ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ" (МГТУ ГА)

Кафедра основ радиотехники и защиты информации

В.Е. Емельянов, Э.А. Болелов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ГРАЖДАНСКОЙ АВИАЦИИ

Рекомендовано учебно-методическим объединением вузов Российской Федерации по образованию в области эксплуатации авиационной и космической техники для межвузовского использования в качестве учебного пособия

Москва – 2009

Содержание

Введение

Проблемы информационной безопасности отраслевых телекоммуникационных систем (ТКС) в нынешних условиях являются неотъемлемой частью деятельности всей авиационно-транспортной системы страны. Более того, в ряде случаев они стали важнейшими задачами обеспечения гарантированного уровня безопасности полётов наряду с экономической эффективностью деятельности отдельных авиапредприятий и авиакомпаний.

Активное обсуждение вопросов обеспечения информационной безопасности ТКС гражданской авиации (ГА) на проходящих научно-технических конференциях, совещаниях ИКАО свидетельствуют о большой актуальности многих ключевых проблем, связанных с серьёзными разрушительными последствиями при нарушении информационной безопасности (ИБ), недостаточной эффективностью средств защиты и т.д.

Внедрение в отраслевые структуры современных информационных технологий, даст, с одной стороны, существенный эффект в представлении пользователям современных услуг связи, получения оперативной и достоверной информации, а, с другой стороны, создаст эффект блокирования процесса информационного обмена и, как следствие, экономического, социального и других видов ущерба пользователю. Нарушители (злоумышленники), вторгающиеся в работу ТКС ГА, способны не только добывать циркулирующую в них информацию, но и искажать достоверность информации, например, о воздушной обстановке, параметрах самолётовождения, данных коммерческого характера и т.п., которые негативно скажутся на различных процессах управления и организации воздушного движения.

Вскрытие в используемых ТКС технологиях недостатков (уязвимостей), способствующих успешным действиям нарушителя, и принятие активных мер защиты по поддержанию устойчивого функционирования сетей связи в

условиях возможного воздействия нарушителя – являются основными задачами при решении проблем по обеспечению ИБ.

1. Задачи защиты информации в телекоммуникационных системах гражданской авиации

1.1. Особенности телекоммуникационных систем гражданской авиации

Большинство специалистов ИКАО предполагают, что дальнейшее развитие телекоммуникационных технологий будет реализовываться в направлениях увеличения скорости передачи информации, обеспечения мобильности пользователей и интеллектуализации сетей.

Высокие скорости необходимы для передачи информации в виде изображений, интеграции различных видов информации при её компенсировании в мультимедийных приложениях, организации связи локальных и специализированных сетей.

Интеллектуальность позволяет повысить оперативность и подлинность сети, упростит процессы управления.

Мобильность обеспечит реальность задачи предоставления услуг информационного обмена в любое время и в любом месте.

Вместе с тем необходимо отметить следующие, в случае, когда речь идёт о вычислительных сетях связи или системах вопросы защиты информации проработаны на высоком уровне и давно находятся в поле зрения высококвалифицированных специалистов. Однако в ГА существует большое количество разнородных средств, образующих специфические информационные системы. Так, например, на борту современных воздушных судов функционирует цифровой комплекс пилотажно-навигационного оборудования (КПНО), позволяющий решать весь круг задач самолётовождения. Для решения задач управления воздушным движением используются радиотехнические средства обеспечения полётов и электросвязи, позволяющие обеспечить управление воздушным движением (УВД) и его организацию (ОрВД). К ним относятся различные виды радиолокационного, радионавигационного и связного оборудования.

Отдельное место в этом перечне занимают автоматизированные системы (АС) УВД и спутниковые системы навигации и связи (ССНС).

Приведённое многообразие средств предопределяет, в свою очередь, широкую гамму методов и средств обеспечения информационной безопасности в них.

Развитие средств вычислительной техники (СВТ) и создаваемых на их основе АС УВД сделало актуальной задачу защиты информации от несанкционированного доступа, одним из актуальнейших методов разрешения которой является криптографическая защита.

Быстрое развитие вычислительной техники, компьютерных сетей, распределенных баз данных, когда возрастает ценность информации и достигается принципиальная возможность доступа к информации через глобальную сеть Интернет на первое место выходят задачи обеспечения безопасности информации, связанные с предотвращением несанкционированного доступа (НДС) к информации и других возможностей воздействия на информацию.

В этих условиях создаются защищённые операционные системы и программные средства, обеспечивающие защиту и разграничение пользователей информации в отдельных СВТ и распределенных информационных системах (компьютерных сетях). Одним из средств обеспечения ИБ в компьютерных сетях является использование «туннелированных» протоколов для канального, сетевого и сеансового уровней эталонной модели взаимодействия открытых систем (ЭМВОС). При информационном обмене с помощью туннелированных протоколов решается несколько задач защиты информации, обеспечивая взаимную аутентификацию, а также конфиденциальность, подлинность и целостность циркулирующих по туннелю данных.

В АС УВД и ряде иных специализированных отраслевых АС информация является средством обеспечения процесса принятия решения, доведения управляющих воздействий до объектов управления, например, ВС, и

получения сведений о результатах выполнения объектам управления выданных им управляющих воздействий и сбора сведений (в том числе диагностики контроля) о функционировании всей системы управления и её отдельных элементов.

Очевидно, что если передаваемая ими хранимая информация исполняется, доводится не своевременно, становится известной субъектам, заинтересованным в дезорганизации управления, процессу управления может быть нанесён ущерб. Представляется целесообразным рассматривать под защитой информации организационные и технические меры по предотвращению ущерба процессом управления, вызываемым любым воздействием на информацию при её хранении или передаче.

1.2. Уязвимость информации

На сообщения, представляющие различные виды сигналов и являющиеся переносчиками информации, при передаче их по каналам связи, коммутационной сети или хранящиеся в памяти ЭВМ могут различными путями производиться воздействия, приводящие к одному из видов ущерба для отправителя или получателя информации.

Можно представить следующую совокупность участников процесса обеспечения защиты информации при обработке соответствующего сообщения (передаче или хранении информации):

а) источники сообщения I_i, $i = \overline{1, N_1}$;

б) потребители сообщения L_j, $j = \overline{1, N_2}$;

в) прибор: передача-хранение Z - некий субъект, функцией которого является передача и (или) хранение сообщения от источника I_v получателю Z_q в требуемое время t в целостном виде;

г) субъект-злоумышленник – Y, имеющий ряд стратегий (моделей поведения) для нанесения ущерба сообщению;

д) информация в виде сообщения J_{egt} от источника I_v получателю Z_q во время t при допустимой задержке выдачи сообщения Δt.

Схематично указанный процесс изобразим на рисунке 1.1.

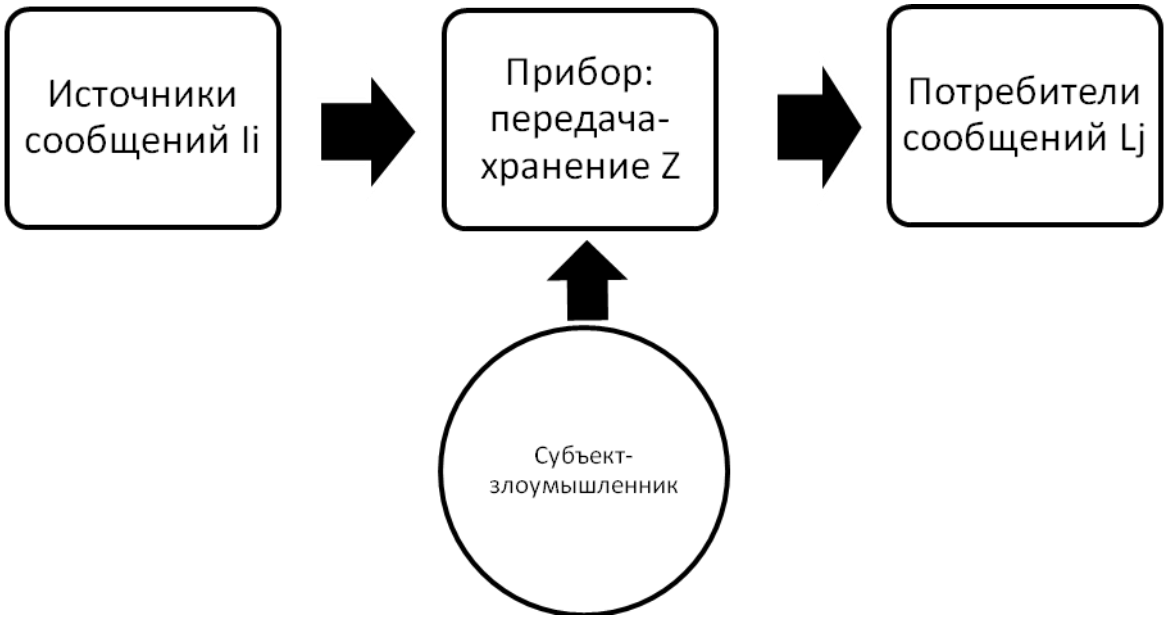

Рисунок 1.1.

Каждому из возможных видов ущерба, наносимого потребителю сообщений или владельцу хранящейся информации соответствует некоторая стратегия (или несколько стратегий) злоумышленника Y, направленная на достижение ущерба:

1. Недоведение (пропажа, потеря) сообщения, т.е.

$$J_{egt} \rightarrow O_{qt}, \quad (1.1)$$

где $\{O_{qt}\}$ - отсутствие переданной информации у получателя в интервале времени $\{t, t + \Delta t\}$. (1.2)

2. Доведения информации до получателя с не выявленным искажением:

$$J_{egt} \neq J^*_{egt}, \quad (1.3)$$

где $J^*_{egt} + J_{egt} = j_{egt}$ - вектор не выявленной ошибки в сообщении.

3. Ознакомление злоумышленника с содержанием сообщения, т.е.

$$J_{egt} \to Y. \tag{1.4}$$

4. Недопустимая задержка сообщения:

$$J_{egt} \to J_{egt2}, \tag{1.5}$$

где $t_2 > t + \Delta t$.

5. Переадресование сообщения:

$$\{J_{egt}\} \to L_l, l \neq g. \tag{1.6}$$

6. Переадресование сообщения с возвратом его в адрес отправителя:

$$\{J_{egt}\} \to L_{eet}. \tag{1.7}$$

7. Ввод ложной информации:

$$Y \xrightarrow{J_{egt}} L_{egt}. \tag{1.8}$$

8. Подмена информации:

$$\{J_{egt}\} \xrightarrow{J_{egt}} Y \xrightarrow{J^*_{egt}} \{L_{egt}\}. \tag{1.9}$$

9. Повторная передача сообщения или передача с неприемлемой для получателя задержкой:

$$\{J_{egt}\} \xrightarrow{J_{egt}} Y \xrightarrow{J_{egt2}} \{L_{egt}\}, \tag{1.10}$$

где $t_2 > t + \Delta t$.

Соотношения (1.1)-(1.10) можно использовать в любой физической среде функционирования ТКС, где существует возможность перечисленных выше вариантов атак на информационные потоки, в первую очередь в отдельных каналах связи, в сетях передачи данных, в меньшей степени – в локальных (корпоративных) сетях и блоке памяти процессорных устройств ПЭВМ.

1.3. Принципы квалиметрирования степени защиты информации

Установим возможную совокупность параметров для оценки степени ущерба от воздействия на информацию злоумышленника, под которым будем понимать либо природу, противодействующую передаче или хранению информации воздействием различных помех (ошибок), либо “противника“, т.е. активного субъекта, имеющего целый ряд стратегий воздействия на информационные сообщения, циркулирующие и формирующиеся в ТКС.

1. Недоведение информации возможно как из-за помеховых воздействий, уровень влияния, которых превышает возможности алгоритма передачи и защиты информации противостоять им, так и из-за активного воздействия приёмо-передающие тракты формирования и обработки информационных сообщений, среду (каналы) передачи и т.д.

Количественной оценкой в этом случае является вероятность $P_{\text{дов.}}(V, P_o, T)$, где P_o – параметр оценки воздействия помех, доведения до потребителя сообщения заданного объёма V в заданных условиях воздействия помех в течение заданного интервала времени T.

2. За счёт различных видов воздействия на информацию, защищаемую от искажений помехоустойчивыми кодами или в общем случае методами контроля и восстановления достоверности информационных сообщений, возможны ситуации, когда код не обнаруживает или не устраняет ошибки без отказа от декодирования оцениваемые вероятностью ошибки декодирования (необнаруженной ошибки, исправления с ошибкой - $P_{\text{ош.}}(P_{\text{но}}, P_{\text{ни}})$.

При задании начальных условий вероятность ошибки декодирования может определяться в пересчёте на один знак, на сообщение и т.д.

3. Способность парирования несанкционированного доступа к информации путём ее шифрования характеризуется стойкостью шифрования, оцениваемой соотношением времени, в течение которого сообщение считается конфиденциальным, и времени расшифровки сообщения.

4. Виды ущерба, перечисленные в пп. 4-7 предыдущего раздела (1.2), могут быть обусловлены искажением служебной области некоторого блока

(кадра) передаваемой информации либо целенаправленным воздействием злоумышленника.

В первой случае качество защиты оценивается вероятностью ошибки декодирования $P_{ош.}$, пересчитанной с учётом структуры передаваемой информации и особенностей алгоритма её передачи. Во втором случае злоумышленник может знать структуру передаваемой информации и алгоритм её обработки и его стратегий является имитация алгоритмически допустимых, но ложных по содержанию информационных ситуаций (например, данных о воздушной обстановке, распределению ВС по эшелонам и т.п.), от которых должен быть защищён получатель. Степень противодействия злоумышленнику оценивается допустимой вероятностью навязывания информации, которая может варьироваться для различных стратегий действий злоумышленника $P_{нав}$.

Пути решения задач защиты информации в соответствии с моделью уязвимости в рамках единого алгоритма обработки информации, существующие методы решения этих задач рассмотрены в [8].

Контрольные вопросы к разделу 1:

1. Приведите классификацию ТКС ГА.
2. Раскройте основные методы защиты информации в АС УВД.
3. Каким образом реализуется ИБ в СВТ?
4. Что понимается под защитой информации в ТКС ГА?
5. Приведите модель процесса защиты информации.
6. Раскройте параметры уязвимости ТКС.
7. Дайте определения параметров оценки степени защиты информации.
8. Каковы оценки качества защиты информации?
9. Какие новые аспекты ИБ определяются современными информационными технологиями?
10. К чему может привести нарушение ИБ при функциональном использовании ТКС ГА различного назначения?

2. Формирование политики безопасности

Основной для организации процесса обеспечения ИБ ТКС является принятая политика безопасности. Данная политика должна быть сформирована таким образом, чтобы определить, от каких именно угроз и каким образом защищается информация в объектах, вычислительной системе и т.д.

Под **политикой безопасности** понимается комплекс правовых, организационных и технических мер по защите информации, принятый в конкретном авиационном подразделении. Таким образом, политика безопасности подразделения описывает множество условий, при которых пользователи информации могут получить доступ к соответствующим ресурсам без потери свойства ИБ этой системы.

Политика безопасности должна быть оформлена в виде специального документа (или комплекса документов), с которым должны быть ознакомлены все пользователи.

С одной стороны, политика безопасности информирует пользователей о том, как правильно эксплуатировать систему, с другой – определяет множество механизмов безопасности, которые должны использоваться в каждом конкретном случае.

2.1 Процесс разработки политики безопасности

На рисунке 2.1 приведена возможная схема процесса разработки политики безопасности локальной вычислительной сети (ЛВС) некоторого подразделения. На представленном рисунке показано, что политика безопасности локальной вычислительной сети предприятия может быть представлена на трёх уровнях рассмотрениях.

