DOI: 10.25728/iccss.2023.97.57.067

Пантелеймонов И.Н., Лещенко В.В., Монастыренко А.А., Захаров Е.А., Щербатых Л.В., Королев П.С., Тодуркин М.В.

Организация передачи и защита информации управления в системах спутниковой связи и информационного обмена с космическими аппаратами

Аннотация: Одним из основных аспектов управления в сложных системах является обеспечение защиты информации в канале управление. Изложены ключевые технологии защиты информации на примере управления работой в системах спутниковой связи и управления полетом космического аппарата (КА), которые могут быть применены в системах радиосвязи и спутниковой связи различного назначения, а также системах удаленного управления любыми автономными аппаратами, например, беспилотными летательными аппаратами (БПЛА) и т.д.

Ключевые слова: криптошлюз, канал управления, информационный канал, команды управления, телеметрическая информация, ключ, алгоритм, аутентификация, шифрование

При рассмотрении проблем систем и средств спутниковой связи в России [1] были изложены результаты научно-исследовательской работы, в которой приведен сравнительный анализ результатов интеллектуальной деятельности в сфере систем и средств связи. В частности, систем спутниковой связи в России и за рубежом.

В данной работе изложено одно из актуальных предложений по решению этих проблем – ключевые технологии защиты информации на примере управления работой в системах спутниковой связи и управления полетом космического аппарата (КА).

Защита канала удаленного управления работой модема в сетях спутниковой связи VSAT

В настоящее время в системах спутниковой связи (ССС) VSAT работой модемов абонентских станций (АС) управляет центральная станция (ЦС), от которой передаются сигналы управления для автоматической регулировки:

– мощности усиления усилителя мощности передающего тракта;

– автоматической регулировки ширины полосы пропускания;

– автоматической регулировки модуляционно-кодовой конструкции. Это обеспечивает поддержание в норме соотношения сигнал/шум на входе приемного тракта и обеспечение качественной передачи информации в канале спутниковой связи, в котором защищается только информационный канал, а в канале управления средства защиты информации отсутствуют.

Отсутствие защиты в канале управления может привести к тому, что ложная центральная станция может осуществить подлог и выдать управляющие воздействия на уменьшения мощности излучения ниже требуемого уровня и тем самым подавить работу системы спутниковой связи.

Организация защиты канала удаленного управления работой модема в сетях спутниковой связи VSAT изображена на рисунке 1.

Предлагаемое техническое решение отличается простотой реализации, т.к. требует установки только дополнительной сетевой карты Ethernet, выполняющей роль интерфейса модуля управления (Manager Module) [2, 3]. Работа системы спутниковой связи с защитой каналов управления заключается в том, что информация управления (ИУ) передаются в виде IP-пакетов вместе с информацией трафика в едином потоке данных, защищенном с помощью криптошлюза (КШ). Закрытая информация с модема поступает на криптошлюз, где дешифруется и затем, информация управления передается на вход модуля управления.

