УДК 621.391

А.С. Корсунский

АНАЛИЗ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ АБОНЕНТСКИХ ТЕРМИНАЛОВ В СЕТЯХ ПОДВИЖНОЙ РАДИОСВЯЗИ

Корсунский Андрей Сергеевич, *кандидат технических наук, окончил факультет радиосвязи Ульяновского филиала Военного университета связи, адъюнктуру Военной академии связи им. С.М. Буденного. Ведущий инженер-программист ФНПЦ ОАО «НПО «Марс». Имеет статьи и изобретения в области радиоэлектронной защиты, безопасности связи и информации. [e-mail: aksspb@mail.ru].*

Аннотация

Исследуются вопросы обеспечения подлинности и доступности информации и услуг в существующих и перспективных сетях подвижной радиосвязи (СПРС). Показано, что в перспективных технологиях имеются существенные уязвимости к атакам на доступность информации и информационных ресурсов.

Ключевые слова: аутентификация, безопасность информации, сети подвижной радиосвязи.

Abstract

The actual article presents studies in ensuring authenticity and availability of data and services in existing and future-proof mobile radio networks. It also shows that some ad-vanced technologies are considerably vulnerable in case of information attack from the point of view of information and information resource availability.

Key words: authentication, information security, mobile radio networks.

Введение

Развитие современных телекоммуникационных технологий значительно повысило доступность услуг связи для пользователей различных систем, дало возможность существенно повысить качество и удобство пользования информационными услугами, а также обеспечило достоверность связи. Однако их непосредственное внедрение в ряд СПРС приводит к усилению опасности ранее существовавших и появлению новых атак нарушителей информационной безопасности на подлинность и доступность информации и услуг. Активное внедрение в СПРС новых технологий заставляет по-новому взглянуть на проблему обеспечения безопасности информации, в частности на обеспечение подлинности корреспондентов и передаваемой от них мультимедийной информации [1].

Методы обеспечения подлинности информации в СПРС

Исследуем принципы построения, достоинства и недостатки существующих и перспективных технологий обеспечения подлинности и доступности информации в сетях сотовой и транкинговой связи.

Рассмотрим протокол аутентификации корреспондентов в сетях сотовой связи *GSM* и транкинговой связи *TETRA*. Анализ работ [2–4] дает возможность заключить, что обеспечение безопасности связи в стандартах *GSM* и *TETRA* базируется на одинаковых принципах. Для достижения требуемого уровня безопасности связи в данных СПРС с помощью соответствующих механизмов решаются задачи обеспечения аутентификации объектов, конфиденциальности информации и скрытности перемещения абонента. Механизмы обеспечения безопасности связи и информации в данных СПРС реализуются с помощью соответствующих алгоритмов: аутентификации (в *GSM* – A3), шифрования/расшифрования сообщений (в *GSM* – A5), формирования ключа шифрования (в *GSM* – A8). В стандарте *TETRA* данные криптоалгоритмы объединены общим названием TA12.

На рисунке 1 показаны протокол аутентификации корреспондентов и шифрование информации в СПРС на основе стандартов GSM и TETRA.

В процедуре установления связи в данных СПРС можно выделить три этапа: регистрация (предварительный этап), этап аутентификации объектов и формирования сеансового ключа шифрования, а также этап установления сеанса шифрованной связи.

В *SIM*-карте (*Subscriber Identity Module* – модуль идентификации абонента) каждого АТ записаны индивидуальный ключ K_i и международный