На первом уровне агрегируется “информационная политика безопасности “. При этом чаще всего особенности ЛВС (как, впрочем, и иных ТКС) во внимание не принимаются. На I-ом уровне политика безопасности

выражается в самых общих терминах, например, “все информационные потоки в ЛВС должны иметь защиту от злоумышленного или непреднамеренного (случайного) доступа, изменения или задержки в представлении“. Объектом рассмотрения на данном этапе являются информация и принятые методы управления, принятые в авиапредприятии.

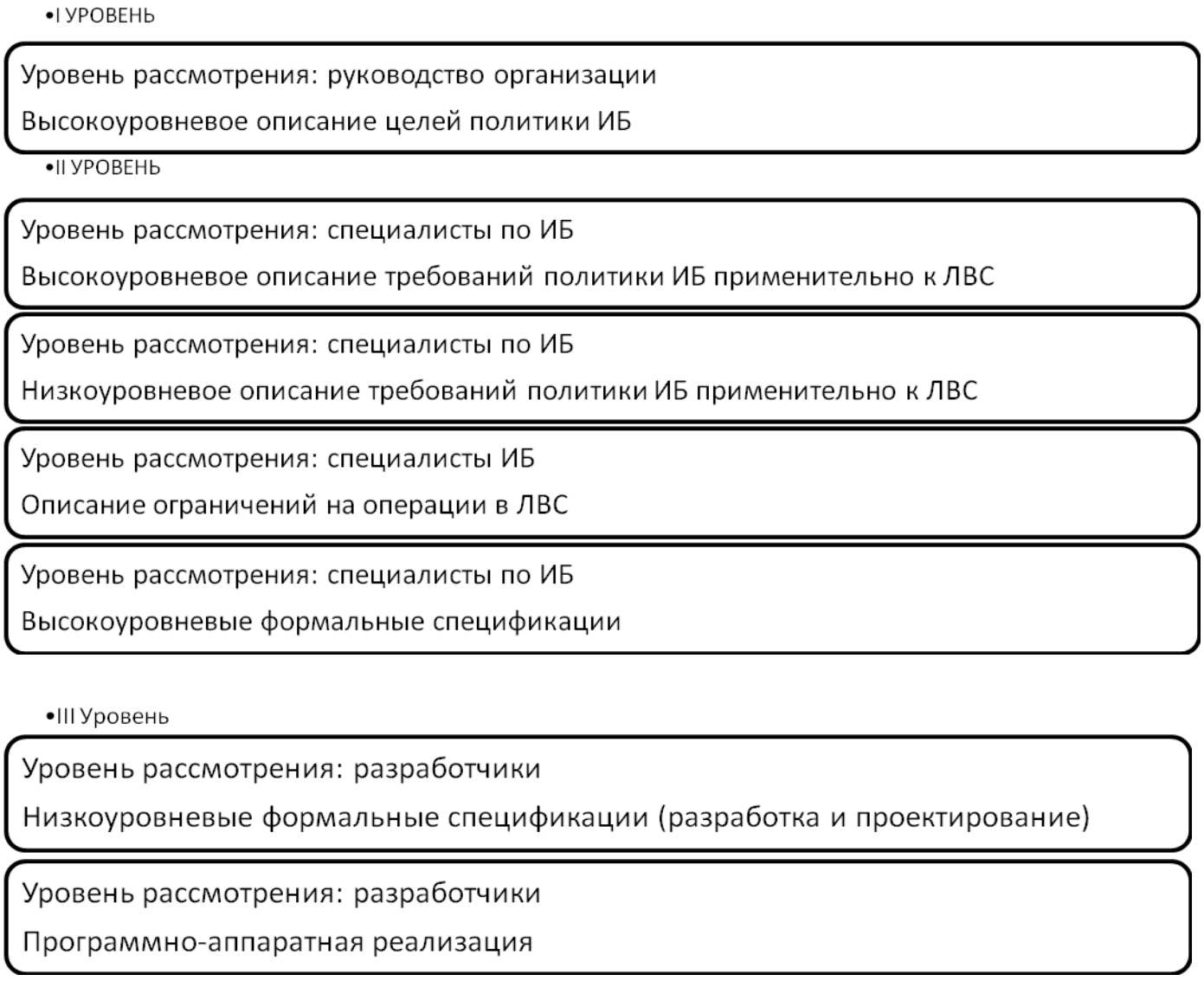

Рисунок 2.1.

Однако в ряде случаев для различных отраслевых структур раскрытие общих требований политики безопасности может иметь различные последствия. Процесс трансформации политики безопасности, принятой на

высоком уровне, включает выбор многих решений – от правил доступа к информации до определения программно-аппаратных решений и, по существу, представляет собой результат решения многокритериальной задачи оптимизации.

На втором уровне политика безопасности, сформулированная руководством авиапредприятия, обычно раскрывается инженерами по информационной безопасности ТКС, имеющим более глубокие знания о последних, чем управляющие структуры. Объектом рассмотрения политики безопасности становятся пользователи системы, для которых система представляется как программное обеспечение. На этом уровне формируется политика безопасности по отношению, как к ЛВС, так и СВТ. Кроме этого, на данном этапе определяются непосредственно политика разграничения доступа и вспомогательные политики безопасности.

И наконец, на третьем уровне политики безопасности, определённая специалистами (инженерами) по ИБ ТКС, непосредственно реализуется разработчиками системы. Объектом политики безопасности являются процессы в системе, а ЛВС рассматривается как множество серверов, представляемых компонентами системы пользователю. На данном уровне идентифицируются компоненты, ответственные за обработку запросов пользователей.

Необходимо отметить, что политики ИБ на различных уровнях должны быть полностью скоординированы, т.е. специалисты по информационной безопасности ТКС должны реализовывать только требования политики безопасности, предписанные руководством, а разработчики - требования, определённые инженерами по ИБ.

При разработке политики безопасности в указанном аспекте могут использоваться следующие правила [8,12].

1. Каждая операция, специфицированная политикой безопасности высокого уровня, должна поддерживаться политикой безопасности низкого уровня.

2. Ни одна из операций, разрешённых политикой безопасности низкого уровня, не должна, дополнять или изменять структуру политики высокого уровня.

Аргументация о соответствии представлений политики безопасности на различных уровнях может быть выражена с использованием следующих форм описания.

1. Естественный язык. К недостаткам этого способа можно отнести противоречивость и различные интерпретации положений политики безопасности, которые должны содержать чёткие определения попыток нарушения ИБ (риски).

2. Математическое формальное описание (на основе принятой математической модели). Уменьшает противоречивость естественного языка, позволяет использовать средства верификации политики безопасности. К недостаткам метода можно отнести его относительную сложность.

3. Нематематическое формальное описание. Промежуточное решение, приемлющее достоинства и недостатки описания с использованием естественного языка математического формального описания.

Таким образом, политика безопасности может агрегироваться и описываться как с использованием формального и неформального подходов, рассматриваемых ниже.

2.2. Неформальное представление политики безопасности

Широкое распространение для представления неформальных способов представления политик разграничения доступа получило описание правил доступа в табличном виде. Чаще всего такие таблицы подразумевают, что субъекты, объекты и типы доступов для данной системы определены. Это позволяет использовать систематизацию при построении таблиц с изображением одной колонки для различных типов доступа, определённых в

системе, и другой колонки, описывающей правила, регламентирующие доступ субъектов к объектам.

Описание поддерживающих политик ИБ целесообразно выполнять в виде списков, определяющих соответствующие требования.

В работе [8] приведены примеры неформального описания политики безопасности.

Рассмотрим описание политики разграничения доступа некоторой организации. На уровне её управления описание политики разграничения может выглядеть следующим образом: “информация при обработке и хранении должна быть защищена от неавторизованного раскрытия и модификации“.

Для формирования политики в форме высокоуровневых спецификаций разграничения доступа необходимо описать свойства и характеристики субъектов и объектов организации, а также операционные взаимоотношения субъектов и объектов системы.

Субъектов в системе принято характеризовать с помощью следующих понятий.

Степень доверия к субъекту – используется при доступе субъектов к информации с учётом классификации информационных ресурсов.

Необходимость доступа субъекта – признак, указывающий, что субъект имеет доступ к информационному ресурсу.

Ролевая функция субъекта – используется при описании соответствующих полномочий этого пользователя.

Группы, к которым относится субъект – используется при группировке пользователей с равными привилегиями.

Соответственно, объекты могут характеризоваться следующим.

Метка чувствительности объекта – используется при классификации информационных ресурсов, необходимой, в свою очередь, при определении относительной ценности информации и выработке мероприятий по сохранению данной ценности. Корректная классификация ресурсов обеспечивает максимальную стоимость информации для предприятия.

Для авиапредприятий чаще всего вся информация, создаваемая пользователем, должна иметь одну из следующих категорий: “конфиденциальная“, “для служебного пользования (ДСП)“, “свободно доступная“.

Раскрытие конфиденциальной информации может повлечь:

- нарушение отдельных секретов;
- причинение ущерба организации;
- уменьшение потенциала организации в конкурентной борьбе.

Информация ДСП – информация, которая используется соответствующими работниками для функционирования организации.

Свободно доступная информация – информация, которая может свободно распространяться для общественного использования через авторизованные каналы организации. Данная информация не предусматривает организацию контроля доступа.

1. Идентификатор объекта – может использоваться для определения источника информации или её владельца.

2. Метки атрибута объекта, используемые дискредиционной политикой доступа (списки контроля доступа, биты защиты и другие).

В качестве основных операций, выполняемых субъектами системы над объектами, можно выделить следующие:

1) создание объектов и задание атрибутов доступа к ним; в том числе классификация объектов;

2) периодическая корректировка классификации объектов; классификация информационных ресурсов имеет тенденцию к уменьшению с течением времени (конфиденциальная информация может стать информацией ДСП, а информация ДСП может стать общедоступной); если пользователь, создающий информацию, знает дату корректировки классификации информации, он может пометить её “конфиденциальная до…“;

3) уничтожение объектов;

4) чтение информации из объектов;

5) запись информации в объекты;

6) копирование объектов.

При описании ограничений на операции необходимо учитывать следующие внешние условия.

1) Расположение – разрешение доступа может основываться на действующем положении.

2) Время – разрешение доступа реализуется в отведённое время.

3) Иные условия.

Резюмируя, можно опираясь на вышеизложенное, составить таблицу, содержащую правила доступа субъектов системы к объектам (см. таблицу 2.1.).

Иным примером неформального описания политики безопасности служит описание политики безопасности использования электронных коммуникаций организации. В этом описании учитываются не только требования, соответствующие политике разграничения доступа, но и требования вспомогательных политик ИБ.

Описание содержит следующие положения.

1. Собственность. Под информационными сообщениями электронных коммуникаций понимаются речевая и электронная почта, а также факсы. Все сообщения, создаваемые и обрабатываемые с помощью электронных коммуникаций организации (включая дубликаты, резервные копии) принадлежат организации, а не пользователям электронных коммуникаций.

2. Авторизация. Система электронных коммуникаций используется только в коммерческих целях. Личное использование электронных коммуникаций возможно, если оно:

- занимает минимум ресурсов;
- не влияет на производительность труда;
- не влияет на бизнес-процесс.

3. Минимальные привилегии. Пользователям должен быть представлен минимум привилегий по использованию электронных коммуникаций, необходимых им для выполнения работы.

Таблица 2.1.

Операция	Конфиденциальная информация	Информация для служебного пользования	Общедоступная информация
1	2	3	4
Создание документов	Пользователь, создающий информацию, отвечает за её немедленную классификацию. Нежелательно присваивать информации классификацию сверх необходимости, т.к. это замедляет информационный обмен в организации	Пользователь, создающий информацию, отвечает за её немедленную классификацию. Нежелательно присваивать информации классификацию, т.к. это замедляет информационный обмен в организации	Пользователь, создающий информацию, отвечает за её немедленную классификацию. Нежелательно присваивать информации классификацию, т.к. это замедляет информационный обмен в организации
Маркировка документов	Документ должен идентифицировать владельца и быть отличен “конфиденциально“ на обложке или титульном листе	Отсутствие специальных требований	Документ должен быть отмеченным “общедоступный“ на обложке или титульном листе
Размножение документов	Осуществляется владельцем информации, определяющим полномочия доступа	Размножение только для деловых целей	Нет специальных требований

1	2	3	4
Посылка документов по почте	Отсутствие классификации на внешнем конверте. Метка “конфиденциально“ на обложке или титульном листе. Подтверждение о получении по требованию владельца информации	Требования определяются владельцем информации	Нет специальных требований
Уничтожение документов	Владелец наблюдает за уничтожением документов и невозможностью их восстановления	Контролируется физическое разрушение	Нет специальных требований
Хранение документов	Заперты, если не используются	Оригинал охраняется от уничтожения	Нет специальных требований
Доступ к документу	Владелец организует правила доступа к документу, обычно сильно ограниченные	Владелец организует правила доступа к документу, обычно широко доступные	Нет специальных требований. Доступность документов внутри и вне организации
Рассмотрение уровня классификации документа	Владелец определяет дату пересмотра классификации документа (не реже 1 раза в год)	Владелец пересматривает классификацию документа (не реже 1 раза в год)	Нет специальных требований

4. Разделение пользователей. Система должна по возможности разделять деятельность разных пользователей, распознаваемых с помощью идентификаторов пользователей и паролей.

5. Полномочия пользователей. Пользователи не должны разделять пароли или сообщения. При необходимости обмена полученными сообщениями следует использовать механизм распространения и другие авторизованные механизмы обмена информацией.

6. Отсутствие защиты по умолчанию. В системе не используется шифрование сообщений по умолчанию. При пересылке чувствительной к раскрытию информации она должна быть зашифрована или защищена с помощью аналогичных шифрованию технологий.

7. Уважение права на тайну. За исключением специально оговорённых ситуаций, пользователи не могут вмешиваться в нормальную работу системы электронных коммутаций с целью нарушения целостности или конфиденциальности сообщений. Организация должна уважать различную конфиденциальность сообщений пользователей, организуя защиту системы электронных коммутаций.

8. Отсутствие гарантий тайны сообщений. Организация не может гарантировать тайну сообщений. Пользователи должны быть осведомлены, что система электронных коммутаций базируется на технологиях, которые не могут дать полной уверенности в соблюдении конфиденциальности информации. В ряде особых случаев их сообщения могут быть доступны иным пользователям.

9. Регулярный мониторинг сообщений. Содержимое сообщений не просматривается регулярно. Однако такой мониторинг может быть реализован в целях безопасности коммерческой деятельности (бизнеса), а также при расследовании инцидентов. Пользователи должны быть проинформированы о возможности мониторинга.

10. Статистика. В организации должен постоянно осуществляться сбор статистических данных по использованию системы электронных коммутаций.

11. Раскрытие при происшествиях. Администратору системы может понадобиться просмотр сообщений при расследовании конфликтных ситуаций. При этом запрещается беспричинный просмотр сообщений.

12. Распространение сообщений. Вследствие того, что некоторые виды информации носят выборочный характер (определённые пользователи), необходимо аккуратно распространять сообщения. Служебная информация организации не должна распространяться за пределы системы электронных коммутаций организации без специального разрешения.

13. Удаление сообщений. Сообщения, необходимость которых для целей коммерческой деятельности исчерпана, должны периодически удаляться. По истечении определённого периода (обычно 6 месяцев) резервные копии сообщений удаляются. Если организация находится в особом режиме работы, то сообщения могут удаляться только по разрешению специально установленного лица.

14. Запрещена посылка спама, в том числе рекламных сообщений, без получения предварительного запроса.

15. Запрещается подделка заголовка сообщений электронной почты.

Приведённая политика безопасности сформулирована в виде списка требований. Требования, относящиеся к политике разграничения доступа, желательно определять отдельно.

Достоинством такого способа представления политики ИБ является то, что она легко понимается пользователем и значительно проще, чем формальное описание, для понимания которого требует соответствующий уровень математической подготовки. Это снижает вероятность атак на ЛВС по причине её некорректной эксплуатации вследствие непонимания принципов разработки системы.

