, ASLAN – засекреченная локальная сеть, ISDN BRI, VoIP – интернет-телефония, VTC – видеоконференцсвязь, proprietary – любой нестандартный протокол.

Отсюда делаем важный вывод: наличие сети SS7 не препятствует переходу на IP протоколы, а скорее наоборот – облегчает переход на пакетную коммутацию, делает его постепенным. Лишь базы данных на весь период перехода будут размещаться не в узлах IMS, а в IN и будут доступны как по протоколу SS7, а затем и по протоколу SIP.

## III Основы сигнализации SIP и AS-SIP

SIP (Session Initiation Protocol) — протокол установления сеанса связи и описывает способ установления и завершения интернет-сеанса, включающего обмен мультимедийным содержанием (видео- и аудиоконференции, мгновенные сообщения, онлайн-игры). Допускается добавление или удаление каналов в течение установленного сеанса, а также подключение и отключение дополнительных клиентов (конференц-связь).

SIP участвует только в сигнальной части сеанса связи. При передаче информации, SIP используется наряду с протоколами SDP, RTP, SOAP, HTTP, XML, VXML, WSDL, UDDI и другими.

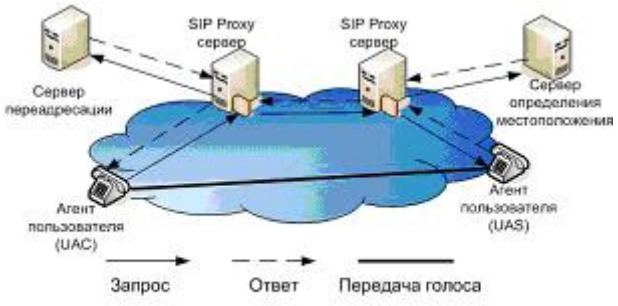



Рис. 6. Как работает протокол SIP.

Протокол SIP определяет три основных сценария установления соединения (рис. 6): 1) с участием прокси-сервера, 2) с участием сервера переадресации и 3) непосредственно между пользователями. Сценарии различаются в том, как осуществляется поиск и приглашение вызываемого пользователя.

Между двумя протоколами сигнализации SS7 и SIP имеются существенные различия. SS7 характеризуется сложной, централизованной интеллектуальной сетью и простыми, неинтеллектуальными, терминалами (традиционные телефонные аппараты). SIP — наоборот, требует очень простую (и, соответственно, хорошо масштабируемую) сеть, а интеллект встроен в оконечные элементы на периферии (терминалы, построенные как физические устройства, или программы).

Работа SIP регламентируется менее строго, чем SS7. Имеется всего три основных SIP таймера: T1, B и F. Таймер T1 определяет расчетное время передачи пакета IP туда и обратно. По умолчанию, T1 равен 500 мс, но допускаются и другие значения T1. Таймер B определяет максимальное время ожидания ответа на запрос INVITE. Таймер F определяет максимальное время ожидания ответа на другие запросы: REFER, INFO, MESSAGE, BYE и CANCEL (кроме запроса INVITE).

Рассмотрим типы запросов и ответов протокола SIP. В первоначальной версии протокола SIP (стандарт IETF RFC 3261) было определено шесть типов запросов:

1. INVITE — Приглашает пользователя к сеансу связи. Обычно содержит SDP-описание сеанса
2. ACK — Подтверждает приём ответа на запрос INVITE
3. BYE — Завершает сеанс связи. Может быть передан любой из сторон, участвующих в сеансе
4. CANCEL — Отменяет обработку ранее переданных запросов, но не влияет на запросы, которые уже закончили обрабатываться
5. REGISTER — Переносит адресную информацию для регистрации пользователя на сервере определения местоположения
6. OPTIONS — Запрашивает информацию о функциональных возможностях сервера

В процессе внедрения в протокол SIP было добавлен ряд других запросов, которые дополнили его функциональность:

1. PRACK — временное подтверждение
2. SUBSCRIBE — подписка на получение уведомлений о событии
3. NOTIFY — уведомление подписчика о событии
4. PUBLISH — публикация события на сервере
5. INFO — передача информации, которая не изменяет состояние сессии
6. REFER — запрос получателя о передаче запроса SIP
7. MESSAGE — передача мгновенных сообщений средствами SIP
8. UPDATE — модификация состояния сессии без изменения состояния диалога)