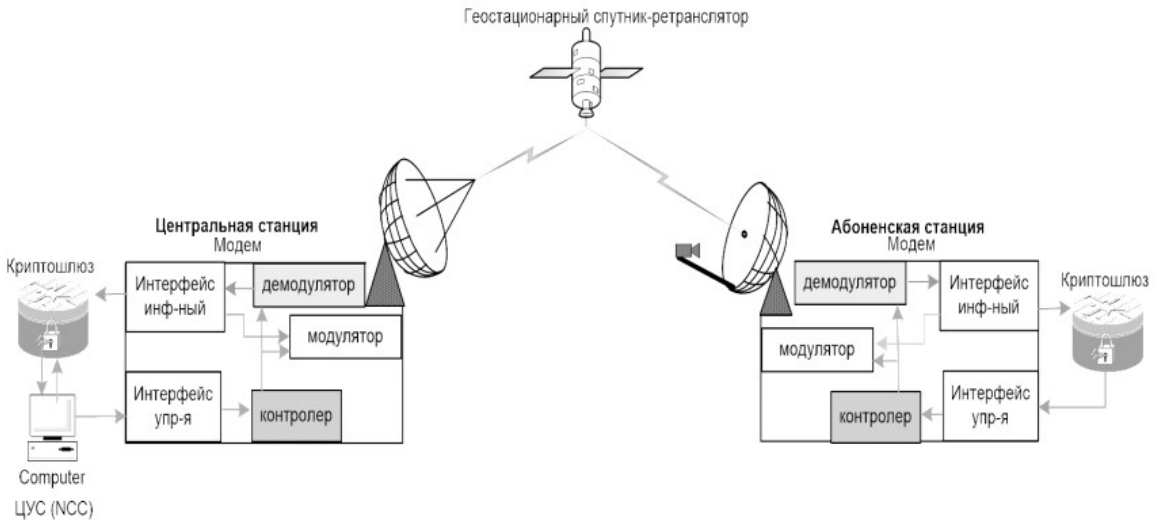

Рисунок 1 – Организация защиты канала удаленного управления работой модема в сетях спутниковой связи VSAT

Организация передачи потоков данных и защиты информации при осуществлении информационного обмена с КА

В существующих системах информационного обмена с КА каждая линия связи (ЛС) и каждый вид информации защищается своими отдельными средствами криптозащиты информации (СКЗИ) [4]:

1) наземная ЛС, передающая командно-программную информацию (КПИ) от центра управления полетом (ЦУП) до наземной командно-измерительной станции (НКИС) и в обратном канале (от НКИС до ЦУП) – защищается СКЗИ, установленными в ЦУП и НКИС;

2) наземная ЛС, передающая телеметрическую информацию (ТМИ) от наземной телеметрической станции (НТС) или НКИС до ЦУП – защищается СКЗИ, установленными в ЦУП, НТС и НКИС;

3) наземная ЛС, передающая целевую информацию (ЦИ) от наземной станции приема целевой информации (СПИ) до центра обработки информации (ЦОИ) в системах космического мониторинга Земли (СМЗ) – защищается СКЗИ, установленными в ЦОИ и СПИ;

4) наземная ЛС, передающая целевую информацию (ЦИ) от наземной шлюзовой станции (ШС) до центра управления сетью (ЦУС) в системах спутниковой связи (ССС) на негеостационарных

спутниках-ретрансляторах (НГСО) – защищается СКЗИ, установленными в ЦУС и ШС;

5) наземная ЛС, передающая КПИ для управления работой полезной нагрузкой (ПН) КА от ЦУС или ЦОИ на соответствующие ЦУП – защищается СКЗИ, установленными в ЦУС или ЦОИ и ЦУП;

6) спутниковая ЛС, передающая КПИ от НКИС на бортовую аппаратуру (БА) командно-измерительной системы (КИС) КА и в обратном канале (от БА КИС КА до НКИС) – защищается СКЗИ, установленными в НКИС и БА КИС;

7) спутниковая ЛС, передающая ТМИ от бортовой телеметрической системы (БТС) КА на НТС или НКИС – защищается СКЗИ, установленными в БТС КА и НТС или НКИС;

8) спутниковая ЛС, передающая ЦИ от ПН КА на СПИ в СМЗ – защищается СКЗИ, установленными в ПН КА и СПИ;

9) спутниковая ЛС, передающая ЦИ от ПН КА на ШС в ССС на НГСО – защищается СКЗИ, установленными в ПН КА и ШС.

Примечание. В ряде случаев отдельные виды информации идут по открытым ЛС.

В современных ССС, применяющие спутники-ретрансляторы (СР) без обработки сигналов на борту, описанные выше принципы не изменяются.

Таким образом, существующая система информационного обмена с КА имеет один недостаток – требуется большое количество СКЗИ и каналообразующей аппаратуры, которое является следствием следующих проблем:

- высокая стоимость космической системы в целом;
- высокие энергозатраты и массогабаритные характеристики бортовой аппаратуры (БА) КА;
- дополнительные задержки информации, вносимые СКЗИ.