Недостатком неформального описания политики ИБ, в первую очередь, является то, что при такой форме представления правил доступа в системе гораздо легче допустить логические ошибки при проектировании системы и её эксплуатации, приводящие к нарушению безопасности системы.

Необходимо отметить, что неформально могут быть описаны не только политики, но и модели безопасности. Примером неформального описания модели безопасности может служить модель Кларка-Вилсона [14].

2.3. Формальное представление политики безопасности

Требования формального описания характерно для систем, область применения которых критична. В частности, можно отметить тот факт, что для защищённых АСУ высокой степени подлинности необходимы формальное представление и формальный анализ системы [3].

Необходимо отметить, что значительная часть ТКС ГА попадает под вышеизложенные требования.

В соответствии с [19] модель защиты (безопасности) есть абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

К модели безопасности должны предъявляться требования, общие для всех моделей:

- адекватность;
- способность к прогнозированию;
- общность.

Для автоматизации процесса доказательства свойств системы используются так называемые “доказатели теорем“ [8] – программное обеспечение, проводящее формальную дедукцию на основе комбинации эвристик и непосредственного поиска. Иной вид программного обеспечения, используемый при формальном анализе систем, представляет собой так называемые “контроллеры доказательств“ – программы, представляющие пользователю возможность проводить последовательность шагов в процессе логических выводах о свойствах системы, но проверяющие корректность каждого шага. Естественно, наиболее эффективными средствами формального

анализа является средства, объединяющие свойства двух приведённых выше видов программного обеспечения.

Достоинством формального описания является отсутствие противоречий в политике безопасности и возможность теоретического обоснования ИБ системы при точном выдерживании условий принятой политики безопасности.

Можно предположить, что применение формальных методов для анализа систем, содержащих программно-математическое обеспечение, имеет недостаток, присущий всем методам моделирования: формальные методы исследуют не саму систему, а её модель, которая может не точно отражать реальные особенности функционирования или отражать их неадекватно.

Отмеченная проблема может возникнуть вследствие использования модели, учитывающей не все факторы, оказывающие непосредственное влияние на реальную систему. С другой стороны, излишняя детализация описания функционирования системы ведёт к значительному росту временных затрат на проведение формального анализа и, соответственно, к снижению эффективности применения данного метода.

Таким образом, возникает проблема корректного выбора уровня абстракции в описании модели безопасности (качественность её построения). Под уровнем абстракции понимается множество требований к реальной системе, которые должны найти своё отражение в модели для адекватного отображения моделируемой системы. Особое внимание необходимо обратить на популярные методы использования виртуальных моделей исследования функционирования систем, учитывая при этом многообразие возможных путей вариации состояний системы.

Недостатки использования формальных методов подробно рассмотрены в работах [8,12], в которой приведены следующие проблемы, возникающие в рассматриваемом случае.

1. Неразрешимость некоторых проблем безопасности с использованием формальных методов; в качестве примера часто приводят модель Харрисона-Руззо-Уильмана [8,12].

2. Использование формальных методов при разработке систем может привести к появлению системы, практическое использование которых затруднительно. В качестве примера в [12] упоминается участие автора в разработке СУБД Sea View; в данной СУБД для внедрения мандатной модели безопасности была исследована концепция (оправданная с теоретической, но не с практической точки зрения), состоящая в поддержании многочисленных составляющих значения поля базы данных (по одному для каждого уровня безопасности), что привело к серьёзным проблемам при реализации и неудобству использования СУБД.

3. Исследование формальных методов при проектировании систем приводит к удорожанию и увеличению временных затрат работы на разработку системы.

4. Многие нарушения ИБ происходят вследствие некорректного использования пользователями АСУ и СВТ; даже в том случае, если в основу разработки системы заложена самая стойкая модель безопасности и устранены все каналы утечки информации, безопасность системы может быть нарушена в результате использования “слабого“ пароля, ошибки реализации.

5. Модели ИБ не всегда обеспечивают безопасность реальной системы; безопасность обеспечивается только в рамках формальной модели, которая может быть упрощённой, но максимально приближённой к реальному исследуемому процессу (системе); любой выход за пределы модели влечёт нарушение безопасности.

С примером формального описания модели безопасности может служить модель Белла и Лападула [8,21,26].

Контрольные вопросы к разделу 2:

1. Сравните формальное и неформальное описание политики безопасности.

2. Для чего разрабатывается политика информационной безопасности?

3. Приведите схему процесса разработки политики безопасности.

4. Каково взаимоотношение политик ИБ на различных уровнях разработки?

5. Какими понятиями характеризуется субъект в системе информационного обмена?

6. Дайте характеристику объектов в информационной системе.

7. Приведите примеры операций, используемых в неформальном описании политики ИБ.

8. Какие требования представляются к моделям безопасности?

9. Каковы недостатки использования формальных методов описания ИБ?

10. Разработайте неформальную (формальную) политику безопасности для одной из ТКС ГА (по указанию преподавателя).

3. Обеспечения информационной безопасности телекоммуникационных систем гражданской авиации

Общие положения

Интенсивное развитие средств связи, в частности, спутниковых систем навигации и связи, автоматизированных систем УВД, источниками информации для которых являются радиолокационные и радионавигационные средства на ряду с широким внедрением информационных технологий во все сферы деятельности отраслевых структур различного назначения делают все более актуальной проблему защиты информации.

Проблема обеспечения безопасности информации передаваемой по разнообразным каналам связи является комплексной и характеризуется способностью информации противостоять различного рода воздействиям, наносящим ущерб собственнику информации. Эти воздействия могут быть различными. Например, некий злоумышленник (законный пользователь сети или постороннее лицо) может попытаться исказить передаваемую информацию путём воздействия на неё в любой точке тракта приемо-передачи, т.е. нарушить её достоверность (целостность). Он может попытаться извлечь из сети конфиденциальные сведения и т.п.

Система обеспечения ИБ – это совокупность различных мероприятий (правовых, организационных, технических), позволяющих существенно затруднить нанесение ущерба интересам потребителей информации. Реализация этих мер должна способствовать:

- обеспечению целостности информации (достоверности, точности, полноты);
- сохранению конфиденциальности информации;
- обеспечению доступа к информации со стороны пользователей, имеющих на то надлежащие полномочия.

Рекомендации МСЭ-Т определяют конфиденциальность, целостность и доступность как параметры безопасности передаваемой информации.

В [16] отмечено, что обеспечить защиту информации от всей гаммы воздействия со стороны злоумышленников нельзя. Поэтому для обеспечения ИБ необходимо проанализировать возможные угрозы безопасности и ущерб, который может быть нанесён собственнику информации из-за потери, хищения, искажения или задержки информации вследствие воздействия на процесс передачи информации.

Приведём наиболее характерные угрозы безопасности информации при её передаче [16]:

- перехват данных;
- анализ трафика;
- изменение потока сообщений (или одного сообщения);
- повтор процесса установления соединения и передачи сообщения;
- отказ пользователя от сообщения;
- маскарад;
- нарушение связи.

В ряде случаев, когда реализуется обработка сообщений (полностью или частично) и их хранение, возможны специфические угрозы:

- угрозы несанкционированного доступа в службу обработки сообщений;
- угрозу устройству хранения данных.

При этом предусматриваются следующие основные элементы защиты:

- шифрование данных;
- обеспечение аутентификации;
- обеспечение целостности данных;
- цифровая подпись;
- контроль доступа.

Механизм шифрования (криптографирования) может обеспечивать конфиденциальность либо передаваемых данных, либо информации о

параметрах трафика и может быть использован в иных механизмах безопасности. Наличие механизма шифрования, как правило, подразумевает использование механизма управления ключами.

При рассмотрении механизмов аутентификации особое внимание уделяется методам передачи в сети информации специального характера (паролей, аутентификации, контрольных сумм и т.п.). При односторонней или взаимной аутентификации обеспечивает процесс проверки подлинности пользователей (передатчика и приёмника сообщений), что гарантирует предотвращение соединения с логическим объектом, образованным злоумышленником.

Механизм обеспечения целостности данных предполагает введение в каждое сообщение некоторой дополнительной информации, функционально зависящей от содержания сообщения. В рекомендациях МОС рассматриваются методы обеспечения целостности двух типов: первые обеспечивают целостность единственного блока данных, вторые – потока данных или отдельных их полей. Отмеченные методы используются как при передаче данных по виртуальному соединению, так и при использовании дейтаграммной передачи. При первом варианте гарантируется устранение неупорядоченных потерь, повторов, вставок или модификации данных при помощи специальной нумерации блоков, либо введением временных меток. В дейтаграммном режиме временные метки позволяют обеспечить только ограниченную защиту целостности последовательности блоков данных и парировать переадресацию отдельных блоков.

Механизм цифровой подписи, реализующий отдельный процесс аутентификации пользователей и сообщения, используется для подтверждения подлинности содержания сообщения и удовлетворения того факта, что оно отправлено абонентом, указанным в заголовке в качестве источника данных. Цифровая подпись (ЦП) также необходима для парирования взаимности отказа передатчика от факта выдачи некоторого сообщения, а приёмника – от его регистрации.

Механизмом ЦП определяются две процедуры [9,16]:

- формирование блока данных, добавляемых к передаваемому сообщению;
- подписание блока данных.

Первая процедура содержит общедоступные способы и в ряде случаев специальные (секретные) ключи преобразования, известные на приёме.

Процесс подписания блока данных использует конфиденциальную (уникальную) информацию, он подразумевает либо шифрование блока данных, либо получение криптографического контрольного значения блока данных с использованием частной информации пользователя.

Механизм контроля доступа могут использовать аутентифицированную идентификацию объекта или информацию объекта либо возможности этого объекта для установления и применения прав доступа к нему.

Механизм заверения обеспечивает гарантию свойств, относящихся к данным, участвующим в информационном обмене, между двумя и более пользователями. Каждый процесс установления соединения может использовать цифровую подпись, шифрование и механизмы целостности в зависимости от требований услуги, получающей заверение. В случае использования механизма заверения, сообщения передаются через защищённые соединения и (или) нотариуса.

3.2. Правовые и организационные аспекты обеспечения информационной безопасности

В большинстве развитых странах мира уже давно применяются законодательные и административные меры для защиты информации на государственном уровне.

С введением нового Гражданского кодекса Российской Федерации впервые в нашем законодательстве информация стала полноправным объектом права (ст. 128 ГК РФ). Ещё большее усиление получило правовое обеспечение

деятельности по защите информации при принятии Федеральным Собранием России закона “Об информации, информатизации и защите информации“ и принятии Федерального Закона (ФЗ) РФ “О коммерческой тайне“.

В целом в области защиты информации на сегодняшний день приняты и действуют несколько десятков нормативно-правовых актов на различных уровнях.

Все действующие в настоящее время в РФ нормативные документы в области защиты информации в целом можно разделить на две большие группы, это:

- документы, составляющие нормативную правовую базу;
- документы, составляющие нормативно-техническую базу.

Нормативную правовую базу образуют документы, регулирующие правовую базу в области защиты информации. Эту базу образуют документы федерального уровня, к которым относятся:

- федеральные законы;
- указы президента Российской Федерации;
- постановления правительства Российской Федерации;
- государственные стандарты Российской Федерации.

К основным документам в этой области можно отнести следующие документы.

Законодательные акты.

- Конституция Российской Федерации (1993 г.).
- Закон Российской Федерации “О безопасности“ (1993 г.).
- Закон Российской Федерации “О сертификации продукции и услуг“ (1993 г.).
- Закон Российской Федерации “Об обеспечение средств измерений“ (1993 г.).
- ФЗ “Об участии в международном информационном обмене“ (1996 г.).
- ФЗ “О связи“ (1995 г.).

- ФЗ “О лицензировании отдельных видов деятельности“ (2001 г.).
- ФЗ “Об информации, информатизации и информационной безопасности“ (2007 г.).
- ФЗ “О коммерческой тайне“ (№ 98 от 29.07.2004 г.).

Нормативно-правовые акты Президента РФ.

- Концепция национальной безопасности РФ (2000 г.).
- Доктрина информационной безопасности РФ (2000 г. № Пр. 1985).
- Об основах государственной политики в сфере информатизации (от 20.01.1994г. № 170).
- Вопросы межведомственной комиссии по защите государственной тайны (от 20.01.1996г. № 71).
- Вопросы государственной технической комиссии при Президенте РФ (от 19.02. 1999г. № 212).
- О перечне сведений конфиденциального характера (от 06.03.1997г. № 188).

Постановления Правительства РФ.

- Положение о государственной системе защиты информации в РФ от иностранных технических разведок и от её утечки по техническим каналам (Извлечения)

(Постановление СМ Правительства РФ 15.09.1993 г. № 912-51).

- Положение о сертификации средств защиты информации

(Постановление Правительства РФ от 11.02.2001 г. № 135).

- Положение о лицензировании деятельности по технической защите конфиденциальности информации

(Постановление Правительства РФ от 30.040.2002 г. № 290).

- Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации

(Постановление Правительства РФ от 27.05.2002 г. № 348).

- Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти

(Постановление Правительства РФ от 03.11.1994 г. № 1233).

Государственные стандарты, используемые в области защиты информации.

- Стандарты, определяющие терминологию и общие положения по организации защиты информации – ГОСТ Р 50922-96; ГОСТ Р 51275-99.
- Комплекс стандартов и руководящих документов Госстандарта России на автоматизированные системы – ГОСТ Р 51583-200; ГОСТ 51241-98; ГОСТ Р ИСО 7498-2-99; ГОСТ 34003-90; ГОСТ 34201-89; ГОСТ 34601-90; ГОСТ 34602-89 и др.
- Стандарты по ЭМС, определяющие предельно допустимые уровни создаваемые ТС помех (ПЭМИН) и методы их испытаний – ГОСТ 22505-97; ГОСТ Р 51318.22-99; ГОСТ Р 51319-99; ГОСТ Р 51320-99 и др.
- Стандарт ЕСКД (ГОСТ 2.114-95; ГОСТ 2.601-95; ГОСТ 2.111-68 и др.) и ЕСПД.
- Санитарные правила и нормы, определяющие требования к предельным уровням ПЭМИН, создаваемые ТС – Сан П и Н 2.2.2.543-96 и др.

Указанные документы формируют механизм получения предприятиями и организациями (независимо от их организационно-правовой форме) лицензии на право осуществления любой деятельности, связанной с информацией, составляющей государственную тайну, а также общий подход сертификации средств, предназначенных для защиты секретной информации. Кроме этого, устанавливаются способы обеспечения информационной безопасности при работе с информационными потоками, содержащими различные виды конфиденциальной информации.

Перечисленные нормативные акты утвердили полномочия и компетенцию ФСТЭК в сфере лицензирования деятельности в области защиты информации и сертификации средств защиты информации.

Организационные аспекты включают в себя выработку политики информационной безопасности; анализ рисков (т.е., ситуаций, в которых может произойти нарушение нормальной работы информационной системы, а также

потеря или рассекречивание данных); планирование действий в чрезвычайных ситуациях; подбор средств обеспечения информационной безопасности.

Как уже отмечалось ранее политика информационной безопасности определяет:

- какую информацию и от чего (кого) следует защищать;
- кому и какая информация требуется для выполнения служебных обязанностей;
- какая степень защиты требуется для каждого вида информации;
- как организовать комплекс мероприятий по защите информации.

Решения по этим вопросам принимают руководители организаций, имеющих полномочия по решению задач, какой риск должен быть исключён, и на каком можно пойти, а также определять объём и порядок финансирования работ по обеспечению необходимого (установленного) уровня информационной безопасности.

Анализ рисков заключается в установлении, изучении и систематизации. Также формируются требования к средствам обеспечения информационной безопасности, и осуществляется выбор программно-аппаратных и технических решений.

