РАКЕТНО-КОСМИЧЕСКОЕ ПРИБОРОСТРОЕНИЕ И ИНФОРМАЦИОННЫЕ СИСТЕМЫ
2020, том 7, выпуск 1, с. 84–94

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ КОСМИЧЕСКИМИ АППАРАТАМИ, ОБРАБОТКА ИНФОРМАЦИИ И СИСТЕМЫ ТЕЛЕМЕТРИИ

УДК 621.391.7 DOI 10.30894/issn2409-0239.2020.7.1.84.94

Методы аутентификации и шифрования информации в сетях связи на основе динамично изменяющихся матриц ключей и матриц алгоритмов

И. Н. Пантелеймонов, *panteleymonov_in@spacecorp.ru*
АО «Российские космические системы», Москва, Российская Федерация

А. А. Монастыренко, *monastyrenko_aa@spacecorp.ru*
АО «Российские космические системы», Москва, Российская Федерация

А. В. Белозерцев, *belozertsev_av@spacecorp.ru*
АО «Российские космические системы», Москва, Российская Федерация

В. В. Боцва, *bakirovamsh@tsniimash.ru*
АО «ЦНИИ машиностроения», г. Королев, Российская Федерация

А.В. Наумкин, *alexander.naumkin@ks54.ru*
ГБПОУ «Колледж связи № 54» имени П. М. Вострухина, г. Москва, Российская Федерация

Аннотация. В сетях подвижной связи стандарта GSM на SIM-карте абонента хранятся постоянные ключ аутентификации и алгоритм аутентификации. Для аутентификации абонента используются постоянные ключ аутентификации, алгоритм аутентификации и алгоритм шифрования, которые задействуются для аутентификации абонента и шифрования передаваемой информации. В случае компрометации ключа аутентификации алгоритм аутентификации и алгоритм шифрования злоумышленника смогут входить в связь с базовой станцией под чужим идентификатором телефона IMSI (International Mobile Subscriber Identity). Представлена технология усиления криптостойкости алгоритмов аутентификации и шифрования информации, применяемых в сетях подвижной связи GSM, в основе которой вместо постоянных ключа аутентификации, алгоритма аутентификации и алгоритма шифрования лежит применение динамично изменяющихся матриц ключей и алгоритмов. Предлагаемое техническое решение может иметь широкое применение в системах радиосвязи, сетях подвижной связи и персональной подвижной спутниковой связи, а также позволит избирательно подходить к дополнительному усилению криптостойкости передаваемой информации для отдельных категорий абонентов. Положительным эффектом также является то, что повышение криптостойкости сети связи осуществляется без значительного увеличения вычислительной нагрузки на процессор абонентского терминала, что обеспечивает экономию заряда аккумуляторной батареи абонентского терминала.

Ключевые слова: ключ, алгоритм, аутентификация, шифрование, базовая станция, абонентский терминал

РАКЕТНО-КОСМИЧЕСКОЕ ПРИБОРОСТРОЕНИЕ И ИНФОРМАЦИОННЫЕ СИСТЕМЫ
2020, том 7, выпуск 1, с. 84–94

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ КОСМИЧЕСКИМИ АППАРАТАМИ, ОБРАБОТКА ИНФОРМАЦИИ И СИСТЕМЫ ТЕЛЕМЕТРИИ

Methods of Authentication and Encryption of Information in Communication Networks Based on Dynamically Changing Key Matrices and Matrix Algorithms

I. N. Panteleymonov, *panteleymonov_in@spacecorp.ru*
Joint Stock Company "Russian Space Systems", Moscow, Russian Federation
A. A. Monastyrenko, *monastyrenko_aa@spacecorp.ru*
Joint Stock Company "Russian Space Systems", Moscow, Russian Federation
A. V. Belozertsev, *belozertsev_av@spacecorp.ru*
Joint Stock Company "Russian Space Systems", Moscow, Russian Federation
V. V. Botsva, *bakirovamsh@tsniimash.ru*
JSC "Central Research Institute of Mechanical Engineering", Korolev, Russian Federation
A. V. Naumkin, *alexander.naumkin@ks54.ru*
"College of Communication No. 54" named after P.M. Vostrukhina, Moscow, Russian Federation

Abstract. In GSM mobile networks, a subscriber's SIM card stores a permanent authentication key and an authentication algorithm. For authentication of the subscriber is used a permanent authentication key, an authentication algorithm, as well as an encryption algorithm, that used to encrypt the transmitted information. If the authentication key is compromised, an attacker will be able to communicate with the base station using someone else's IMSI (International Mobile Subscriber Identity). The technology for enhancing the cryptographic strength of authentication algorithms and information encryption used in GSM mobile networks is presented, which, instead of using a permanent authentication key, authentication algorithm and encryption algorithm, is based on the use of dynamically changing key matrices and algorithms. The proposed technical solution can be widely used in radio communication systems, mobile networks, and personal mobile satellite communications. It will also make it possible to differentiate additional strengthening of the cryptographic stability of the transmitted information for certain categories of subscribers. An additional positive effect is that the increase in the cryptographic strength of the communication network is carried out without a significant increase in the computational load on the processor of the subscriber terminal, which saves the battery power of the subscriber terminal.