Предлагаются следующие принципы обмена информацией с КА [3]:

1) применение универсальной наземной станции (НС), обеспечивающей одновременно прием-передачу ЦИ и информацию управления (ИУ);

2) применение универсального бортового радиотехнического комплекса (БРТК) СР и универсальной бортовой информационной

системы (БИС) КА, обеспечивающих одновременно прием-передачу ЦИ и информацию управления (ИУ);

3) передача ЦИ и ИУ с применением стека протоколов TCP/IP в одной наземной ЛС и в одной спутниковой ЛС, но в разных виртуальных локальных сетях (VLAN);

4) применение СР с обработкой и маршрутизацией информации на борту, обеспечивающее интеграцию и дифференциацию различных потоков информации.

Примечание. В спутниковых ЛС на уровнях L3–L7 образцовой модели OSI на первом этапе можно было бы использовать стек протоколов TCP/IP, а в перспективе разработать и внедрить специализированный протокол передачи информации.

Схема организации защиты информации в сетях передачи информации от КА до наземных пунктов приема целевой информации изображена на рисунке 2.

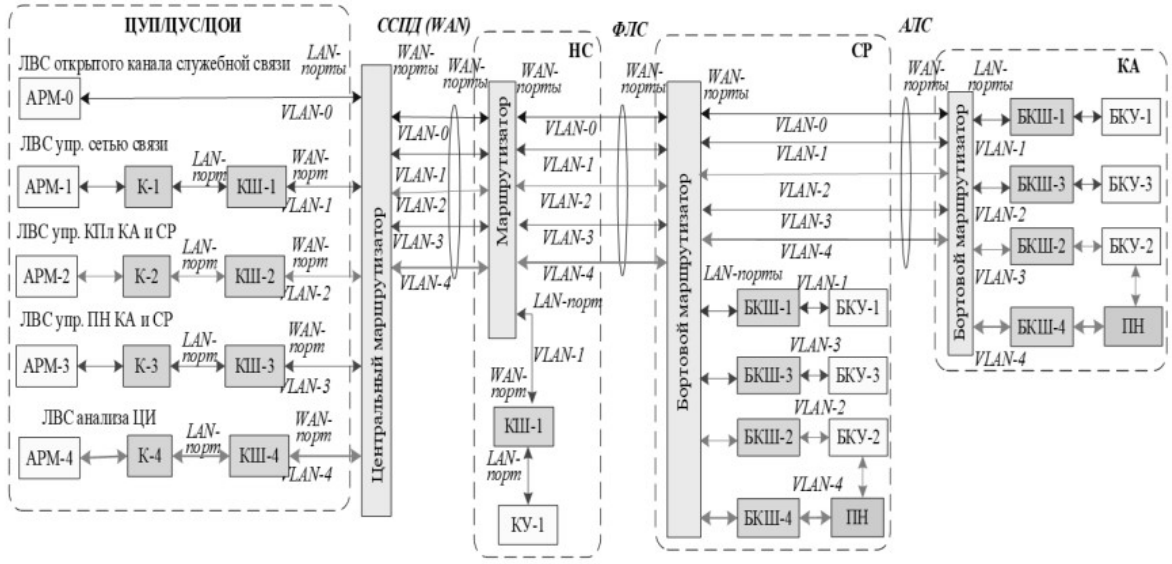

Рисунок 2 – Схема организации защиты информации в сетях связи и передачи информации от МКА до наземных пунктов приема целевой информации с использованием бортовых и наземных терминалов ВКЛС

С целью упрощения схемы на рисунке 2 изображено только сетевое оборудование и не изображено каналообразующее оборудование, а именно – антенные системы, приемники, передатчики, модуляторы и демодуляторы.