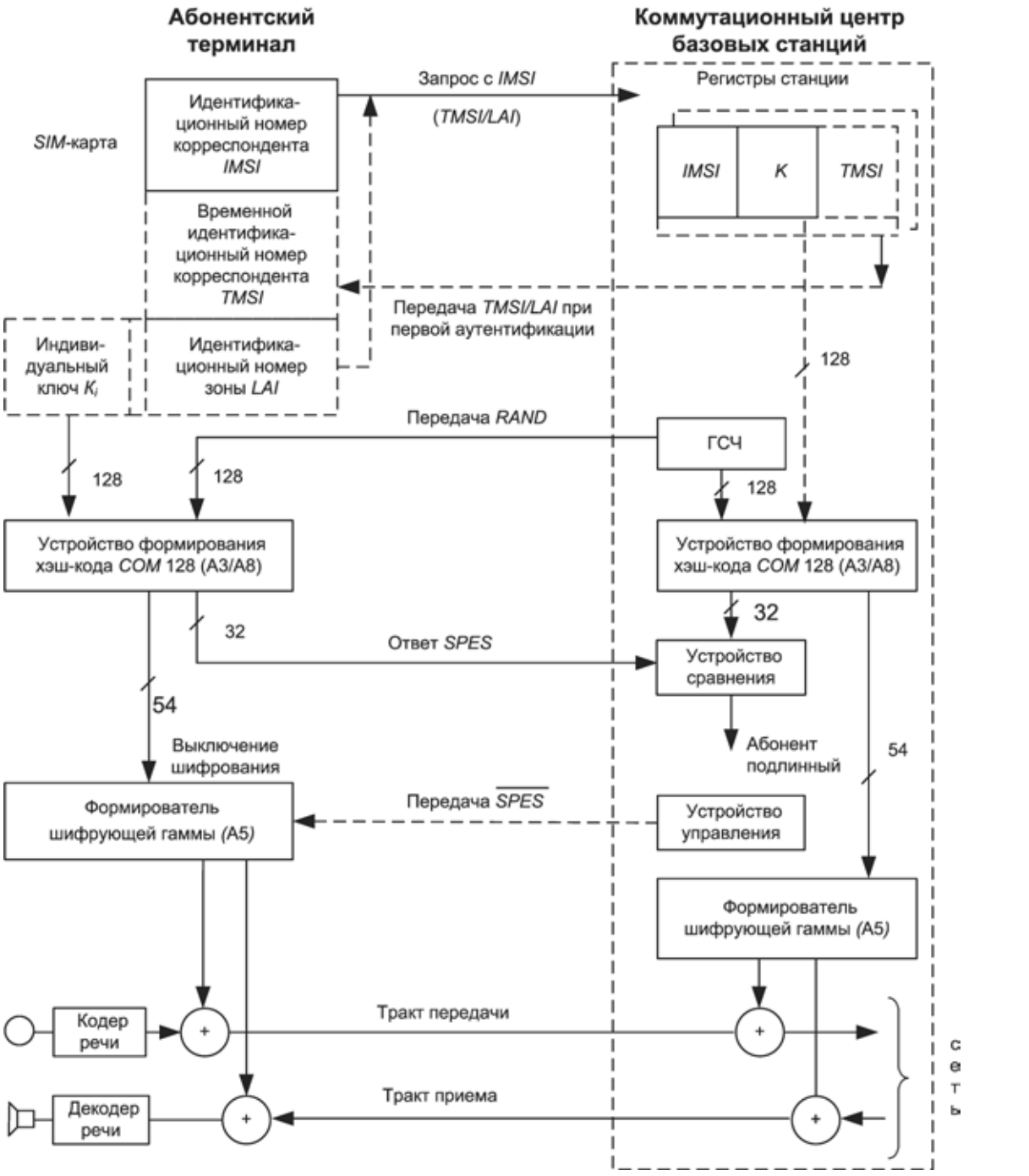

Рис. 1. Протокол аутентификации корреспондентов и шифрование информации в СПРС на основе стандартов GSM и TETRA