Keywords: key, algorithm, authentication, encryption, base station, subscriber terminal

Введение

По оценке аналитиков, уровень потерь операторов мобильной связи от разного рода мошенничества и вредительства составляет от 2–6 % до 25 % от общего объема трафика. Причем атаки мошенников направлены как против операторов, так и против абонентов [1]. Решение проблемы обеспечения безопасности в российских сетях связи осложняется широким использованием технических средств зарубежного производства, что создает возможность реализации не декларируемых поставщиками возможностей [1].

Для передачи информации цифровой телефонии и коротких сообщений (SMS) с использованием персональных абонентских терминалов наибольшее распространение получил стандарт GSM. В сетях подвижной связи (СПС) GSM для аутентификации абонента используются постоянные ключ аутентификации K_i и алгоритм аутентификации A_i, а для шифрования информации применяются постоянный алгоритм шифрования A_8, которые привязаны к SIM-карте абонента [2]. Злоумышленник, который единожды вскрыл ключ аутентификации K_i, алгоритм аутентификации A_i и алгоритм шифрования A_8, может постоянно расшифровывать информацию в абонентском канале связи с конкретным пользователем СПС GSM. Отдельные категории абонентов, например представители крупного бизнеса [3, 4] или госслужащие [5], нуждаются в повышении криптостойкости услуг связи СПС GSM [6] и сетях подвижной персональной спутниковой связи [7].

Алгоритмы аутентификации и шифрования в СПС GSM

В современных сетях подвижной (мобильной) связи применяется алгоритм шифрования, основанный на следующей технологии [2].

Для аутентификации информации абонента в сетях подвижной связи стандарта GSM каждый абонентский терминал (АТ) содержит записанные в SIM-карте свои индивидуальный ключ аутентификации K_i и алгоритм аутентификации A_i. Базовая станция (БС) сети подвижной связи передает на АТ случайное число RAND, а АТ на основании числа RAND, ключа аутентификации K_i и алгоритма аутентификации A_i вычисляет значение ответа SRES: $\mathrm{SRES} = A_i(K_i; \mathrm{RAND})$. Далее АТ отправляет ответ SRES на базовую станцию, которая использует ключ K_i и алгоритм аутентификации A_i вызываемого абонента, хранящиеся в базах данных зарегистрированных абонентов мобильного центра коммутации, вычисляет число SRES и сравнивает вычисленное число SRES с полученным от абонентского терминала. Если вычисленное и полученное от АТ число SRES совпадают, то БС вступает в связь с АТ.

То есть в данном случае используется аутентификация с открытым ключом, характеризующаяся следующими недостатками:

– ключ K_i и алгоритм аутентификации A_i постоянные, следствием чего является низкая криптостойкость;

– случайное число RAND передается по открытому каналу связи и при компрометации ключа и алгоритма аутентификации злоумышленник может осуществить ложное подключение к базовой станции (т. е. создать ложный АТ, осуществив подлог), пока на АТ, ключи и алгоритмы аутентификации которого скомпрометированы, не будет сменена SIM-карта;

– отсутствует возможность увеличения криптостойкости аутентификации для отдельных категорий АТ без применения дополнительных программных средств.

Для шифрования информации абонентской радиолинии в сети подвижной связи стандарта GSM БС передает на АТ случайное число RAND. Абонентский терминал на основании числа RAND, ключа K_i и алгоритма шифрования A_8 вычисляет ключ шифрования на сеанс связи K_c: $K_c = A_8(K_i; \mathrm{RAND})$. Передаваемая в абонентской радиолинии (от базовой станции и от абонентского терминала) информация зашифровывается с применением ключа шифрования на сеанс связи K_c и алгоритма шифрования A_8: $E_c = A_8(K_c; I_c)$, где I_c — открытая информация в сеансе связи.

То есть используют шифрование с открытым ключом, характеризующееся следующими недостатками:

– алгоритм вычисления A_i ключа аутентификации K_i, из которого формируется ключ шифрования информации в сеансе связи K_c, постоянный, поэтому злоумышленник имеет возможность скомпрометировать ключ аутентификации K_i, а затем научится формировать ключи шифрования информации в сеансе связи K_c;

– алгоритм шифрования A_8, используемый для формирования ключа шифрования информации в сеансе связи K_c из ключа аутентификации K_i и применяемый для шифрования информации, постоянный, поэтому данный способ шифрования обладает низкой криптостойкостью;

– случайное число RAND передается по открытому каналу связи и при компрометации ключа аутентификации K_i, алгоритма аутентификации A_i и алгоритма шифрования A_8 злоумышленник может прослушивать трафик АТ, пока не будет сменена SIM-карта;

– для отдельных категорий АТ отсутствует возможность увеличения криптостойкости шифрования без применения дополнительных программных средств.

