ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра технической эксплуатации
радиоэлектронного оборудования воздушного транспорта

Э.А. Болелов

КИБЕРБЕЗОПАСНОСТЬ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ РАДИОПОДАВЛЕНИЮ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

Учебное пособие

Утверждено редакционно-издательским советом МГТУ ГА в качестве учебного пособия

Москва
ИД Академии Жуковского
2024

УДК 004.056:623.746.-519
ББК 6Ф3
Б83

Печатается по решению редакционно-издательского совета
Московского государственного технического университета ГА

Рецензенты:
Кудинов А.Т. (МГТУ ГА) – канд. техн. наук;
Полосин С.А. (ФАУ «ГосНИИАС») – канд. техн. наук

Болелов Э.А.

Б83 Кибербезопасность беспилотных авиационных систем. Методы и средства обеспечения кибербезопасности и противодействия радиоподавлению беспилотных авиационных систем [Текст] : учебное пособие / Э.А. Болелов. – М. : ИД Академии Жуковского, 2024. – 80 с.

ISBN 978-5-907863-46-0

В учебном пособии рассматриваются теоретические методы, а также приводятся данные о средствах обеспечения кибербезопасности и противодействия радиоподавлению беспилотных авиационных систем. Особое внимание уделено вопросам криптографического обеспечения кибербезопасности беспилотных авиационных систем и методам помехоустойчивого кодирования информации для противодействия радиоподавлению беспилотных авиационных систем.

Для каждого раздела приведены вопросы для самопроверки (два уровня обученности). По всем темам рассматриваются примеры. Материал изложен в логической последовательности, понятным языком, содержит пояснительные иллюстрации, математические выкладки сведены к разумному минимуму.

Учебное пособие предназначено для студентов направления подготовки 25.03.03 «Аэронавигация» (профиль «Эксплуатация беспилотных авиационных систем»), изучающих дисциплину «Кибербезопасность беспилотных авиационных систем» всех форм обучения.

Рассмотрено и одобрено на заседаниях кафедры 23.05.2024 г. и методического совета 23.05.2024 г.

УДК 004.056:623.746.-519
ББК 6Ф3
Св. тем. план 2024 г.
поз. 16

БОЛЕЛОВ Эдуард Анатольевич

КИБЕРБЕЗОПАСНОСТЬ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ РАДИОПОДАВЛЕНИЮ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

Учебное пособие

В авторской редакции

Подписано в печать 28.11.2024 г.
Формат 60x84/16 Печ. л. 5 Усл. печ. л. 4,65
Заказ № 1041/0909-УП03 Тираж 30 экз.

Московский государственный технический университет ГА
125993, Москва, Кронштадтский бульвар, д. 20

Издательский дом Академии имени Н. Е. Жуковского
125167, Москва, 8-го Марта 4-я ул., д. 6А
Тел.: (495) 755-55-43 E-mail: zakaz@itsbook.ru

ISBN 978-5-907863-46-0

Содержание

1. МЕТОДЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

1.1. Криптографические методы защиты информации

Криптография - это раздел прикладной математики (криптологии), изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования. На решение взаимообратных задач нацелен криптоанализ. **Криптоанализ** - это раздел прикладной математики (криптологии), изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистем или их входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст. Таким образом, криптография и криптоанализ составляют единое целое и образуют науку - **криптологию**, которая с самого начала развивалась как двуединая наука.

Исторически центральным понятием криптографии является понятие шифра. **Шифром** называется совокупность обратимых криптографических преобразований множества открытых текстов на множество зашифрованных текстов, проводимых с целью их защиты. Конкретный вид криптографического преобразования открытого текста определяется с помощью **ключа** шифрования. **Открытым текстом** называют исходное сообщение, которое подлежит зашифрованию. Под **зашифрованием** понимается процесс применения обратимого криптографического преобразования к открытому тексту, а результат этого преобразования называется **шифртекстом** или **криптограммой**. Соответственно, процесс обратного криптографического преобразования криптограммы в открытый текст называется **расшифрованием**.

Расшифрование нельзя путать с дешифрованием. **Дешифрование** (**дешифровка**, **взлом**) - процесс извлечения открытого текста без знания криптографического ключа на основе перехваченных криптограмм. Таким образом, расшифрование проводится законным пользователем, знающим ключ шифра, а дешифрование - криптоаналитиком.

Криптографическая система - семейство преобразований шифра и совокупность ключей. Само по себе описание криптографического алгоритма не является криптосистемой. Только дополненное схемами распределения и управления ключами оно становится системой.

Классификация криптосистем представлена на рис. 1.1. Более полная классификация криптосистем приведена, например в [2,4].

Симметричные криптосистемы (**криптосистемы с секретным ключом**) построены на принципе сохранения в тайне ключа шифрования. На рис. 1.2 представлена упрощенная структурная схема симметричной криптосистемы.

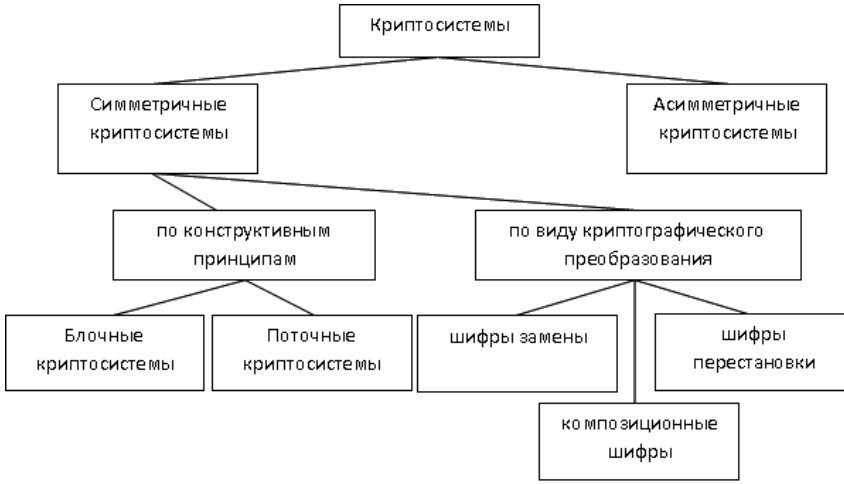

Рисунок 1.1. Классификация криптосистем

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

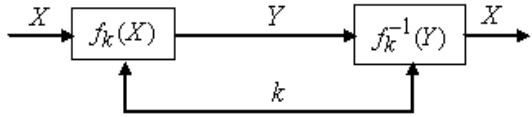

Рисунок 1.2. Структурная схема симметричной криптосистемы

Симметричные криптосистемы классифицируются по различным признакам [4]: 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. Под **шифром замены** понимается преобразование, которое заключается в замене букв исходного сообщения на другие буквы по более или менее сложному правилу. **Композиционные шифры** строятся на основе шифров замены и перестановки. **Блочные симметричные криптосистемы** (БСК) представляют собой семейство обратимых криптографических преобразований блоков исходного сообщения. **Поточные криптосистемы** (ПСК) преобразуют посимвольно исходное сообщение в криптограмму.

Отличительной особенностью **асимметричных криптосистем** (**криптосистем с открытым ключом**) является то, что для зашифрования и расшифрования информации используются разные ключи. На рис. 1.3 представлена упрощенная структурная схема асимметричной криптосистемы. Криптосистема с открытым ключом определяется тремя алгоритмами: генерации ключей, шифрования и расшифрования. Алгоритм генерации ключей позволяет получить пару ключей $(k_o, k_з)$, причем $k_o \neq k_з$. 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 $f_{k_з}^{-1}(f_{k_o}(X)) = X$.

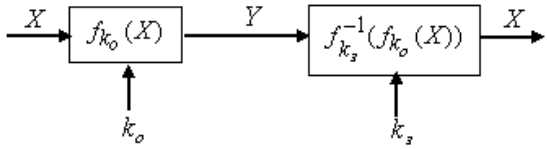

Рисунок 1.3. Упрощенная структурная схема асимметричной криптосистемы

Поточные криптосистемы

Поточные криптосистемы относятся к шифрам замены, преобразующим посимвольно открытый текст в криптограмму [4]. Традиционно шифры замены строились по принципу поточного шифрования. В современных поточных криптосистемах в качестве шифруемых символов фигурируют биты или даже байты. Поточные криптосистемы разделяются на **синхронные** (СПК) и **асинхронные** или **самосинхронизирующиеся** (ССПК). Упрощенная структурная схема СПК представлена на рис. 1.4.

Схема СПК состоит из управляющего и шифрующего блоков. Управляющий блок генерирует управляющую последовательность $\gamma = \{\gamma_i\}$, $i = \overline{1,n}$, которая используется для формирования шифрующих

криптопреобразований $f_\gamma(\cdot)$. Управляющую последовательность часто называют управляющей гаммой, а управляющий блок – генератором гаммы.

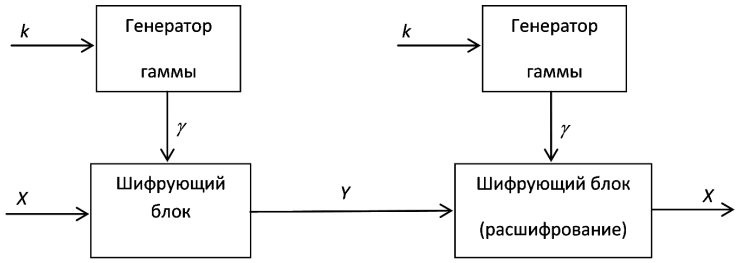

Рисунок 1.4. Упрощенная структурная схема СПК

Шифрующий блок зашифровывает символ открытого текста x_i в символ криптограммы y_i с использованием криптографического преобразования $f_\gamma(\cdot)$. Отправитель сообщения устанавливает заранее оговоренный ключ k генератора и, вычислив криптограмму Y, отправляет ее получателю. Для расшифрования получатель использует идентичный генератор гаммы, в который устанавливается тот же ключ k. Шифрующий блок получателя в режиме расшифрования вычисляет открытый текст X по криптограмме Y используя обратное криптографическое преобразование $f_\gamma^{-1}(\cdot)$. В СПК генерируемая гамма не зависит от открытого текста, т.к. генератор гаммы автономен. В связи с этим СПК функционирует исправно до тех пор, пока устройства, реализующие шифрование и расшифрование на концах линии связи, работают синхронно, то есть не имеет места расшифрование символа криптограммы y_i с использованием символа гаммы γ_j, $i \neq j$. Такие нежелательные сбои, называемые рассинхронизацией, могут наступить из-за различных скоростей работы аппаратуры на приемной и передающем концах, удалении символов при передаче в канале связи и т.д. Сбои могут повлечь неправильное расшифрование всего последующего отрезка сообщения. Если такое случается отправитель и получатель должны восстановить синхронизм работы генераторов гаммы прежде, чем продолжить сеанс связи. Обычно проблемы восстановления синхронизма решаются либо с помощью повторного шифрования с реинициализацией ключа обоими абонентами (повторное использование гаммы крайне нежелательно, а в некоторых криптосистемах недопустимо), либо с помощью разбиения текста на блоки, начала и окончания которых снабжены специальными маркерами. Во втором случае рассинхронизация приводит к некорректному расшифрованию лишь до тех пор, пока получателем не будет принят один из маркеров.