По результатам анализа составляется отчёт, содержащий перечень рисков, упорядоченный по степени их “опасности“, и рекомендации по уменьшению уровня взаимных вероятностей появления опасных ситуаций.

Планирование обеспечения информационной безопасности заключается в подготовке и создании документа, содержащего описание мер, средств и способов обеспечения информационной безопасности. Этот документ определяет порядок проведения мероприятий, направленных на комплексную реализацию мер по обеспечению ИБ, которые должны быть утверждены руководством организации.

Планирование действий в чрезвычайной ситуации состоит в разработке документа, определяющего, за счёт каких резервных ресурсов будет обеспечено функционирование подразделения (организации) в условиях выхода из строя её

информационной системы или каких-либо средств автоматизации и связи, а также намечающего меры по восстановлению работоспособности этой системы. Основной для разработки плана действий в чрезвычайной ситуации являются результаты анализа рисков.

Средства обеспечения ИБ можно условно разделить на следующие группы:

- системы контроля доступа (управляют правами доступа пользователей, регистрируют обращения к защищённым данным, осуществляют аутентификацию пользователей и сетевых систем);
- системы шифрования (криптографирования) информации (кодируют данные, хранящиеся на локальных дисках пользователей и передаваемые по телекоммуникационным каналам);
- системы электронно-цифровой подписи (обеспечивают аутентификацию получаемой информации и контроля целостности);
- системы антивирусной защиты (контролируют состояние памяти вычислительных систем, предотвращают заражение файлов на локальных и сетевых дисках, а также распространение вирусов по сети);
- системы защиты firewall (реализуют авторизацию входящего и исходящего трафика между локальной (корпоративной) компьютерной сетью и Internet);
- системы защиты каналов связи и устройств обработки информации (снижают вероятность доступа злоумышленника к информационным потокам, чем обеспечивается целостность и достоверность информационных сообщений);
- системы резервного хранения и восстановления информации (обеспечивают дублирование информации на резервных носителях и, при необходимости, её восстановлении на жёстких дисках).

3.3. Технические аспекты обеспечения информационной безопасности

Криптографические методы и средства защиты. Методы криптографирования (шифрования) позволяют решить комплекс проблем, связанных с защитой информации. Своей целью они имеют обеспечение информации, содержащейся в сообщении, а также употребляются при аутентификации пользователей и обеспечении достоверности принимаемых сообщений. Исходное сообщение, над которым производится операция шифрования, называется открытым текстом, а результат шифрования – шифртекстом или криптограммой.

В криптографии обычно рассматриваются два типа криптографических алгоритмов [1,14]. Это алгоритмы, основанные на исследовании секретных ключей, и новые криптографические алгоритмы с открытым ключом, основанные на использовании закрытого (секретного) и открытого (двухключевые алгоритмы).

При использовании систем “одноключевой криптографии“ используется только одна единица секретной информации – ключ, знание которого позволяет открывателю зашифровать информацию (текстовое, графическое или речевое сообщение), а получателю – расшифровать. К наиболее известным стандартам относится стандарт по цифровой криптографии (DES – Digital Encryption Standart), принятый в США. Этот стандарт, в частности, определяет размер блока исходного текста в 64 бита и величину ключа 56 бит [1].

Классические (одноключевые) системы шифрования требуют для передачи ключа получателю информации “защищённого канала“, и если число взаимодействующих абонентов велико, то проблема обмена ключами становится весьма затруднительной. Действительно, в сети с N абонентами имеется $\frac{N(N-1)}{2}$ пар абонентов, каждая из которых требует свой ключ шифрования. Таким образом, в сети с числом абонентов $N = 10000$ потребуется $5 \cdot 10^7$ ключей, что, в свою очередь, серьёзно затрудняет их

распределение между абонентами. В связи с этим рекомендации МСЭ X.200, X.400, X.509 в качестве основного метода шифрования предложено использовать двухключевую систему шифрования (ДКСШ).

Использование ДКСШ технологии открытых ключей устраняет сложную проблему, возникающую в большой сети при распространении и хранении большого объёма секретных паролей. Особенностью данной технологии является то, что одновременно генерируется уникальная пара ключей, при этом текст, зашифрованный одним из них, может быть расшифрован только с использованием второго ключа, и, наоборот, каждый пользователь генерирует пару ключей, оставляя один закрытый у себя и никому никогда его не передаёт, а второй открытый передаёт тем, с кем ему необходимо защищённая связь. В случае необходимости собственной аутентификации (поставить электронную подпись) он шифрует текст имеющимся закрытым ключом и передаёт этот текст своим корреспондентам. Если им удаётся расшифровать текст открытым ключом этого пользователя, то становится ясно, что отправитель имеет в своём распоряжении парный закрытый ключ. Если пользователь желает получать засекреченные сообщения, то его корреспонденты зашифровывают их с помощью открытого ключа этого пользователя. Расшифровать эти сообщения может только сам пользователь с помощью своего закрытого ключа. При необходимости взаимной аутентификации и двунаправленного обмена общающиеся стороны генерируют собственную пару ключей и посылают открытый ключ своему корреспонденту.

Очевидно, что информацию об открытом ключе необходимо защищать от подлогов, чтобы злоумышленник под именем легального пользователя не навязал свой ключ.

В следующем разделе будут подробно рассмотрены наиболее распространенные криптографические алгоритмы

Методы и средства аутентификации пользователей и сообщения. Обеспечение подлинности взаимодействующих пользователей и сообщения (его целостности, достоверности) в ТКС заключается в обеспечении

возможности санкционированному терминалу-приёмнику, с определённой вероятностью гарантировать:

- что принятое сообщение действительно послано конкретным терминалом-приёмником;
- что не является дубликатом уже принятого сообщения (вставкой);
- что не произошло искажения информации, содержащейся в этом сообщении.

Зачастую решение этих задач объединяется понятием (термином) – аутентификация.

Существует большое количество методов аутентификации, включая различные схемы паролей, использование признаков и ключей, а также анатомически-физических признаков. Эти методы, за исключением использования ключей шифрования для целей аутентификации, в условиях телекоммуникационной системы связи, в конечном счете, сводятся к передаче идентификатора приёмнику, реализующего аутентификацию. Поэтому механизм аутентификации зависит от методов защиты информации для аутентификации и обеспечивающих парирования возможности раскрытия информации для аутентификации и обеспечивающих подлинность, целостность и упорядоченность сообщений.

Существуют различные подходы к разрешению проблемы аутентификации, которые в зависимости от используемой при этом системы шифрования могут быть разделены на следующие группы:

1) аутентификация с одноключевой системой шифрования;
2) аутентификация с двухключевой системой шифрования.

При этом под “используемой системой шифрования“ понимается наличие в ТКС подсистемы формирования и распределения ключей шифрования, обеспечивающей пользователей (передатчик и приёмник) соответствующими ключами шифрования и организующей контроль за хранением и порядком их использования.

Рекомендации МСЭ (X.400, X.509, X.800) содержат сведения, позволяющие считать перспективными способы защиты информации, базирующиеся на двухключевой системе шифрования. Основным преимуществом данного способа можно считать то, что секретные ключи шифрования в этой системе формируются и хранятся только пользователем, что, во-первых, органично соответствует пользовательскому восприятию своих собственных требований к формированию ключа шифрования и устраняет необходимость организации оперативно смены ключа шифрования вплоть до оптимальной: каждому сообщению новый ключ.

Разделение процедур шифрования даёт возможность абонентам сети связи регистрировать свои открытые ключи в периодически издаваемом справочнике, что, в свою очередь, позволяет обеспечить использование следующих простых протоколов:

1) один абонент может послать секретное сообщение другому абоненту, шифруя сообщение с помощью выбранного в справочнике открытого ключа абонента получателя. При этом только обладатель секретного ключа может верно расшифровать полученное зашифрованное сообщение;

2) Передающий абонент может зашифровать сообщение на своём секретном ключе. При этом любой приёмный абонент, имеющий доступ к открытому ключу, передающего абонента, может расшифровать полученное зашифрованное сообщение, получив подтверждение его истинности.

В одноключевой и двухключевой системах шифрования могут быть использованы алгоритмы избыточного кодирования с последующим обнаружением или исправлении ошибок при декодировании. Это позволяет уменьшить последствия воздействия несанкционированного воздействия на передаваемое сообщение.

Методы и средства управления доступом к информации и вычислительным ресурсам [10]. В ТКС ГА используется достаточно широкий спектр программно-аппаратных средств разграничения доступа, основывающихся на различных методах и подходах, в том числе на

применении криптографии. В общем случае функции разграничения доступа выполняются после установления подлинности пользователя. Поэтому для более полного анализа, возникающих при управлении доступа паролем, имеет смысл рассматривать аутентификацию пользователя как фазу механизма разграничения доступа.

В случае необходимости обеспечения в сети управляемого доступа к собственным ресурсам устройства управления, связанные с этими ресурсами, должны определённым образом определять и проверять подлинность пользователя, выставившего запрос. При этом доминантными представляются следующие вопросы:

- установление подлинности пользователей и устройств сети;
- установление подлинности процессов в сетевых устройствах и ЭВМ;
- проверка атрибутов установления подлинности.

В свою очередь, аутентификация пользователей может основываться на:

- дополнительных сведениях, известных полномочному пользователю (код, пароль и т.д.);
- средствах, действующих аналогично физическому ключу, открывающему доступ к системе;
- индивидуальных характеристиках конкретного лица.

Для повышения подлинности используются комбинации нескольких способов аутентификации пользователя.

С практической точки зрения наиболее удобны парольные схемы, т.к. не требуют специальной аппаратуры и выполняются с помощью программного обеспечения незначительного объёма. В простейшем случае все пользователи одной категории используют один и тот же пароль. В случае необходимости более строго установление подлинности каждый пользователь должен иметь индивидуальный секретный код.

При этом информационный профиль пользователя должен содержать:

- персональный код пользователя;

- секретный параметр доступа;
- возможные варианты работы в сети;
- категории контроля доступа к сетевым ресурсам.

Недостатком этого метода является возможность их использования без признаков того, что имело место нарушение ИБ.

Для более подробного ознакомления с системой защитой информации от несанкционированного доступа к данным, хранящимся и обрабатываемым на ПЭВМ под названием “Кобра“ (Комплекс обеспечения безопасности работ) можно порекомендовать обучаемым ознакомление с материалами, представленными в [5,10].

В следующем разделе более подробно будут рассмотрены технические методы обеспечения информационной безопасности в ТКС ГА.

Контрольные вопросы к разделу 3:

1. Раскройте сущность понятий: целостность информации, конфиденциальность и доступность.
2. Приведите наиболее характерные угрозы безопасности информации.
3. Какие механизмы защиты предусматриваются рекомендациями МСЭ?
4. Дайте краткую характеристику правовых и организационных аспектов ИБ.
5. Каковы недостатки криптографического метода, использующего одноключевые алгоритмы?
6. Что даёт использование двухключевых алгоритмов при криптографических методах защиты информации?
7. Каким ключом шифруется секретное сообщение в двухключевой системе?
8. Дайте краткую характеристику системе защиты информации “Кобра“.

9. Что даёт разделение процедур шифрования?
10. В чём заключается анализ рисков нарушения ИБ?

4 Основные технические методы обеспечения информационной безопасности в телекоммуникационных системах гражданской авиации

Каждая телекоммуникационная система (ТКС) гражданской авиации (ГА) использует свой комплекс методов и способов защиты информации, при этом можно выделить два основных направления защиты информации:

1) обеспечение безопасности информации;
2) защита от ошибок.

Комплекс методов обеспечения безопасности информации имеет целью сокрытые передаваемой информации (а по возможности и факта передачи информации) и недопущение навязывания ложной информации.

Комплекс методов по защите от ошибок имеет целью обеспечение доставки информации от источника сообщений к получателю сообщений в целостности и без искажений в условиях воздействия на ТКС как непреднамеренных, так и преднамеренных разрушающих воздействий различного происхождения.

4.1 Методы обеспечения безопасности информации

К комплексу методов обеспечения безопасности информации относятся [7]:

- криптографические методы защиты информации;
- электронная цифровая подпись;
- аутентификация.

Криптографические методы защиты информации.

Современные криптографические системы, под которыми понимается семейство обратимых криптографических преобразований открытого текста в

криптограмму, подразделяются на *симметричные* (*с секретным ключом*) и *ассиметричные* (*с открытым ключом*).

В симметричных криптосистемах для зашифрования и расшифрования используется один и тот же ключ.

В ассиметричных криптосистемах используются два ключа – открытый (публичный) и секретный (закрытый), которые математически связаны друг с другом. Информация зашифровывается с помощью открытого ключа, а расшифровывается с помощью секретного ключа, известного только получателю сообщения.

Рассмотрим основные симметричные и ассиметричные криптосистемы, которые находят в настоящее время наиболее широкое применение в ТКС.

Симметричные криптосистемы. На рисунке 4.1 представлена обобщенная структурная схема симметричной криптосистемы.

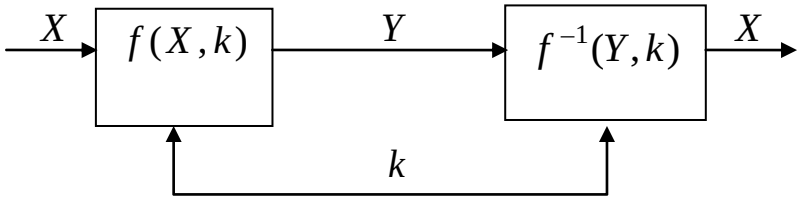

Рисунок 4.1

Перед использованием симметричной криптосистемы пользователи должны получить общий секретный ключ k и исключить доступ к нему злоумышленника (противника). Открытое сообщение X подвергается криптографическому преобразованию $f(X,k)$ и полученная криптограмма Y по открытому каналу связи передается получателю, где осуществляется обратное преобразование $f^{-1}(Y,k)$ с целью выделения исходного открытого сообщения X.

Симметричные криптосистемы классифицируются по различным признакам [1,2,14,20]: по виду криптографического преобразования; по

конструктивным принципам; по виду защищаемой информации; по криптографической стойкости и т.д. Чаще всего используются первые два признака классификации. В связи с этим множество симметричных криптосистем делится:

- по виду криптографического преобразования – на *шифры перестановки*, *шифры замены* и *композиционные шифры*;

- по конструктивным принципам – на *поточные криптосистемы* и *блочные криптосистемы*.

Под **шифром перестановки** понимается переупорядочение букв исходного сообщения, в результате которого он становиться нечитаемым.

Пусть имеется открытое сообщение $X = x_0 x_1 ... x_{n-1}$ длины n в алфавите A_X. Если к этому сообщению применить перестановку $\rho = (\rho(0), \rho(1),..., \rho(n-1))$, то результатом будет криптограмма $Y = y_0 y_1 ... y_{n-1} = x_{\rho(0)} x_{\rho(1)} ... x_{\rho(n-1)}$.

Ключом такого криптопреобразования является заданная перестановка. Шифры перестановки в настоящее время не используются в чистом виде, т.к. их криптостойкость невелика.

Под **шифром замены** (**подстановки**) понимается преобразование, которое заключается в замене букв исходного сообщения на другие буквы по более или менее сложному правилу.

Если имеется открытое сообщение $X = x_0 x_1 ... x_{n-1}$ длины n в алфавите A_X и правило замены $s = (s_0, s_1,.., s_{n-1})$, то применение этого криптографического преобразования к открытому сообщению дает криптограмму $Y = y_0 y_1 ... y_{n-1} = s_0(x_0), s_1(x_1),..., s_{n-1}(x_{n-1})$.