Метод аутентификации абонента с применением динамично изменяющихся матриц ключей и алгоритмов

В предлагаемом методе аутентификации [8] данные аутентификации и шифрования передаваемой информации задействуются при установлении каждого соединения и передаче данных и организованы в памяти каждого составляющего систему устройства как матрица ключей аутентификации M_{Ki}; матрица порядков смены позиций M_{CKi} ключей аутентификации K_i в матрице ключей аутентификации M_{Ki}; матрица алгоритмов аутентификации M_{Ai}; матрица порядков смены позиций M_{CAi} алгоритмов аутентификации A_i в матрице M_{Ai}; матрица M_{A8} алгоритмов шифрования A_8; матрица порядков смены позиций M_{CA8} алгоритмов шифрования A_8 в матрице M_{A8} алгоритмов шифрования.

При работе предложенной системы передачи данных периодические изменения позиций ключей в матрице ключей, а также изменение алгоритмов в матрице алгоритмов являются альтернативой хранения в постоянном запоминающем устройстве большого количества ключей и алгоритмов. Работа системы основана на двух последовательных процессах: аутентификации информации абонентской радиолинии и шифрования абонентской радиолинии. Порядок смены ключей аутентификации K_i, формулы математических операций и механизм смены алгоритмов аутентификации A_i и алгоритмов шифрования A_8 известны каждому центру коммутации системы — наземной станции сети подвижной связи и/или спутнику-ретранслятору сети персональной спутниковой связи. Процесс аутентификации удостоверяет, что абонент имеет право доступа к услугам связи и предшествует процедуре установления соединения. После установления соединения начинает работу процедура шифрования информации в абонентской радиолинии.

Пример простейшей матрицы ключей аутентификации —

$$M_{Ki} = \begin{Vmatrix} K_{i11} & K_{i12} & K_{i13} \\ K_{i21} & K_{i22} & K_{i23} \\ K_{i31} & K_{i32} & R \end{Vmatrix},$$

где R — это принятое от БС число RAND.

Пример простейшей матрицы смены позиций ключей аутентификации —

$$M_{CKi} = \begin{Vmatrix} C_{Ki11} & C_{Ki12} & C_{Ki13} \\ C_{Ki21} & C_{Ki22} & C_{Ki23} \\ C_{Ki31} & C_{Ki32} & C_{Ki33} \end{Vmatrix}.$$

Пример простейшей матрицы алгоритмов аутентификации —

$$M_{Ai} = \begin{Vmatrix} A_{i11} & A_{i12} & A_{i13} \\ A_{i21} & A_{i22} & A_{i23} \\ A_{i31} & A_{i32} & A_{i33} \end{Vmatrix}.$$

Пример простейшей матрицы смены позиций алгоритмов аутентификации —

$$M_{CAi} = \begin{Vmatrix} C_{Ai11} & C_{Ai12} & C_{Ai13} \\ C_{Ai21} & C_{Ai22} & C_{Ai23} \\ C_{Ai31} & C_{Ai32} & C_{Ai33} \end{Vmatrix}.$$

Пример простейшей матрицы алгоритмов шифрования —

$$M_{A8} = \begin{Vmatrix} A_{811} & A_{812} & A_{813} \\ A_{821} & A_{822} & A_{823} \\ A_{831} & A_{832} & A_{833} \end{Vmatrix}.$$

Пример простейшей матрицы смены позиций алгоритмов —

$$M_{Cae} = \begin{Vmatrix} C_{A811} & C_{A812} & C_{A813} \\ C_{A821} & C_{A822} & C_{A823} \\ C_{A831} & C_{A832} & C_{A833} \end{Vmatrix}.$$

Аутентификация АТ выполняется следующим образом.

Шаг 1. Матрицы M_{K_i} ключей аутентификации, матрицы порядков смены позиций M_{CKi} ключей аутентификации, матрицы алгоритмов аутентификации M_{A_i}, матрицы порядков смены позиций M_{CAi} алгоритмов аутентификации, матрицы алгоритмов шифрования M_{A8} и матрицы порядков смены позиций M_{A8} алгоритмов шифрования записываются в постоянное энергонезависимое запоминающее устройство (ПЗУ) каждого АТ (или на SIM-карту), в защищенные базы данных центров коммутации и являются уникальными для каждого АТ.

Шаг 2. Принятое АТ от центра коммутации случайное число RAND записывается в одну из позиций матрицы M_{Ki} ключей аутентификации для проведения процедуры вычисления числа SRES. Позиция матрицы M_{Ki} ключей аутентификации, в которую записывается принятое случайное число RAND, определяется порядком смены позиций C_{Ki} ключа аутентификации.