К достоинствам СПК следует отнести то, что они не размножают искажений символов текста, которые довольно часто имеют место при

передаче по каналам связи. Если при отправлении сообщения был искажен символ x_i или передаче по каналу связи был искажен символ y_i, то при синхронной работе генераторов эти искажения не повлияют на правильность расшифрования всех символов, кроме $i-$го. Также СПК защищают передаваемое сообщение от несанкционированных вставок и удаления отрезков текста, так как в этих случаях произойдет рассинхронизация и «вмешательство» злоумышленника будет немедленно обнаружено. В то же время СПК не вполне защищают от умышленной подмены отрезка сообщения на другой отрезок такой же длины. Если злоумышленнику известен отрезок открытого текста, то ему не составляет труда подменить его таким отрезком, который расшифруется в требуемый фрагмент текста.

Схема ССПК также состоит из управляющего и шифрующего блоков с аналогичным функциональным назначением. Однако имеются отличия в построении управляющего блока и в схеме взаимодействия блоков. Как видно из рис. 1.5, ССПК имеет обратную связь по криптограмме, что является важным отличием ССПК. Генерируемая гамма зависит от предшествующих битов криптограммы:

$$\gamma_{i+1} = f\left(y_{i-n+1}, y_{i-n+2}, ..., y_i, k\right),\ i \geq n.$$

Каждое внутренне состояние управляющего блока СППК (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 ССПК на приемном и передающем концах устанавливаются в одинаковые внутренние состояния и, следовательно, вырабатывают при этом одинаковые символы гаммы. Т.е. происходит самосинхронизация ССПК. Как правило, каждое шифруемое сообщение начинается не с содержательного текста, а со случайного отрезка из n символов, который шифруется, передается и затем расшифровывается. И хотя расшифрование этого отрезка реализуется некорректно в силу несовпадения начальных состояний генераторов, после передачи n начальных знаков генераторы синхронизируются. Для затруднения криптоанализа по первым n символам криптограммы начальное состояние ССПК выбирается случайным образом для каждого сообщения.

Основным недостатком ССПК является размножение ошибок. Единичная ошибка в криптограмме порождает n ошибок в открытом тексте. Также ССПК уязвимы к имитации сообщения. Злоумышленник может записать некоторый перехваченный отрезок криптограммы и позже отправить его в адрес. После нескольких нестыковок в начале сообщения (до n символов) посланный отрезок расшифруется верно, и получатель не сможет определить, что принято устаревшее сообщение. Подобная имитация невозможна, если использовать метки времени, а также менять ключи при каждом новом сообщении.

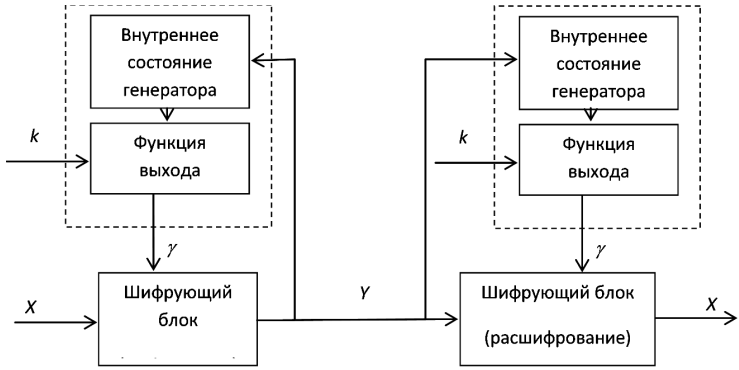

Рисунок 1.5. Упрощенная структурная схема ССПК

Поточные криптосистемы, как правило, являются строятся на основе шифров гаммирования. При этом различаю табличное и модульное гаммирование. **Табличное гаммирование** заключается в том, что криптографическое преобразование $f(x,\gamma)$ представляется в виде латинского квадрата в алфавите A_X. При этом, как и в случае шифра Полибия, символ криптограммы определяется на пересечении строки и столбца, которые задаются символами открытого текста и гаммы. Таким образом, шифр Полибия является примером шифра табличного гаммирования. Наиболее удобными с точки зрения практического применения являются **шифры модульного гаммирования**, которым соответствует уравнение:

$$y_i = x_i \oplus \gamma_i,\ i = \overline{1,n},$$

где символ $\oplus$ определяет операцию сложения по модулю 2 (операция XOR). Удобство шифров модульного гаммирования заключается в их обратимости:

$$x_i = y_i \oplus \gamma_i = (x_i \oplus \gamma_i) \oplus \gamma_i = x_i,\ i = \overline{1,n}.$$

Для обеспечения высокой криптографической стойкости при применении шифров гаммирования не допускается [4]:

- повторное использование гаммы;
- использование неравновероятной гаммы.

Блочные криптосистемы

Блочные симметричные криптосистемы (БСК) представляют собой семейство обратимых криптографических преобразований блоков (частей фиксированной дины) исходного текста [4]. Фактически БСК – система подстановки на алфавите блоков (она может быть моно- или многоалфавитной в зависимости от режима блочного шифра).

Первым опытом создания блочной криптосистемы явилась разработанная американской фирмой IBM криптосистема LUCIFER. Блоки открытого и шифрованного текста, обрабатываемые криптосистемой LUCIFER, представляют собой двоичные векторы длиной 128 бит. Криптосистема построена по принципу «сэндвича», составленного из нескольких слоев – преобразований замены S (substitution) блоков и преобразований перестановки P (permutation) элементов блоков. Такие схемы получили название **SP-сетей**, т.е. сетей перестановок и замен. Криптографическая идея SP-сетей заключается в построении сложного криптопреобразования с помощью композиции нескольких относительно простых, удобно реализуемых преобразований (см. рис. 1.6).

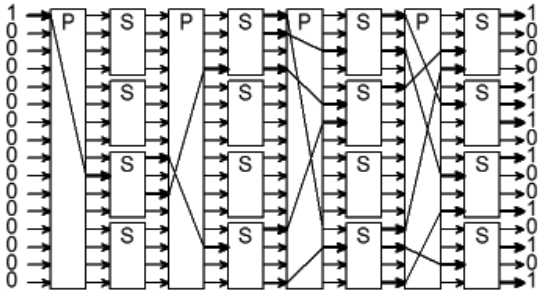

Рисунок 1.6. Пример реализации SP-сети

Однако полученная криптосистема LUCIFER получилась достаточно громоздкой и обладала низкой производительностью. Скорость шифрования при программной реализации криптосистемы не превышала 8 кбайт/с, аппаратная реализация давала скорость шифрования не более 97 кбайт/с. К тому же у разработчиков были опасения по поводу криптостойкости, которые впоследствии подтвердились. Вместе с тем, накопленный разработчиками опыт при создании криптосистемы LUCIFER пригодились при разработки последующих блочных криптосистем.

В 1974 году фирмой IBM был разработана криптосистема, получившая название DES (Data Encryption Standart) [4]. Подобно криптосистеме LUCIFER криптосистема DES частично реализует принцип SP-сети и построена по **итеративному** принципу, то есть на основе нескольких однотипных преобразований. В дальнейшем итеративный принцип использовался в подавляющем большинстве разработок блочных криптосистем. Рассмотрим криптографическое преобразование $F(\cdot)$ итеративной блочной криптосистемы. Как правило, блок открытого текста x подвергается предварительному шифрованию (как правило, перестановке) $f_0(x,k_0)$, где k_0 - **ключ входного криптопреобразования**. Затем полученная криптограмма многократно подвергается шифрованию с помощью однотипного криптопреобразования $\varphi_i(y_i',k_i)$, $i=\overline{1,r}$, где k_i - **цикловой (раундовый) ключ**, y_i' - входной блок $i-$го цикла шифрования.

Криптопреобразование $\varphi_i(\cdot)$ называется **цикловой функцией**, а переменная r определяет количество **циклов** (**раундов**) шифрования. После реализации всех r раундов шифрования осуществляется еще одно финальное преобразование (как правило, перестановка) $f_{r+1}(y'_r, k_{r+1})$, где y'_r - выходной блок последнего раунда шифрования, k_{r+1} - **ключ выходного криптопреобразования**. Таким образом, криптографическое преобразование итеративной блочной криптосистемы имеет вид:

$$y = F(x,k) = f_{r+1}(y'_r, k_{r+1}) \cdot \varphi_r(y'_{r-1}, k_r) \cdot \ldots \cdot \varphi_1(y'_0, k_1) \cdot f_0(x, k_0). \quad (2.13)$$

Криптопреобразование $f_0(x, k_0)$ называется **входным преобразованием**, а $f_{r+1}(y'_r, k_{r+1})$ - **выходным преобразованием**. Обратное криптографическое преобразование определяется равенством:

$$x = F^{-1}(y,k) = f_0^{-1}(y'_0, k_0) \cdot \varphi_2^{-1}(y'_1, k_1) \cdot \ldots \cdot \varphi_r^{-1}(y'_r, k_r) \cdot f_{r+1}^{-1}(y, k_{r+1}).$$

Многократное использование цикловой функции должно обеспечить следующие свойства криптопреобразования:

- рассеивание (позволяет скрыть статистические зависимости между символами открытого текста и обеспечивает невозможность определения ключа по частям);
- перемешивание (позволяет усложнить зависимость между ключом и криптограммой).

Один из первых способов построения цикловой функции основан на использовании отображения типа регистра сдвига. Конструкция была признана удачной и нашла широкое применение в дальнейших разработках блочных криптосистем (FEAL, Khufu, Khafre, LOKI, Blowfish, ГОСТ 28147-89). Эта конструкция названа в честь разработчика **схемой Фейстеля** [4]. Схема Фейстеля представляет собой блочный симметричный шифр, криптографическая функция которого оперирует «половинами» входных блоков и имеет вид:

$$f\{(x_1, x_2), k\} = x_2 \,\|\, \psi(x_2, k) \oplus x_1,$$

где x_1 и x_2 - половины входного блока; $\psi(x_2, k)$ - функция усложнения; $\|$ - операция конкатенации. На рис. 1.7 представлена структура схемы Фейстеля. Варианты схемы Фейстеля отличаются конструкцией функции усложнения.

Для получения криптопреобразования, обладающего хорошими криптографическими свойствами, функция усложнения реализуется в виде композиции элементарных преобразований, называемых слоями функции усложнения (или цикловой функции). Конструктивные слои функции усложнения имеют следующие назначения: подмешивание раундовых ключей; перемешивание входных блоков; реализацию сложной нелинейной зависимости между знаками ключа, входного и выходного блоков.