В зависимости от вида криптографической функции $s(\cdot)$ шифры замены делятся на шифры моноалфавитной замены и шифры многоалфавитной замены. **Моноалфавитные замены** – наиболее простой вид преобразований, заключающийся в замене по определенному правилу букв исходного сообщения на другие буквы из этого же алфавита, т.е. каждая буква исходного

текста преобразуется в букву криптограммы по одному и тому же закону. В случае **многоалфавитной замены** закон преобразования меняется от буквы к букве.

Необходимо заметить, что один и тот же шифр может рассматриваться и как моно-, и как многоалфавитная замена в зависимости от определяемого алфавита. Например, замена биграмм с точки зрения обычного алфавита является моноалфавитной заменой, а с точки зрения алфавита биграмм – многоалфавитным.

Поточные криптосистемы (шифры) относятся к шифрам замены, преобразующие посимвольно исходное сообщение в криптограмму.

Поточные криптосистемы представляют собой, по сути, разновидность гаммирования и преобразуют открытое сообщение в криптограмму последовательно по одному биту

$$y_i = x_i \oplus k_i, \qquad (4.1)$$

где k_i, $i = \overline{0, n-1}$ - ключевая последовательность; x_i и y_i, $i = \overline{0, n-1}$ - биты исходного сообщения и криптограммы, соответственно, $\oplus$ - операция сложения по mod2.

На приемной стороне операция получения исходного сообщения аналогична

$$x_i = y_i \oplus k_i. \qquad (4.2)$$

Стойкость поточных криптосистем целиком зависит от внутренней структуры генератора ключевой последовательности. В случае если генератор выдает ключевую последовательность небольшого периода, то стойкость поточной криптосистемы будет невелика. Напротив, если генератор выдает бесконечную последовательность истинно случайных (не псевдослучайных!) бит, то получаем поточную криптосистему с идеальной стойкостью.

Поточные шифры разделяются на **синхронные** (**СПШ**) и **самосинхронизирующиеся** (**ССПШ**).

Схема СПШ представлена на рисунке 4.2. Отправитель сообщения устанавливает заранее оговоренный ключ, в соответствии с которым генератор

ключевой последовательности (ГКП) формирует ключевую последовательность k_i. Шифрующий блок (ШБ) в режиме зашифрования формирует криптограмму y_i в соответствии (4.1), которая оправляется получателю. Получатель использует аналогичный ГКП, в который устанавливает тот же ключ. Шифрующий блок получателя в режиме расшифрования вычисляет открытый текст по криптограмме в соответствии с выражением (4.2).

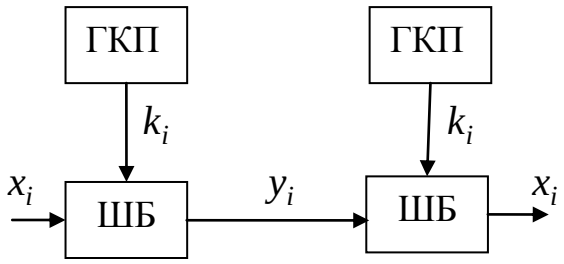

Рисунок 4.2.

В СПШ ключевая последовательность не зависит от открытого текста, поэтому СПШ функционирует исправно до тех пор, пока устройства, реализующие шифрование и расшифрование на концах линии связи, работают синхронно, т.е. не имеет места расшифрование символа криптограммы y_j с использованием символа ключевой последовательности k_i, $i \neq j$. Такие сбои, называемые *рассинхронизацией*, могут наступать из-за различных скоростей работы аппаратуры на приемном и передающем концах, удаления символов при передаче в канале связи и т.п.

Таким образом, основным недостатком таких систем является необходимость синхронизации ГКП на приемной и передающей сторонах.

Положительным свойством СПШ является отсутствие эффекта размножения ошибок, которые довольно часто возникают в канале передачи информации. Другим важным достоинством СПШ является их способность защищать передаваемое сообщение от вставок или удалений отрезков сообщения, т.к. в этих случаях произойдет рассинхронизация и «вмешательство» злоумышленника будет обнаружено. Вместе с тем СПШ не

вполне защищают от умышленной подмены отрезка сообщения на другой отрезок такой же длины.

Структурная схема ССПШ представлена на рисунке 4.3. Каждое внутренне состояние ГКП (за исключением первых n состояний) заполняется n предыдущими знаками криптограммы. Поэтому если n следующих подряд знаков криптограммы не подвергаются искажению при передаче по линии связи, то ГКП на приемной и передающей стороне устанавливаются в одинаковые внутренние состояния и, следовательно, вырабатывают одинаковые ключевые последовательности, т.е. происходит самосинхронизация.

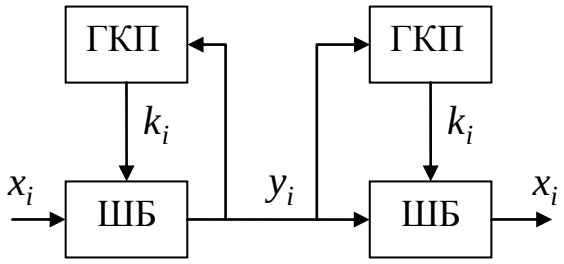

Рисунок 4.3.

Как правило, каждое шифруемое сообщение начинается не с содержательного текста, а со случайной последовательности из n символов, которая необходима для обеспечения самосинхронизации ССПШ.

Недостатком ССПШ является размножение ошибок, т.е. единичная ошибка в криптограмме порождает n ошибок в расшифрованной сообщении. ССПШ уязвимы к имитации сообщения. Так, например, злоумышленник может записать некоторое перехваченное сообщение и позже отправить его. После нескольких нестыковок в начале сообщения (до n символов) посланный отрезок расшифруется верно, и получатель не сможет определить, что принял устаревшее сообщение, в том случае если оно не содержит метки времени.

Достоинством ССПШ является отсутствие необходимости иметь специальные устройства обеспечения синхронизма.

Поточные криптосистемы наиболее пригодны для шифрования непрерывных потоков данных. Наиболее распространенными в настоящее время являются криптосистемы [1,14,20]: RC4, SEAL (Software Encryption ALgorithm), WAKE (Word Auto Key Encryption) и др.

Блочные симметричные криптосистемы (**БСК**) представляют собой семейство обратимых криптографических преобразований блоков исходного сообщения. Фактически блочная криптосистема - система замены на алфавите блоков (она может быть моно- или многоалфавитной в зависимости от режима использования блочного шифра). В настоящее время блочные криптосистемы наиболее распространены. Наибольшее распространение получили такие БСК как [1,14,20]: американский стандарт DES (Data Encryption Standard), американский стандарт AES (Advanced Encryption Standard) в основу которого положен алгоритм Rijndael, российский стандарт ГОСТ 28147-89, алгоритм IDEA (International Data Encryption Algorithm) и др.

Рассмотрим кратко и сравним наиболее часто используемые БСК – американский стандарт DES и российский стандарт ГОСТ 28147-89. Это выбор обусловлен тем обстоятельством, что в обоих БСК используется схема Фейстеля.

Схема Фейстеля представляет собой блочный симметричный шифр, криптографическая функция которого оперирует «половинами» входных блоков и имеет вид:

$$f(x_1, x_2, k) = x_2 \| \psi(x_2, k) \oplus x_1, \qquad (4.3)$$

где x_1 и x_2 - половины входного блока; $\psi(x_2, k)$ - функция усложнения; || - операция конкатенации.

На рисунке 4.4 представлена структура схемы Фейстеля. Варианты схемы Фейстеля отличаются конструкцией функции усложнения.

Криптосистема DES – итеративный 16-раундовый обратимый блочный шифр на основе схемы Фейстеля (см. рисунок 4.5). Размер входного блока - 64 бита. Размер ключа K – 56 бита. Раундовые ключи $k_1, k_2, ..., k_{16}$ есть алгоритмически вырабатываемые выборки 48 бит из 56 бит ключа K.

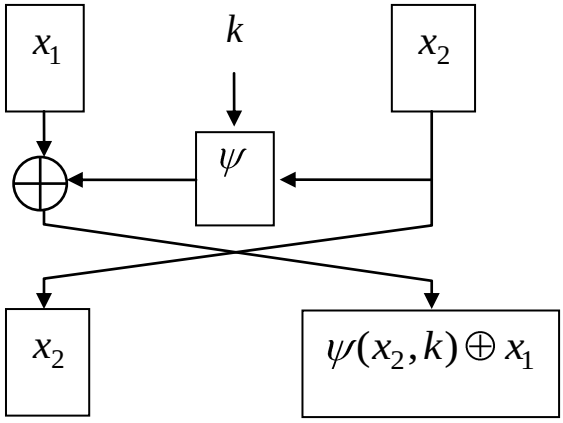

Рисунок 4.4.

Рисунок 4.5.

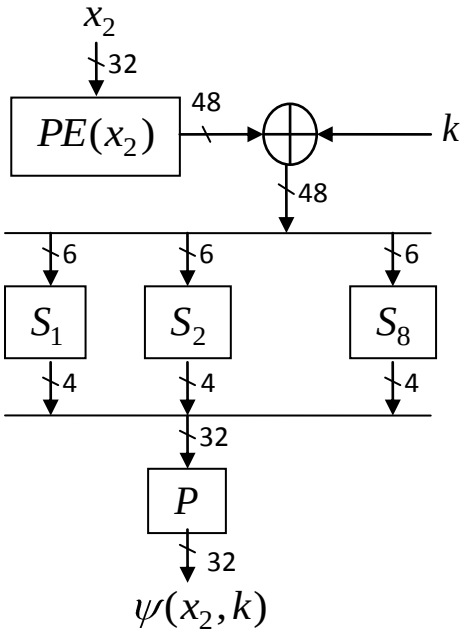

Рисунок 4.6.

Структурная схема функции усложнения представлена на рисунке 4.6. Функция усложнения $\psi(\cdot)$ состоит из следующих слоев:

1) перестановки с расширением РЕ 32 битового вектора до 48 битового вектора;
2) подмешивания 48 битового раундового ключа путем операции сложения по mod2;
3) нелинейной замены с помощью S-блоков 48 битового вектора на 32 битовый вектор;
4) перестановки Р координат 32 битового вектора.

Криптосистема ГОСТ 28147-89 – блочный 32 раундовый итерационный шифр на основе схемы Фейстеля. Российский стандарт формировался на основе мирового опыта и, в частности, были учтены недостатки и нереализованные возможности криптосистемы DES. Размер входного блока 32 бита, размер ключа K - 256 бит. Раундовые ключи $k_1, k_2, ..., k_{32}$ есть 32 битовые векторы, выбираемые из восьми независимых векторов $q_1, q_2, ..., q_8$ по правилу:

$$(k_1, k_2, ..., k_{32}) = (q_1, q_2, ..., q_8, q_1, q_2, ..., q_8, q_1, q_2, ...q_8, q_8, q_7, ..., q_1).$$

Функция усложнения представленная на рисунке 4.7 имеет следующие слои:

1) подмешивание 32 битового раундового ключа путем суммирования по $\mathrm{mod}2^{32}$;

2) нелинейную замену с помощью S-блоков, отображающих входные 4 битовых векторы в 4 битовые выходные векторы;

3) перемешивание координат 32 битового вектора с помощью циклического сдвига на 11 бит влево.

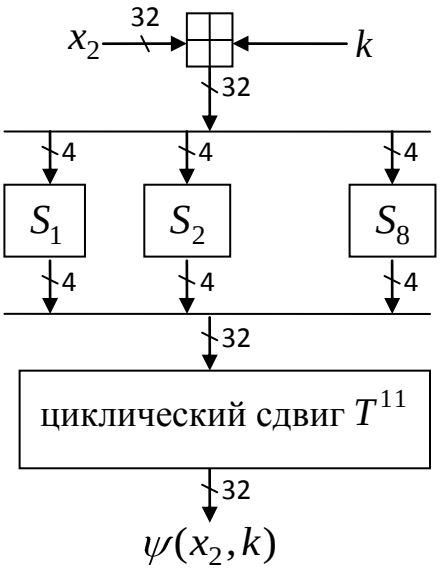

Рисунок 4.7.

Отличительной особенностью отечественной криптосистемы является то, что S-блоки выбираются для каждой сети отдельно и, по сути, служат долговременным ключом алгоритма.

Криптосистемы DES и ГОСТ 28147-89 являются стойкими алгоритмами шифрования, в том смысле, что все известные криптоанализа блочных криптосистем кардинально не отличаются по трудоемкости от метода полного перебора. Однако, так как у DES, по современным меркам, ключ слишком короткий, данный алгоритм уже не является надежным.

Что касается ГОСТ 28147-89, то на сегодняшний день не известно никаких реальных подходов, позволяющих дешифровать криптограммы, не имея ключа. Вместе с тем российский стандарт имеет ряд недостатков, общих с DES. Во-первых, на одном и том же ключе одинаковые 64 битовые блоки перейдут в одинаковые блоки криптограммы. Во-вторых, при использовании простой замены (S-блоки) легко незаметно произвести подмену одной криптограммы, или ее части, другой криптограммой (если они зашифрованы на одном ключе), можно также поменять местами отдельные участки одной криптограммы.

Асимметричные криптосистемы (системы с открытым ключом). На рисунке 4.8 представлена обобщенная структурная схема асимметричной криптосистемы.

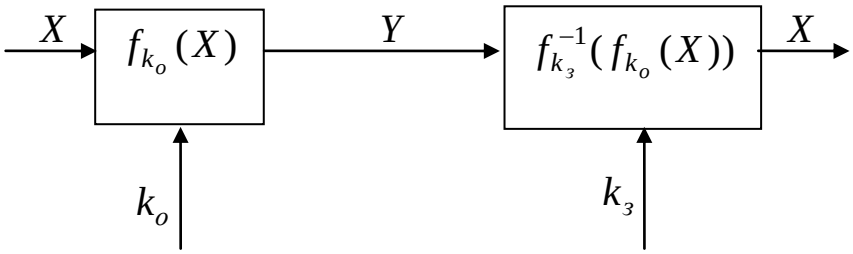

Рисунок 4.8.

Криптосистема с открытым ключом определяется тремя алгоритмами: генерации ключей, шифрования и расшифрования. Алгоритм генерации ключей открыт, всякий может подать на вход случайное число r требуемой длины и получить пару ключей $(k_o, k_з)$. Один из ключей k_o публикуется, он называется открытым, а второй $k_з$, называется закрытым (или секретным) и храниться в тайне. Алгоритмы шифрования $f_{k_o}(\cdot)$ и расшифрования $f_{k_з}^{-1}(\cdot)$ таковы, что для любого открытого текста X выполняется равенство $f_{k_з}^{-1}(f_{k_o}(X)) = X$.

Центральным понятием в теории асимметричных криптосистем является понятие односторонней функции [1,2,20]. Под **односторонней функцией** понимается эффективно вычисляемая функция, для обращения которой, т.е. поиска хотя бы одного значения аргумента по заданному значению функции, не существует эффективных алгоритмов. Необходимо заметить, что обратная функция может и не существовать. Собственно, односторонние функции в криптографии не используются. Практическое применение находят односторонние функции с секретом (односторонние функции с «лазейкой» или функции-ловушки). **Односторонней функцией с секретом** называется односторонняя функция, для которой обратную функцию вычислить просто,

если имеется некоторая дополнительная информация, и сложно, если такая информация отсутствует.

В качестве задач, приводящих к односторонним функциям можно привести следующие:

1) дискретное логарифмирование;

2) разложение числа на простые множители.

Наиболее известными и часто используемыми асимметричными криптосистемами являются криптосистема Эль-Гамаля и RSA (Ron Rivest, Adi Shamir, Leonard Adleman).

Криптосистема Эль-Гамаля – система с открытым ключом, основанная на проблеме дискретного логарифма.

Пусть имеется группа абонентов ТКС, которые хотят передавать друг другу зашифрованные сообщения, не имея защищенных каналов связи. Для всей группы выбираются некоторые большие простые числа p и g, такие что различные степени g суть различные числа по модулю p.