Шаг 3. Значения ключей аутентификации K_i и принятое случайное число RAND, записанных в матрице M_{Ki} ключей аутентификации, периодически перемещаются по позициям матрицы ключей аутентификации по определенному алгоритму в соответствии с действующим на данный момент порядком смены позиций C_{Ki} ключей аутентификации. Порядковые номера порядков смены позиций C_{Ki} ключа аутентификации записаны в матрице M_{CK_i} порядков смены позиций ключа аутентификации, и каждому номеру порядков смены позиций C_{Ki} ключа аутентификации соответствует определенная последовательность смены позиций.

После прохождения полного цикла смены позиций ключами аутентификации K_i и принятым случайным числом RAND ключи аутентификации K_i и принятое случайное число RAND возвращаются на исходные позиции и изменяется порядок смены их позиций C_{Ki}. После прохождения полного цикла изменения порядков смены позиций C_{KAi} ключами аутентификации порядки смены позиций C_{KAi} возвращаются на исходные позиции в матрице M_{CKi} порядков смены позиций и порядок смены позиций C_{KAi} изменяется по определенному закону.

Шаг 4. Номера алгоритмов A_i вычисления числа SRES (алгоритмов аутентификации) записываются в матрицу аутентификации алгоритмов M_{Ai}, и каждому порядковому номеру соответствует своя математическая формула.

Шаг 5. Номера алгоритмов аутентификации A_i, записанных в матрице M_{Ai} алгоритмов аутентификации, перемещаются по позициям матрицы алгоритмов аутентификации по определенному правилу в соответствии с действующим на данный момент порядком смены позиций C_{Ai} алгоритмов аутентификации. Вначале номера алгоритмов аутентификации A_i изменяются по одному правилу C_{A_i}, действующему в настоящий момент, затем порядок смены позиций алгоритма аутентификации C_{Ai} изменяется. Номера порядков смены позиций C_{Ai} алгоритма аутентификации записаны в матрице M_{CAi} порядков смены позиций алгоритма аутентификации, и каждому номеру порядков смены позиций C_{Ai} алгоритма аутентификации соответствует определенная последовательность смены позиций.

После прохождения полного цикла смены позиций номерами алгоритмов аутентификации A_i номера алгоритмов аутентификации возвращаются на исходные позиции и изменяется порядок смены их позиций C_{Ai}. После прохождения полного цикла изменения порядков смены позиций C_{Ai} номерами алгоритмов аутентификации A_i порядки смены позиций C_{Ai} возвращаются на исходные позиции в матрице M_{CAi} порядков смены позиций и порядок смены позиций C_{Ai} изменяется по определенному закону.

Смена позиций ключами аутентификации K_{Ai} и номеров алгоритмов аутентификации A_i осущест-

вляется через строго определенные интервалы времени (от 1 суток до полугода), известные АТ и центрам коммутации. Все алгоритмы вычислений A_i ответа SRES содержат однонаправленные функции.

Шаг 6. В АТ на основании матрицы M_{Ki} ключей аутентификации, принятого случайного числа RAND и матрицы алгоритмов аутентификации M_{Ai} производятся математические операции для вычисления числа SRES.

Шаг 7. Вычисленное число SRES передается в центр коммутации, где также вычисляется число SRES. Вычисленное число SRES сравнивается с полученным от АТ числом SRES. Абонент считается прошедшим аутентификацию при совпадении чисел SRES, вычисленных АТ и центром коммутации.

Криптостойкость процесса аутентификации определяется:

– длиной ключа аутентификации L_{Ki} (для увеличения криптостойкости длина ключа шифрования L_{Ki} должна стремится к максимально возможному значению);

– количеством применяемых ключей аутентификации N_{Ki} и количеством перестановок ключей N_{CKi} (для увеличения криптостойкости количество применяемых ключей аутентификации и количество перестановок ключей должны стремиться к максимально возможным значениям);

– сложностью и количеством алгоритмов аутентификации N_{Ai} (для увеличения криптостойкости сложность и количество алгоритмов аутентификации должны стремиться к максимально возможным значениям);

– количеством перестановок алгоритмов аутентификации N_{CAi} (для увеличения криптостойкости количество перестановок алгоритмов аутентификации должно стремиться к максимально возможным значениям);

– периодом действия ключей аутентификации T_{Ki} и алгоритмов аутентификации T_{Ai} (для увеличения криптостойкости период действия ключей аутентификации и алгоритмов аутентификации должны стремиться к минимально возможным значениям).

Алгоритм работы АТ и центра коммутации СПС или СР сети ПСС при выполнении процедуры аутентификации изображен на рис. 1 и 2.

Метод шифрования информации с применением динамично изменяющихся матриц ключей и алгоритмов

В предлагаемом методе [8] шифрование информации выполняется следующим образом.

Шаг 1. Ключ шифрования K_c на сеанс связи определяется из вычисленного на этапе аутентификации ключа аутентификации K_i с применением действующего в настоящий момент алгоритма шифрования A_8.

