электронный научно-технический журнал
ИНЖЕНЕРНЫЙ ВЕСТНИК
издатель ФГБОУ ВПО «Московский государственный технический университет им. Н.Э. Баумана»

Защита речевой информации в радиосетях связи

77-48211/501059

09, сентябрь 2012

Нелюб С. А.

УДК 004.773

Россия, МГТУ им. Н.Э. Баумана
sanelub@mail.ru

Введение

Обеспечение безопасности при ведении переговоров в радиосистеме встает на первое место, когда передаваемая информация имеет конфиденциальный характер или является информацией ограниченного доступа, что особенно актуально для государственных ведомств и крупных коммерческих предприятий. Однако, именно тот факт, что информация представляет некий интерес, может побудить потенциального нарушителя к противоправным действиям.

Хорошим примером описания возможных угроз информационной безопасности может послужить открытый стандарт построения цифровых радиосетей APCO-25, основные положения которого используются в данной статье. В стандарте описываются угрозы информационной безопасности и пути их нейтрализации, на основе криптографических алгоритмов AES и DES, использование которых невозможно в нашей стране. Также в стандарте APCO-25 не рассматриваются методы защиты речевой информации в ближней зоне оператора радиостанции. В данной статье описываются пути применения отечественных криптографических алгоритмов, например ГОСТ 28147-89, акцентируется важность борьбы с ПЭМИН радиостанции, предлагается краткий перечень конструктивных мер по минимизации ПЭМИН и организационных мер для защиты речевой информации в ближней зоне оператора.

Целью работы является описание структуры радиосети, в которой ведутся защищенные переговоры с использованием радиооборудования, определение типов потенциальных нарушителей информационной безопасности, рассмотрение угроз информационной безопасности, рассмотрение средств защиты информации, выдача рекомендаций по минимизации ПЭМИН и защите информации в ближней зоне оператора.

1 Постановка задачи

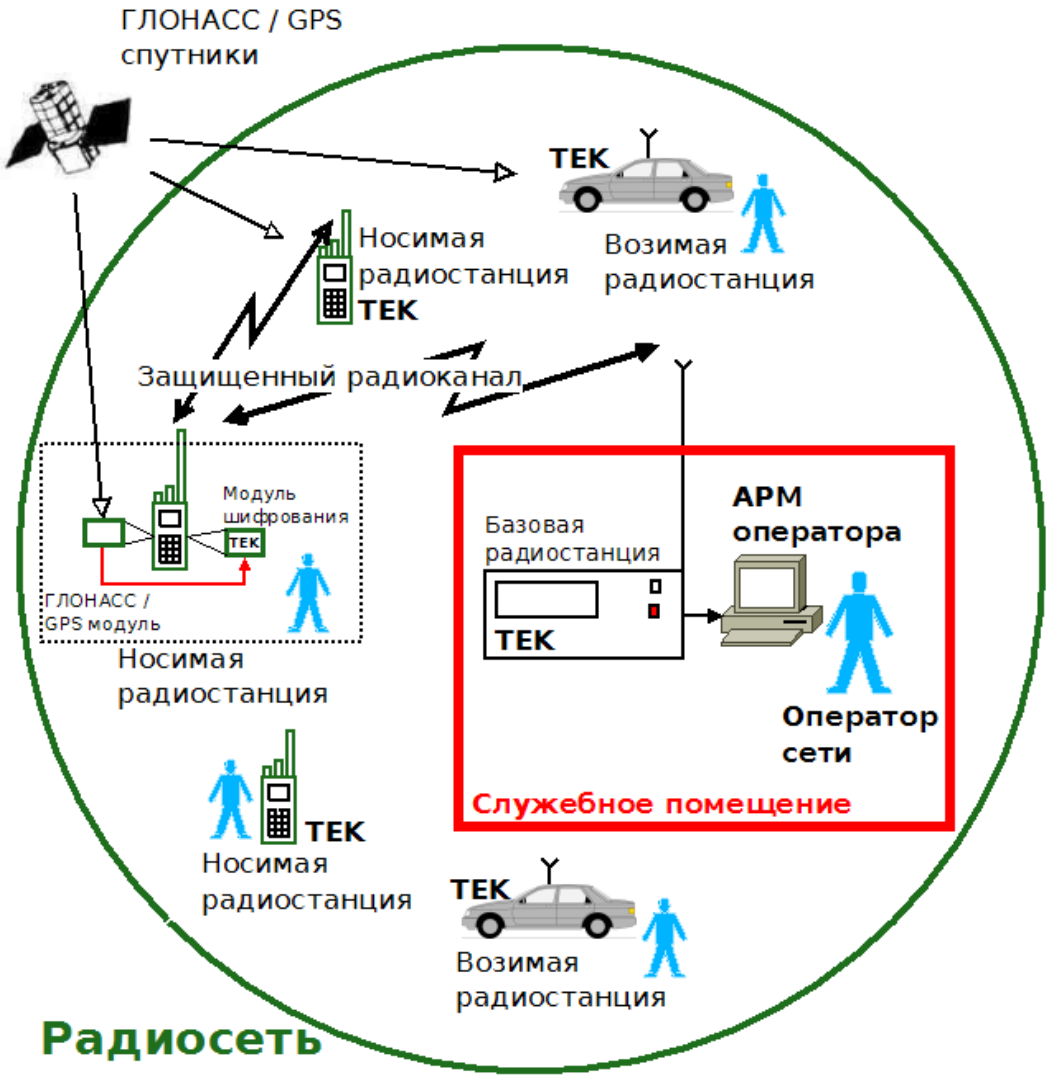
Для достижения поставленных целей решаются следующие задачи:

1) Определение типов потенциальных нарушителей и перечня возможных угроз с их стороны
2) Рассмотрение средств защиты информации для противодействия угрозам информационной безопасности
3) Формулирование рекомендаций по минимизации ПЭМИН и указание необходимости применения организационных мер для снижения вероятности утечки информации в ближней зоне

2 Структура радиосети

В радиосети осуществляются как общие вызовы, так и индивидуальные вызовы. В радиостанции запрограммированы набор оперативных ключей шифрования.

– В соответствии с рисунком 1 в радиосети используются радиостанции :
– Базовая радиостанция – выполняет функции мониторинга и управления,
– Носимая радиостанция,
– Возимая радиостанция.
–
– Основные технические характеристики радиосети связи:
– прием и отображение на дисплее информации об абоненте радиосети (ID абонента, местоположения абонента, текущего ключа шифрования, времени начала, конца и длительности сеанса связи),
– отображение местоположения абонента радиосети на электронной карте при его выходе на передачу, периодически и по запросам,
– ведение переговоров в радиосети,
– получение информации об абоненте при его выходе на передачу, по запросу с базовой станции или периодически,
– сохранение радио-переговоров и журнала оператора в БД,
– дистанционное прослушивание абонентских радиостанций,
– дистанционное выключение и включение приёмного и передающего трактов абонентских радиостанций,
– дистанционный опрос абонентских радиостанций по заданным ID кодам,
– шифрование информации и имитозащита.



–

Рисунок 1 – Структура радиосети

3 Модель нарушителя

–

– Нарушитель – это заинтересованное лицо, которое пытается осуществить НСД к информации или техническим средствам системы радиосвязи.

– Нарушители подразделяются на два типа:

– Внешние нарушители. Данные лица не имеют физического доступа к информации или техническим средствам радиосети

– Внутренние нарушители. Данные лица имеют физический допуск к информации или техническим средствам радиосети, могут являться зарегистрированными пользователями и пытаться получить доступ за пределами своих полномочий.

–

–

–

– 3.1 Угрозы со стороны внешнего нарушителя

–

Как показано на рисунке 2, внешний нарушитель в зависимости от уровня технической оснащенности может применять различные способы получения информации. Он может перехватить сигнал и попытаться дешифровать закрытое речевое сообщение. Нарушитель также может быть нацелен не на получение информации, а на выведение радиосистемы из работоспособного состояния. Он может перехватывать радиопереговоры, записывать их, может вносить некоторые изменения и снова повторять их в нужный момент в эфире [2]. Нарушитель может создавать помеху, делая невозможным ведение переговоров на данной радиочастоте.