Условные обозначения на рисунке 2:

Центр управления сетью включает в себя, следующее вычислительное и сетевое оборудование:

АРМ-0 – автоматизированное рабочее место (АРМ) оператора управления работой сетевого оборудования в открытом канале связи;

АРМ-1 – автоматизированное рабочее место оператора управления сетью связи, БИС КА, БРТК СР и НС;

К-1 – коммутатор Ethernet локальной вычислительно сети (ЛВС) №1 управления сетью связи, БИС КА, БРТК СР и НС;

КШ-1 – криптошлюз (КШ) ЛВС №1.

Центр управления полетами в себя, следующее вычислительное и сетевое оборудование:

АРМ-2 – автоматизированные рабочие места операторов управления космическими платформами КА и СР;

К-2 – коммутатор Ethernet локальной вычислительно сети №2 управления КПл КА и СР;

КШ-2 – криптошлюз ЛВС №2.

Центр обработки и анализа информации КА и СР в себя, следующее вычислительное и сетевое оборудование:

АРМ-3 – автоматизированные рабочие места операторов управления полезными нагрузками КА и СР;

АРМ-4 – АРМ оператора обработки и анализа целевой информации от КА и от СР;

К-3 – коммутатор Ethernet локальной вычислительно сети №3 управления сетью связи, БИС КА, БРТК СР и НС;

К-4 – коммутатор Ethernet локальной вычислительно сети №4 анализа ЦИ от КА и от СР;

КШ-3 – криптошлюз ЛВС№3;

КШ-4 – криптошлюз ЛВС №4.

В состав НС входит следующее вычислительное и сетевое оборудование:

М – маршрутизатор;

КШ-1 – криптошлюз виртуальной ЛВС (VLAN) №1;

КУ-1 – компьютер управления работой НС.

В состав СР и КА входит следующее вычислительное и сетевое оборудование:

БМ – бортовой маршрутизатор КА и СР;

БКШ-1 – криптошлюз виртуальной ЛВС №1;

БКШ-2 – криптошлюз виртуальной ЛВС №2;

БКШ-3 – криптошлюз виртуальной ЛВС№3;

БКШ-4 – криптошлюз виртуальной ЛВС №4;

БКУ-1 – бортовой комплекс управления (БКУ) БИС КА и БРТК СР;

БКУ-1 – бортовой комплекс управления КПл КА и СР;

БКУ-3 – бортовой комплекс управления ПН КА и СР;

ПН – целевая аппаратура.

Техническим результатом предлагаемой технологии является уменьшение количества бортовых и наземных СКЗИ и каналообразующей аппаратуры, что приводит к:

– уменьшению энергозатрат и массогабаритных характеристик БА КА;

– снижению задержки информации, вносимой СКЗИ;

– снижению стоимости космической системы в целом.

Технический результат достигается за счет применения технологий:

– обеспечения сквозной передачи информации в закрытом виде между оконечными устройствами без снижения уровня криптостойкости;

– передача различных видов информации в едином потоке по единой физической проводной и беспроводной линии связи и соответственно, применение единой каналообразующей аппаратуры для обеспечения передачи различных видов информации.

Реализация отмеченных выше технологий осуществляется за счет применения следующего оборудования:

– маршрутизаторов, обеспечивающих интеграцию и дифференциацию различных потоков информации;

– унифицированных бортовых и наземных СКЗИ, представляющих собой КШ, обеспечивающие раздельное шифрование и дешифрование различных видов информации.

Принцип действия заключается в том, что организуются виртуальные ЛВС (Virtual LAN, VLAN) для каждого вида трафика, где оконечные однотипные устройства (т.е.: АРМ наземных служб, КУ НС и БКУ всех КА и СР) находятся в одной ЛВС, разделенной закрытым каналом связи, состоящим из наземных и спутниковых линий связи, где ЗС – выполняет функции ретрансляции, маршрутизаторы – объединяют

и разделяют потоки информации, а КШ – закрывают канал связи между оконечными устройствами.