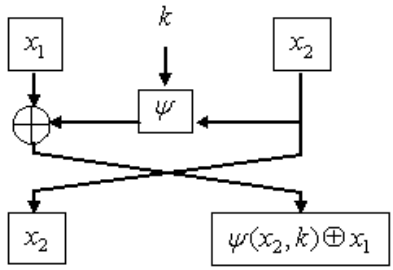

Рисунок 1.7. Схема Фейстеля

Цикловая функция должна удовлетворять ряду условий:

- цикловая функция должна быть обратимой (функция усложнения схемы Фейстеля в принципе может не удовлетворять этому требованию, так как обратимость преобразования обеспечивается за счет использования операции XOR);

- цикловая функция должна быть нелинейной;

- перемешивающие слои цикловой функции должны реализовывать связи между входными и выходными битами S-блоков (блоков замены) таким образом, чтобы каждый S-блок удовлетворял критериям лавинного эффекта, а также совокупность входных битов каждого S-блока зависела от выходов нескольких S-блоков предыдущего цикла;

- цикловая функция должна обладать свойствами, затрудняющими применение методов дифференциального и линейного криптоанализа, т.е. цикловая функция должна иметь минимальную корреляцию между разностью открытых текстов и соответствующих криптограмм.

Для затруднения применения методов криптоанализа блочные криптосистемы должны использовать в качестве входного и выходного преобразований операции XOR. Эти операции получили название отбеливания, а использующий эти операции шифр называют шифром с отбеливанием. Операция отбеливания улучшает криптографические свойства шифра, не нарушая при этом обратимости криптопреобразования.

Режимы шифрования. Для шифрования исходного открытого текста БСК могут использоваться в различных режимах [4]. Далее будут рассмотрены четыре режима шифрования наиболее часто встречающиеся на практике:

- режим электронной кодировочной книги - ECB (Electronic Code Book);

- режим сцепления блоков криптограммы - CBC (Cipher Block Chaining);

- режим обратной связи по криптограмме - CFB (Cipher Feed Back);

- режим обратной связи по выходу - OFB (Output Feed Back).

Режим электронной кодировочной книги ECB. Исходный текст разбивается на блоки, равные размеру блока шифра. Затем каждый блок шифруется независимо от других с использованием одного ключа

шифрования (см. рис. 1.8). Непосредственно этот режим применяется для шифрования небольших объемов информации, размером не более одного блока или для шифрования ключей. Это связано с тем, что одинаковые блоки открытого текста преобразуются в одинаковые блоки криптограмма, что может дать криптоаналитику определенную информацию о содержании сообщения.

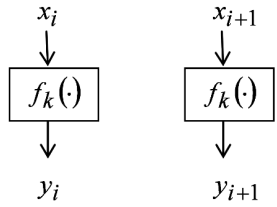

Рисунок 1.8. Режим электронной кодировочной книги ECB

Стойкость режима ECB равна стойкости самого шифра, однако, структура исходного текста при этом не скрывается. Скорость шифрования равна скорости блочного шифра. Основным достоинством этого режима является простота реализации.

Режим сцепления блоков криптограммы CBC. В данном режиме каждый блок исходного текста складывается по модулю 2 с предыдущим блоком криптограммы, а затем шифруются (см. рис. 1.9). Для начала процесса шифрования используется **синхропосылка** (или **начальный вектор**) y_0. Процессы шифрования и расшифрования описывается выражениями:

$$y_i = f_k(x_i \oplus y_{i-1}),\ i = \overline{1,n}.$$
$$x_i = f_k^{-1}(y_i) \oplus y_{i-1},\ i = \overline{1,n}.$$

Стойкость режима CBC равна стойкости блочного шифра, лежащего в его основе. Структура исходного текста скрывается за счет сложения по модулю 2 предыдущего блока криптограммы с очередным блоком открытого текста. Стойкость шифрованного текста увеличивается, поскольку становиться невозможным прямая манипуляция исходным текстом. Скорость шифрования равна скорости работы блочного шифра, однако простого способа распараллеливания процесса шифрования, как для режима ECB, не существует.

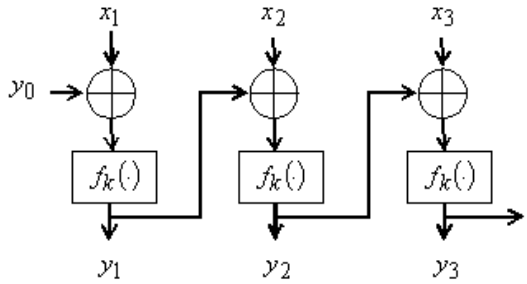

Рисунок 1.9. Режим сцепления блоков криптограммы CBC

Начальный вектор y_0 может передаваться по линии связи как в открытом, так и в шифрованном виде. Однако следует избегать повторения начального вектора, это позволит затруднить криптоатаку. Искажение одного бита в блоке открытого текста x_i влечет за собой искажение в среднем половины битов во всех блоках криптограммы, начиная с y_i. Для расшифрования это несущественно, так как восстановленный текст будет содержать ту же единственную ошибку. Искажение бита в блоке y_i влечет за собой искажение около половины битов в блоке x_i, начиная с этого бита, и в блоке x_{i+1} Следующие блоки расшифровываются корректно.

Режим обратной связи по криптограмме CFB. В данном режиме предыдущий блок криптограммы шифруется еще раз, и для получения очередного блока криптограммы результат складывается по модулю 2 с блоком исходного текста (см. рис. 1.10). Для начала процесса шифрования также используется начальный вектор y_0. Процессы шифрования и расшифрования описывается выражениями:

$$y_i = x_i \oplus f_k(y_{i-1}),\ i = \overline{1,n}.$$
$$x_i = f_k(y_{i-1}) \oplus x_i,\ i = \overline{1,n}.$$

Искажение одного бита в блоке x_i влечет за собой искажение одного бита в y_i и в среднем половины битов во всех блоках криптограммы, начиная с y_{i+1}, но при расшифровании получается открытый текст с той же единственной ошибкой.

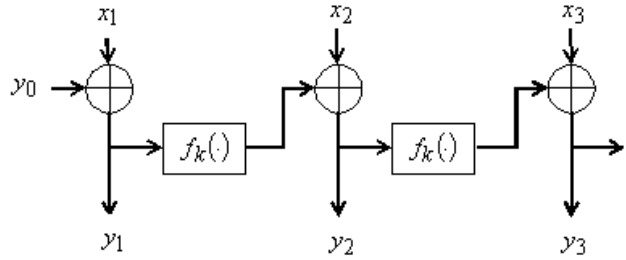

Рисунок 1.10. Режим обратной связи по криптограмме CFB

Искажение бита в блоке y_i влечет искажение соответствующего бита в блоке x_i. Затем ошибка искажает в среднем половину битов в каждом из последующих блоков, но в дальнейшем блоки расшифровываются корректно. Данный режим, как и ССПК, самостоятельно восстанавливается после ошибок синхронизации. Стойкость режима равна стойкости блочного шифра, лежащего в его основе, и структура исходного текста скрывается за счет использования операции сложения по модулю 2. Скорость шифрования равна скорости работы блочного шифра, и простого способа распараллеливания процесса шифрования не существует.

Режим обратной связи по выходу OFB. Данный режим подобен режиму CFB, за исключением того, что величины, складываемые по модулю 2 с блоками исходного текста, генерируются независимо от исходного текста и криптограммы (см. рис. 1.11).

Процессы шифрования и расшифрования описывается выражениями:

$$y_i = x_i \oplus s_i,\ s_i = f_k(s_i)\ i = \overline{1,n}.$$
$$x_i = y_i \oplus s_i,\ i = \overline{1,n}.$$

Для начала процесса шифрования используется начальный вектор s_0.

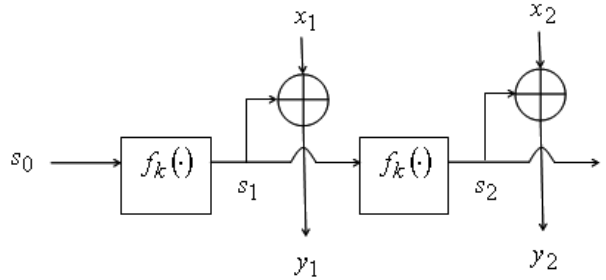

Рисунок 1.11. Режим обратной связи по выходу OFB

В данном режиме ошибки не распространяются, что является преимуществом при передаче шифрованных речевых сигналов и

видеоизображений. Блочный шифр в данном режиме можно рассматривать как СПК. В связи с этим, при использовании режима OFB чрезвычайно важно сохранять синхронизм.

Усложнение блочных криптосистем. Постоянное развитие методов криптоанализа не позволяет долгое время использовать блочную криптосистему без определенного рода ее усовершенствований, которые усложняют работу криптоаналитика. Наиболее простым методом усложнения блочных криптосистем является увеличение длины ключа, однако этот метод не всегда приемлем и, к тому же, требует существенной перестройки базовой блочной криптосистемы. Другим методом усложнения является многократное шифрование с использованием базовой блочной криптосистемы. Этот метод применим к любой блочной криптосистеме, но его использование снижает скорость шифрования. Рассмотрим различные схемы многократного шифрования.

Простейшая схема кратного шифрования - **двойное шифрование** с использованием независимых ключей:

$$y_i = f_{k_2}\left(f_{k_1}(x_i)\right),\ i = \overline{1,n}.$$

Эта схема была отвергнута сразу, так как ключи можно определить по открытому тексту и криптограмме методом согласования.

Другой способ двойного шифрования, называемый **методом Дэвиса-Прайса**, построен на идеи режима шифрования CBC:

$$y_i = f_{k_2}\left(x_i \oplus f_{k_1}\left(y_{i-1}\right)\right),\ i = \overline{1,n}.$$

Более стойкие схемы используют тройное шифрование. Схему тройного шифрования Тачмена с парой независимых ключей называют часто **схемой EDE**:

$$y_i = f_{k_1}\left(f_{k_2}^{-1}\left(f_{k_1}(x_i)\right)\right),\ i = \overline{1,n}.$$

При $k_1 = k_2$ эта схема равносильна однократному шифрованию.

Наиболее надежной схемой тройного шифрования является **схема тройного шифрования с тремя независимыми ключами**:

$$y_i = f_{k_3}\left(f_{k_2}^{-1}\left(f_{k_1}(x_i)\right)\right),\ i = \overline{1,n}.$$

Еще одна схема усложнения блочный криптосистемы, определяемая выражением:

$$y_i = k_2 \oplus f_k\left(k_1 \oplus x_i\right),\ i = \overline{1,n},$$

использует «зашумляющие» ключи и называется **схемой Рона Ривеста**. Здесь ключи k_1, k_2 являются не ключами шифрования, а «зашумляющими» ключами.