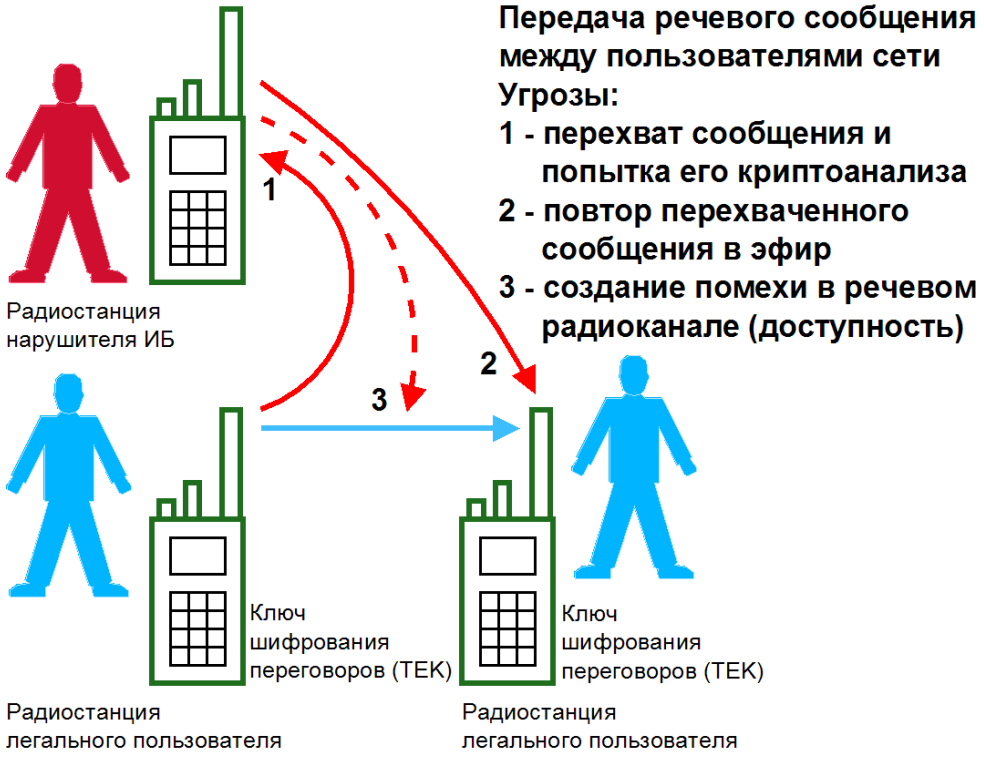


Рисунок 2 – Внешний нарушитель

В соответствии с рисунком 3 нарушитель может пытаться выдавать себя за базовую радиостанцию радиосети, перехватывая управляющие сообщения, изменяя их и передавая их в эфир в произвольные моменты времени.

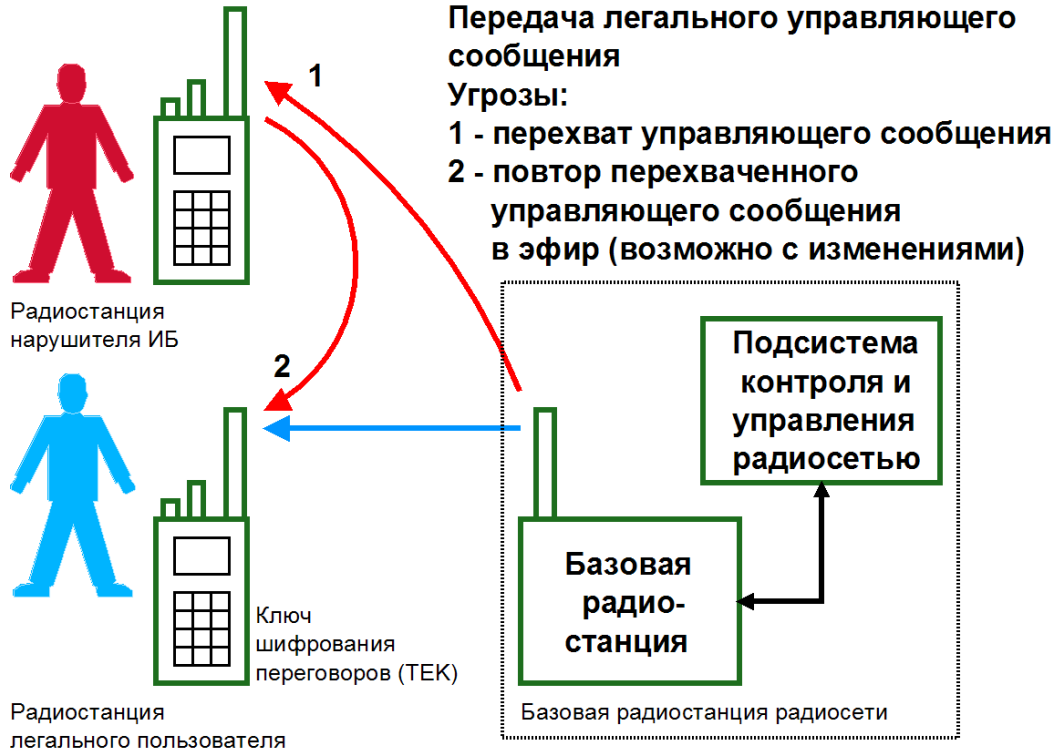


Рисунок 3 – Внешний нарушитель перехватывает управляющие сообщения

–

– 3.2 Угрозы со стороны внутреннего нарушителя

–

– Внутренний нарушитель может внедрять программно-аппаратные закладки в процессе разработки оборудования и его эксплуатации и, тем самым, контролировать радиоканал.

– Защиту от внутреннего нарушителя на этапе разработки обеспечивает сертификация СКЗИ, проверка его аппаратной части и поиск НДВ в исходных кодах. На этапе эксплуатации защиту от внутреннего нарушителя обеспечивают средства контроля целостности программного обеспечения радиостанции. Также в процессе эксплуатации радиостанции должны проходить периодический контроль.

4 Информационная безопасность в сетях радиосвязи

Информационная безопасность в сетях радиосвязи разделяется на три части: конфиденциальность, целостность и аутентификация, и управление ключами. Защита информации по этим трем направлениям позволит добиться наилучшего результата в обеспечении безопасности радиопереговоров.

Для обеспечения конфиденциальности должны применяться средства криптографической защиты информации (СКЗИ) определенного класса (уровня защиты). В основном алгоритмы криптоядра в СКЗИ – это алгоритмы блочного шифрования ГОСТ 28147-89, Уступ. Средства защиты импортного производства могут строиться на блочных алгоритмах AES и DES. Возможно применение

алгоритмов поточного шифрования, например RC4. Для обеспечения работы шифраторов требуется их надежная синхронизация на передающей и приёмной стороне.