Шаг 2. Номера алгоритмов шифрования A_8 записываются в матрицу алгоритмов шифрования M_{A8}. Каждому порядковому номеру соответствует заданная математическая формула. Номера алгоритмов шифрования A_8, записанных в матрице алгоритмов шифрования M_{A8}, перемещаются по позициям данной матрицы по определенному правилу в соответствии с действующим на данный момент порядком смены позиций C_{A8} алгоритмов шифрования.

Вначале номера алгоритмов шифрования A_8 изменяются по одному правилу C_{A8}, действующему в настоящий момент, затем порядок смены позиций алгоритма шифрования C_{A8} изменяется. Номера порядков смены позиций C_{A8} алгоритма шифрования записаны в матрице M_{CA8} порядков смены позиций алгоритма шифрования, и каждому номеру порядков смены позиций C_{A8} алгоритма шифрования соответствует определенная последовательность смены позиций. После прохождения полного цикла смены позиций номерами алгоритмов шифрования A_8 номера алгоритмов шифрования возвращаются на исходные позиции и изменяется порядок смены их позиций C_{A8}.

После прохождения полного цикла изменения порядков смены позиций C_{A8} номерами алгоритмов шифрования A_8 порядки смены позиций C_{A8} возвращаются на исходные позиции в матрице M_{CA8} порядков смены позиций и порядок смены позиций C_{A8} изменяется по определенному закону.

Смена позиций номеров алгоритмов шифрования A_8 осуществляется через строго определенные интервалы времени (от 1 суток до полугода), известные АТ и центрам коммутации. Все алгоритмы