К методам многократного шифрования относится и **схема двойного гаммирования**:

$$y_i = x_i \oplus \gamma_i^{(1)} \oplus \gamma_i^{(2)},\ i = \overline{1,n}.$$

Гаммы $\left\{\gamma_i^{(1)}\right\}$ и $\left\{\gamma_i^{(2)}\right\}$ генерируются с использованием независимых ключей k_1, k_2.Перечисленные схемы кратного шифрования не являются единственными. Существует множество схема с использованием нескольких алгоритмов шифрования, переменным размером ключей и обрабатываемых блоков [4].

Теория стойкости криптосистем

Предположим, что имеется конечное число возможных открытых сообщений $X = \{X_1, X_2, ..., X_m\}$, множество возможных ключей $K = \{k_1, k_2, ..., k_l\}$ и множество криптограмм $Y = \{Y_1, Y_2, ..., Y_n\}$. Задано криптопреобразование:

$$Y_j = f(X_i, k_l).$$

Считаем, что на множестве открытых сообщений $X = \{X_1, X_2, ..., X_m\}$ задано априорное распределение вероятностей, т.е. определены априорные вероятности $P(X_i)$, $i = \overline{1,m}$. Это априорное распределение известно противнику. После того как шифровальщик противника перехватил некоторую криптограмму Y_j, $j = \overline{1,n}$, он может вычислить, по крайней мере в принципе, апостериорные вероятности различных сообщений $P(X_i \mid Y_j)$.

Криптосистема называется **совершенно стойкой** (**совершенно секретной**), если выполняется условие:

$$P(X_i \mid Y_j) = P(X_i), \text{ при всех } X_i,\ Y_j \text{ и } k_l.$$

В этом случае перехват криптограммы не дает криптоаналитику противника никакой информации. Он не может корректировать никакие свои действия в зависимости от информации, содержащейся в криптограмме, так как все вероятности, относящиеся к содержанию криптограммы, не изменяются. Смысл выражения заключается в том, что открытый текст и криптограмма статистически независимы.

Теорема Шеннона. *Если система является совершенно стойкой, то справедливо равенство:*

$$P(Y_j \mid X_i) = P(Y_j), \text{ при всех } i \text{ и } j.$$

Верно и обратное утверждение.

☐ Используя определение условной вероятности, при $P(Y_j) \neq 0$, можно записать:

$$P(X_i \mid Y_j) = \frac{P(X_i Y_j)}{P(Y_j)} = \frac{P(X_i)P(Y_j \mid X_i)}{P(Y_j)}.$$

Принимая во внимание $P(Y_j \mid X_i) = P(Y_j)$, получаем:

$$P(X_i \mid Y_j) = \frac{P(X_i \mid Y_j)P(Y_j \mid X_i)}{P(Y_j)}, \text{ то есть } \frac{P(Y_j \mid X_i)}{P(Y_j)} = 1.\blacksquare$$

Другими словами, полная вероятность всех ключей, переводящих сообщение X_i в данную криптограмму Y_j, равна полной вероятности всех ключей, переводящих сообщение X_k в ту же самую криптограмму Y_j для всех X_i, X_k, и Y_j. К. Шеннон доказал, что совершенно стойкие криптосистемы существуют.

Теорема о совершенной стойкости шифра Вернама. *Шифр Вернама является совершенно стойкой криптосистемой*.

☐ Согласно теореме Шеннона имеем:

$$P(Y_j \mid X_i) = P(y^n \mid x^n) = P(k_1 = y_1 \oplus x_1; \ldots, k_n = y_n \oplus x_n) =$$
$$= P(k_1, k_2, \ldots, k_n) = 2^{-n}.$$

Здесь использовано предположение о равновероятности ключей. Найдем $P(Y_j)$. По формуле полной вероятности $P(Y_j) = \sum_{i=1}^{2^n} P(X_i)P(Y_j \mid X_i)$. Учитывая, что $P(Y_j \mid X_i) = 2^{-n}$, получаем:

$$P(Y_j) = 2^{-n} \sum_{i=1}^{2^n} P(X_i) = 2^{-n}, \text{ при } \sum_{i=1}^{2^n} P(X_i) = 1.\blacksquare$$

На рис. 1.13 представлен граф совершенно стойкой криптосистемы.

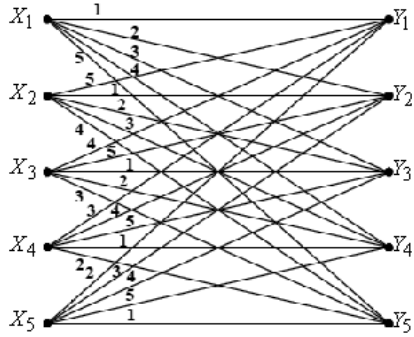

Рисунок 1.13. Граф совершенно стойкой криптосистемы

Совершенно стойкие криптосистемы, характеризуются следующими свойствами: каждое открытое сообщение X_i связывается с криптограммой X_j только одной линией; все ключи равновероятны.

Идеально стойкие криптосистемы. Криптосистема включает в себя два статистических выбора: выбор сообщения и выбор ключа. Можно измерять количество информации, создаваемой при выборе сообщения, через энтропию [4]:

$$H(X) = -\sum_{X} P(X) \log P(X).$$

Суммирование производиться по всем сообщениям. Аналогично, неопределенность, связанная с выбором ключа, определяется выражением:

$$H(K) = -\sum_{K} P(K) \log P(K).$$

В совершенно стойких криптосистемах количество информации в сообщении равно самое большое $\log n$, где n - число открытых сообщений (эта величина достигается для равновероятных сообщений). Эта информация может быть скрыта полностью лишь тогда, когда неопределенность ключа не меньше $\log n$. Это является первым примером общего принципа, который будет часто встречаться ниже: существует предел, которого нельзя превзойти при заданной неопределенности ключа – количество неопределенности, которое может быть введено в решение, не может быть больше, чем неопределенность ключа.

Предположим теперь, что, например, для английского текста используется шифр простой замены и что перехвачено определенное число, скажем N, букв зашифрованного текста. Если N достаточно велико, то

почти всегда существует единственное решение задачи криптоанализа, т.е. единственная последовательность, имеющая смысл на английском языке, в которую переводится перехваченный материал с помощью простой подстановки. Для меньших N шансы на не единственность решения увеличиваются; и для определенных малых значений N, вообще говоря, будет существовать некоторое число подходящих отрывков осмысленного английского текста. При N=1, очевидно, возможна любая буква открытого текста и апостериорная вероятность любой буквы будет равна ее априорной вероятности. Для одной буквы система является совершенно стойкой.

В теории связи показано, что естественной математической мерой неопределенности того, что действительно было передано, при условии, что известен только искаженный шумом вариант – принятый сигнал, является условная энтропия передаваемого сигнала при условии, что принятый сигнал известен. Эта условная энтропия носит название ненадежности.

С криптографической точки зрения криптосистема почти тождественна системе связи при наличии шума. На сообщение действует некоторый статистический элемент (криптосистема к выбранным ключом). В результате получается криптограмма, подлежащая дешифрованию. Основное различие заключается в следующем: во-первых, в том, что преобразование при помощи шифра имеет обычно более сложную природу, чем возникающее за счет шума в канале; и, во-вторых, ключ в секретной системе обычно выбирается из конечного множества, в то время как шум в канале чаще является непрерывным, выбранным по существу из бесконечного множества.

Учитывая эти соображения, естественно использовать ненадежность в качестве теоретической меры секретности. Следует отметить, что имеются две основные ненадежности: **ненадежность ключа** и **ненадежность сообщения**. Они будут обозначаться через $H(K|Y)$и $H(X|Y)$, соответственно. Их величины определяются соотношениями:

$$H(K|Y) = -\sum_{K,Y} P(K,Y)\log P(K|Y),$$
$$H(X|Y) = -\sum_{X,Y} P(X,Y)\log P(X|Y).$$

где $P(K,Y)$, $P(X,Y)$ - совместные вероятности ключа и криптограммы и сообщения и криптограммы, соответственно; $P(K|Y)$, $P(X|Y)$ - апостериорные вероятности ключа и сообщения при перехваченной криптограмме.

Суммирование осуществляется по всем возможным ключам и сообщениям, соответственно, а также по криптограммам определенной длины N. Таким образом, $H(K|Y)$ и $H(X|Y)$ являются функциями числа N, т.е. числа перехваченных символов криптограммы. Если ненадежность равна нулю, следует, что одно сообщение (или ключ) имеет единичную вероятность, а все другие - нулевую. Этот случай соответствует полной осведомленности криптоаналитика. Постепенное убывание ненадежности с

ростом N соответствует увеличению сведений об исходном ключе или сообщении. В совершенно стойких криптосистемах для сообщений неограниченной длины требуется ключ бесконечного объема. Если использовать ключ конечного объема, то ненадежности ключа и сообщения, вообще говоря, будут стремиться к нулю, хотя это и не обязательно. На самом деле можно удерживать значение $H(K|Y)$ равным ее начальному значению $H(K)$. Тогда, независимо от того, сколько зашифрованного материала перехвачено, единственного решения не будет, а будет много решений со сравнимыми по величине вероятностями. Определим **идеально стойкую криптосистему** как такую, в которой величины $H(K|Y)$ и $H(X|Y)$ не стремятся к нулю при $N \to \infty$. **Строго идеально стойкая криптосистема** - это такая криптосистема, в которой величина $H(K|Y)$ остается равной $H(K)$. Неформально, строгая идеальность означает, что количество решений криптограммы равно количеству различных ключей и все решения равновероятны.

Примером строго идеальной криптосистемы может служить простая подстановка, примененная к искусственному языку, в котором все буквы равновероятны и последовательные буквы выбираются независимо. В этом случае $H(K|Y)=H(K)$ и $H(X|Y)$ растет линейно по прямой с наклоном $\log m$, где m - мощность алфавита, до тех пор, пока она не пересечет линию $H(K)$, после чего она остается равной этой константе. Из сказанного выше очевидно, что одной из важнейших характеристик языка является его избыточность. **Избыточность языка** – это количественная мера взаимной зависимости символов и их неравновероятности. Избыточность языка определяется как:

$$R = \log m - h,$$

где $h = -\sum_{i=1}^{m} P(i) \log P(i)$ - энтропия на букву сообщения.

Таким образом, на основании рассмотренного можно ввести понятие расстояния единственности криптосистемы. Пусть рассматривается криптосистема и $H(K)$ - энтропия ключа. Пусть R - избыточность шифруемого сообщения, а n_p - длина сообщения, такая, что $H(K|Y) \approx 0$, т.е. при этой длине перехваченной криптограммы ключ почти однозначно восстановлен. Тогда справедливо неравенство:

$$n_p \geq \frac{H(K)}{R}.$$

Число n_p называется **расстоянием единственности криптосистемы**. Анализ неравенства позволяет сделать следующие выводы: для восстановления ключа с высокой вероятностью достаточно перехватить n_p

символов криптограммы; если значение избыточности R=0, то ключ никогда не будет определен, так как $n_p \to \infty$; с практической точки зрения требуется менять ключ криптосистемы задолго до достижения n_p; для уменьшения R требуется преобразовывать исходный текст (например, использовать сжимающее кодирование), так как в этом случае значение R уменьшается, а энтропия преобразованного текста не изменяется. Оценку расстояния единственности криптосистемы можно использовать при ее разработке.