Для обеспечения целостности сообщения должны функционировать механизмы выработки MAC в режиме CFB в алгоритмах AES и DES или в режиме имитовставки алгоритма ГОСТ 28147-89, что более актуально для СКЗИ. Должны быть предусмотрены механизмы обеспечения хронологической целостности и аутентификации источника сообщения.

Для алгоритмов шифрования и аутентификации требуется своевременная смена криптографических ключей по надежному каналу. Механизм управления ключами определяет момент смены и обновления ключей. При компрометации ключевой информации должна быть запущена процедура установки новых ключей [3].

Таблица 1 – Структура информационной безопасности в радиосетях

<table>
<tr><th>Конфиденциальность переговоров</th><th>Целостность и Аутентификация</th><th>Управление ключами</th></tr>
<tr><td>Должны применяться СКЗИ (средства криптографической защиты информации) определенного класса (уровня защиты)</td><td>Аутентификация и целостность сообщения: выработка имитовставки в режиме алгоритма ГОСТ 28147-89 (в СКЗИ) или MAC в режиме CFB в алгоритмах AES или DES</td><td>Программирование ключей в радиостанцию с помощью программаторов ключей или устройств Key Loader.</td></tr>
<tr><td>Возможные алгоритмы блочного шифрования ГОСТ 28147-89, Уступ, AES, DES. Возможно применение алгоритмов поточного шифрования, например RC4.</td><td>Хронологическая целостность используется для предотвращения появления в эфире передаваемых ранее сообщений. Используются окна допустимых номеров и MI.</td><td>Безопасная передача ключей шифрования трафика TEK, применяя технологию OTAR (Over-the-Air Rekeying)</td></tr>
<tr><td>Требуется надежная синхронизация шифраторов на передающей и приёмной стороне</td><td>Аутентификация источника сообщения позволяет определить подлинность передающего абонента</td><td>Механизм управления ключами определяет момент смены и обновления ключей</td></tr>
<tr><td colspan="2">Для алгоритмов шифрования и аутентификации требуется своевременная смена криптографических ключей по надежному каналу</td><td>При компрометации ключевой информации должна быть запущена процедура установки новых ключей</td></tr>
</table>

5 Общая модель передатчика

Как показано на рисунке 4, для передачи в эфир речевой сигнал оцифровывается с помощью АЦП, цифровой поток поступает на вокодер, затем на шифратор, после этого к зашифрованному цифровому потоку применяется помехоустойчивое кодирование и после этих преобразований цифровой поток поступает на модулятор.

Служебная информация и пользовательские данные, например навигационные данные, также проходят предварительную обработку. Вначале данные шифруются, затем шифрованный цифровой поток разбивается на пакеты (в том случае, если исходные данные имеют большой объём), к которым также применяется операция помехоустойчивого кодирования и этот цифровой поток подается на модулятор. Также на модулятор поступает и информация синхронизации и адресации [1]. Сигнал с выхода модулятора поступает на модулятор радиостанции и излучаются в эфир.