Ответы на запросы сообщают о результате обработки запроса либо передают запрошенную информацию. Структуру ответов и их виды протокол SIP унаследовал от протокола HTTP. Определено шесть типов ответов, несущих разную функциональную нагрузку. Тип ответа кодируется трёхзначным числом, самой важной является первая цифра, которая определяет класс ответа:

1. 1XX — показывают, что запрос находится в стадии обработки.
2. 2XX — запрос был успешно обработан.
3. 3XX — информация о новом местоположении вызываемого пользователя.
4. 4XX — информация об ошибке при обработке или выполнении запроса.
5. 5XX — запрос не может быть обработан из-за отказа сервера..
6. 6XX — соединение с вызываемым пользователем установить невозможно.

Главными недостатками протокола SIP являются трудности с обеспечением секретности (в условиях кибервойны) и обслуживанием приоритетных вызовов, что важно для военных применений, для экстренной службы. Поэтому по заказу МО США разработали защищенный протокол AS-SIP [5]. Протокол AS-SIP получился очень громоздким. Если обыкновенный SIP использует 11 других стандартов RFC, то AS-SIP требует учета почти 200 стандартов RFC.

Поясним правила установления приоритетных вызовов по протоколу AS-SIP. Приоритетные вызовы приводят к прерыванию ведущихся сеансов связи. При поступлении вызова более высокого приоритета, чем любой из двух существующих вызовов, вызов более низкого приоритета вытесняется. Прерванный вызов переводится в состояние ожидания, и сооединение восстанавливается после завершения приоритетного вызова.

Переход от сети коммутации каналов, где господствует протокол SS7 (рис. 5), к коммутации пакетов и протоколу SIP (к AS-SIP) требует установки

шлюзов - программных коммутаторор SoftSwitch (рис. 7). SoftSwitch имеет две важные функции: управляет согласованием протоколов сигнализации SIP и SS7 (посредством шлюза SGW) и преобразованием IP пакетов в TDM посылки (посредством шлюза MGW). В МО США разработаны детальные методические материалы по внедрению AS-SIP [6]. Фрагмент работы будущей сети DSN показан на рис. 8. Сегодня еще трудно предсказать время, в течение которого сеть DSN окончательно перейдет на протокол AS-SIP.

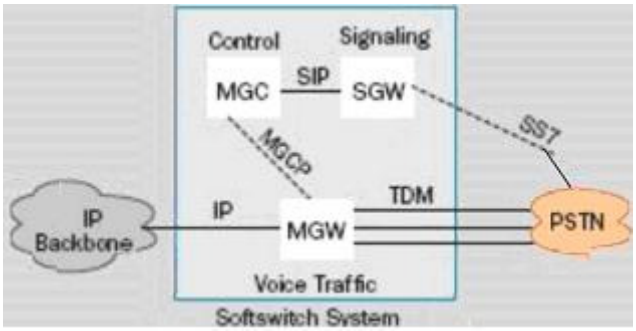



Рис. 7. Схема взаимодействия сети коммутации пакетов с традиционной сетью коммутации каналов посредством шлюза SoftSwitch

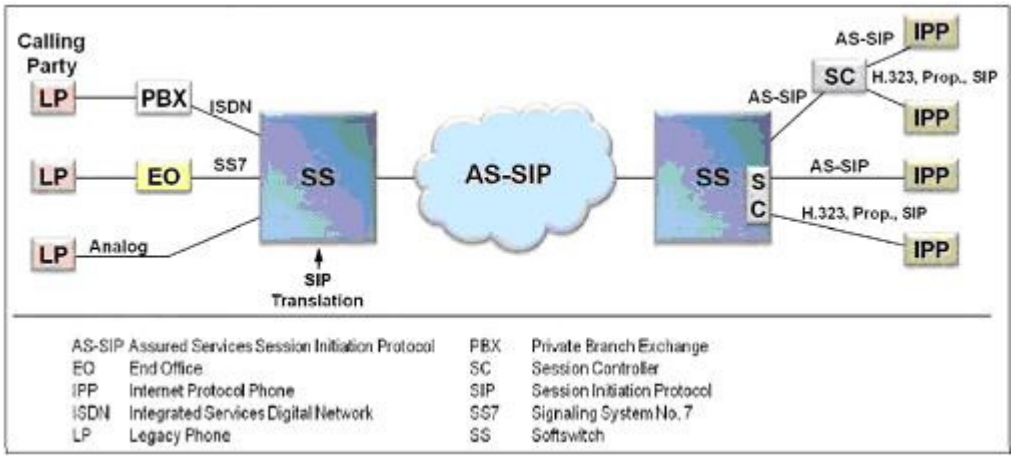



Рис. 8. Установление TDM вызова с IP абонентом через базовую сеть AS-SIP [6]