Организуемые VLAN при организации информационного обмена с КА без применения СР:

VLAN-0 – ОКСлС НС, СР и КА;

VLAN-1 – ЛВС управления сетью связи, БИС КА, БРТК СР и РТК НС;

VLAN-2 – ЛВС управления КПл КА;

VLAN-3 – ЛВС управления ПН КА;

VLAN-4 – ЛВС анализа ЦИ.

Предлагаемый способ организации передача потоков данных и защиты информации при осуществлении информационного обмена с КА обладает свойствами гибкости и универсальности, что позволяет эффективно организовать защиту информации при различных следующих вариантах организации связи.

Для повышения криптостойкости аутентификации абонентов и передаваемой информации в сетях радиосвязи и спутниковой связи различного назначения должны быть использованы нижеследующие методы.

Метод аутентификации абонента и шифрования информации в сетях подвижной связи

В современных сетях подвижной (мобильной) связи (СПС) стандарта GSM, применяется алгоритм шифрования, основанный на следующей технологии [5].

Алгоритм аутентификации абонента и шифрования информации в СПС представлен на рисунке 3.

Для аутентификации информации абонента в сетях подвижной связи стандарта GSM каждый абонентский терминал (АТ) содержит, записанные в SIM-карте, свои индивидуальный ключ аутентификации Ki и алгоритм аутентификации Ai. Базовая станция (БС) сети подвижной связи передает на АТ случайное число RAND, а АТ на основании числа RAND, ключа аутентификации Ki и алгоритма аутентификации Ai вычисляет значение ответа SRES: SRES=Ai(Ki; RAND). Далее, АТ отправляет ответ SRES на базовую станцию, которая использует ключ Ki и алгоритм аутентификации Ai 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.

Для шифрования информации абонентской радиолинии в сети подвижной связи стандарта GSM БС передает на АТ случайное число RAND. Абонентский терминал на основании на числа RAND, ключа Ki и алгоритма шифрования A8 вычисляет ключ шифрования на сеанс связи Kc: Kc=A8(Ki; RAND). Передаваемая в абонентской радиолинии (от базовой станции и от абонентского терминала) информация зашифровывается с применением ключа шифрования на сеанс связи Kc и алгоритма шифрования A8.

Ec=A8(Kc; Ic), где Ic– открытая информация в сеансе связи.