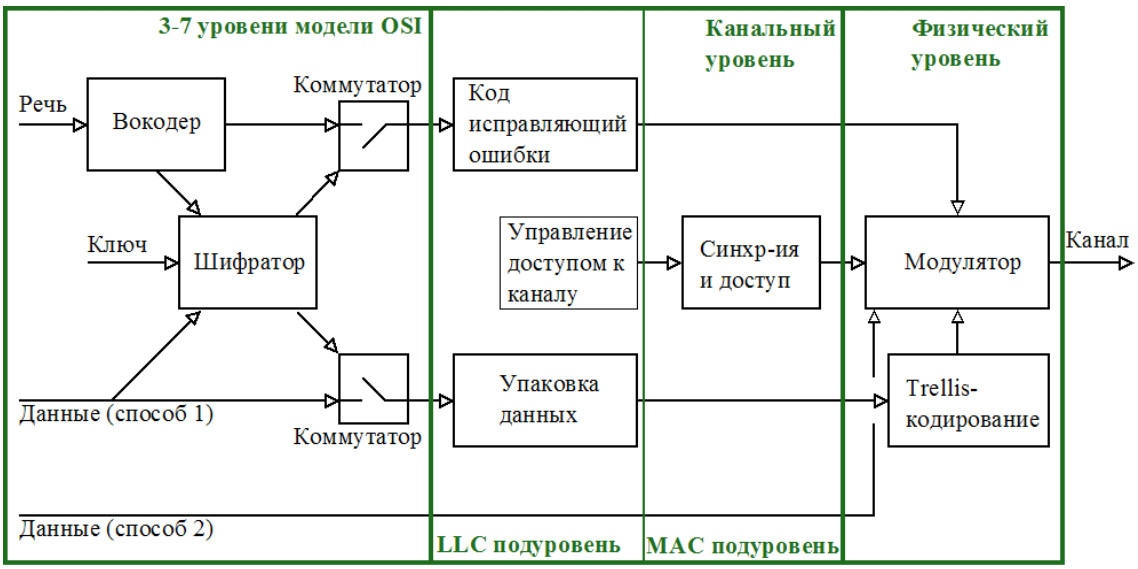


Рисунок 4 – Процессы обработки речи и данных на передающей стороне

6 Обеспечение конфиденциальности переговоров

В соответствии с рисунком 5 для синхронизации шифраторов используется индикатор сообщения MI. Приёмник находит MI в первом сообщении установки сеанса связи и инициализирует им свой регистр LFSR. Теперь приёмник с помощью LFSR может вырабатывать MI сам и сравнивать его с MI передатчика. Однако, для поддержания устойчивой работы, в последующие сообщения того же сеанса связи передатчик все равно вставляет MI. Если механизм обнаружения и исправления ошибок (FEC) сможет обнаружить и исправить все ошибки, то будет использован MI передатчика, в противном случае, используется выработанный приёмником MI и данные будут расшифрованы [3].

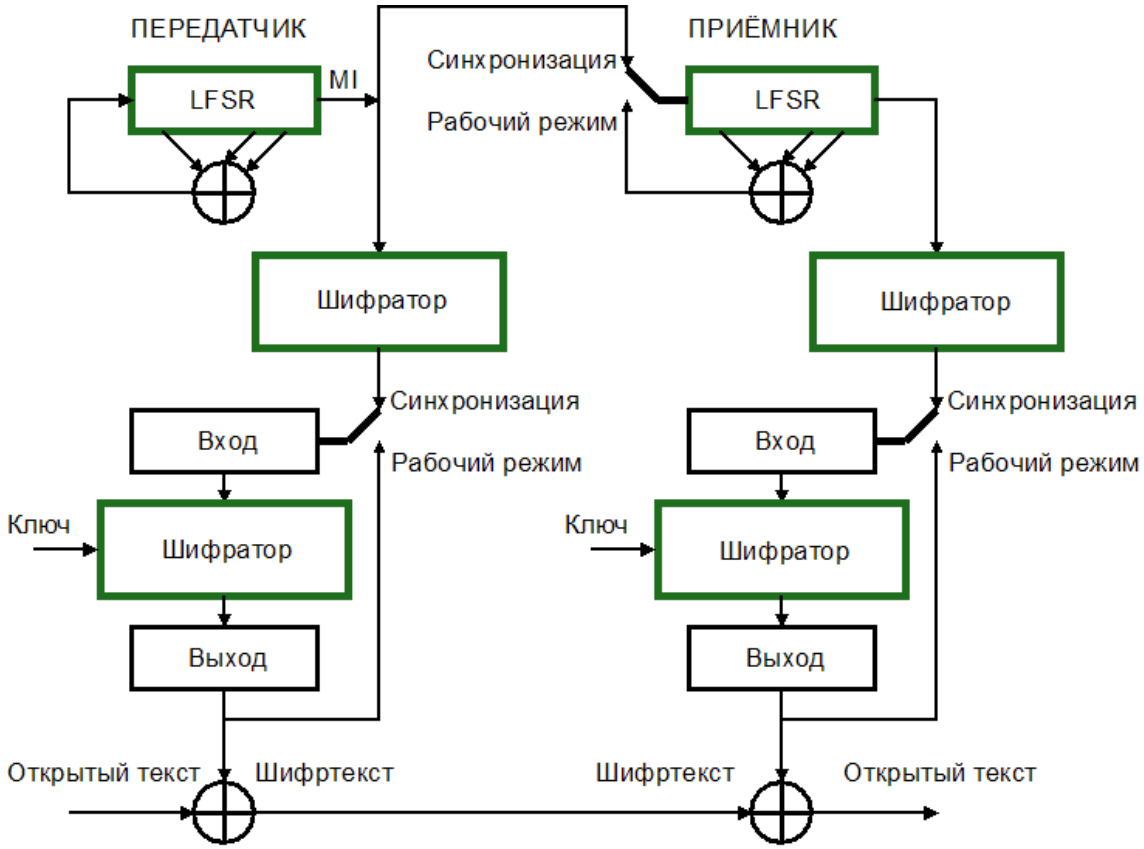


Рисунок 5 – Структурная схема синхронизации шифраторов с генерацией MI

В соответствии с рисунком 5 блок шифратор выполняет операцию шифрования информации в режиме простой замены. Возможно применение алгоритмов ГОСТ 28147-89, AES и DES. Организация механизма зацепления блоков может быть разной, на рисунке 5 приведен вариант использования режима OFB [3]. Стойкость выбранного алгоритма шифрования, его конкретная реализация и ключевая информация определяют защищенность речевых сообщений от криптоанализа.