идентификационный номер *IMSI* (*International Mobile station Subscriber Identity*). При подключении к сети связи АТ передает ближайшей базовой станции (БС) свой *IMSI*. Коммутационный центр базовой станции в результате его регистрации назначает ему временный идентификационный номер *TMSI* (*Time Mobile station Subscriber Identity*) и идентификационный номер зоны *LAI* (*Location Area Identification*). БС при каждом запросе на установление соединения с помощью генератора случайных чисел генерирует случайное число *RAND* (*Random number*) длиной 128 бит и передает его АТ. Из этого случайного числа с использованием секретного ключа K_i АТ и БС независимо друг от друга в устройствах формирования хэш-кода *COM*128 (алгоритм A3/A8) вычисляют хэш-код длиной 32 бита. АТ передает его в виде сигнала «Ответ *SRES* (*Signed response*)», БС при совпадении принятого от АТ и сформированного на БС хэш-кодов убеждается в подлинности АТ и устанавливает сеанс связи. В устройствах формирования хэш-кода также формируется сеансовый ключ шифрования длиной 54 бита, на основе которого в формирователях шифрующей гаммы в БС и АТ синхронно формируются одинаковые шифргаммы, которые зашифровывают и расшифровывают передаваемую между ними

информацию. При установлении соединения БС может дистанционно выключить шифратор АТ передачей инвертированного сигнала $\overline{SRES}$.

Необходимо отметить, что в СПРС, построенных с применением стандартов транкинговой связи, особые проблемы вызывает обеспечение подлинности при установлении прямой связи (режим *DMO — Direct Mode Operation*). В этом режиме БС непосредственно не участвует в контроле подлинности сторон. Взаимодействующие корреспонденты при вхождении в сеанс связи выполняют криптопротокол взаимной аутентификации типа «рукопожатие» или протокол на основе электронных цифровых подписей (ЭЦП) этих корреспондентов. В первом случае протокол выполняется за несколько шагов, что увеличивает время вхождения в связь. Во втором случае число шагов выполнения протокола может быть уменьшено, но для этого требуется безошибочно передавать заверяющие параметры устанавливаемого соединения и подписи значительного размера, что вызывает определенные затруднения в реальных радиоканалах.

Рассмотрим протокол аутентификации абонентского терминала в СПРС с кодовым разделением каналов согласно стандарту *IS-95*, представленный на рисунке 2.

В АТ записан ключ аутентификации *A-key*.