## IV Уязвимость SS7 на фиксированной сети

Изначально протокол SS7 был разработан для фиксированных сетей, закрытых по своей природе, поэтому в SS7 предусмотрены лишь ограниченные процедуры аутентификации. Следовательно, любой способен генерировать сообщения SS7 и внедриться в работу сети. Хакеры пользуются уязвимыми местами SS7 сообщения (рис. 9).

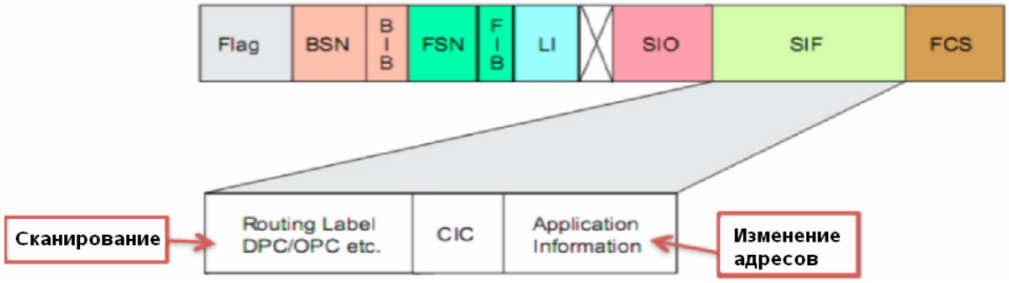



Рис. 9. Уязвимые места SS7 сообщения.

Рисунок 10 (из статьи [7]) определяет три потенциальных точки входа для хакерских атак. Пользуясь ISDN аппаратом можно ввести сообщение в сеть SS7 (атака 1). Конвергенция телефонных сетей и Интернета дает новые точки входа в сеть (атака 2). В качестве третьего входа для атаки указан соседний оператор связи.

Сами же атаки направлены на изменения маршрутизации в STP и для доступа к базам данных, что подсказываетмеры борьбы со злоумышленниками:

- Установить экраны (SS7 Firewall) у выходов из SSP и проводить аутентификацию сообщений,
- Установить перехватчики пакетов (SS7 packet sniffers), которые следят за всеми каналами сети SS7,
- Контролировать доступ к контроллерам SCP. На каждом SCP устанавить анализатор мошенничество (fraud analyser). Анализатор изучает все SCP запросы (TCAP сообщения). Например, анализирует последовательности TCAP сообщений, которые стремятся изменить телефонные номера в базе данных переадресации.