7 Обеспечение целостности переговоров

Механизмы обеспечения целостности речевого сообщения включают в себя проверку того, что сообщение завершено, не изменено и не является копией сообщения передаваемого ранее. Как показано на рисунке 6, в теле сообщения должно находиться поле, содержимое которого является необратимой функцией данных и ключа, что позволит гарантировать неизменяемость сообщения [3]. Для такой цели может служить код аутентификации сообщения (MAC). Следует отметить, что ошибки в канале связи, вызванные возможными помехами в эфире, исправляют средства обнаружения и исправления ошибок (FEC).

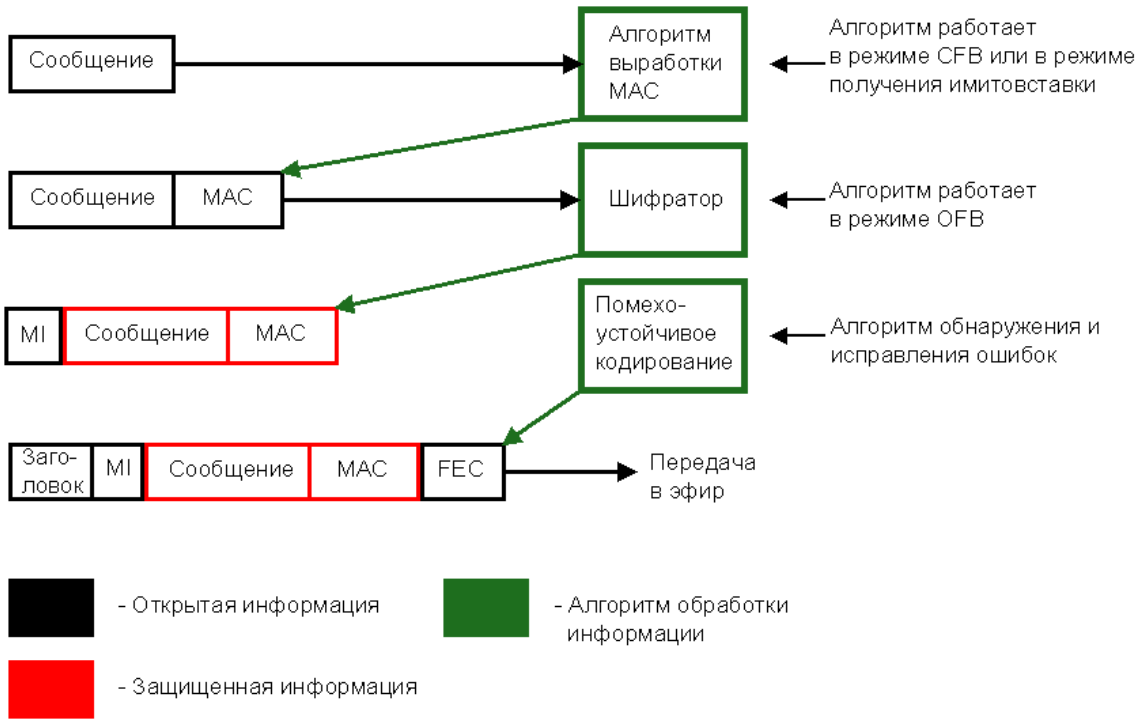


Рисунок 6 – Общая схема работы механизмов обеспечения целостности

Как показано на рисунке 7, для обеспечения целостности сообщения также может использоваться алгоритм ГОСТ 28147-89 в режиме выработки имитовставки. К сообщению прибавляется имитовставка. На приёмной стороне выполняется сравнение имитовставки, полученной из эфира, с выработанной имитовставкой. При несовпадении речевое сообщение считается неправильным и отбрасывается.

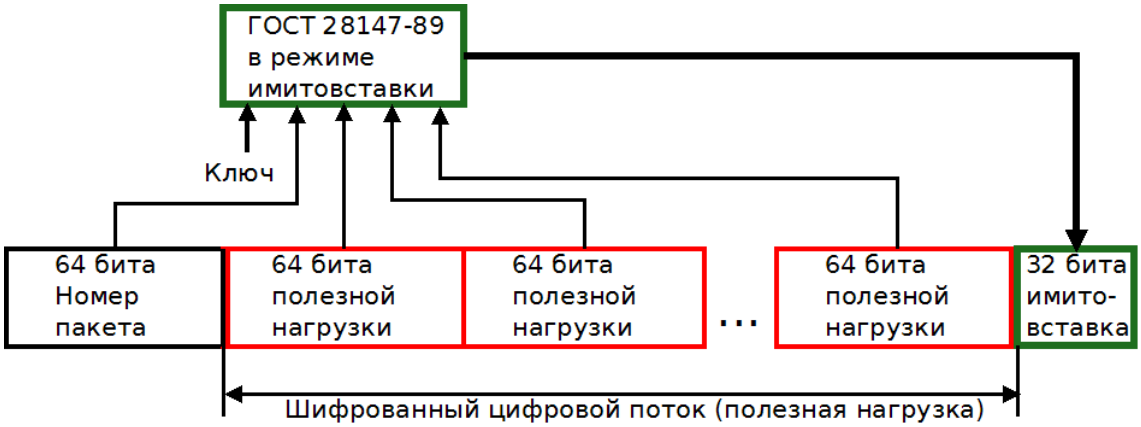


Рисунок 7 – Применение режима выработки имитовставки ГОСТ 28147-89

В соответствии с рисунком 8 для обеспечения хронологической целостности защиты от повторных копий передаваемого ранее сообщения могут применяться 2 варианта. В первом случае к сообщению добавляется номер, значение которого проверяется на приёмной стороне. Если номер