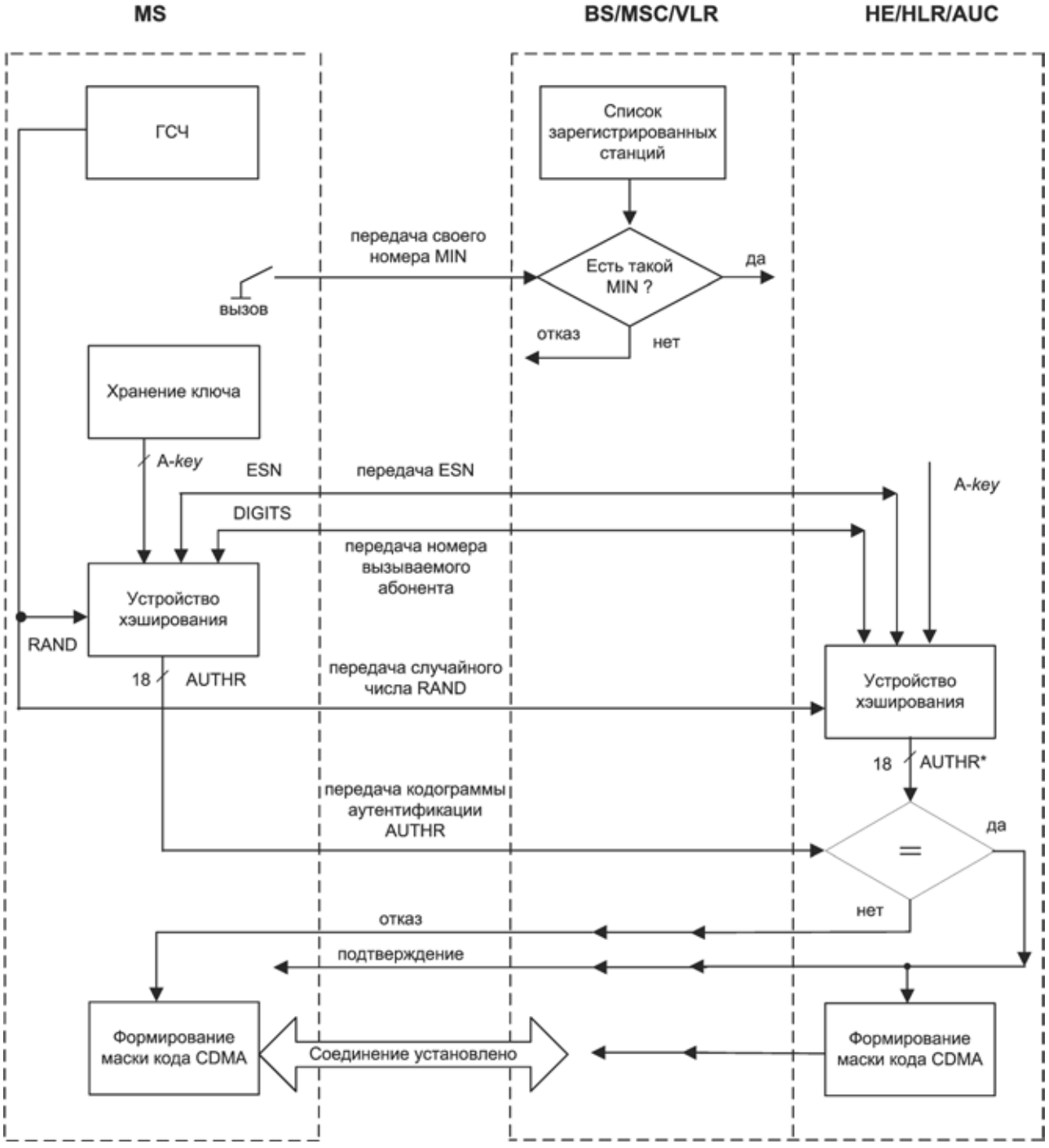

Рис. 2. Протокол аутентификации АТ в СПРС согласно стандарту IS-95

При исходящем вызове АТ передает на БС начальное сообщение, которое содержит электронный порядковый номер АТ — *ESN* (*Electronic Serial Number*), идентификатор мобильной сети — *MIN* (*Mobile Identity Network*) и набранные знаки номера вызываемого абонента (*DIGITS*). БС запрашивает в гостевом регистре местоположения АТ *VLR* (*Visited Location Register*) подтверждение наличия *MIN* в списке зарегистрированных станций. При получении подтверждения в центре аутентификации абонентов *AuC* (*Authentication Centre*) устройство хэширования с применением параметров *A-key*, *ESN*, *DIGITS* и значения случайного числа *RAND*, принятого от АТ, вычисляет кодограмму аутентификации *AUTHR**, которая сравнивается с кодограммой аутентификации *AUTHR* независимо от БС вычисленной АТ и переданной на БС. При совпадении этих значений подлинность АТ подтверждается. Однако недостаточная длина ключа аутентификации (64 бита) и длина кодограммы аутентификации корреспондентов (18 бит) потенциально допускают вероятность имитонавязывания ложного корреспондента порядка 10^{-5} [2].

Итак, механизмы безопасности, реализованные в СПРС, построенных на основе технологий второго поколения, таких как *GSM* и *IS-95*, обладают рядом существенных недостатков:

— односторонняя аутентификация абонентского терминала;

— шифрование передаваемой информации только в радиоинтерфейсе;

— отсутствие имитозащиты передаваемых сообщений;

— недостаточная криптографическая стойкость используемых алгоритмов шифрования и протоколов аутентификации;

— недостаточная длина ключа аутентификации;

— низкая защищенность ключа в оборудовании абонента и сети.

В последующих поколениях технологий подвижной радиосвязи эти недостатки частично устраняются. В СПРС стандарта *CDMA2000* в соответствии с протоколом безопасности *IS-41C* реализуется взаимная аутентификация АТ и БС, ключи шифрования и ключи аутентификации формируются и используются независимо друг от друга, появляется возможность дистанционной смены ключа в АТ, ведется контроль числа вызовов от каждого АТ, увеличивается длина ключа и длина случайного числа, меняемого при каждом вызове и вхождении в связь.