Каждый абонент группы генерирует свое секретное число $k_з$, $1 < k_з < p-1$, и вычисляет соответствующее ему открытое число $k_о$,

$$k_о = g^{k_з} \bmod p. \qquad (4.4)$$

Числа $k_о$ и $k_з$ являются открытым и секретным ключом, соответственно.

Алгоритм шифрования заключается в следующем.

Абонент А генерирует случайное число c, $1 \le c \le p-2$ и вычисляет:

$$l = g^c \bmod p, \qquad (4.5)$$

$$y = x \cdot k_o^B \bmod p \qquad (4.6)$$

и передает пару (y, l) абоненту В.

Абонент В, получив пару (y, l), вычисляет:

$$x = y \cdot l^{p-1-k_o^B} \bmod p. \qquad (4.7)$$

Криптосистема RSA – система с открытым ключом, основанная на задаче разложения числа на простые множители.

Пусть каждый абонент группы выбирает случайно два больших простых числа p и g, затем вычисляет:

$$N = pg, \tag{4.8}$$

$$\phi = (p-1)(g-1), \tag{4.9}$$

и выбирает число $k_o < \phi$, взаимно простое с ϕ. Далее по обобщенному алгоритму Евклида находят число $k_з$, такое, что

$$k_з k_o \bmod \phi = 1. \tag{4.10}$$

Пара $\{k_o, N\}$ и число $k_з$ являются открытым и секретным ключом, соответственно.

Алгоритм RSA состоит в последовательном выполнении следующих операций.

Абонент А шифрует сообщение в соответствии с выражением:

$$y = x^{k_o^B} \bmod N_B. \tag{4.11}$$

Абонент В, получив криптограмму расшифровывает ее используя выражение:

$$x = y^{k_з^B} \bmod N_B. \tag{4.12}$$

Алгоритм RSA находит широкое применение в системах мобильной связи.

Как уже отмечалось выше, все асимметричные криптосистемы основаны на функциях считающихся односторонними. Однако, следует заметить, что это свойство не было доказано не для одной из этих функций. Значит, теоретически возможно создание алгоритма, позволяющего легко вычислять обратную функцию без знания дополнительной информации (секрета). В этом случае криптосистема, основанная на этой функции, станет бесполезной.

Электронная цифровая подпись и аутентификация. В практической деятельности важно не только защищать информацию от злоумышленника, но и иметь возможность проверить авторство принятого сообщения и временя его

создания, а также проверить подлинность абонентов ТКС. Первая задача решается применением электронной цифровой подписи (ЭЦП), вторая – применением алгоритмов аутентификации [1,7,14,20].

Под **электронной цифровой подписью** понимается реквизит сообщения (электронного документа), предназначенный для его защиты от подделки и полученный в результате криптографического преобразования информации.

ЭЦП обеспечивает:

- подлинность источника сообщения;

- защиту сообщения от изменений.

- невозможность отказа от авторства.

Алгоритмы ЭЦП могут быть основаны как на асимметричных криптосистемах, так и на симметричных криптосистемах. Наиболее широкое распространение получили алгоритмы ЭЦП на основе асимметричных криптосистем, например, на основе рассмотренных выше алгоритмов Эль-Гамаля и RSA. При этом схема ЭЦП обычно включает в себя:

1) выбор параметров;

2) функцию вычисления подписи;

3) функцию проверки подписи.

Функция вычисления подписи на основе сообщения и секретного ключа абонента вычисляет собственно подпись. В зависимости от алгоритма функция вычисления подписи может быть детерминированной или вероятностной. Детерминированные функции всегда вычисляют одинаковую подпись по одинаковым входным данным, поэтому в настоящее время детерминированные схемы практически не используются. Вероятностные функции вносят в подпись элемент случайности, что усиливает криптостойкость алгоритмов ЭЦП. Однако, для вероятностных схем необходим надежный источник случайности, например, криптографический генератор, что усложняет их реализацию.

Поскольку подписываемые сообщения переменной длины (и достаточно большой), в схемах ЭЦП зачастую подпись ставится не на сам документ, а на

его хэш. Для вычисления хэша используются криптографические хэш-функции, что гарантирует выявление изменений документа при проверке подписи. Хэш-функции не являются частью алгоритма ЭЦП, поэтому в схеме может быть использована любая надежная хэш-функция.

Функция проверки подписи проверяет, соответствует ли данная подпись данному сообщению и открытому ключу пользователя. Открытый ключ абонента доступен всем, так что любой может проверить подпись под данным сообщением.

Рассмотрим самые популярные алгоритмы ЭЦП на основе криптосистем RSA и Эль-Гамаля.

ЭЦП на основе криптосистемы RSA. Вначале необходимо выбрать параметры алгоритма RSA. Для этого абонент А выбирает два больших простых числа p и g, и затем вычисляет N и ϕ в соответствии с (4.8) и (4.9).

Затем абонентом А выбирается число k_o, взаимно простое с ϕ, и вычисляется число:

$$k_з = k_o^{-1} \bmod \phi. \qquad (4.13)$$

Абонент А публикует числа k_o и N ассоциировав их со своим именем, а число $k_з$ хранит в секрете. Числа p, g и ϕ в дальнейшем не потребуются.

Теперь абонент А готов подписывать сообщение X. Для этого вначале он вычисляет хэш-функцию:

$$h_X = h(X). \qquad (4.14)$$

Алгоритм вычисления хэш-функции известен всем абонентам. Злоумышленник практические не может изменить основное сообщение не изменив при этом значение хэш-функции. Поэтому в дальнейшем абоненту А достаточно снабдить подписью не само сообщение, а только хэш h_X.

Затем абонент А вычисляет число:

$$s = h_X^{k_з} \bmod N, \qquad (4.15)$$

которое и является цифровой подписью.

Вычисленная цифровая подпись добавляется к сообщению $\langle X, s \rangle$. Каждый, кто знает открытые параметры абонента А, ассоциированные с его именем, т.е. числа k_o и N, может проверить подлинность его подписи.

Для этого необходимо вычислить значение хэш-функции в соответствии с (4.14) и затем вычислив число:

$$\eta = s^{k_o} \bmod N \tag{4.16}$$

проверить выполнение равенства $h_X = \eta$. Если подпись подлинная, то равенство выполняется, иначе подпись фальшивая или в подписанное сообщение внесено изменение.

ЭЦП на основе криптосистемы Эль-Гамаля. Как и в рассмотренном выше алгоритме вначале абонент А должен выбрать требуемые параметры криптосистемы Эль-Гамаля - большие простые числа p и g, такие что различные степени g суть различные числа по модулю p. Затем абонент А генерирует секретное число $k_з$, $1 < k_з < p-1$, и вычисляет соответствующее ему открытое число k_o в соответствии с (4.4). Абонент А публикует свой открытый ключ k_o.

Теперь абонент А готов подписывать сообщение X. Вначале абонент А вычисляет значение хэш-функции (4.14), которая должна удовлетворять неравенству $1 < h_X < p$. Затем абонент А выбирает случайное число k, $1 < k < p-1$, и вычисляет:

$$l = g^k \bmod p. \tag{4.17}$$

Далее абонент А вычисляет числа:

$$s_1 = (h_X - k_з l) \bmod (p-1), \tag{4.18}$$

$$s_2 = k^{-1} s_1 \bmod (p-1), \tag{4.19}$$

где k^{-1} удовлетворят уравнению:

$$k^{-1} k \bmod (p-1) = 1. \tag{4.20}$$

В заключении абонент А формирует подписанное сообщение $\langle X, l, s_2 \rangle$.

Получатель сообщения, прежде всего, заново вычисляет значение хэш-функции (4.14). Затем он проверяет подпись, используя равенство:

$$k_o^l l^{s_2} = g^{h_X} \bmod p. \qquad (4.21)$$

Если подпись верна, то условие (4.21) выполняется.

Вариант алгоритма Эль-Гамаля лежит в основе алгоритма DSA (Digital Signature Algorithm), на котором базируются американский стандарт ЭЦП FIPS 186 и российский стандарт – ГОСТ Р34.10-94.

Под **аутентификацией** понимается подтверждение подлинности абонента за счет проверки предъявленного им идентификатора.

Все возможные методы аутентификации [1,7] можно разделить на четыре группы:

1. Методы, основанные на знании некоторой секретной информации. Классическим примером таких методов является парольная защита. Данные методы являются наиболее распространенными.

2. Методы, основанные на использовании уникального предмета. В качестве такого предмета могут быть использованы: смарт-карта, электронный ключ и т.п.

3. Методы, основанные на использовании биометрических характеристик человека. На практике чаще всего используются:

- отпечатки пальцев;
- рисунок сетчатки и радужной оболочки глаз;
- голос;
- почерк;
- тепловой рисунок кисти руки;
- фотография или тепловой рисунок лица.

Методы, основанные на информации, ассоциированной с пользователем. Примером такой информации могут служить координаты пользователя, определяемые, например, с помощью GPS или ГЛОНАСС.

В последнее время всё чаще применяется, так называемая, расширенная или многофакторная аутентификация. Она построена на использовании

нескольких компонент, таких как: информация, которую пользователь знает (пароль), использовании физических компонентов (например, идентификационные брелки или смарт-карты), и технологии идентификации личности (биометрические данные).

В качестве примера рассмотрим механизм аутентификации, используемый в системе мобильной связи стандарта GSM. Каждый мобильный абонент на время пользования системой связи получает стандартный модуль подлинности (SIM-карту), которая содержит:

- международный идентификационный номер мобильного абонента (IMSI);

- свой индивидуальный ключ аутентификации K_i;

- алгоритм аутентификации (АЛГ-А).

Процедура аутентификации иллюстрируется на рисунке 4.9. Процедура проверки подлинности абонента реализуется следующим образом. Сеть передает случайный номер $RAND$ на мобильную станцию. Мобильная станция определяет значение отклика $SRES$, используя $RAND$, K_i и АЛГ-А. Мобильная станция посылает вычисленное значение $SRES$ в сеть, которая сверяет значение принятого $SRES$ со значением $SRES$, вычисленным сетью.

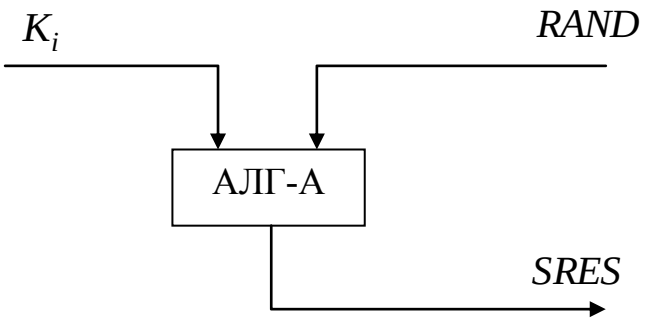

Рисунок 4.9.

Если оба значения совпадут, мобильная станция сможет осуществлять передачу сообщений. В противном случае связь прервется и индикатор мобильной станции покажет, что опознавание не состоялось. В интересах обеспечения безопасности вычисление $SRES$ происходит в рамках SIM-карты.

4.2 Методы защиты от ошибок

К основным мерам защиты от ошибок можно отнести [7, 15,17]:

- помехоустойчивое кодирование и перемежение символов;
- использование сигналов с расширенным спектром;
- изменение параметров сигнала;
- применение узконаправленных антенн.

Помехоустойчивым кодированием называется процесс введения избыточности в исходное сообщение [11,15,17]. Эта избыточность представляет собой помехоустойчивый код.

Помехоустойчивые коды делятся на два класса: коды для исправления ошибок и коды для обнаружения ошибок. Реализованные при этом методы являются взаимодополняющими в борьбе с ошибками.

Помехоустойчивые коды характеризуются следующими величинами:

1) коэффициентом избыточности, который характеризует обнаруживающие и исправляющие возможности кодов и определяется выражением:

$$K_И = 1 - \frac{\log_2 N_P}{\log_2 N_k}, \qquad (4.22)$$

где: $N_k = 2^n$; $N_p = 2^k$; n - длина кодовой комбинации; k - число информационных символов;

2) минимальным кодовым расстоянием $d_{\min}$, под которым понимается наименьшее из кодовых расстояний[1] всех возможных пар комбинаций данного кода. Если $d_{\min}$=1 - коды называются *первичными*, при $d_{\min} = 1 + n - k$ получаются коды с максимальным кодовым расстоянием;

[1] **Кодовым расстоянием** между двумя комбинациями одинаковой длины называется число элементов, которыми комбинации отличаются друг от друга

3) числом обнаруживаемых $\tilde{s} \le d_{\min} - 1$ и исправляемых ошибок $\tilde{t} = \dfrac{d_{\min} - 1}{2}$;

4) скоростью кода $R = \dfrac{n}{k}$;

5) вероятностью поступления кодовой комбинации с необнаруженной ошибкой $P_{нош}$:

- для канала с независимыми ошибками

$$P_{нош} \approx \frac{1}{2^{n-k}} \sum_{i=d_{\min}}^{n} C_n^i p^i (1-p)^{n-i}, \qquad (4.23)$$

- для канала с зависимыми ошибками

$$P_{нош} \approx \frac{p}{2^{n-k}} \left(\frac{n}{d_{\min}} \right)^{1-\alpha}, \qquad (4.24)$$

где α - параметр, характеризующий степень группирования ошибок (показатель группирования);

5) коэффициентом повышения достоверности

$$K_{пд} = \frac{P_{ош}}{P_{нош}}, \qquad (4.25)$$

который показывает во сколько раз уменьшается вероятность появления ошибочных кодовых комбинаций на выходе декодера по сравнению с вероятностью искажения кодовых комбинаций в канале связи и тем самым характеризует эффективность применение кода.

На рисунке 4.10 приведена обобщенная структурная схема ТКС применительно к передаче сообщений помехоустойчивыми кодами.

Для введения избыточности в первичное сообщение, поступающее от отправителя, необходимо специальное устройство – кодер. На выходе кодера формируется сообщение, представленное кодовым словом $\mathbf{X}$. Из-за наличия помех в канале связи отдельные символы в кодовом слове искажаются, поэтому на входе приемного устройства сигнал представлен кодовым словом:

$$\mathbf{Y} = \mathbf{X} \oplus \boldsymbol{\xi}, \qquad (4.26)$$

где ξ - вектор ошибок.

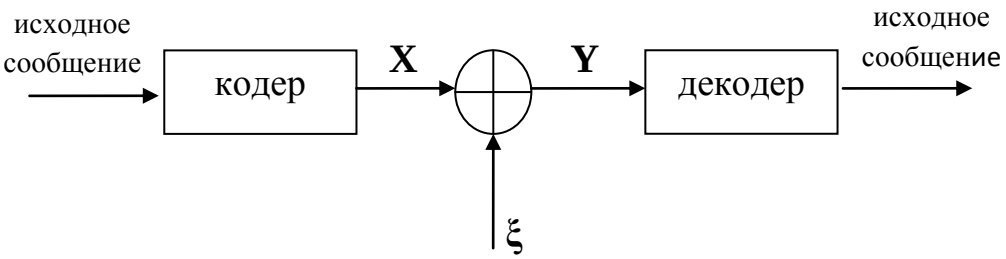

Рисунок 4.10.

В декодере осуществляется обнаружение и исправление ошибок, т.е. декодер анализируя $\mathbf{Y}$, должен решить какое $\mathbf{X}$ было передано, т.е. определить наиболее вероятный вектор ошибок ξ^*. После определения ξ^* декодер выдает оценку принятого сообщения

$$\mathbf{X}^* = \mathbf{Y} \oplus \xi^*, \qquad (4.27)$$

и далее на основании (4.27) - оценку исходного сообщения.

В настоящее время известны десятки помехоустойчивых кодов, которые теоретически могут обнаруживать или исправлять ошибки. Помехоустойчивые коды можно разделить на два больших класса: *блочные* и *непрерывные* (см. рисунок 4.11).