попадает в окно допустимых номеров, то сообщение принимается, в противном случае, сообщение отбрасывается. Также целостность сообщения может быть обеспечена по MI. Если нарушитель перехватит сообщение и снова передаст его в эфир, то существует большая вероятность того MI на приёмнике уже сдвинется и сообщение также будет отбрасывать [3].

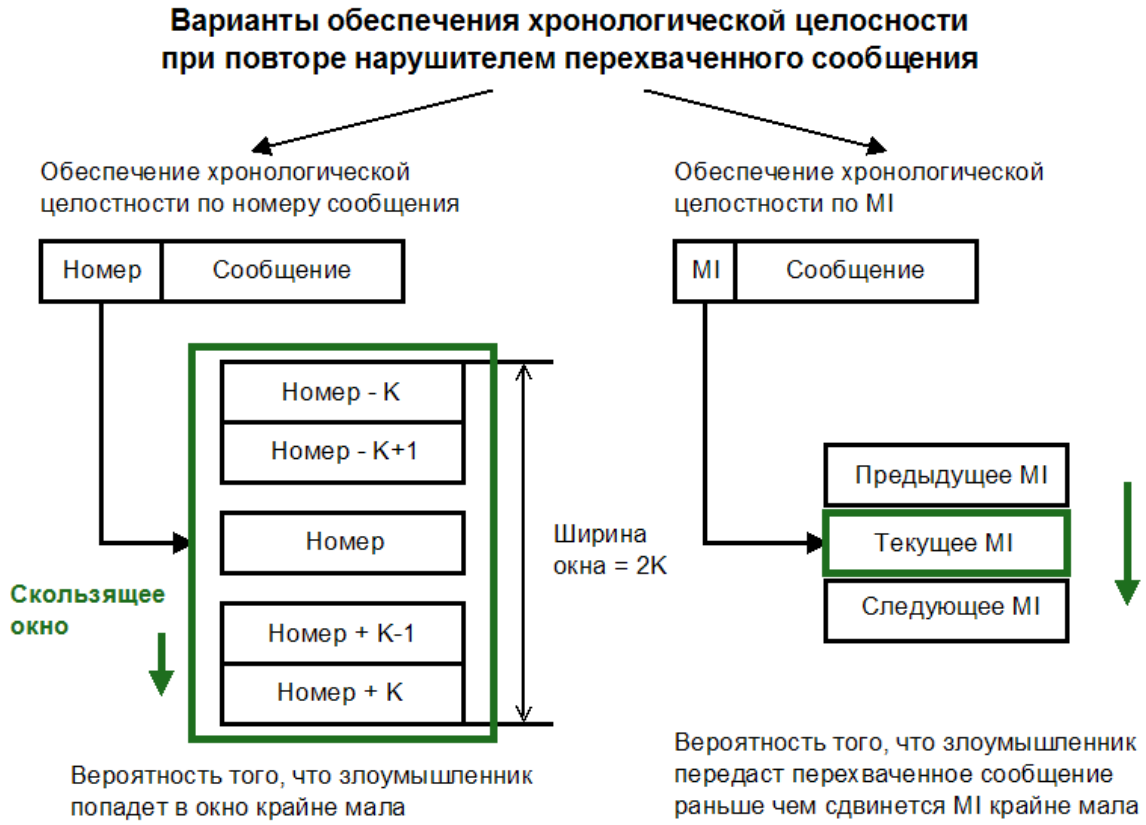


Рисунок 8 – Обеспечение хронологической целостности сообщения

Подлинность сообщения и его источника должны обеспечивать функции аутентификации.

8 Управление ключами

Криптографические алгоритмы шифрования и аутентификации требуют ключи, поэтому в радиосистемах должны быть использованы механизмы управления ключами. Ключи могут программироваться в радиостанции заранее, однако, это является сложной и трудоёмкой задачей для больших радиосетей, так как требуется отзывать пользовательские радиостанции. Как показано на рисунке 9, технология OTAR позволяет избежать эту проблему, загружая ключ шифрования трафика TEK (Traffic Encryption Key) дистанционно, используя радиоинтерфейс. Сообщение, содержащие TEK, в свою очередь, защищается

ключом шифрования ключа KEK (Key Encryption Key). Ключ KEK должен быть известен как устройству управления ключами KMF, так и радиостанции. Для технологии OTAR может также применяться и ассиметричная криптография. В таком случае сообщение, содержащие TEK, зашифровывается открытым ключом радиостанции. Принимая сообщение, радиостанция использует свой закрытый ключ и получает ключ TEK [4,5].