В СПРС *UMTS* (*WCDMA*), кроме того, предусмотрена имитозащита передаваемых пакетов данных, а также в каждом пакете передается его порядковый номер. Длины ключей шифрования и аутентификации возрастают до 128 бит, планируется использовать стойкие алгоритмы шифрования типа *Kasumi* и *AES*, протокол аутентификации и согласования ключей *AKA*, включающий:

— контроль *USIM*-картой (*an Upgrade SIM*) подлинности обслуживающей сети *SN*;

— обеспечение контроля подлинности как пользователя со стороны обслуживающей сети, так и подлинности обслуживающей сети со стороны оборудования пользователя;

— использование последовательных номеров для защиты от повторного использования нарушителями векторов аутентификации;

— выбор для каждого пользователя используемых для обеспечения его безопасности алгоритмов аутентификации, времени действия ключа и т.д.;

— раздельное формирование сеансовых ключа шифрования СК и ключа имитозащиты IK, используемых для защиты конфиденциальности и для контроля подлинности передаваемой информации соответственно.

Также, дополнительно к ранее известным методам обеспечения безопасности в СПРС *UMTS* (*WCDMA*) планируется обеспечить следующее [5, 6]:

— контроль использования ключей шифрования и ключей имитозащиты со стороны пользователя: *USIM*-карта контролирует количество устанавливаемых защищенных соединений с использованием текущей пары ключей и при превышении допустимой нагрузки на ключ инициирует новую процедуру аутентификации при очередном соединении;

— контроль времени использования ключей шифрования и ключей имитозащиты со стороны обслуживающей сети: обслуживающая сеть SN следит за регулярностью смены ключей;

— идентификация и реагирование на неуспешные попытки взаимной аутентификации: информация об этом факте передается оборудованию домашней сети *HLR/AuC* для выявления возможных атак нарушителей под видом законной обслуживающей сети;

— обеспечение конфиденциальности и аутентичности передаваемой информации между БС и контроллером радиосети *RNC* (*Radio Network Control*) с использованием ключей длиной 128 бит, что вполне достаточно для существующих и перспективных приложений;

— открытость и всесторонний анализ используемых алгоритмов шифрования и имитозащиты информации, а также протоколов аутентификации пользователей и сетевого оборудования.

Протокол аутентификации и согласования ключей AKA построен как протокол «запрос-ответ» с использованием симметричных криптографических алгоритмов. По сравнению с реализованным в *GSM* протоколом аутентификации он обладает следующими достоинствами:

— проверка подлинности обслуживающей сети *SN* и в неявном виде подлинности оборудования домашней сети *HE* со стороны пользователя;

– согласование ключа имитозащиты данных *IK* между пользователем и обслуживающей сетью;

– взаимная проверка новизны (неповторяемости) используемых между пользователем и обслуживающей сетью *SN* ключей шифрования и имитозащиты.

В *USIM*-карте пользователя и в центре аутентификации AuC его домашней сети записан конфиденциальный ключ K пользователя. В этих устройствах используются функции аутентификации сообщений $f1$ и $f2$, а также функции формирования ключей $f3$–$f5$. Рассмотрим выполнение протокола аутентификации и согласования ключей между пользователем и сетью *UMTS*, представленного на рисунке 3, который включает два основных этапа.

Этап формирования векторов аутентификации

АТ пользователя появляется в зоне обслуживания одной из БС обслуживающей сети *SN* и запрашивает обслуживание. Получив запрос от пользователя, обслуживающая сеть выдает заявку на аутентифицирующую информацию домашней сети этого пользователя. Получив такую заявку, центр аутентификации *AuC* домашней сети генерирует матрицу из n (обычно n = 5) векторов аутентификации AV_i, где $i = 1, 2, \ldots, n$, каждый из которых состоит из пяти частей: случайного неповторяющегося числа $RAND_i$, ожидаемого значения ответа пользователя $XRES_i$, сеансового ключа шифрования CK_i, сеансового ключа имитозащиты IK_i и токена аутентификации $AUTN_i$. Эта матрица пересылается сети *SN*.