Практическая стойкость криптосистем. Вопрос о практической стойкости, поставленный К.Шенноном, формулируется так: «Надежна ли криптосистема, если криптоаналитик располагает ограниченным временем и ограниченными вычислительными возможностями для анализа перехваченных криптограмм?». С одной стороны, криптосистема должна обеспечивать надежную защиту информации, с другой стороны, должна быть удобна с точки зрения технической реализации и эксплуатации. Так как криптосистемы, обеспечивающие идеальную стойкость, в большинстве случаев практически неприменимы, то вопрос относиться прежде всего к криптосистемам, использующим ключи ограниченного размера и способным обрабатывать большие объемы информации.

По К.Шеннону, практически стойкая криптосистема по своим свойствам должна быть близка к идеальным криптосистемам. Например, высокая стойкость шифра гаммирования обеспечивается при использовании шифрующей последовательности, близкой по своим свойствам к равномерно распределенной случайной последовательности, поэтому криптографические свойства шифра гаммирования определяется свойствами используемого генератора гаммы.

Системный подход к оценке стойкости криптосистемы подразумевается определенную детализацию понятия стойкости криптосистемы. В результате этой детализации формируется ряд критериев математического и технического характера, которым должна удовлетворять стойкая криптосистема.

Основной количественной мерой стойкости криптосистемы является **вычислительная сложность** решения задачи дешифрования. Вычислительная сложность определяется несколькими характеристиками. Предположим, перед криптоаналитиком поставлена задача дешифрования криптосистемы $f(\cdot)$ по набору криптограмм Y_j, $j=\overline{1,m}$. Пусть Ψ_Y - класс применимых к криптосистеме $f(\cdot)$ алгоритмов дешифрования, которыми располагает криптоаналитик. При этом криптоаналитик рассматривает как вероятностное пространство W элементарных событий множество пар ключей и открытых текстов, если открытые тексты неизвестны, или множество ключей, если открытые тексты известны. Для алгоритма $\psi \in \Psi_Y$ обозначим через $T(\psi)$ среднюю трудоемкость его реализации, измеряемую в некоторых условных вычислительных операциях. При этом величина трудоемкости обычно усредняется по множеству W.

Одной из основных характеристик практической стойкости криптосистемы $f(\cdot)$ является **средняя трудоемкость** T_Y **дешифрования**, определяемая как

$$T_Y = \min_{\psi \in \Psi_Y} T(\psi).$$

При этом важно отметить следующее.

1. Существуют алгоритмы дешифрования, определенные не на всем вероятностном пространстве W, а лишь на некоторой его части. Кроме того, некоторые алгоритмы дешифрования устроены так, что их реализация приводит к успеху не на всей области определения, а лишь на некотором ее подмножестве. Поэтому к важнейшим характеристикам алгоритма дешифрования $\psi \in \Psi_Y$ необходимо отнести не только его трудоемкость, но и **надежность алгоритма дешифрования** $\nu(\psi)$, под которой понимается средняя доля информации, дешифруемой с помощью алгоритма ψ.

Если надежность алгоритма дешифрования мала, то с точки зрения криптографа он является неопасным, а с точки зрения криптоаналитика неэффективным. Таким образом, при получении оценки (4.13) целесообразно рассматривать лишь те алгоритмы дешифрования, надежность которых велика. При этом для определения наилучшего алгоритма дешифрования криптосистемы $f(\cdot)$ можно использовать различные критерии в зависимости от конкретных условий. Например, можно считать наилучшим алгоритм дешифрования ψ, для которого наименьшее значение принимает величина $\frac{T(\psi)}{\nu(\psi)}$. Эту величину можно интерпретировать как **средние трудозатраты**, необходимые для успешного дешифрования криптосистемы.

2. Сложность дешифрования зависит от количественных и качественных характеристик криптограмм, которыми располагает криптоаналитик. Количественные характеристики определяются числом перехваченных криптограмм и их длинами. Качественные характеристики связаны с достоверностью перехваченных криптограмм (наличие искажений, пропусков и т.д.).

По К. Шеннону, каждая криптосистема имеет объективную характеристику $T_Y(n)$ - **среднюю вычислительную сложность дешифрования** (по всем криптограммам длины n и ключам). Величина $\lim_{n\to\infty} T_Y(n)$ характеризует предельные возможности дешифрования криптосистемы при неограниченном количестве шифрматериала и абсолютной квалификации криптоаналитика. Оценивая стойкость криптосистемы, криптоаналитик получает верхние оценки предельной стойкости, так как практическое дешифрование использует ограниченное

количество шифрматериала и ограниченный класс так называемых известных методов дешифрирования.

3. Важной характеристикой криптостойкости криптосистемы является **временная сложность** ее дешифрования. Оценка временной сложности дешифрования криптосистемы подразумевается более детальную проработку реализации алгоритмов дешифрования с учетом характеристик вычислительного устройства, используемого для дешифрования. К таким характеристикам вычислительного устройства, реализующего алгоритмы дешифрования, относятся архитектура, быстродействие, объем и структура памяти, быстрота доступа к памяти и др. Следовательно, время дешифрования криптосистемы определяется имеющимся классом алгоритмов дешифрования Ψ_Y и вычислительными возможностями криптоаналитика.

Выбор наилучшего алгоритма осложняется и тем, что различным вычислительным устройствам могут соответствовать различные наилучшие алгоритмы дешифрования. Вопрос о криптостойкости криптосистемы имеет некоторые особенности с точки зрения криптоаналитика и криптографа. Криптоаналитик атакует криптосистему, располагая конкретными интеллектуальными, вычислительными и экономическими ресурсами. Его цель - успешное дешифрование криптосистемы.

Криптограф оценивает стойкость криптосистемы, имитируя атаку на криптосистему со стороны криптоаналитика противника. Для этого криптограф моделирует действия криптоаналитика, оценивая по максимуму интеллектуальные, вычислительные, технические и другие возможности противника. Цель криптографа – убедиться в высокой криптостойкости разработанной криптосистемы. Используя понятие практической криптостойкости, можно классифицировать криптосистемы по величине стойкости, или по продолжительности временного периода, в течение которого криптосистема с высокой надежностью обеспечивает требуемый уровень защиты информации. Кроме рассмотренных подходов к оценке стойкости криптосистем существуют еще ряд подходов [4,7].

Асимметричные криптосистемы

Ассиметричная криптосистема или криптосистема с открытым ключом определяется тремя алгоритмами: генерации ключей, шифрования и расшифрования. Алгоритм генерации ключей позволяет получить пару ключей $(k_o, k_з)$, причем $k_o \neq k_з$. Один из ключей k_o публикуется, он называется **открытым**, а второй $k_з$, называется **закрытым** (или секретным) и храниться в тайне.

Под криптосистемой с открытым ключом понимают систему [5]:

$$ACS = (X, Y, K, x, y, k_o, k_з, E, D),$$

где X - множество открытых текстов, Y - множество криптограмм, K - множество ключей, $x \in X$ - некоторый открытый текст, $y \in Y$ - некоторая криптограмма, $k_o \neq k_з$, $(k_o, k_з) \in K$ - пара ключей, E - функция шифрования, D - функция расшифрования.

Центральным понятием теории асимметричных криптосистем является понятие односторонней функции [5]. Пусть дана функция:

$$y = f(x),$$

определенная на множестве $X, x \in X$, для которой существует обратная функция:

$$x = f^{-1}(y).$$

Функция называется **односторонней**, если вычисление y является сравнительно простой задачей, требующей немного времени, а вычисление x – задача сложная, требующая привлечения массы вычислительных ресурсов, например 10^6-10^9 лет работы мощного суперкомпьютера. Данное определение, конечно, не является строгим.

Собственно односторонняя функция в криптографии не используется. Применяется **односторонняя функция с секретом** (односторонняя функция с «лазейкой», односторонняя функция с «ловушкой»).

Пусть X и Y - конечные множества. Односторонней функцией с секретом

$$f : X \to Y,$$

называется обратимая функция, удовлетворяющая следующим условиям:

1) f легко вычисляется, т.е. если дано $x \in X$, $y = f(x)$ вычислима за полиномиальное время (существует полиномиальный алгоритм вычисления y);

2) f^{-1} - обратная функция к f, трудно вычисляется, т.е. если дано $y \in Y$, $x = f^{-1}(y)$ является вычислительно неразрешимой (не существует полиномиального алгоритма вычисления x).

3) f^{-1} легко вычисляется, если известен секрет, связанный с параметрами функции.

Таким параметром в асимметричных криптосистемах является, как правило, закрытый ключ $k_з$. Рассмотрим односторонние функции, используемые в криптографии [5].

Дискретное экспоненцирование и логарифмирование. Пусть

$$y = a^x \bmod p,$$

где p - некоторое простое число, а $x \in \{1,2,..., p-1\}$. Обратная функция обозначается:

$$x = \log_a y \bmod p,$$

называется **дискретным логарифмом**.

Умножение и факторизация. Другим примером односторонней функции является задача факторизации. Существо ее базируется на двух фактах из теории чисел:

1) задача проверки чисел на простоту является сравнительно легкой;

2) задача разложения чисел вида:

$$n = pq,$$

является очень трудновыполнимой, если известно только n, а p и q - большие простые числа.

Криптосистема RSA названа была так в честь ее разработчиков: Рона Ривеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman). Криптосистема RSA является одной из самых используемых в мире асимметричных криптосистем.

Криптосистема с открытым ключом RSA формально определяется следующим образом [5]:

$$RSA = (X, Y, K, x, y, k_o, k_з, N, E, D),$$

где X - множество открытых текстов, Y - множество криптограмм, K - множество ключей, $x \in X$ - некоторый открытый текст, $y \in Y$ - некоторая криптограмма, $k_o \neq k_з$, $(k_o, k_з) \in K$ - ключи шифрования и расшифрования, удовлетворяющие условию $k_o k_з \bmod \varphi(N) = 1$, $N = pq$ - натуральное число, причем p и q - простые числа, E - функция шифрования, D - функция расшифрования.