При блочном кодировании последовательность элементарных сообщений источника разбивается на отрезки и каждому отрезку ставится в соответствие определенная кодовая комбинация. Множество всех кодовых комбинаций, возможных при данном способе блочного кодирования, и есть блочный код.

Длина блока может быть как постоянной, так и переменной. Различают *равномерные* $n = const$ и *неравномерные* блочные коды. К неравномерным кодам относится код Морзе (редко используемые символы кодируются большим числом точек и тире). Помехоустойчивые коды являются, как правило, равномерными.

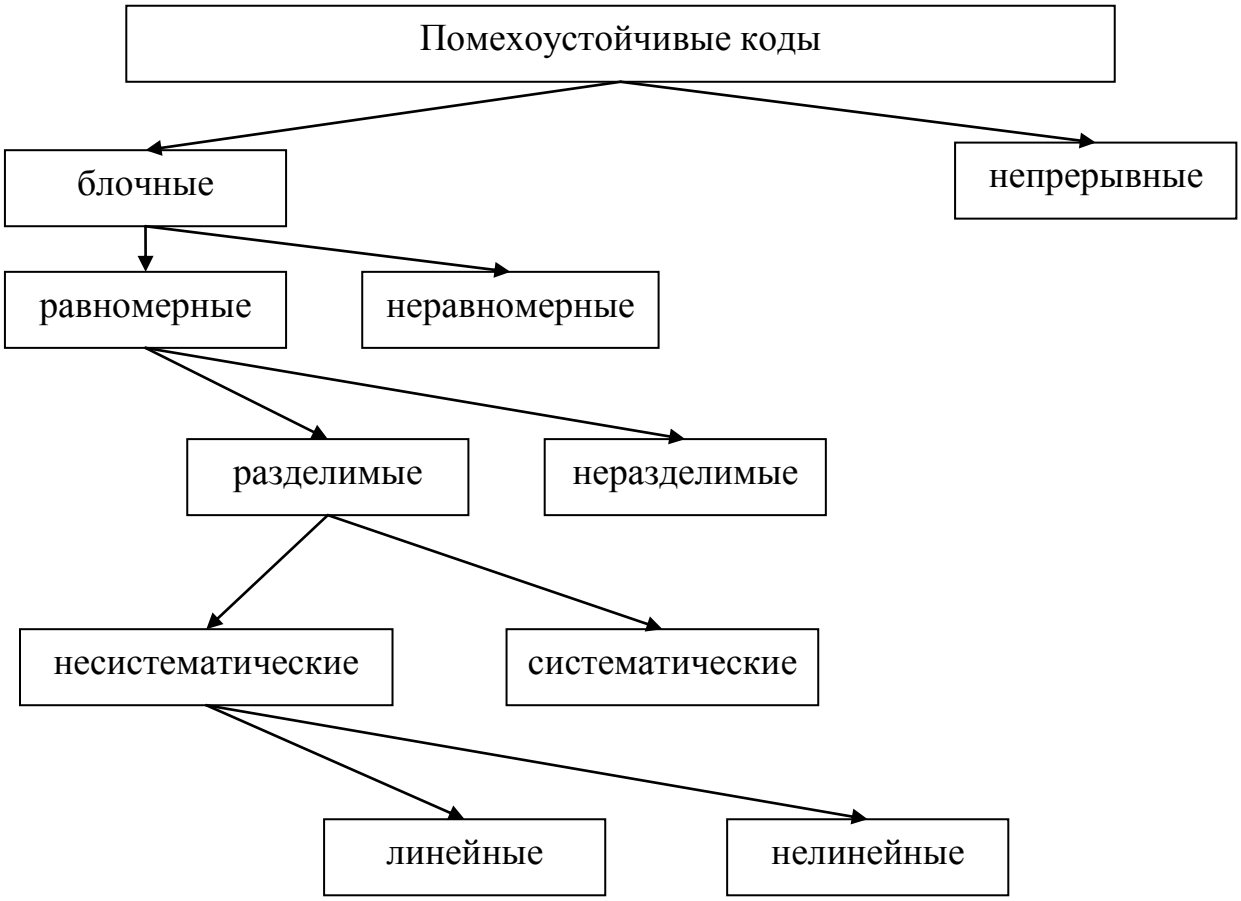

Рисунок 4.11

Блочные коды бывают *разделимыми* и *неразделимыми*. К разделимым относятся коды, в которых символы по их назначению могут быть разделены на информационные символы, несущие информацию о сообщениях и проверочные. Такие коды обозначаются как (n, k). К неразделимым относятся коды, символы которых нельзя разделить по их назначению на информационные и проверочные.

Среди разделимых кодов различают *систематические* и *несистематические*. Код называется систематическим, если первые k символов его любой кодовой комбинации являются информационными, остальные $(n-k)$ символов - проверочными. К несистематическим кодам относится код с постоянным весом. Коды с постоянным весом характеризуются

тем, что их кодовые комбинации содержат одинаковое число единиц: Примером такого кода является код «3 из 7», в котором каждая кодовая комбинация содержит три единицы и четыре нуля (стандартных телеграфный код №3).

Систематические коды делятся на *линейные* и *нелинейные*. Если избыточные элементы образуются применением к информационным элементам линейной операции, то такой код называется линейным, иначе код нелинейный.

Среди линейных систематических кодов наиболее простой код (n, n-k), содержащий один проверочный символ, который равен сумме по модулю 2 всех информационных символов. Этот код, называемый кодом с проверкой на четность, позволяет обнаружить все сочетания ошибок нечетной кратности.

Подклассом линейных кодов являются *циклические* коды. Они характеризуются тем, что все наборы, образованные циклической перестановкой любой кодовой комбинации, являются также кодовыми комбинациями. Это свойство позволяет в значительной степени упростить кодирующее и декодирующее устройства, особенно при обнаружении ошибок и исправлении одиночной ошибки. Примерами циклических кодов являются: коды Хэмминга, коды Рида-Соломона (РС-коды), коды Боуза-Чоудхури-Хоквингема (БЧХ - коды) и др.

Примером нелинейного кода является код Бергера, у которого проверочные символы представляют двоичную запись числа единиц в последовательности информационных символов.

Непрерывные коды характеризуются тем, что операции кодирования и декодирования производятся над непрерывной последовательностью символов без разбиения ее на блоки. Среди непрерывных наиболее применимы *сверточные* коды.

Перемежение символов представляет собой процедуру, обеспечивающую преобразование пакета ошибок в одиночные ошибки.

В ТКС мобильной связи (например, стандарта GSM) используются сверточное и блочное кодирование. Сверточное кодирование является мощным

средством борьбы с одиночными ошибками. В каналах с замираниями, что имеет место в системе мобильной связи, сверточное кодирование используется совместно с перемежением. Блочное кодирование главным образом используется для обнаружения нескорректированы ошибок.

Использование сигналов с расширенным спектром. Сигналами с расширенным спектром или **широкополосными** (сложными, шумоподобными) **сигналами** (ШПС) называют такие сигналы, у которых произведения активной ширины спектра Δf_c на длительность информационного символа T много больше единицы [17]. Это произведение называется **базой сигнала** B. Для ШПС

$$B = \Delta f_c T >> 1. \qquad (4.28)$$

Широкополосными сигналы иногда называют сложными в отличие от простых сигналов (например, прямоугольные, треугольные и т.д.) с $B = 1.$

Повышение базы в ШПС достигается путем дополнительной модуляции (или манипуляции) по частоте или фазе на времени длительности сигнала. В результате, спектр сигнала Δf_c (при сохранении его длительности) существенно расширяется. В системах связи с ШПС ширина спектра излучаемого сигнала Δf_c всегда много больше ширины спектра информационного сообщения.

ШПС получили применение в широкополосных системах связи (ШПСС), так как они [9,17]:

- обеспечивают высокую помехоустойчивость связи;
- обеспечивают скрытность передачи информации;
- обеспечивают высокую разрешающую способность по времени прихода сигнала;
- обеспечивают многостанционный доступ (связь многих абонентов в общей полосе частот);
- обеспечение электромагнитной совместимости (ЭМС).

Высокая помехоустойчивость ШПСС при воздействии как неорганизованных, так и организованных помех является их важнейшим свойством.

Помехоустойчивость приема сигналов на фоне широкополосной помехи типа белого гауссовского шума определяется только отношением энергии сигнала E_c к спектральной плотности шума $N_ш$ или помехи N_n:

$$q = \frac{2E_c}{N_ш} = \frac{2E_c}{N_n}, \qquad (4.29)$$

и не зависит от вида сигнала.

Поэтому при заданной спектральной плотности помех помехоустойчивость оптимального приема ШПС к широкополосным помехам равна помехоустойчивости оптимального приема узкополосных сигналов с этих условиях.

Однако, если задана не спектральная плотность помехи N_n, а мощность помехи P_n (в реальных условиях обычно существует ограничение на мощность передатчика помех) и ширина спектра помехи Δf_n поддерживается меньшей или равной ширине спектра сигнала Δf_c, то применение ШПС обеспечивает существенное увеличение отношение сигнал-помеха относительно узкополосных сигналов. Действительно, при $\Delta f_n = \Delta f_c$ и $\frac{N_n}{2} = \frac{P_n}{\Delta f_n} = \frac{P_n}{\Delta f_c}$ отношение сигнал-помеха на выходе корреляционного приемника (согласованного фильтра):

$$q = \frac{2E_c}{N_n} = \frac{P_c T}{\frac{P_n}{\Delta f_c}} = \frac{P_c}{P_n}\Delta f_c T = B\frac{P_c}{P_n}. \qquad (4.30)$$

Как следует из (4.30) отношение сигнал-помеха в ШПСС увеличивается пропорционально базе сигнала.

Скрытность передачи информации в ШПСС связана с уменьшением спектральной плотности сигнала в результате увеличения его базы. Действительно, спектральная плотность ШПС при фиксированной энергии

$$\frac{N_c}{2} = \frac{P_c}{\Delta f_c} = \frac{P_c T}{\Delta f_c T} = \frac{P_c T}{B}, \qquad (4.31)$$

т.е. в B раз меньше, чем у узкополосного сигнала при равных мощностях и скоростях передачи информации.

Отношение спектральной плотности сигнала N_c к спектральной плотности входных шумов разведывательного приемника N (внутренний шум и другие излучения)

$$\frac{N_c}{N} = \frac{2P_c}{N\Delta f_c} = \frac{1}{B}\frac{2E_c}{N}, \qquad (4.32)$$

мало (в B раз меньше чем у узкополосных сигналов). Следовательно, в точке приема ШПС разведывательным приемником при его неизвестной структуре вероятность обнаружения ШПС на фоне шума низкая (см. рисунок 4.12).

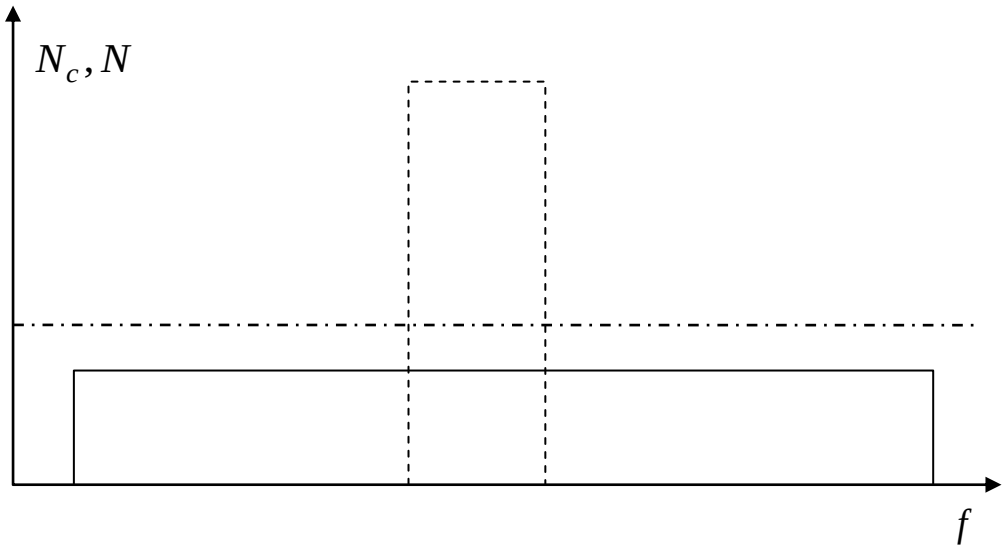

Рисунок 4.12.

На рисунке 4.12 представлены графические зависимости спектральной плотности сигналов с различными базами (пунктирная линия – узкополосный сигнал, сплошная линия – ШПС, штрихпунктирная линия – уровень входных шумов разведывательного приемника).

Эффект уменьшения спектральной плотности сигнала в B раз сказывается не только на скрытности передачи информации, но и позволяет обеспечивать *электромагнитную совместимость* ТКС.

Высокая разрешающая способность по времени прихода сигнала основана на том, что ШПС имеют корреляционную функцию с узким пиком, длительность которого обратно пропорциональна ширине спектра сигнала. Как известно [9,17], оптимальная обработка ШПС дает на выходе сигнал, пропорциональный корреляционной функции ШПС. Если принимаемые сигналы узкополосны, то на выходе согласованного фильтра образуются импульсы, которые накладываются друг на друга и отдельные лучи не разделяются (см. рисунок 4.13а,б).

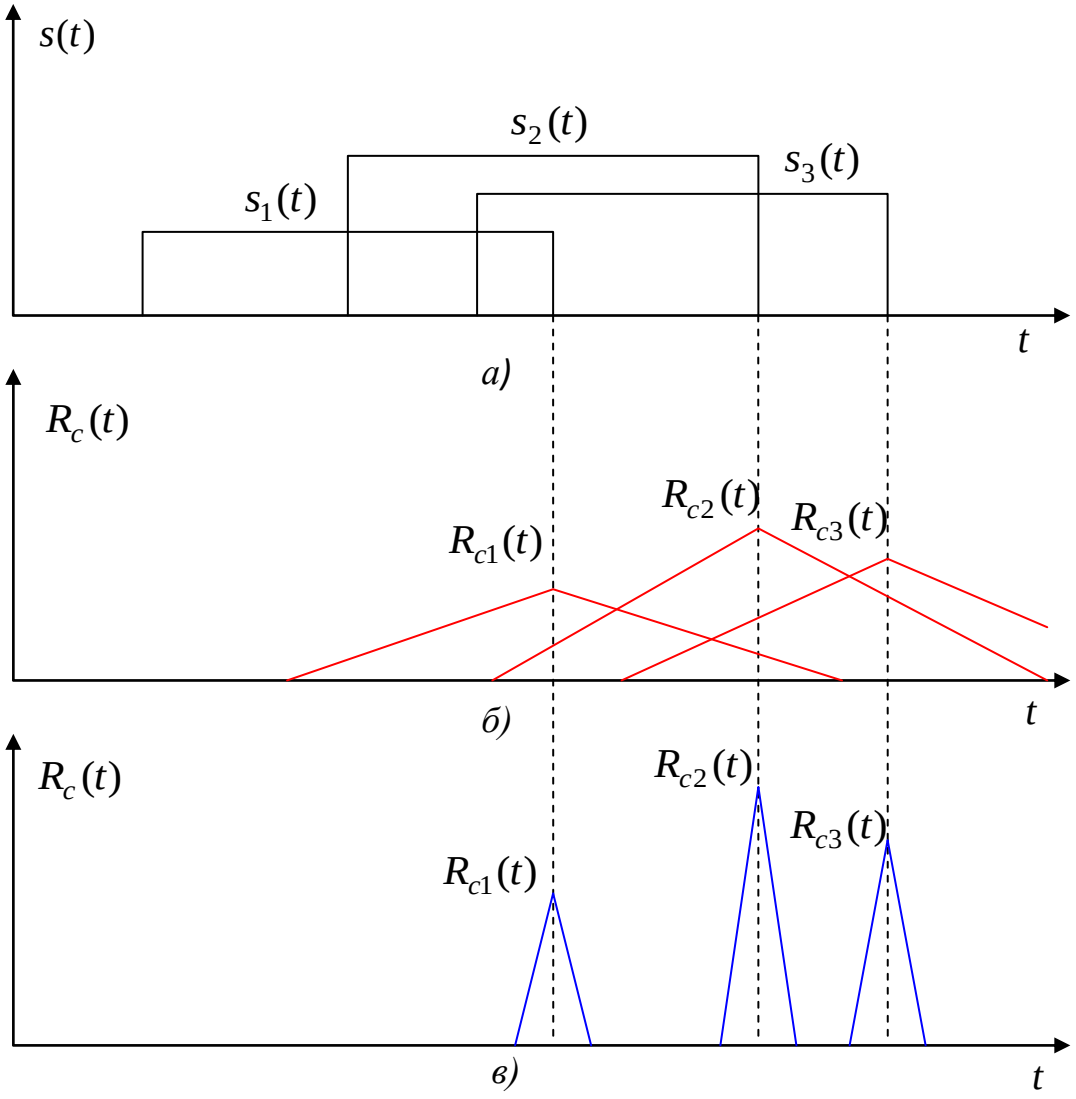

Рисунок 4.13.