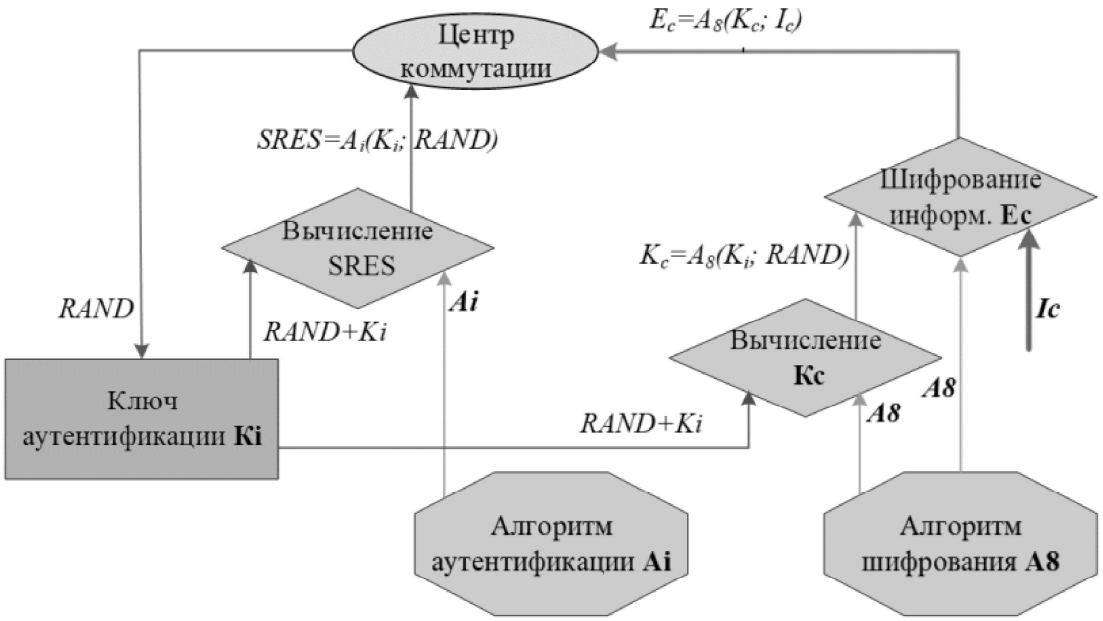

Рисунок 3 – Алгоритм аутентификации абонента и шифрования информации в СПС

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

– ключ Ki и алгоритм аутентификации Ai постоянные, следствием чего является низкая криптостойкость аутентификации;

– 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;

– алгоритм вычисления Ai ключа аутентификации Ki, из которого формируется ключ шифрования информации в сеансе связи Kc, постоянный, поэтому злоумышленник имеет возможность скомпрометировать сперва ключ аутентификации Ki, а затем и научится формировать ключи шифрования информации в сеансе связи Kc;

– алгоритм шифрования A8, используемый для формирования ключа шифрования информации в сеансе связи Kc из ключа аутентификации Ki и применяемый для шифрования информации постоянный, поэтому данный способ шифрования обладают низкой криптостойкостью;

– случайное число RAND передается по открытому каналу связи и при компрометации ключа аутентификации Ki, алгоритма аутентификации Ai и алгоритма шифрования A8 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 и шифрования информации с применением динамично изменяющихся матриц ключей и алгоритмов

Алгоритм аутентификации абонента и шифрования информации с применением динамично изменяющихся матриц ключей и алгоритмов отображен на рисунке 4.

В предлагаемом методе аутентификации и шифрования передаваемой информации [6, 7] в памяти каждого составляющего систему связи устройства хранятся:

1) как матрица ключей аутентификации МКi;

2) матрица порядков смены позиций МСКi ключей аутентификации Ki в матрице ключей аутентификации МКi;

3) матрица алгоритмов аутентификации МАi;

4) матрица порядков смены позиций МСАi алгоритмов аутентификации Ai в матрице МАi;

5) матрица МА8 алгоритмов шифрования A8;

6) матрица порядков смены позиций МСА8 алгоритмов шифрования А8 в матрице МА8 алгоритмов шифрования.

Таким образом, имеются множества: ключей аутентификации вместо одного ключа, алгоритмов аутентификации вместо одного алгоритма и алгоритмов шифрования вместо одного алгоритма, кроме того, изменяющиеся по определенным законам.

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 Ki, формулы математических операций и механизм смены алгоритмов аутентификации Ai и алгоритмов шифрования А8 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.

Смена позиций номеров алгоритмов и ключей осуществляется через строго определенные интервалы времени (от 1 суток до полугода), известные абоненту и центрам коммутации. Все алгоритмы вычислений содержит однонаправленные функции.

После прохождения полного цикла смены позиций их значения возвращаются на исходные позиции и изменяется порядок смены их позиций. После прохождения полного цикла изменения порядков смены позиций порядки смены позиций возвращаются на исходные позиции в матрице и порядок смены позиций изменяется по определенному закону.