Рассмотрим алгоритм работы криптосистемы RSA. Пусть имеется сеть, состоящая из M абонентов. Каждый m-й абонент, $m = \overline{1, M}$, сети случайно выбирает два больших простых числа p_m, q_m и затем вычисляется число $N_m = p_m q_m$. Число N_m является открытой информацией, доступной другим абонентам сети. Далее каждый абонент вычисляет функцию Эйлера $\varphi(N_m) = (p_m - 1)(q_m - 1) = \phi_m$ и выбирает число $k_{om} < \phi_m$, взаимно простое с ϕ_m, а затем по обобщенному алгоритму Евклида находит число $k_{зm}$, такое что:

$$k_{om}k_{зm} \bmod \phi_m = 1,\ m = \overline{1, M}\ .$$

Пара $\langle N_m, k_{om} \rangle$ является открытым ключом криптосистемы, а число $k_{зm}$ представляет собой закрытый ключ и храниться абонентом в тайне.

Рассмотренные действия являются подготовительными. Будем считать, что абонент m хочет передать абоненту $m+1$ сообщение x. Сообщение x должно удовлетворять условию $x < (N_{m+1})$.

Абонент m осуществляет шифрование в соответствии с выражением:

$$y = x^{k_{om+1}} \bmod N_{m+1},$$

при этом, как видно, используется открытый ключ абонента $m+1$.

Абонент $m+1$, получивший криптограмму y расшифровывает ее:

$$x = y^{k_{зm+1}} \bmod N_{m+1}.$$

На основании вышесказанного можно сделать следующие выводы:

1) протокол криптосистемы RSA шифрует и расшифровывает информацию корректно;

2) злоумышленник, перехватывающий криптограммы и знающий все открытые ключи, не сможет найти исходное сообщение при больших p и q.

Действительно, злоумышленник знает только открытый ключ $\langle N_m, k_{om} \rangle$. Для того чтобы найти $k_{зm}$, злоумышленник должен знать значение функции Эйлера $\phi_m = (p_m - 1)(q_m - 1)$, а для этого он должен определить параметры p_m и q_m, разложив N_m на множители, т.е. решить задачу факторизации. Однако, для него это задача трудновыполнимая.

С другой стороны, односторонняя функция $y = x^{k_{om}} \bmod N_m$, также применяемая в RSA, обладает «секретом», позволяющим легко вычислить обратную функцию $x = \sqrt[k_{om}]{y} \bmod N_m$, если известно разложение на множители числа $N_m = p_m q_m$. Действительно, это легко сделать, вычислив сначала $\phi_m = (p_m - 1)(q_m - 1)$, а затем $k_{зm} = k_{om}^{-1} \bmod \phi_m$. Таким образом, параметры p_m и q_m являются «секретом» или, как еще говорят, «лазейкой».

Иногда рекомендуется выбирать открытый ключ k_{om} одинаковым для всех абонентов сети, например k_{om}=3. Это обеспечивает увеличение скорости шифрования.

Криптосистема Эль Гамаля. Криптосистема с открытым ключом Эль Гамаля формально определяется следующим образом [5]:

$$ElGamal = (X, Y, K, x, y, k_o, k_з, p, g, E, D),$$

где X - множество открытых текстов, Y - множество криптограмм, K - множество ключей, $x \in X$ - некоторый открытый текст, $y \in Y$ - некоторая криптограмма, $k_o \neq k_з$, $(k_o, k_з) \in K$ - ключи шифрования и расшифрования, удовлетворяющие условию: $k_o = g^{k_з} \bmod p$, p - большое простое число, g - число, такое что, различные степени числа g суть различные числа по модулю p, E - функция шифрования, D - функция расшифрования.

Для всей группы $m = \overline{1, M}$ абонентов сети выбирается некоторое большое простое число p и число g. Выбор числа g может оказаться трудной задачей при произвольно заданном числе p, т.к. это связано с разложением на простые множители числа $p-1$. Дело в том, что для обеспечения высокой стойкости алгоритма шифрования число $p-1$ должно обязательно содержать большой простой множитель, в противном случае с помощью алгоритма Полига-Хеллмана быстро вычисляется дискретный логарифм. В связи с этим простое число p выбирается таким, чтобы выполнялось равенство:

$$p = 2q + 1,$$

где q - простое число. Тогда в качестве g можно взять любое число, для которого справедливы неравенства:

$$1 < g < p - 1,\ g^q \bmod p \neq 1.$$

Числа p и g передаются абонентам сети в открытом виде. Затем каждый абонент сети выбирает секретный ключ $k_{зт}$, $m = \overline{1, M}$, удовлетворяющее условию: $1 < k_{зт} < p - 1$, и вычисляет открытый ключ:

$$k_{от} = g^{k_{зт}} \bmod p,\ m = \overline{1, M}.$$

Пусть абонент m хочет передать абоненту $m+1$ сообщение x, при этом необходимо выполнение условия: $x < p$.

Шифрование исходного сообщения x происходит следующим образом. Абонент m формирует случайное число c, причем $1 \le c \le p - 2$ (эту операцию выполняют все абоненты сети), и вычисляет числа

$$r = g^c \bmod p,$$
$$y = x \cdot k_{от+1}^c \bmod p,$$

а затем передает пару $\langle r, y \rangle$ абоненту $m+1$.

Абонент $m+1$ получив криптограмму $\langle r, y \rangle$ вычисляет исходный текст

$$x = y \cdot r^{p-1-k_{зm+1}} \bmod p.$$

Злоумышленник должен определить закрытый ключ $k_{зm}$ или отыскать число c, но для этого ему необходимо решить задачу дискретного логарифмирования.

Особенностью криптосистемы Эль Гамаля является то, что объем передаваемой криптограммы в два раза превышает объем исходного сообщения. Следствием этого является большее, по сравнению с алгоритмом RSA, время шифрования и больший объем вычислений.

1.2. Электронная подпись

Одна из важнейших проблем, решаемых с использованием асимметричных методов шифрования - проблема подтверждения авторства (достоверности источника информации). Данная проблема возникает при следующих обстоятельствах:

- когда некоторый абонент m получает сообщение, предположительно от абонента $m+1$, как подтвердить, что получено сообщение именно от абонента m, а не от третьего лица;
- когда абонент m получает от абонента $m+1$ сообщение, как подтвердить, что оно не было изменено третьим лицом.

Для решения этой проблемы были разработаны алгоритмы электронной подписи. Определение электронной подписи дано федеральным законом №63-ФЗ от 6.04.2011 г.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Во многих странах мира, в том числе в России, введены в действие стандарты на электронную подпись. В Европе и США, вместо термина «электронная подпись», чаще используется термин «цифровая подпись». Оба термина означают одно и то же.

Электронная подпись (ЭП) должна обладать следующими свойствами:

1) подписать документ может только законный владелец ЭП;

2) автор ЭП не может от нее отказаться;

3) в случае возникновения спора возможно участи третьих лиц (например, суда) для установления подлинности ЭП.

Из рассмотренных свойств можно определить злонамеренные действия, к которым относятся:

- **отказ (ренегатство)** – отправитель впоследствии отказывается от переданного сообщения;

- **фальсификация** – получатель (или третье лицо) подделывает сообщение;

- **изменение** - получатель (или третье лицо) вносит изменение в сообщение;

- **маскировка** – злоумышленник маскируется под легального пользователя.

Схема ЭП включает в себя:

- параметр безопасности n;

- пространство исходных сообщений;

- алгоритм G генерации пары ключей $(k_з, k_o)$;

- алгоритм S формирования подписи;

- алгоритм V проверки подписи.

Электронная подпись $s = S(k_з, x)$ называется **допустимой** для документа x, если она принимается алгоритмом V. **Подделкой** ЭП документа x называется нахождение злоумышленником, не имеющим секретного ключа, допустимой подписи для документа x.

Обобщенная схема ЭП имеет следующий вид (см. рис.1.14) [5]:

1. Отправитель А вычисляет $(k_з, k_o) = G(n)$ и посылает получателю В k_o.

2. Для получения подписи документа x отправитель вычисляет $s = S(k_з, x)$ и посылает $\langle x, s \rangle$ получателю.

3. Получатель вычисляет $V(x, s, k_o)$ и в зависимости от результата принимает или отвергает подпись s отправителя А.

В классической схеме ЭП предполагается, что отправитель знает содержание подписываемого документа, а получатель проверяет подлинность ЭП без какого-либо разрешения и участия отправителя А.

При формировании ЭП по классической схеме отправитель А вычисляет хеш-функцию (хеш-образ) документа $h_x = h(x)$ и при необходимости дополняет его до требуемой длины. Алгоритм вычисления хеш-функции известен всем абонентам сети. Не будем пока останавливаться на свойствах и способах вычисления хеш-функции, этот вопрос буде рассмотрен подробнее в следующей главе. Отметим только важные для нас сейчас свойства:

1) хеш-функция обеспечивает преобразование входного массива данных любого размера в выходной массив данных (хеш) фиксированного размера;

2) практически невозможно внести изменения в входной массив данных, не изменив выходной массив данных (хеш).

Отправителю А достаточно снабдить подписью не сам документ x, а его хеш-образ h_x.

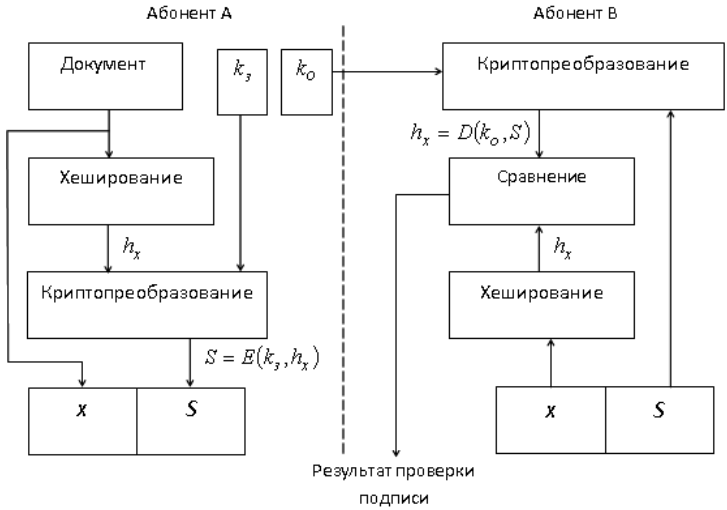

Рисунок 1.14. Обобщенная схема формирования и проверки ЭП

Электронная подпись на основе криптосистемы RSA. Пусть некоторая сеть включает в себя M абонентов. Абонент m планирует подписывать документы. Вначале абонент должен сформировать параметры криптосистемы RSA (см. пункт 1.3). Для этого абонент выбирает два больших простых числа p_m, q_m и вычисляет $N_m = p_m q_m$, $\phi_m = (p_m - 1)(q_m - 1)$. Затем абонент выбирает число $k_{om} < \phi_m$, взаимно простое с ϕ_m, а затем находит $k_{зm} = k_{om}^{-1} \bmod \phi_m$.

Абонент публикует в сети, ассоциировав со своим именем, числа $\langle N_m, k_{om} \rangle$, а число $k_{зm}$ хранит в тайне. Числа p_m, q_m, ϕ_m в вычислениях больше не используются. На этом шаге формирование параметров криптосистемы заканчивается. Абонент готов подписывать документы.