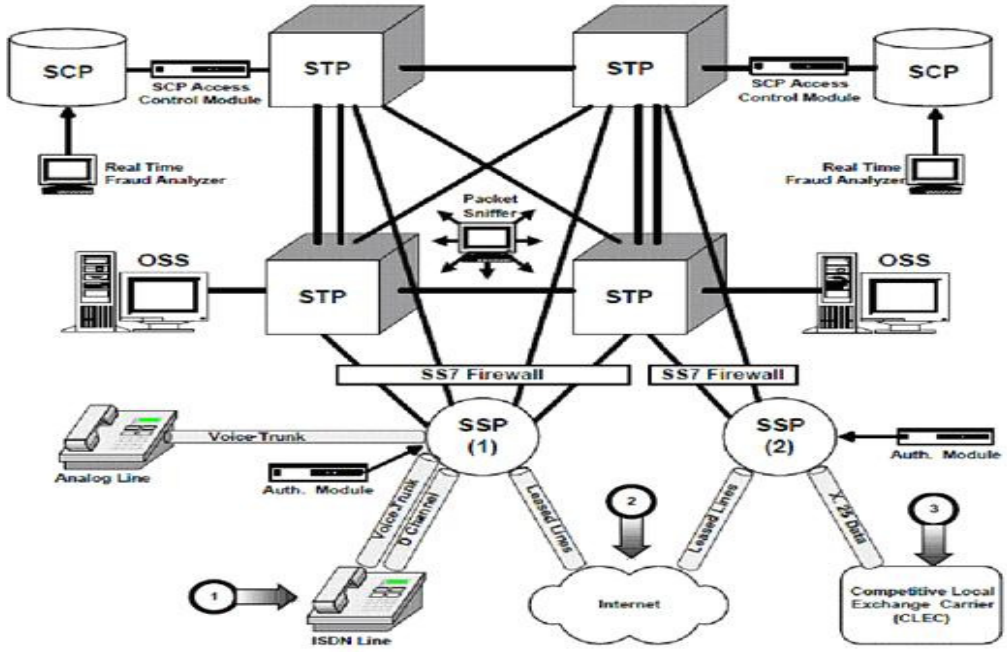



Рис. 10. Сеть SS7: уязвимые точки и средства борьбы с хакерскими атаками [7].

## V Уязвимость SS7 на мобильной сети

В сетях мобильной связи возможны различные хакерские атаки (см. ниже рис. 13). Рассмотрим подробно одну из них — раскрытие местоположения абонента с точностью до определения соты [8]. Размер соты не является величиной постоянной. В плотных городских застройках сота может обеспечивать покрытие порядка сотен метров, а в условиях междугородной трассы — нескольких километров.

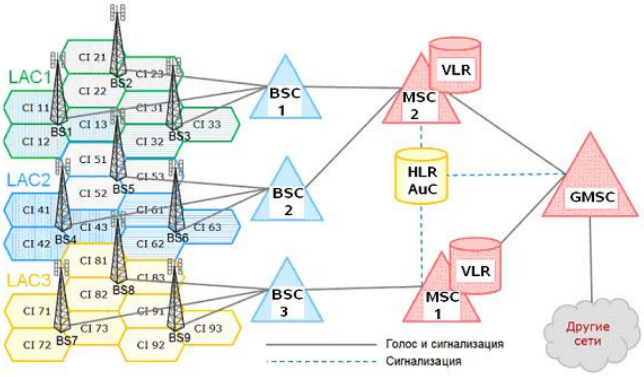



Рис. 11. Схема мобильной сети GSM

Покрытие обеспечивается базовыми станциями (Base Station, BS), каждая из которых, как правило, имеет несколько антенн, направленных в разные стороны (рис. 11). Антенна обеспечивает радиопокрытие соты, каждая сота имеет свой идентификатор (Cell Identity, CI). Базовые станции группируются в географические зоны. Идентификатор такой группы называется LAC (Location Area Code). Базовые станции подсоединяются к контроллеру базовых станций (Base Station Controller, BSC). Все контроллеры BSC подключаются к коммутатору (Mobile Switching Center, MSC). По сути, MSC представляет собой обычный коммутатор голосовых телефонных вызовов.

Регистр местоположения визитных абонентов (Visited Location Register, VLR) функционально считается отдельным элементом сети, но фактически всегда интегрирован с MSC. В базе данных VLR содержится информация об абонентах, которые в данный момент находятся в зоне действия данного MSC. Так как речь идет о местоположении абонента, то стоит упомянуть, что для каждого абонента в БД VLR хранится информация о текущем идентификаторе LAC, и идентификаторе той соты (CI), которая была при последнем радиоконтакте мобильного телефона с сетью. То есть, если абонент передвигается по территории покрытия одного LAC, не совершая и не принимая вызовов, в базе данных VLR информация о его местоположении не меняется.

Еще два функциональных узла — регистр местоположения домашних абонентов (Home Location Register, HLR) и центр аутентификации (Authentication Center, AuC) — размещаются физически в едином модуле. HLR/AuC хранит профили абонентов своей сети. В профиле содержится следующая информация:

- телефонный номер абонента,
- уникальный идентификатор SIM-карты (International Mobile Subscriber Identity, IMSI),
- ключи для обеспечения безопасности, категория абонента (предоплатная система расчетов /постоплатная система расчетов),
- список разрешенных и запрещенных услуг,
- адрес биллинг-центра (для абонентов предоплатной системы),
- адрес MSC/VLR, в зоне действия которого находится абонент в настоящий момент.

Этот же профиль с некоторыми изменениями копируется в VLR, когда абонент регистрируется в зоне его действия.