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:

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

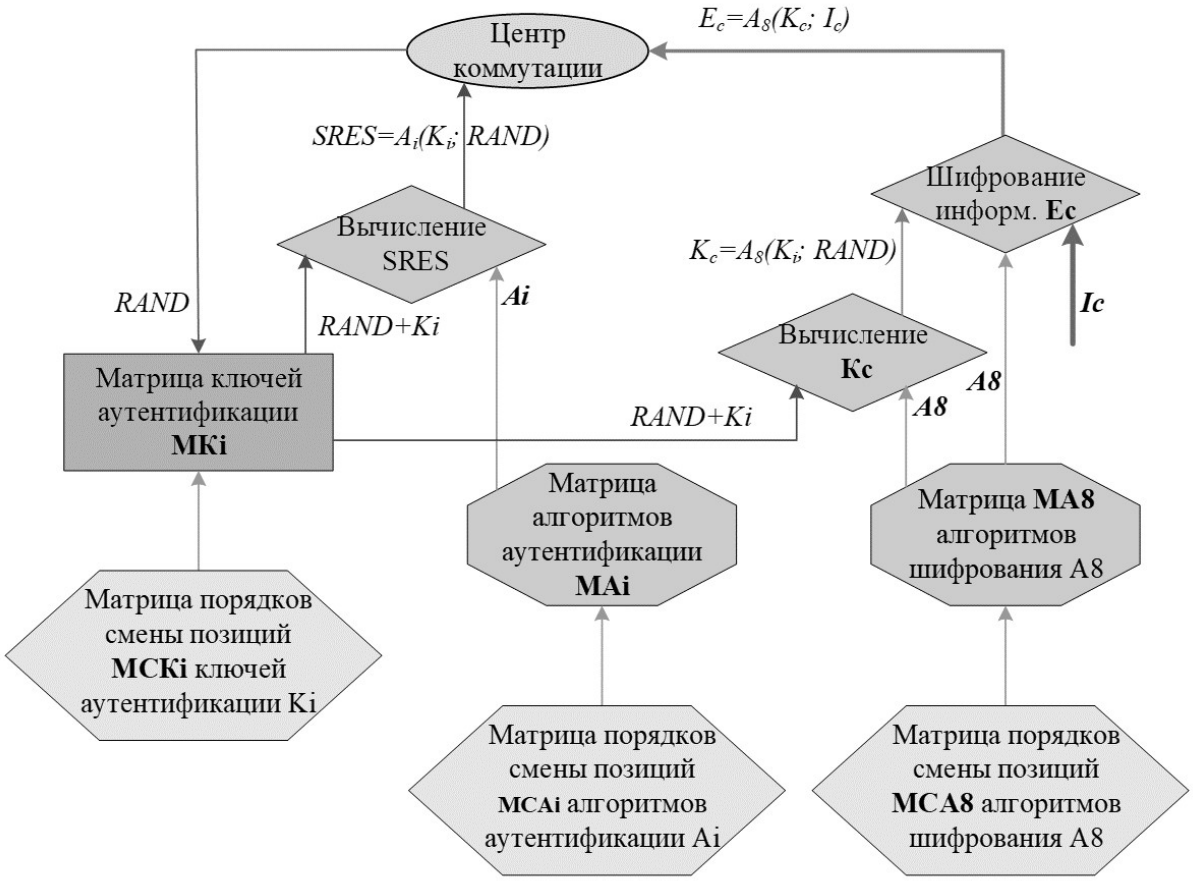

Рисунок 4 – Алгоритм аутентификации абонента и шифрования информации с применением динамично изменяющихся матриц ключей и алгоритмов

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:

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

Криптостойкость процессов аутентификации и шифрования определяется:

– длиной ключа аутентификации LKi, для увеличения криптостойкости длина ключа шифрования LKi должна стремится к максимально возможному значению;

– количеством применяемых ключей аутентификации NKi и количеством перестановок ключей NCKi, для увеличения криптостойкости количество применяемых ключей аутентификации и количество перестановок ключей должны стремится к максимально возможным значениям;

– сложностью и количеством алгоритмов аутентификации NAi и шифрования NA8, для увеличения криптостойкости сложность и количество алгоритмов должны стремится к максимально возможным значениям;

– количеством перестановок алгоритмов, для увеличения криптостойкости количество перестановок алгоритмов должно стремится к максимально возможным значениям;

– периодом действия ключей аутентификации TKi и алгоритмов TA, для увеличения криптостойкости период действия ключей аутентификации и алгоритмов аутентификации должны стремится к минимально возможным значениям.