Этап аутентификации и согласования ключей

В выполнении протокола аутентификации участвует гостевой регистр *VLR* сети *SN*. Из полученной матрицы выбирается очередной i-й ($1 \le i \le n$) вектор аутентификации, и из этого вектора БС передает АТ пользователя значения $RAND_i$ и $AUTN_i$. Получив эти значения, *USIM*-карта пользователя с использованием записанного в ней ключа K проверяет корректность принятого токена аутентификации, т.е. оборудование пользователя устанавливает, подлинна ли обслуживающая сеть. При положительном решении *USIM*-карта вычисляет и передает БС обслуживающей сети ответ RES_i, который последняя сличает с имеющимся у нее значением ожидаемого ответа $XRES_i$. При совпадении этих значений подлинность пользователя подтверждается. После отправки ответа RES_i *USIM*-карта вычисляет для устанавливаемого сеанса связи сеансовые ключ шифрования CK_i и ключ имитозащиты IK_i, которые будут использоваться для криптографической защиты информации, передаваемой по радиоканалу между оборудованием пользователя и БС обслуживающей сети *SN*.

Рассмотрим более подробно протокол *AKA*. Получив запрос от обслуживающей сети *SN* на аутентифицирующую информацию, центр аутентификации *AuC* вычисляет очередной номер SQN_i и генерирует новое случайное число $RAND_i$. Для каждого пользователя оборудование домашней сети *HE* хранит в памяти последнее значение ранее использованных номеров SQN_{HE}. Значение нового номера SQN_i длиной 48 бит всегда больше ранее использованных номеров, что потенциально позволяет выявлять атаки нарушителей с повтором ранее использованной аутентифицирующей информации. Затем на основе ключа пользователя K центр аутентификации формирует следующие значения:

1) код аутентификации
$MAC_i = f1_K(SQN_i||RAND_i||_{AFM})$;
2) ожидаемое значение ответа пользователя
$XRES_i = f2_K(RAND_i)$;
3) сеансовый ключ шифрования
$CK_i = f3_K(RAND_i)$;
4) сеансовый ключ имитозащиты
$IK_i = f4_K(RAND_i)$;
5) сеансовый ключ анонимности
$AK_i = f5_K(RAND_i)$.

Из вычисленных значений собирается i-й токен аутентификации

$$AUTN_i = (SQN_i \oplus AK_i)||AMF||MAC_i,$$

состоящий из трех частей, и i-й вектор аутентификации $AV_i = RAND_i||XRES_i||CK_i||IK_i||AUTN_i$, состоящий из пяти частей, где $..\|..$ есть операции конкатенации.

Передача пользователю токена $AUTN_i$ и случайного числа $RAND_i$ позволяет при реализации протокола аутентификации взаимно проверить подлинность взаимодействующих сторон, то есть АТ и БС, и исключить возможность атаки «вторжение ложной БС в середину». Обслуживающая сеть SN использует вектора аутентификации в порядке их номеров.

Получив токен $AUTN_i$ и случайное число $RAND_i$, *USIM*-карта оборудования пользователя выполняет следующие действия. Сначала при обеспечении анонимности из принятого случайного числа $RAND_i$ вычисляется сеансовый ключ анонимности $AK_i = f5_K(RAND_i)$ и снимается маска с принятого замаскированного номера $SQN_i = (SQN_i \oplus AK_i) \oplus AK_i$. Затем *USIM*-карта вычисляет код аутентификации $\widehat{MAC}_i$ и сравнивает вычисленное значение с принятым. При их несовпадении подлинность обслуживающей сети не подтверждается, и оборудованием пользователя передается сигнал «ошибка аутентификации». Получив этот сигнал, обслуживающая сеть