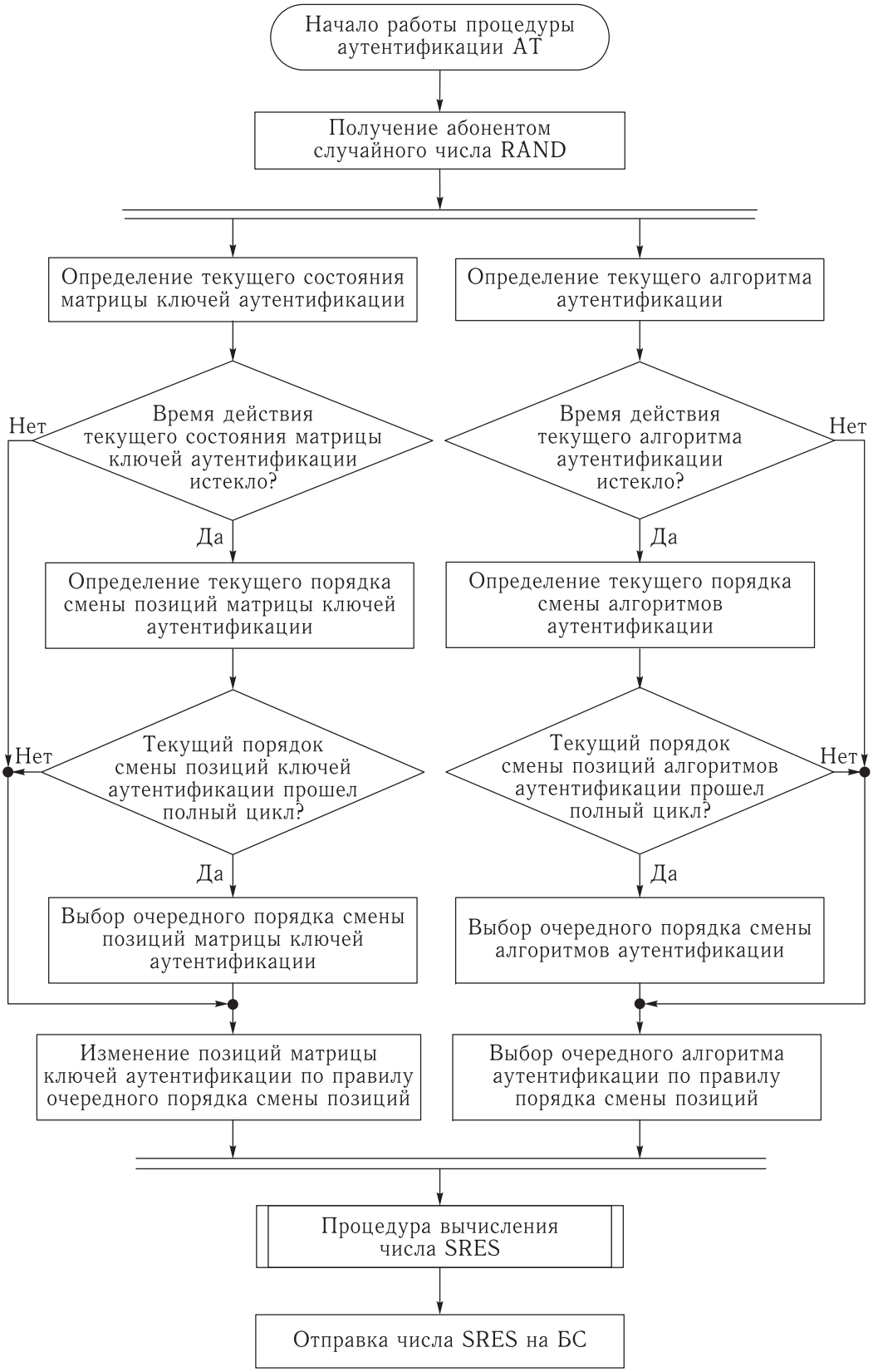

Рис. 1. Алгоритм работы АТ при выполнении процедуры аутентификации

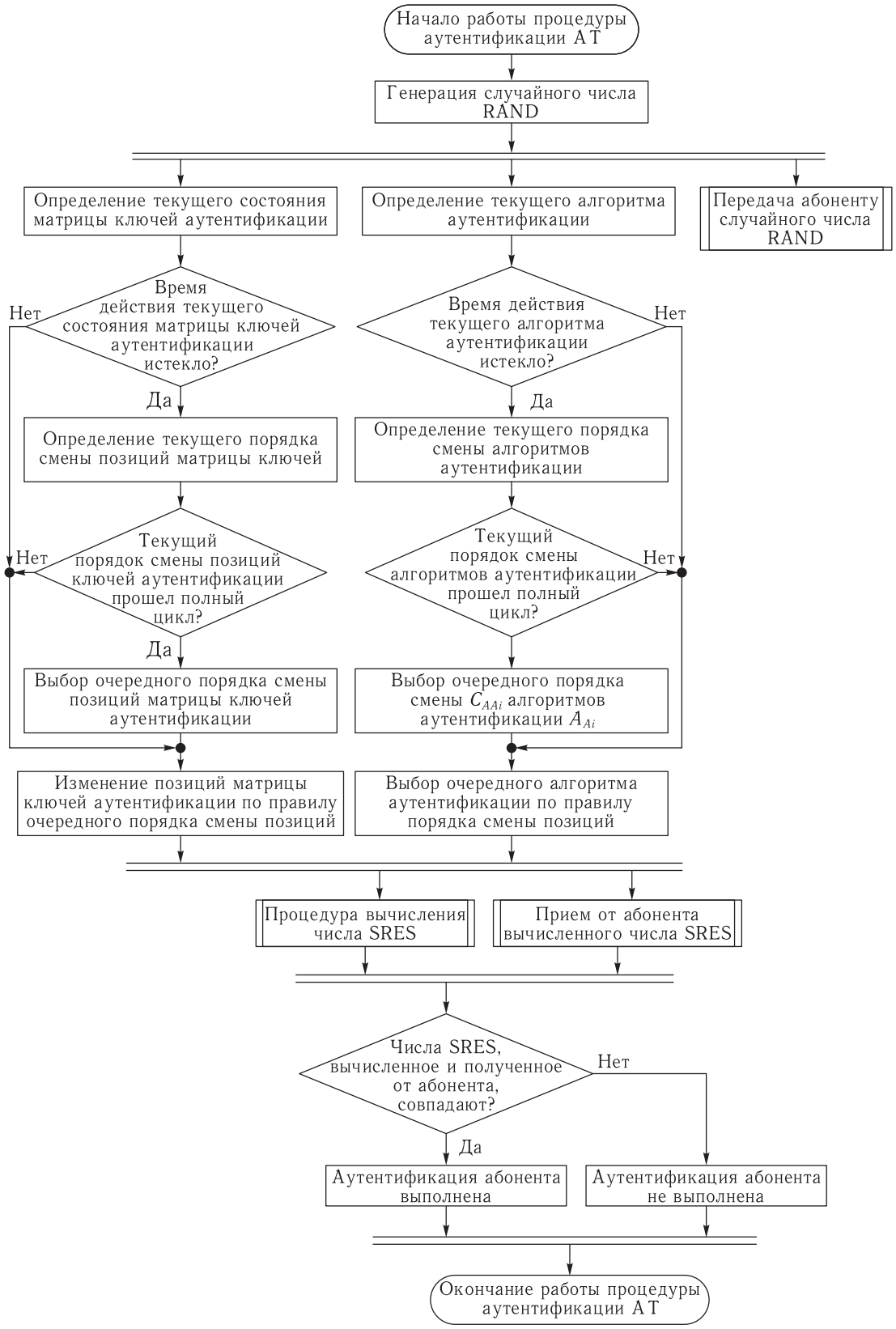

Рис. 2. Алгоритм работы центра коммутации сети подвижной связи или спутника-ретранслятора сети подвижной персональной спутниковой связи при выполнении процедуры аутентификации

вычислений A_8 ключа шифрования K_c содержат однонаправленные функции.