Шлюзовой коммутатор (Gateway MSC, GMSC)

является приемной точкой для входящих вызовов. Он на основе информации, полученной из HLR, маршрутизирует вызов на тот коммутатор, в зоне действия которого находится вызываемый абонент. В процессе установления вызова, отправки SMS и прочих транзакций, узлы связи обмениваются между собой сигнальными сообщениями по протоколу SS7. И работа хакера основана на знании деталей протокола SS7 и сети GSM.

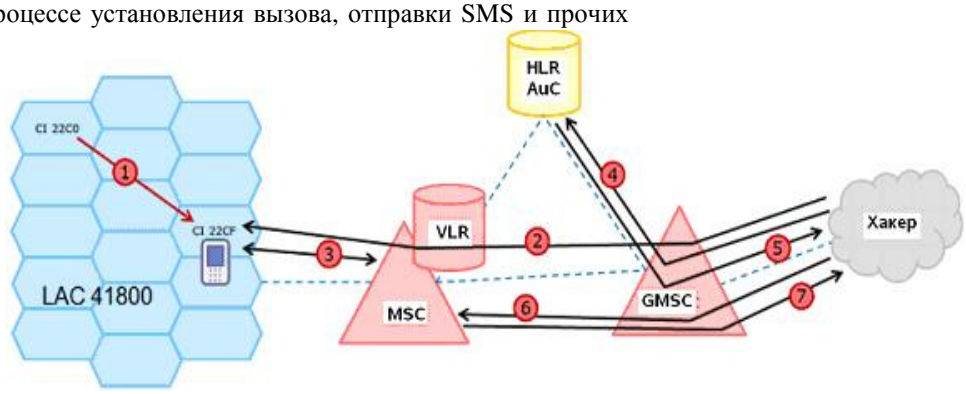



Рис. 12. Алгоритм раскрытия местоположения абонента [8].

Процесс раскрытия местоположения абонента можно проследить по стрелкам на рис. 12:

1. Мобильный телефон искомого абонента зарегистрирован в сети мобильного оператора. В какой-то момент абонент входит в зону покрытия LAC 41800 со стороны сектора CI 22C0 и продолжает движение вплоть до сектора CI 22CF. Когда телефон оказывается в зоне покрытия LAC 41800, то инициируется процедура *Location Update*, обновляя в базе данных VLR значения LAC и CI. По мере движения абонента до сектора CI 22CF в базе данных VLR не происходит более никаких изменений.
2. Чтобы узнать местоположение абонента, формируем SMS сообщение с атрибутом Type-0 и отправляем на его номер.
3. У SMS сообщения Type-0 есть другое название — SMS-пинг. Это сообщение не отображается на экране мобильного телефона и не сохраняется в списке принятых SMS. Оно производит обновление атрибутов местоположения в базе данных VLR. Теперь в VLR хранится актуальное значение сектора, в котором находится абонент, то есть CI 22CF.
4. Чтобы выудить данные, формируем сигнальное сообщение *sendRoutingInfoForSM*, где в качестве параметра указывается мобильный номер абонента, и отправляем это сообщение на HLR оператора.
5. HLR находит в своих базах данных идентификатор IMSI абонента и адрес MSC/VLR, в зоне действия которого находится абонент с заданным номером, и в ответе сообщает эти данные.
6. Теперь мы формируем сообщение *provideSubscriberInfo*, где в качестве параметра задаем идентификатор IMSI, и отправляем это сообщение на адрес мобильного коммутатора. Все нужные параметры (IMSI и адрес MSC/VLR) мы получили на предыдущем шаге.
7. Коммутатор воспринимает сообщение как вполне легальное и сообщает в ответ идентификаторы сети MCC/MNC, значение LAC и недавно обновленное значение сектора CI.

Итак, все значения, нужные для пеленгации, получены:

- MCC — код страны;
- MNC (Mobile Network Code) — код мобильного оператора;
- LAC;
- CGI (Cell Global Identity) — код соты.