На следующем шаге абонент вычисляет хеш-функцию (или просто - хеш) подписываемого документа $h_x = h(x_m)$. Далее абонент вычисляет число

$$s = h_x^{k_{зm}} \bmod N_m,$$

которое представляет собой ЭП. Число s добавляется к документу x_m и абонент получает подписанный документ $\langle x_m, s \rangle$.

Каждый абонент сети, который знает параметры абонента m, может проверить подлинность его подписи. Для этого необходимо из подписанного документа $\langle x_m, s \rangle$ взять x_m и вычислить хеш-образ h_x. Затем вычислить число

$$\omega = s^{k_{om}} \bmod N_m,$$

и проверить выполнение равенства $\omega = h_x$. Если ЭП подлинная, то $\omega = h_x = h(x_m)$.

Электронная подпись на основе криптосистемы Эль Гамаля. Пусть, как и в предыдущем случае, абонент m собирается подписывать документы. На первом шаге формируются параметры криптосистемы Эль Гамаля. Абонент выбирает большое простое число p и число g, такое, что различные степени g суть различные числа по модулю p. Эти числа храниться в открытом виде и могут быть общими для целой группы абонентов. Затем абонент m выбирает случайное число $k_{зm}$, $1 < k_{зm} < p-1$, которое держится в секрете. Затем абонент вычисляет число

$$k_{om} = g^{k_{зm}} \bmod p,$$

которое является открытым. Теперь абонент готов подписывать документы.

На следующем шаге абонент вычисляет хеш-функцию исходного документа $h_x = h(x_m)$, которая должна удовлетворять условию $1 < h_x < p$.

На третьем шаге абонент выбирает случайное число c, $1 < c < p-1$, взаимно простое с $p-1$ и вычисляет числа

$$\begin{gathered} r = g^c \bmod p, \\ u = (h_x - k_{зm} \cdot r) \bmod (p-1), \\ s = c^{-1} \cdot u \bmod (p-1). \end{gathered}$$

где $c^{-1} c \bmod (p-1) = 1$. Числа $\langle s, r \rangle$ является ЭП. Таким образом, подписанное сообщение имеет вид $\langle x_m; s, r \rangle$.

Получатель подписанного документа заново вычисляет хеш-функцию $h_x = h(x_m)$. Затем проверяет подлинность подписи, используя равенство

$$k_{om}^r \cdot r^s = g^{h_x} \bmod p.$$

Если ЭП верна, то условие выполняется.

Первое свойство ЭП выполняется, т.к. никто кроме законного владельца не знает $k_з$. По этой же причине выполняются второе и третье свойства ЭП.

Основное отличие ЭП на базе криптосистемы Эль Гамаля от ЭП на базе криптосистемы RSA заключается в длине подписи. ЭП на базе

криптосистемы RSA $\langle x_m, s \rangle$, практически в два раза короче, чем ЭП на базе криптосистемы Эль Гамаля $\langle x_m; s, r \rangle$, т.е. если длина ЭП RSA 1024 бит, то длина ЭП Эль Гамаля 2048бит.

В многих странах мира, включая РФ, существуют национальные стандарты ЭП.

Как показано выше, в алгоритмах ЭП используются алгоритмы вычисления хэш-образа документа. Определим понятие хэш функции.

Хеш-функцией называется преобразование h, превращающее последовательность x произвольной длины в информационную последовательность h_x фиксированной длины [5].

В общем случае h_x гораздо меньше, чем x, например, h_x может быть 128 или 256 бит, тогда как x может быть размером в мегабайты и более.

Хеширование иногда считают видом криптографического преобразования. Вместе с тем, криптографическое преобразование, по определению, является обратимым, а хеширование представляет собой необратимое преобразование.

Для того чтобы хеш-функция могла быть использована в криптографических алгоритмах она должна обладать следующими свойствами [5]:

- преобразование h может быть применено к x любого размера;
- выходное значение h_x должно иметь фиксированный размер;
- значение h_x достаточно просто вычисляется для любого x;
- для любого значения h_x с вычислительной точки зрения невозможно найти x;
- для любого значения x с вычислительной точки зрения невозможно найти $x' \neq x$, такое, что $h(x) = h(x')$;
- значение хеш-функции h_x должно быть чувствительным к любым изменениям входной информационной последовательности x.

Если хеш-функция обладает перечисленными свойствами, то она считается качественной. Для качественной хеш-функции три следующие задачи являются вычислительно неразрешимыми.

1. **Задача нахождения прообраза** – это задача нахождения входной последовательности x по заданному хеш-образу h_x. Хеш-функция должна быть стойкой в смысле обращения.

2. **Задача нахождения коллизий** – это задача нахождения последовательностей x' и x'', причем $x' \neq x''$, для которых $h(x') = h(x'')$. Хеш-функция должна быть стойкой в смысле нахождения коллизий.

3. **Задача нахождения второго прообраза** – это задача нахождения для заданной входной последовательности x другой входной последовательности x', причем $x' \neq x$, такой, что $h(x) = h(x')$. Эта задача является разновидностью задачи нахождения коллизий.

Подавляющее большинство современных алгоритмов хеширования строится или по итерационной схеме, или на основе симметричных блочных криптосистем.

1.3 Методы аутентификации

Для предотвращения работы с системой незаконных пользователей, необходима процедура распознавания каждого законного пользователя (или групп пользователей). Для этого в системе храниться информация, по которой можно опознать пользователя, а пользователь при входе в систему, при выполнении определенных действий, при доступе к ресурсам обязан себя **идентифицировать**, т.е. указать идентификатор, присвоенный ему в данной системе. Получив идентификатор, система проводит его аутентификацию, т.е. проверяет его подлинность - принадлежность множеству идентификаторов. Если бы идентификация не дополнялась аутентификацией, то сама идентификация теряла бы всякий смысл. Обычно устанавливается ограничение на число попыток предъявления некорректного идентификатора.

Аутентификация пользователя основана на следующих принципах [7]:

- на предъявлении пользователем пароля;
- на предъявлении пользователем доказательств, что он обладает секретной ключевой информацией;
- на ответах на некоторые тестовые вопросы;
- на предъявлении пользователем некоторых неизменных признаков, неразрывно связанных с ним;
- на предоставлении доказательств того, что он находится в определенном месте в определенное время;
- на установлении подлинности пользователя некоторой третьей доверенной стороной.

Процедуры аутентификации должны быть устойчивы к подлогу, подбору и подделке.

После распознавания пользователя система должна выяснить, какие права предоставлены этому пользователю, какую информацию он может использовать и каким образом (читать, записывать, модифицировать или удалять), какие программы может выполнять, какими ресурсы ему доступны, а также другие вопросы подобного рода. Этот процесс называется авторизацией. Таким образом, вход пользователя в систему состоит из идентификации, аутентификации и авторизации. В процессе дальнейшей работы иногда может появиться необходимость дополнительной авторизации в отношении каких-либо действий.

Методы аутентификации можно разделить в зависимости от целей аутентификации. Если целью аутентификации является доказательство подлинности предъявленного субъектом идентификатора, то такая аутентификация является **аутентификацией субъекта**. Если в процессе аутентификации проверяется подлинность идентификатора, представленного

с некоторыми данными, то такая аутентификация является а**утентификацией объекта**. В отличие от аутентификации субъекта в этой ситуации субъекту не нужно быть активным участником процесса аутентификации.

Рассмотрим методы аутентификации субъекта и объекта [7].

Аутентификация субъекта. Классическим средством аутентификации субъекта являются парольные схемы. При этом для устранения последствий несанкционированного доступа злоумышленника к информации, хранящейся в памяти системы, передаваться может не сам пароль pw (password), а его хеш-образ $h_{pw} = h(pw)$ (см. рис. 1.15). Функция h_{pw} в этой ситуации может быть определена как:

$$h_{pw} = h(pw) = E_{pw}(ID),$$

если длина пароля и длина ключа функции шифрования E одинаковы $|pw| = |k|$, или как

$$h_{pw} = h(pw) = E_{pw \oplus k}(ID)$$

если длина пароля меньше длины ключа $|pw| < |k|$.

Верификатор системы заранее вычисляет значения $h_{pw} = h(pw)$ и для каждого идентификатора ID хранит эти значения.

Пользователь, прошедший идентификацию, вводит пароль pw^*, затем вычисляет его хеш-образ $h^*_{pw} = h(pw^*)$, а верификатор системы проверяет выполнение условия $pw = pw^*$. При выполнении условия принимается решение о правильности пароля и разрешается доступ пользователя в систему.

Вместе с тем такая схема не позволяет защищать от злоумышленника, который может передавать информацию, подключаясь непосредственно к линии связи. В этом случае применяется другая схема (см. рис. 1.16). В данной схеме процедура вычисления $h^*_{pw} = h(pw^*)$ возложена на верификатора системы.

Обе рассмотренные схемы парольной аутентификации не защищают от атак перехвата и повтора, когда злоумышленник записывает информацию, передаваемую пользователем, и организует ее повторение для входа в систему.

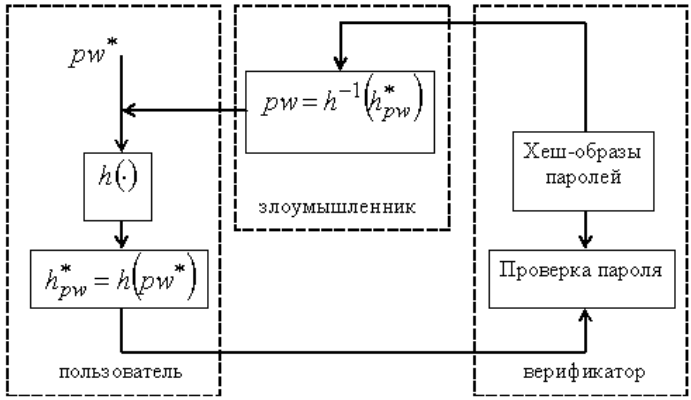

Рисунок 1.15 Парольная схема аутентификации (вариант 1)

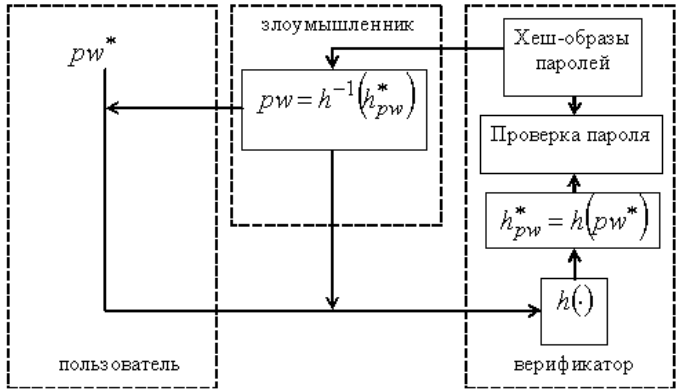

Рисунок 1.16 Парольная схема аутентификации (вариант 2)

Для устранения последствий перехвата информации, передаваемой пользователем, или несанкционированного доступа злоумышленника к информации, хранящейся в памяти верификатора, может быть рекомендована схема, представленная на рис. 1.17, предполагающая использование двух хеш-функций h_1 и h_2, причем результат работы второй из них зависит от неповторяющегося блока данных RB.