Шаг 3. Информация зашифровывается с помощью ключа шифрования K_c на сеанс связи и алгоритма шифрования A_8.

Криптостойкость процесса шифрования информации определяется:

– длиной ключа аутентификации L_{Ki} (для увеличения криптостойкости длина ключа шифрования L_{Ki} должна стремиться к максимально возможному значению);

– количеством применяемых ключей аутентификации N_{Ki} и количеством перестановок ключей N_{CK_i} (для увеличения криптостойкости количество применяемых ключей аутентификации и количество перестановок ключей должны стремиться к максимально возможным значениям);

– сложностью и количеством алгоритмов аутентификации N_{Ai} и алгоритмов шифрования N_{A8} (для увеличения криптостойкости сложность и количество алгоритмов аутентификации и алгоритмов шифрования должны стремиться к максимально возможным значениям);

– количеством перестановок алгоритмов аутентификации N_{CAi} и алгоритмов шифрования N_{CA8} (для увеличения криптостойкости количество перестановок алгоритмов аутентификации должно стремиться к максимально возможным значениям);

– периодом действия ключей аутентификации T_{Ki}, алгоритмов аутентификации T_{Ai} и алгоритмов шифрования T_{A8} (для увеличения криптостойкости период действия ключей аутентификации, алгоритмов аутентификации и алгоритмов шифрования должен стремиться к минимально возможным значениям).

Алгоритм процедуры шифрования в сети подвижной связи или спутника-ретранслятора в сети подвижной персональной спутниковой связи изображен на рис. 3.

Дешифрование информации выполняется следующим образом.

Шаг 1. В центре коммутации так же, как и в АТ, на основании вычисленного на этапе аутентификации ключа аутентификации K_i и матрицы алгоритмов шифрования M_{A8i} производятся математические операции для вычисления ключа шифрования на сеанс связи K_c.

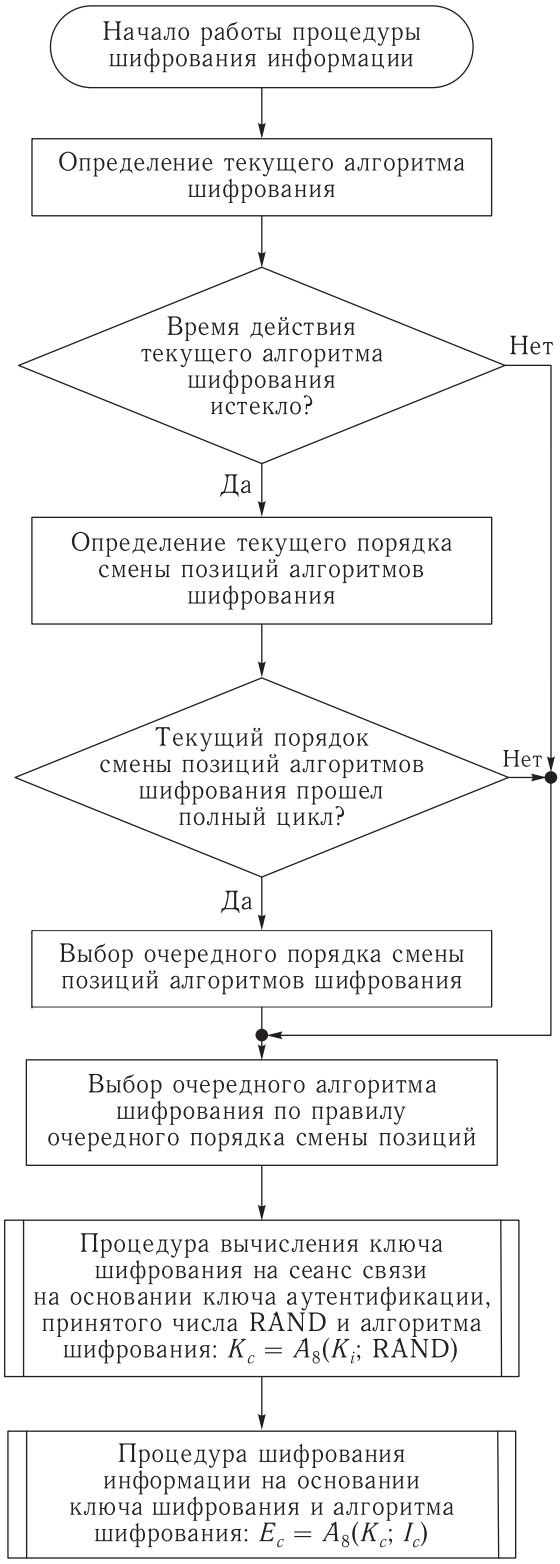

Рис. 3. Алгоритм процедуры шифрования в сети подвижной связи или спутника-ретранслятора в сети подвижной персональной спутниковой связи

Шаг 2. Затем в центре коммутации на основании вычисленного ключа шифрования на сеанс связи K_c и действующего в настоящий момент алгоритма шифрования A_8 выполняется дешифрование информации (функция, обратная шифрованию).