Метод управления степенью криптостойкости передаваемой информации

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

1) абоненты с минимальными требованиями к криптостойкости – 0-й, 1-й, 2-ой 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 на 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 алгоритмов шифрования;

– разные по сложности алгоритмы аутентификации и алгоритмы шифрования;

– разную длительность интервала времени действия определенной комбинации ключей аутентификации, алгоритмов аутентификации и алгоритмов шифрования 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 матрицу, а – в две матрицы и производить операцию умножения одной матрицы на другую.

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:

– простота реализации, не требующая высокой производительности вычислительных средств;

– универсальность применения в различных системах радиосвязи и спутниковой связи, в том числе в СПС и в СППСС различного назначения;

– гибкий подход к изменению степени криптостойкости для различных категорий трафика и различных категорий абонентов.

Заключение

Применение предлагаемых технологий защиты в канале управления в коммерческих и ведомственных системах спутниковой, подвижной и радиорелейной связи повышает степень защиты от деструктивного воздействия и при массовом производстве и внедрении может принести значительную прибыль предприятию изготовителю, обладающему данной технологией.

Литература:

1. *Лещенко В.В.* О проблемах систем и средств спутниковой связи в России / Проблемы управления безопасностью сложных систем: материалы XXX Международной конференции. 14 декабря 2022 г., Москва. – Москва: ИПУ РАН, 2022. – С. 374-378. – DOI: 10.25728/iccss.2022.82.10.057.

2. *Гладков И.А., Пантелеймонов И.Н., Корниенко В.И., Абрамов Д.П., Тодуркин В.В.* Архитектурные решения защиты канала удаленного управления работой модема в сетях спутниковой связи // Труды НИИР. – 2015. – № 1. – С. 12-18.

3. Система спутниковой связи с защитой канала удаленного управления работой: патент № 2647631 Российская Федерация / Пантелеймонов И.Н. Заявка 2017118784 30.05.2017 заявл. 30.052017 опубл. 16.03.2018. Бюл. № 8.

4. Способ и система защиты информации при организации информационного обмена с космическими аппаратами: патент № 2795117 Российская Федерация / Пантелеймонов И.Н., Ментус О.В., Мырова Л.О., Потюпкин А.Ю., Горожанкин Л.В., Монастыренко А. А., Захаров Е.А., Лещенко В.В., Пантелеймонова А.В., Пантелеймонов И.И., Феденев А.В., Данилов Н.Д., Яхин И.Х., Жуков А.С., Окулов К.Ю., Степанов И.Б., Филатов В.В., Тодуркин А.В., Королихина Ю.О. Заявка 2022109019 заявл. 05.04.2022; опубл. 28.04.2023. Бюл. № 13.

5. *Чекалин А.А., Заряев А.В., Скрыль С.В., Вохминцев В.А., Обухов А.Н., Хохлов Н.С., Немцов А.Д., Щербаков В.Б., Потанин В.Е.* Защита информации в сетях подвижной связи: Учебное пособие для ВУЗов. 2-е изд. испр. и доп. – М.: Горячая линия – Телеком, 2005. – 171 с.

6. *Пантелеймонов И.Н., Белозерцев А.В., Монастыренко А.А., Боцва В.В., Наумкин А.В.* Методы аутентификации и шифрования информации в сетях связи на основе динамично изменяющихся матриц ключей и матриц алгоритмов // Ракетно-космическое приборостроение и информационные системы. – 2020. – Т. 7. Вып. 1. – С. 84-94.

7. Система защищенной передачи данных: патент № 2684488 Российская Федерация / Пантелеймонов И.Н., Толкачев В.И., Пантелеймонова А.В., Адамсон Н.В., Тодуркин В.В. Заявка 2018116591, заявл. 04.05.2018; опубл. 09.04.2019. Бюл. № 10.