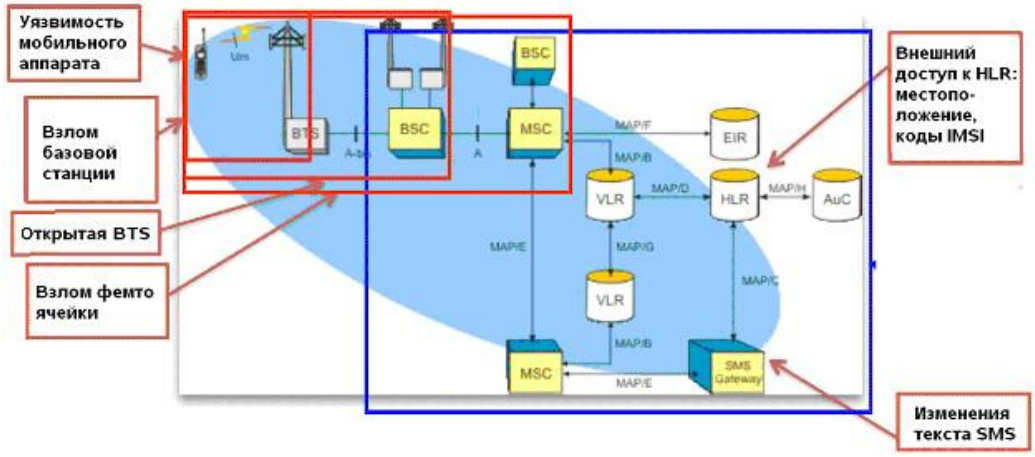



Рис. 13. На мобильной сети имеется множество уязвимых мест [9].

## VI Уязвимость протокола SIGTRAN

Для конвергенции сетей ТфОП и IP был разработан протокол SIGTRAN (Signaling Transport), позволяющий передавать сигнальные сообщения SS7 поверх IP. Он разделяется на транспортный протокол SCTP и уровни адаптации (рис. 14). В нашем примере из статьи [10] указан протокол адаптации M3UA (MTP3 User Peer-to-Peer Adaptation). Протокол SCTP занимает место TCP и расположен в стеке протоколов над IP, он используется другими уровнями адаптации для передачи сообщений SS7. SCTP обеспечивает надежную доставку пакетов при искажениях в сети. M3UA реализует передачу сигнальных сообщений SS7, поддерживает соединения SCTP для передачи трафика между SG и одним или более MGC.

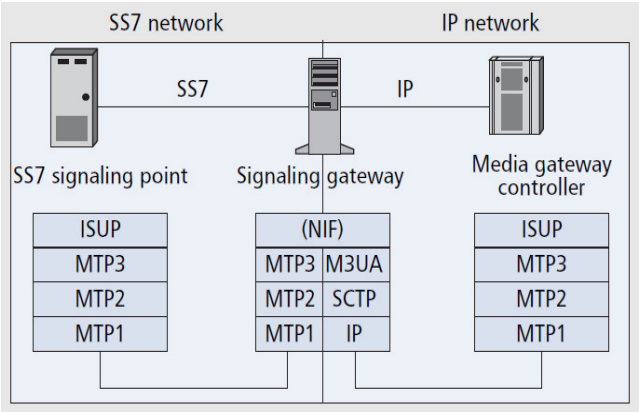



Рис. 14. Транспорт сообщений SS7 через IP сеть с использованием протокола M3UA

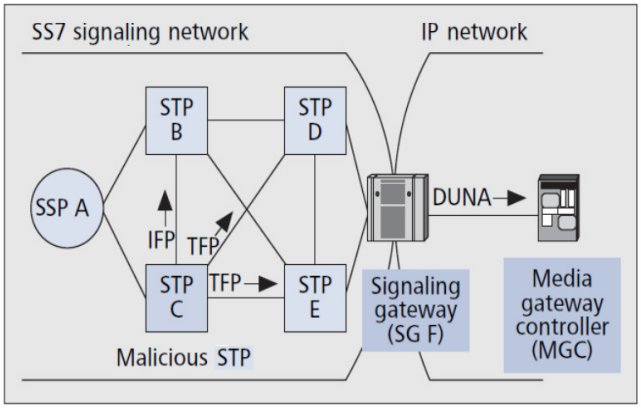



Рис. 15. Атака на сеть посредством сообщения DUNA [10].

В статье [10] указаны многие слабые места протокола SIGTRAN и рассмотрены средства борьбы с ними. Мы приведем один пример – атаку сети с использованием сообщения DUNA (destination unavailable).

Предположим, что хакер захватывает доступ к узлу STP или подключает к сети SS7 собственный STP (malicious STP). Тем самым хакер получает доступ к управлению сетью. Сообщения DUNA отправляются от SG ко всем MGCs и сигнализируют о недостижимости некоторых направлений в сети SS7. Если MTP3-пользователь не может найти альтернативный маршрут через другой SG, то обслуживание вызовов блокируется. На рис. 15 шлюз SG-F имеет связи с STP-D и STP-E. Сигнальный трафик от MGC к коммутатору SSP-A может быть направлен через STP-D или STP-E в зависимости от алгоритма распределения нагрузки.