Методика управления степенью криптостойкости передаваемой информации

Для управления степенью криптостойкости передаваемой информации и, соответственно, отказа от усложнения системы в ряде случаев абонентов классифицируют по восьми категориям от 0-й до 7-й [8]:

1) абоненты с минимальными требованиями к криптостойкости — 0-й, 1-й, 2-й категорий — «массовый» пользователь (потенциальный нарушитель — хакер, работающий единолично на обычных бытовых компьютерах);

2) абоненты с повышенными требованиями к криптостойкости — 3-й, 4-й категорий — высокопоставленные представители бизнеса и госслужащие (потенциальный нарушитель — организованная группа хакеров, работающая в интересах преступных организаций или конкурентной разведки в небольших центрах обработки данных);

3) абоненты с высокими требованиями к криптостойкости — 5-й, 6-й, 7-й категорий — высокопоставленные госслужащие и представители силовых структур и ведомств (потенциальный нарушитель – инженеры, имеющие в распоряжении крупные центры обработки данных).

В зависимости от категории абонентов применяют:

– разные по размеру матрицы ключей аутентификации, матрицы порядков смены позиций ключей аутентификации, матрицы алгоритмов аутентификации и матрицы порядков смены позиций алгоритмов аутентификации;

– разные по размеру матрицы алгоритмов шифрования и матрицы порядков смены позиций алгоритмов шифрования;

– разные временные сроки действия определенной комбинации ключей аутентификации;

– разные временные сроки действия определенного алгоритма аутентификации и определенного алгоритма шифрования;

– разные по сложности алгоритмы аутентификации и алгоритмы шифрования;

– разную длительность интервала времени действия определенной комбинации ключей аутентификации, алгоритмов аутентификации и алгоритмов шифрования, которая должна быть меньше периода, необходимого для компрометации ключей и алгоритмов.

Например, для категории абонентов с максимальными требованиями к криптостойкости информации ключи можно записывать не в одну, а в две матрицы и производить операцию умножения одной матрицы на другую.

Заключение

В рассмотренных методах аутентификации и шифрования информации за счет одновременного обеспечения на всех устройствах большого количества вариантов числа аутентификации и ключа шифрования информации абонентского канала связи обеспечивается повышение криптостойкости системы передачи данных с минимальной дополнительной нагрузкой на вычислительные мощности АТ.

Таким образом, разработана и обоснована методика аутентификации абонентов и шифрования информации, обладающая следующими преимуществами:

– простотой реализации, не требующей высокой производительности вычислительных средств;

– универсальностью применения в различных системах радиосвязи и спутниковой связи, в том числе в СПС и в СППСС военного и двойного назначения;

– гибким подходом к изменению степени криптостойкости для различных категорий трафика и различных категорий абонентов.

Список литературы

1. *Барсуков В.С.* Безопасность GSM: реальная или виртуальная? // GSM guard. http://www.gsm-guard.net/press1_2.html (Дата обращения 19.02.2020).

2. *Чекалин А. А.*, *Зарев А. В.*, *Скрыль С. В.*, *Вохминцев В. А. и др*. Защита информации в системах мобильной связи: Учеб. пособ. для вузов. 2-е изд., испр. и доп. М.: Горячая линия–Телеком, 2005. 171 с.

3. Организация для защиты корпоративной сотовой связи на базе SafePhone Plus. Решения операторов персональных данных. https://www.niisokb.ru/upload/solutions-for-operators-of-personal-data.pdf (Дата обращения 19.02.2020).

4. Требования по защите информации в корпоративной системе мобильной связи при обработке данных в государственных информационных системах. https://www.niisokb.ru/upload/the-infosecurity-requirements-for-state-information-systems.pdf (Дата обращения 19.02.2020).

5. Приказ от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Список изменяющих документов (В ред. «Приказов ФСТЭК России» от 15.02.2017 № 27, от 28.05.2019 № 106). https://www.fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (Дата обращения 27.02.2020).

6. *Максименко В. Н*. Организационно-режимные процессы защиты информации в сетях сотовой подвижной связи. https://studfile.net/preview/8102488/ (Дата обращения 19.02.2020).

7. Приказ от 21 июля 1999 г. № 22 «Об утверждении Положения о порядке, общих условиях и принципах использования на территории Российской Федерации систем глобальной подвижной персональной спутниковой связи (ГППСС) и требованиях по обеспечению информационной безопасности для российских сегментов указанных систем». https://www.base.garant.ru/181201 (Дата обращения 27.02.2020).

8. *Пантелеймонов И. Н.*, *Толкачев В. И.*, *Пантелеймонова А. В.*, *Адамсон Н. Н.*, *Тодуркин В. В.* Патент № 2684488 Российской Федерации. Система защищенной передачи данных: № 2018116591/08: заявл. 05.04.18; опубл. 04.09.19.