Для ШПС, если выбрать полосу сигнала Δf_c такой, чтобы длительность свернутого импульса была меньше времени запаздывания соседних лучей, то можно осуществить раздельный прием одного или ряда запаздывающих лучей (см. рисунок 3.13в). Когерентно суммируя их отклики на выходе согласованного фильтра, можно не только устранить интерференцию, но и получить увеличение мощности принимаемого сигнала.

Из определения точности синхронизации ТКС [17] известно, что она определяется отношением сигнал-шум и шириной спектра сигнала, поэтому при заданной скорости передачи информации, чем больше база сигнала, тем точнее синхронизация.

Многостанционный доступ различных абонентов в общей полосе частот может быть обеспечен при кодовом разделении каналов на основе использования ШПС. В отличие от частотного разделения, когда абоненты осуществляют работу на разных частотах, и временного разделения, когда все абоненты занимают один частотный диапазон, но работают последовательно во времени, при кодовом разделении абонентам предоставлена возможность одновременно работать в общей полосе частот. При кодовом разделении отдельные абоненты имеют разные формы ШПС (расширение спектра осуществляется, как правило, за счет модуляции или кодирования, различных для каждого канала). Сигналы различных абонентов выбираются такими, чтобы они были приблизительно ортогональными:

$$\int s_i(t) s_j(t) dt \approx 0. \qquad (4.33)$$

Условие (4.33) выполняется при больших базах сигнала и соответствующим выбором кодирующей последовательности.

ШПС подразделяются на следующие виды [9]:

- частотно-модулированные (ЧМ) сигналы;
- многочастотные (МЧ) сигналы;
- фазоманипулированные (ФМ) сигналы (сигналы с кодовой фазовой модуляцией - КФМ сигналы);

- дискретные частотные (ДЧ) сигналы (сигналы с кодовой частотной модуляцией - КЧМ сигналы, частотно-манипулированные (ЧМ) сигналы);
- дискретные составные частотные (ДСЧ) сигналы (составные сигналы с кодовой частотной модуляцией - СКЧМ сигналы).

Частотно-модулированные (ЧМ) сигналы являются непрерывными сигналами, частота которых меняется по заданному закону.

База ЧМ сигнала по определению (4.28) равна:

$$B = \Delta f_c T = \Delta f_\partial T, \qquad (4.34)$$

где Δf_∂ - девиация частоты.

Частотно-модулированные сигналы нашли широкое применение в радиолокационных системах, поскольку для конкретного ЧМ сигнала можно создать согласованный фильтр на приборах с поверхностными акустическими волнами (ПАВ). В ТКС необходимо иметь множество сигналов. При этом необходимость быстрой смены сигналов и переключения аппаратуры формирования и обработки приводят к тому, что закон изменения частоты становится дискретным. При этом от ЧМ сигналов переходят к ДЧ сигналам.

Многочастотные (МЧ) сигналы являются суммой N гармоник $u_1(t),...,u_N(t)$, амплитуды и фазы которых определяются в соответствии с законами формирования сигналов. База МЧ сигнала совпадает с числом гармоник:

$$B = \frac{\Delta f_c}{\Delta f_0} = N, \qquad (4.35)$$

где $\Delta f_0 \approx \frac{1}{T}$ - ширина спектра элемента МЧ сигнала.

МЧ сигналы являются непрерывными и для их формирования и обработки трудно приспособить методы цифровой техники. Кроме этого недостатка, они обладают также и другими, например:

- у них плохой пик-фактор;

- для получения большой базы B необходимо иметь большое число частотных каналов N.

В связи с этим МЧ сигналы не находят широкого применения в ТКС.

Фазоманипулированные (ФМ) сигналы представляют последовательность радиоимпульсов, фазы которых изменяются по заданному закону. Обычно фаза принимает два значения (0 или π). При этом радиочастотному ФМ сигналу соответствует видео-ФМ сигнал, состоящий из положительных и отрицательных импульсов. Если число импульсов N_u, то длительность одного импульса равна $\tau_0 = \frac{T}{N_u}$, а ширина его спектра равна приближенно ширине спектра сигнала $\Delta f_0 = \frac{1}{\tau_0} = \frac{N_u}{T}$

База ФМ сигнала:

$$B = \Delta f_c T = \frac{\Delta f_c}{\tau_0} = N_u, \qquad (4.36)$$

т.е. B равна числу импульсов в сигнале.

Возможность применения ФМ сигналов в качестве ШПС с базами $B = 10^4 ... 10^6$ ограничена в основном аппаратурой обработки. При использовании согласованных фильтров в виде приборов на ПАВ возможен оптимальный прием ФМ сигналов с максимальными базами $B_{\max} = 1000 ... 2000$. ФМ сигналы, обрабатываемые такими фильтрами, имеют широкие спектры (порядка 10 ... 20 МГц) и относительно короткие длительности (60 ... 100 мкс). Обработка ФМ сигналов с помощью видеочастотных линий задержки при переносе спектра сигналов в область видеочастот позволяет получать базы $B = 100$ при $\Delta f \approx 1$ МГц, $T \approx 100$ мкс.

Весьма перспективными являются согласованные фильтры на приборах с зарядовой связью (ПЗС). С помощью согласованных фильтров ПЗС можно обрабатывать ФМ сигналы с базами $10^2 ... 10^3$ при длительностях сигналов $10^{-4} ... 10^{-1}$ с. Цифровой коррелятор на ПЗС способен обрабатывать сигналы до базы $4 \cdot 10^4$.

Следует отметить, что ФМ сигналы с большими базами целесообразно обрабатывать с помощью корреляторов (на БИС или на ПЗС). При этом,

B=4·10^4 представляется предельной. Но при использовании корреляторов необходимо в первую очередь решить вопрос об ускоренном вхождении в синхронизм. Так как ФМ сигналы позволяют широко использовать цифровые методы и технику формирования и обработки, и можно реализовать такие сигналы с относительно большими базами, то поэтому ФМ сигналы являются одним из перспективных видов ШПС.

Дискретные частотные (ДЧ) сигналы представляют последовательность радиоимпульсов, несущие частоты которых изменяются по заданному закону. Пусть число импульсов в ДЧ сигнале равно M, длительность импульса равна $\tau_0 = \frac{T}{M}$, его ширина спектра $\Delta f_0 = \frac{1}{\tau_0} = \frac{M}{T}$. Тогда база ДЧ сигналов

$$B = \Delta f_c T = M \Delta f_0 M \tau_0 = M^2, \qquad (4.37)$$

Из (4.37) следует основное достоинство ДЧ сигналов: для получения необходимой базы B число каналов $M = \sqrt{B}$, т. е. значительно меньше, чем для МЧ сигналов. Именно это обстоятельство и обусловило внимание к таким сигналам и их применение в ТКС. Вместе с тем для больших баз B=10^4 ... 10^6 использовать только ДЧ сигналы нецелесообразно, так как число частотных каналов M=10^2 ... 10^3, что представляется чрезмерно большим.

Дискретные составные частотные (ДСЧ) сигналы являются ДЧ сигналами, у которых каждый импульс заменен шумоподобным сигналом.

База ДСЧ сигнала, содержащего в качестве элементов ФМ сигналы (ДСЧ-ФМ сигнал):

$$B = \Delta f_c T = M^2 \Delta f_0 \tau_0 = N_{u0} M^2. \qquad (4.38)$$

Число импульсов полного ФМ сигнала $N_u = N_{u0} M$.

Если в качестве элементов ДСЧ сигнала можно взять ДЧ сигналы, учитывая, что база элемента ДЧ сигнала $B = M_0^2$, то база всего сигнала $B = M_0^2 M^2$. Такой сигнал можно сокращенно обозначать ДСЧ-ЧМ.

Наиболее перспективными ШПС для ТКС являются ФМ, ДЧ, ДСЧ-ФМ сигналы.

Еще одним методом повышения энергетической скрытности ТКС является **изменение (перестройка) параметров сигнала**, приводящее к снижению вероятности обнаружения сигнала благодаря уменьшению времени контакта средств радио- и радиотехнической разведки злоумышленника (противника) с сигналом ТКС [7,9].

Необходимость защиты информации, передаваемой в дискретных каналах радиосвязи, привела к появлению широкополосных адресных систем передачи данных (ШАСПД), в которых используются сигналы, максимально защищенные от разведки и воздействия помех за счет их формирования двойной модуляцией несущей: передаваемым информационным сигналом и широкополосным кодирующим сигналом.

Широкополосный кодирующий сигнал определяет программу (алгоритм) перестройки рабочих параметров (ПРП) сигнала. Каждая линия радиосвязи (ЛРС), организуемая ШАСПД, работает по своей программе ПРП, известной только абонентам данной ЛРС, что существенно усложняет задачу злоумышленника по обнаружения, приему и обработке сигналов данной ЛРС.

Следовательно, широкополосный кодирующий сигнал выполняет функции адреса конкретной ЛРС и может быть представлен некоторой несущей адресной последовательностью (НАП), определяющей изменение нулевых уровней параметров сигнала в рассматриваемой ЛРС. Несущая адресная последовательность представляет собой последовательность векторов $\vec{\alpha}(t)$, определяющих нулевой уровень параметров сигнала, и в общем виде может быть представлена выражением:

$$\vec{\alpha}(t) = \vec{\beta}(t), \gamma(t),..., \nu(t),$$

где $\beta(t), \gamma(t),..., \nu(t)$ - символы частных НАП, определяющих значения параметров сигнала в текущий момент времени t.

При синхронной перестройке параметров НАП может быть представлена выражением:

$$\alpha_i \rightarrow \beta_i, \gamma_i, ..., \nu_i ,$$

где α_i - символ НАП; $\beta_i, \gamma_i, ..., \nu_i$ - символы частных НАП на i-м шаге программы ПРП.

Таким образом, применение ТКС, использующих сигналы с ПРП, позволяет существенно усложнить задачу злоумышленника по обнаружению, пеленгованию, определению принадлежности источника радиоизлучения и осуществлению несанкционированного радиодоступа к передаваемой информации.

Контрольные вопросы к разделу 4:

1. Основные меры по обеспечению информационной безопасности ТКС ГА.
2. Симметричные и асимметричные криптосистемы.
3. Шифры замены и перестановки.
4. Блочные и поточные криптосистемы.
5. Криптосистема DES.
6. Криптосистема ГОСТ28147-89.
7. Понятие односторонней функции и односторонней функции с секретом.
8. Криптосистемы RSA и Эль-Гамаля.
9. Понятие электронной цифровой подписи.
10. Алгоритмы электронной цифровой подписи.
11. Понятие аутентификации.
12. Помехоустойчивое кодирование. Классификация помехоустойчивых кодов.
13. Основные характеристики помехоустойчивых кодов.
14. Понятие широкополосного сигнала.
15. Виды широкополосных сигналов.
16. Свойства широкополосных систем связи.

Литература

1. Баричев С.Г., Гончаров В.В. Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд. – М.: Горячая линия-Телеком, 2002.

2. Бабаш А.В., Шанкин Г.П. Криптгграфия. – М.: СОЛОН-ПРЕСС, 2007.

3. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А.. Основы информационной безопасности. М.: Горячая линия–Телеком, 2006.

4. Барсуков В.С.. Обеспечение информационной безопасности. (справочное пособие) // Технологии электронных коммутаций. М.: Эко трэнд. 1996, т.63.

5. Демин В.В., Суворов Е.В.. Интегрированная система информационной безопасности \\ Сети и системы связи, 1996. № 9. –с. 13-133.

6. Защита от несанкционированного доступа к информации. Термины и определения: Руководящий документ // Сборник руководящих документов по защите информации от несанкционированного доступа. М.: Гостехкомиссия России, 1998.

7. Защита информации в системах мобильной связи: Учебное пособие для вузов/А.А. Чекалин, и др., под обшей научной редакцией А.В. Заряева и С.В. Скрыля. – 2-е изд.. – М.: Горячая линия-Телеком, 2005.

8. Корт С.С.. Теоретические основы защиты информации. М.: Гелиос АРВ, 2004.

9. Кулаков В.Г., Гаранин М.В., Заряев А.В. и др. Информационная безопасность телекоммуникационных систем. (Технические аспекты). - М.: Радио и связь, 2004.

10. Лагутин В.С., Петраков А.В.. Утечка и защита информации в телефонных каналах. М.: Энергоатомиздат, 1996.

11. М. Вернер. Основы кодирования. Учебник для вузов. – М.: Техносфера, 2006.

12. Новиков А.А., Устинов Г.Н.. Уязвимость и информационная безопасность телекоммуникационных технологий. М.: Радио и связь, 2003.

13. Осмоловский С.А.. Стохастические методы защиты информации. М.: Радио и связь, 2003.

14. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2005.

15. Р. Морелос-Сарагоса. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2006.

16. Телекоммуникационные системы и сети. Современные технологии. Том 1/ Под ред. В.П. Шувалова. М.: Горячая линия – Телеком, 2004.

17. В.И. Тихонов. Авиационные радиосвязные устройства. - М.: ВВИА им. Н.Е. Жуковского, 1986.

18. Угрозы безопасности информации – ГОСТ 51632 – 00. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.

19. Устинов Г.Н.. Обеспечение безопасности информации при её передаче в телеметрических службах // Технологии электронных коммутаций. М.: Эко-Тренд, 1993. – т.33.-с.244…288.

20. Фомичев В.М. Дискретная математика и криптология. Курс лекций/ Под общ. ред. Н.Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003.

21. D. Denning. The Limits of Formal Security Models. National Computer Systems Security Award Acceptance Speech, 1999.

22. M. Harrison, W. Ruzzo, J. Uhlman. Protection in operating systems. Communication of the ACM, 1976.

23. M. Harrison, W. Ruzzo. Monotonic protection systems. Foundation of secure computation, 1978.

24. J. McLean. A comment on the “ Basic security Teorem“ of Bell and La Padula, Information Processing Letters, 1985.

25. P. Ning, S. Jajodia, X. Wang. Abstraction based Intrusion Detection in Distributed Environments. 2000.

26. G. Vert, D. Frincke, J. McConnell. A Visual Mathematical Model for Intrusion Detection, Proc. 21st NIST – NCSC National Information Systems Security Conference, 1998.

27. A. Ghosh, A. Schwartzbard, M. Schatz. Learning Program Behavior Profiles for Intrusion Detection Proceedings 1st USENIX Workshop on Instusion Detection and Network Monitoring, 1999.

28. M. Howard, D. Leblanc. Writing secure code, 2nd.ed. – Microsoft Press, 2003.