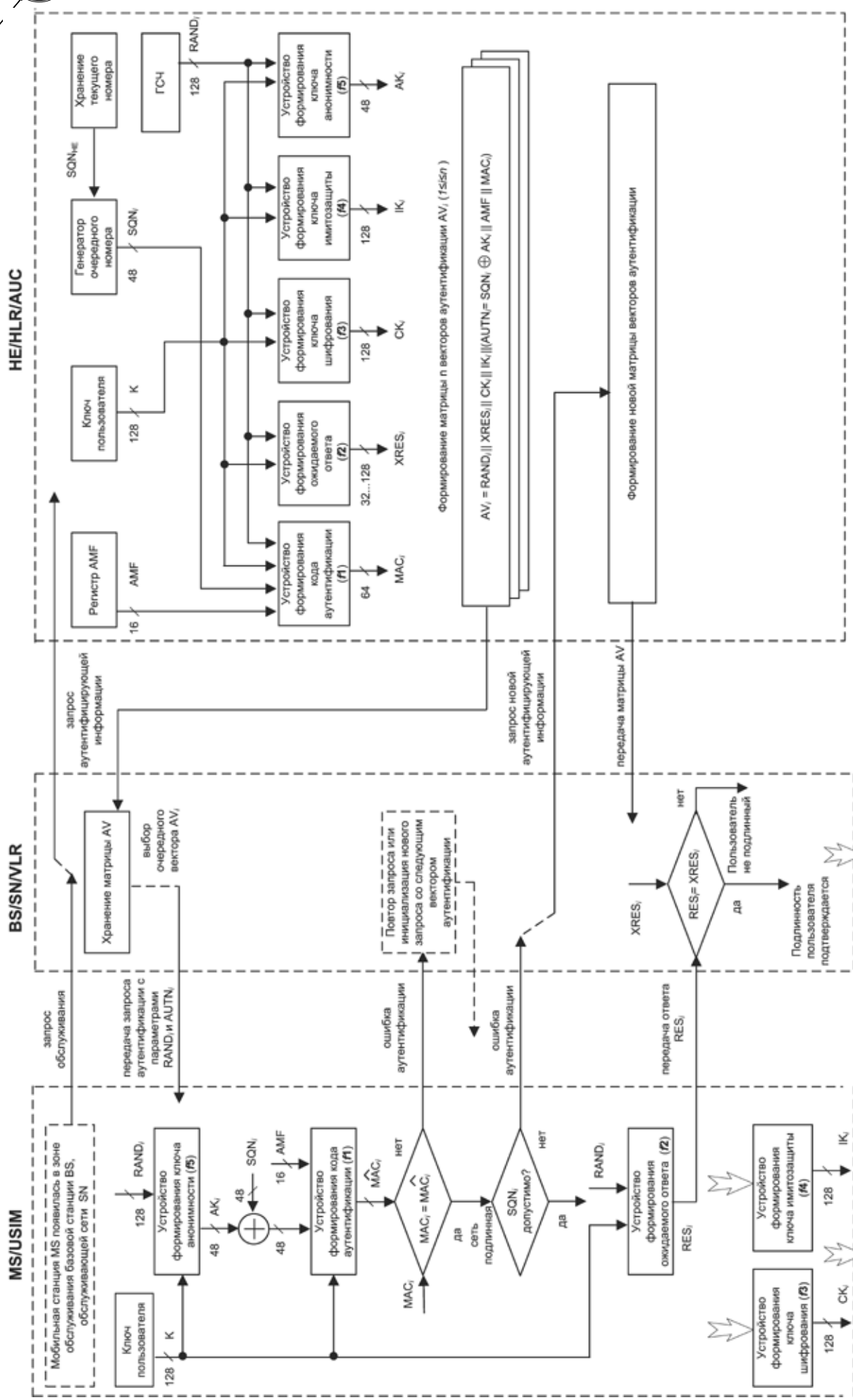

Рис. 3. Протокол аутентификации и согласования ключей между пользователем и сетью *UMTS*

может или повторить этот запрос аутентификации, или инициировать новый запрос со следующим вектором AV_{i+1} .