Рисунок 9 – Два варианта программирования ключей в радиостанцию

9 Минимизация ПЭМИН

Наличие вышеперечисленных мер является необходим условием для защиты радиопереговоров, но эти меры могут оказаться недостаточными. Нарушитель может анализировать побочные излучения, которые могут быть промодулированы открытым речевым сигналом и которые могут появиться в результате конструктивных недостатков радиостанции в его аппаратной части. Открытый речевой сигнал может проникать в радиоэфир, модулируя частоту гетеродина и даже несущую частоту. Механизмы проникновения могут быть различными, например, через вибрации элементов радиостанции, вызванные голосом человека. Поэтому должен быть принят целый комплекс мер по аппаратной доработке радиостанции, направленный на локализацию ПЭМИН и подавлению нежелательных вибраций. Проверка возможных ПЭМИН должна

осуществляться на этапе сертификации СКЗИ.

Меры по минимизации ПЭМИН:

- экранирование опасных элементов
- покрытие опасных элементов виброгасящими материалами
- применение генераторов шума
- правильное размещение динамиков радиостанции
- установка специальных фильтров
- контроль питания

10 Организационные меры

Для предотвращения вероятности утечки речевой информации необходим контроль доступа к СКЗИ, в том числе путем ограничения физического доступа к СКЗИ на безопасное от перехвата побочных излучений расстояние. В процессе эксплуатации радиооборудования должны применяться специальные инструкции, исключающих нахождение посторонних лиц и размещение несанкционированной аппаратуры в ближней зоне оператора радиостанции. В соответствии с рисунком 10 выделяются три зоны безопасности. В зоне 1 запрещено размещение приёмопередающих устройств и сторонних проводников. В зоне 2 запрещено размещение связной аппаратуры, например телефонов, передатчиков, антенн. Зона 3 является контролируемой зоной, в которой исключено нахождение посторонних лиц. Зону 3 обозначим как ближнюю зону для оператора радиостанции. Подробное рассмотрение организационных мер выходит за рамки данной статьи.

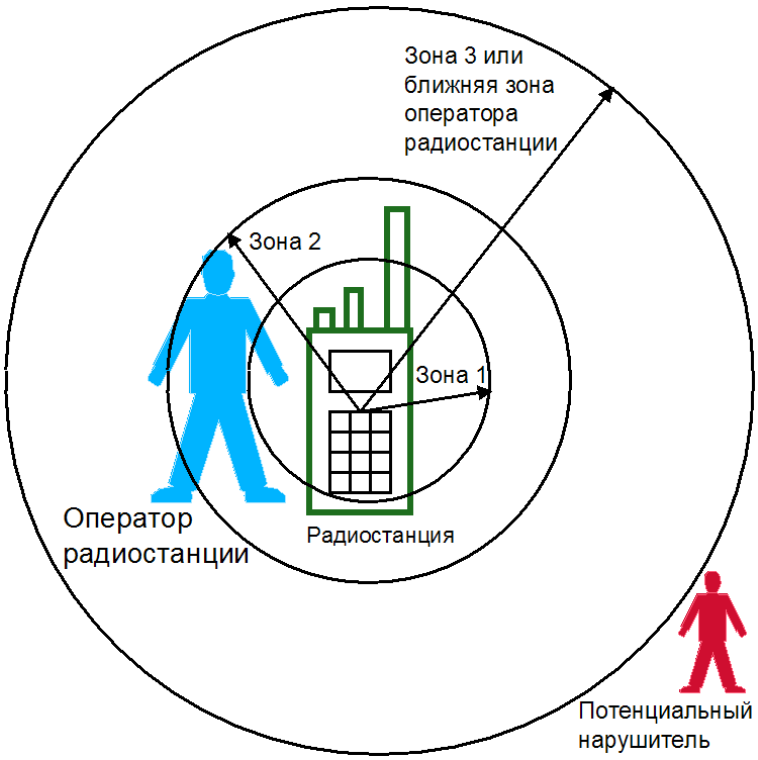


Рисунок 10 – Ограничение физического доступа к СКЗИ

Заключение

Для защиты радиосвязи нужно применять комплексный подход и учитывать все возможные угрозы информационной безопасности и нейтрализовывать их техническими и организационными мерами.

ЛИТЕРАТУРА

1. TIA/EAI Standard. ANSI/TIA/EIA 102.BAAA, Project 25 FDMA Common Air Interface, May 1998
2. TIA/EAI Standard. TSB102.AAAB, APCO Project 25 Security Services Overview, January 1996.
3. TIA/EAI Standard. IS102.AAAA-A, APCO Project 25 DES Encryption Protocol, February 1997.
4. TIA/EAI Standard. TSB102.AACA, APCO Project 25 Over-The-Air-Rekeying (OTAR) Protocol, January 1996
5. TIA/EAI Standard. TSB102.AACB, Over-The-Air-Rekeying (OTAR) Operational Description, January 1997.