Теперь предположим, что хакер захватил доступ к STP-C и посылает сообщение TFP (transfer prohibited) к своим соседям STP-B, STP-D и STP-E о недоступности коммутатора SSP-A. Если STP-C находится в легальном списке контроля доступа, то он тем самым инициирует внесение изменений в таблицах маршрутизации вызовов соседних STP. В итоге шлюз SG-F рассылает по IP сети сообщения о недоступности коммутатора SSP-A. Таким образом хакер, рассылая сообщения DUNA, изолирует часть телефонной сети и/или перегружает другие маршруты.

## VII Заключительные слова: уроки для Ростелекома

ОАО «Ростелеком» объявило курс на импортозамещение. Если действительно идти на строительство сетей связи собственными силами, то, на наш взгляд, следует вернуться к тому состоянию знаний, которые были достигнуты ранее – лет 20 назад и развивать их далее. В данном случае такой точкой отсчета условно можно назвать систему сигнализации SS7.

С этой целью мы рассмотрели международный опыт обеспечения надежной работы протокола SS7 на фиксированной и мобильной сети, особое внимание обращая на построение сети DSN MO США, где поныне господствует протокол SS7.

Ранее мы рассматривали задачи Ростелекома в свете эволюции телекоммуникационных сервисов при переходе к пакетной коммутации и протоколу AS-SIP на сети DSN MO США [11]. Эти новые сервисы являются залогом роста доходов оператора и могут внедряться постепенно при господстве протокола SS7 [12].

## Библиография

[1] http://servernews.ru/597356 Retrieved: Mar, 2015.
[2] FCC. Technology Transitions, Order, Report & Order and Further Notice of Proposed Rulemaking, Report Order, Order and Further Notice of Proposed Rulemaking, Proposal for Ongoing Data Initiative, GN Docket No. 13-5, FCC 14-5 (rel. Jan. 31, 2014).
[3] http://www.phworld.org/history/attcrash.htm Retrieved: Mar, 2015.
[4] http://jitc.fhu.disa.mil/tssi/cert_pdfs/tekeleceagle_tn1030701.pdf/ Retrieved: Mar, 2015.
[5] Department of Defense Assured Services (AS) Session Initiation Protocol (SIP) 2013 (AS-SIP 2013) Errata-1, July 2013.
[6] Department of Defense. Unified Capabilities Framework 2013. January 2013.
[7] G. Lorenz, T. Moore, G. Manes, J. Hale, S. Shenoi. Securing SS7 Telecommunications Networks// Proceedings of the 2001 IEEE. Workshop on Information Assurance and Security W2A3 1115 United States Military Academy, West Point, NY, 5-6 June 2001, 273-278.
[8] Блог компании Positive Technologies, информационная безопасность. 26 августа 2013. http://habrahabr.ru/company/pt/blog/191384/ Retrieved: Mar, 2015.
[9] www.hachitsergosum.org/2010/HES2010-planglois-Attacking-SS7.pdf/ Retrieved: Mar, 2015.
[10] H. Sengar, R. Dantu, D. Wijesekera, S. Jajodia. SS7 Over IP:Signaling Interworking Vulnerabilities// IEEE Network, November/December, 2006, 32-41.

[11] Шнепс-Шнеппе М. А., Намиот Д. Е. Об эволюции телекоммуникационных сервисов на примере GIG //International Journal of Open Information Technologies. – 2015. – Т. 3. – №. 1. – С. 1-13.

[12] Шнепс-Шнеппе М. А., Намиот Д. Е., Сухомлин В. А. О создании единого информационного пространства общества //International Journal of Open Information Technologies. – 2015. – Т. 3. – №. 2. – С. 1-10.

# SS7 signaling system and its vulnerability

Manfred Sneps-Sneppe

*Abstract*—**In the context of the policy of import substitution in communication systems has become actual modernization of traditional circuit-switched networks, where the most valuable innovation is the signaling system SS7. The article covers the basics of SS7 signaling and its vulnerability to the fixed and mobile networks as well as SIGTRAN protocol vulnerability.**

*Keywords* —**SS7 signaling system; SIP; AS-SIP; SS7 vulnerability; SIGTRAN vulnerability.**