При выполнении равенства $\widehat{MAC}_i = MAC_i$ подлинность сети подтверждается, и далее *USIM*-карта проверяет, находится ли номер SQN_i в допустимом диапазоне значений, то есть нет ли признаков атаки «повтора». При невыполнении указанного равенства *USIM*-карта выдает сигнал «ошибка синхронизации» и отказывается от полученного вызова. Если принятый номер SQN_i допустим, то *USIM*-карта вычисляет значение $RES_i = f2_K(RAND_i)$ и передает его БС, которая сличает его с ожидаемым значением ответа пользователя $XRES_i$. При выполнении равенства $XRES_i = RES_i$ протокол взаимной аутентификации успешно завершен. Передав ответ аутентификации, оборудование пользователя вычисляет сеансовые ключ шифрования $CK_i = f3_K(RAND_i)$ и ключ имитозащиты $IK_i = f4_K(RAND_i)$.

Из проведенного анализа данного протокола аутентификации и согласования ключей следует, что использованные в нем проверки гарантируют корректность формирования одинаковых для *USIM*-карты и сети *SN* ключей шифрования и имитозащиты, причем практически исключается возможность для нарушителя навязать ранее использованную ключевую информацию.

Однако при реализации технологий подвижной радиосвязи, таких как *CDMA2000* и *UMTS* (*WCDMA*), с учетом специфики их функционирования механизмы безопасности таких сетей будут обладать следующими недостатками:

— слабая защищенность каналов доступа от атак «отказ в обслуживании» и распределенных атак «отказ в обслуживании» [7];

— низкая разведзащищенность вызовов корреспондентов сети;

— недостаточная помехоустойчивость передачи сигналов вызова.

Необходимо отметить, что защищенность от атак нарушителя СПРС, построенных с применением технологий беспроводного радиодоступа, таких как 802.11*i* (*Wi-Fi*), 802.16 (*Wi-Max*) и др., в целом оценивается ниже, чем у исследованных выше технологий сотовой и транкинговой связи [1]. В связи с этим в настоящее время интенсивно прорабатываются вопросы повышения безопасности технологий беспроводного доступа, что дает основание планировать их возможное применение в перспективных СПРС.

Таким образом, поскольку существующие способы решения задач обеспечения подлинности и доступности информации и услуг в существующих и перспективных технологиях сотовой и транкинговой связи обладают рядом указанных недостатков принципиального характера, то представляется целесообразным разработка специальных способов аутентификации корреспондентов и имитозащищенных способов доступа к услугам для СПРС.

СПИСОК ЛИТЕРАТУРЫ

1. Оков И.Н. Аутентификация речевых сообщений и изображений в каналах связи / под ред. В.Ф. Комаровича. — СПб.: Изд-во Политехн. ун-та, 2006.

2. Корсунский А.С. Анализ методов обеспечения подлинности и доступности информации и услуг в сетях подвижной радиосвязи // Научно-технические ведомости СПбГПУ. — 2008. — № 2. — С. 55—59.

3. Комарович В.Ф., Корсунский А.С. Подход к построению сигнальной аутентификации корреспондентов сетей связи с подвижными объектами специального назначения: материалы 5-й Всероссийской научной конференции, 8—9 февраля 2007 г. В 8-ми частях. Часть 4 /под общей редакцией профессора В. М. Щекотихина. — Орел: Академия ФСО России, 2007.

4. Волчков А.А., Ткачев Ю.А. Сравнительный анализ механизмов безопасности в стандартах GSM и TETRA // Мобильные системы. — 2006. — № 1. — С. 12—15.

5. Technical Specification Group Services and System Aspects. 3G Security: Cryptographic algorithm requirements. 3GPP TS 33.105 V5.3.0. France, 2003.

6. Technical Specification Group Services and System Aspects. Security Threats and Requirements. 3GPP TS 21.133 V 4.1.0. France, 2002.

7. Ulrike Meyer, Susanne Wetzel. A Man-in-the-Middle Attack on UMTS. WiSe04, October 1, 2004, Philadelphia, Pennsylvania, USA.