Аутентификация субъекта может быть как **односторонней**, так и **взаимной**. В первом случае процедуру аутентификации проходит один субъект, во втором случае аутентифицируют друг друга два взаимодействующих субъекта, например связывающиеся между собой по линиям связи. Взаимная аутентификация не есть простое объединение двух сеансов односторонней аутентификации, так как в последнем случае противник легко может осуществить атаку перехвата и повтора, выдавая себя

за верификатора перед пользователем и за пользователя перед верификатором.

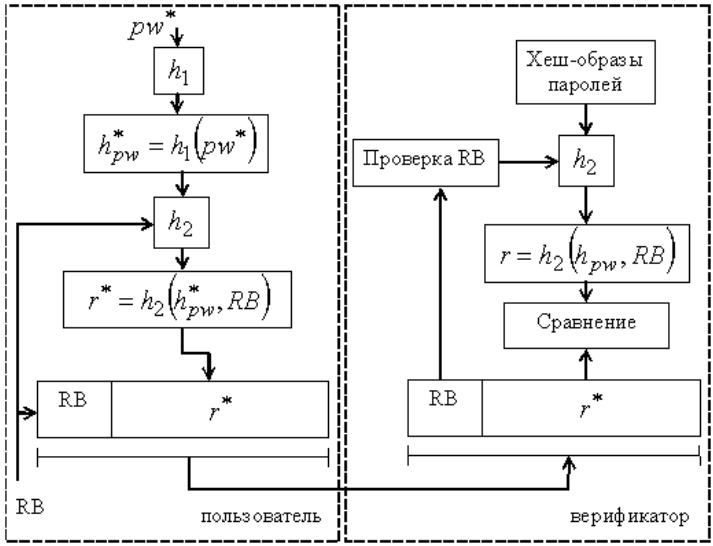

Рисунок 1.17. Парольная схема аутентификации, защищенная от повтора

Проверка подлинности предполагает использование неповторяющихся блоков данных, в качестве которых используются временные метки, механизмы запрос-ответ и процедуры рукопожатия (см. рис. 1.18).

Использование **меток времени** позволяет регистрировать время отправки конкретного сообщения, что дает возможность получателю определить, насколько «устарело» пришедшее сообщение, а значит, защититься от повтора. При использовании меток времени возникает проблема допустимого времени задержки, связанная, во-первых, с невозможностью мгновенной передачи сообщения, а во-вторых, с невозможностью абсолютной синхронизации хода часов получателя и отправителя.

Механизм **запрос-ответ** предполагает включение пользователем А в сообщение для пользователя В запроса x_A - некоторого случайного числа. Перед ответом пользователь В обязан выполнить над числом x_A некоторую операцию, например вычислить хеш-образ $h(x_A)$. Получив ответ с правильным результатом вычислений, пользователь А может быть уверен, что В - подлинный.

Процедура **рукопожатия** заключается во взаимной проверке ключей, используемых субъектами взаимодействия. Последние признают друг друга

законными партнерами, если докажут друг другу, что обладают правильными ключами.

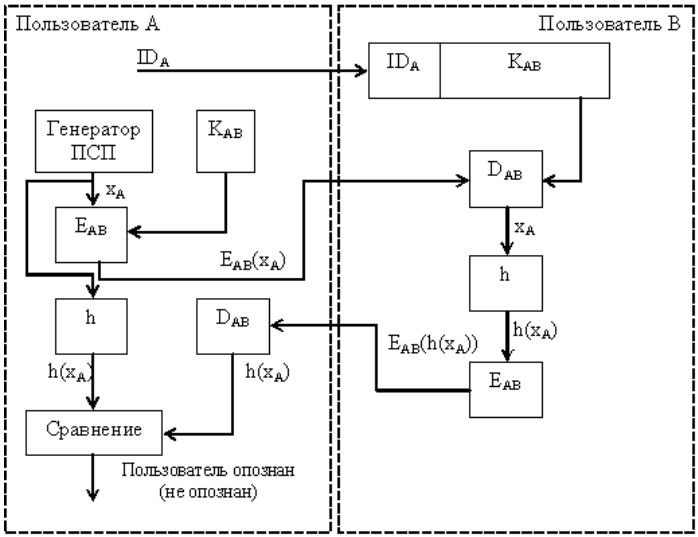

Рисунок 1.18. Парольная схема с механизмом запрос-ответ и рукопожатием

Аутентификация субъекта может осуществляться с помощью симметричных и ассиметричных криптосистем.

Аутентификация с использованием симметричных криптосистем в системах с большим числом пользователем требует введения в сеанс связи доверенной стороны. Такая схема аутентификации носит название **схемы аутентификации Нидхэма-Шредера** (см. рис. 1.19). На рисунке показано процедура взаимной аутентификации двух пользователей А и В с использованием третьей доверенной стороны – С, обладающей секретными ключами k_{AC} и k_{BC}. Последовательность шагов процедуры следующая:

1) пользователь А, который хочет взаимодействовать с пользователем В, посылает С сообщение, содержащее идентификаторы субъектов запрашиваемого взаимодействия

$$\{ID_A, ID_B\};$$

2) С, получив сообщение, формирует сеансовый ключ k_{AB} для взаимодействия пользователей А и В и посылает А зашифрованное сообщение

$$E_{k_{AC}}\left(ID_B, k_{AB}, E_{k_{BC}}\left(ID_A, k_{AB}\right)\right),$$

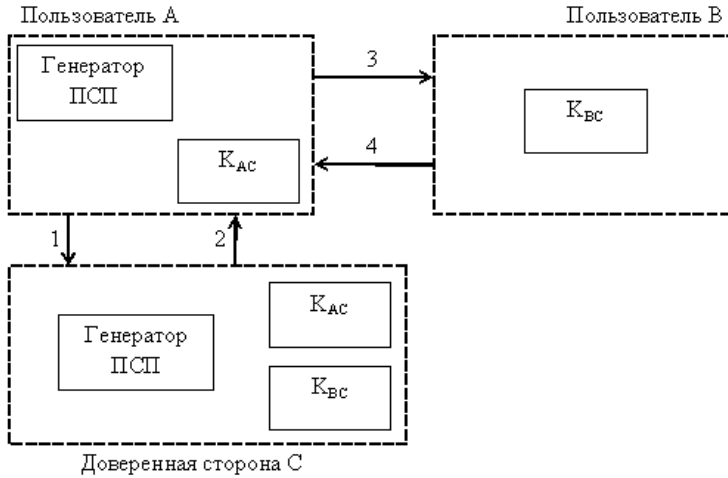

Рисунок 1.19. Схема аутентификации Нидхэма-Шредера

содержащее сеансовый ключ для работы с В и криптограмму, которая по сути является разрешением для А на работу с В;

3) пользователь А, расшифровав полученное сообщение, определяет ключ k_{AB} и разрешение

$$E_{k_{BC}}(ID_A, k_{AB}),$$

которое он расшифровать не может, так как не знает ключа k_{BC}; после этого А отправляет В сообщение

$$\left\{E_{k_{AC}}(ID_A, x_A), E_{k_{BC}}(ID_A, k_{AB})\right\},$$

содержащее зашифрованный запрос x_A и разрешение, полученное от С;

4) В, расшифровав криптограмму

$$E_{k_{BC}}(ID_A, k_{AB})$$

узнает идентификатор пользователя взаимодействия и сеансовый ключ k_{AB} для работы с ним, читает запрос x_A; после этого В формирует ответ на запрос $h(x_A)$ и отправляет А сообщение

$$E_{k_{AB}}(ID_B, h(x_A));$$

5) пользователь А, получив сообщение, расшифровывает его и проверяет ответ В; в случае положительного результата проверки процесс аутентификации успешно завершается.

В качестве третьей доверительной стороны выступает центр генерации и распределения ключей (ЦГРК). Данная трехсторонняя схема, по сути, является аутентифицированной схемой распределения сеансовых колючей. ЦГРК должен обладать высокой защищенностью, т.к. его компрометация приводит к компрометации всей сети.

Рассмотрим двусторонние схемы аутентифицированного распределения ключей.

Пусть пользователи А и В располагают заранее известным ключом k_{AB}, используемым не для шифрования, а для пересылки ключевой информации. Передача разового сеансового ключа k от А к В осуществляется с помощью пересылки криптограммы $E_{k_{AB}}(I)$, где

$$I = (k, t, ID_B).$$

Здесь t - метка времени, ID_B - идентификатор абонента В.

Для аутентификации сеанса можно использовать следующую схему, основанную на методе запрос-ответ.

Пользователь В генерирует случайное число x_B и отправляет его пользователю А. Пользователь А вычисляет криптограмму

$$E_{k_{AB}}(I), \text{ где } I = (k, x_B, ID_B),$$

и отправляет ее В, который расшифровав криптограмму убеждается, что имеет дело с пользователем А.

Взаимная аутентификация сеанса может быть осуществлена по протоколу, являющемуся модификацией предыдущего.

Пусть k_A и k_B - случайные числа, сгенерированные пользователями А и В. Последовательность шагов процедуры следующая:

1) пользователь В генерирует случайное число x_B и отправляет его абоненту А (впоследствии абонент А должен предъявить это число абоненту В);

2) пользователь А генерирует случайное число x_A (впоследствии абонент В должен предъявить это число абоненту А), вычисляет криптограмму

$$E_{k_{AB}}(I), \text{ где } I = (k_A, x_A, x_B, ID_B),$$

и отправляет ее пользователю В. Последний расшифровывает криптограмму, и тем самым А предъявляет число x_B абоненту В;

3) пользователь В вычисляет криптограмму

$$E_{k_{AB}}(J), \text{ где } J = (k_B, x_A, x_B, ID_A),$$

и отправляет ее абоненту А. Последний расшифровывает криптограмму, и тем самым В предъявляет число x_A абоненту А;

4) каждая из сторон вычисляет сеансовый ключ с помощью заданной функции

$$k = f(k_A, k_B).$$

Ни один из пользователей заранее не знает сеансового ключа.

Аутентификация с использованием ассиметричных криптосистем. Использование ассиметричных криптосистем позволяет отказаться от серверов аутентификации, однако в системе должен существовать сервер, выдающий сертификаты на используемые пользователями сети открытые ключи. **Сертификатом** принято называть электронный документ, удостоверяющий принадлежность данного открытого ключа данному пользователю сети, иначе говоря, аутентичность ключа.

Классическим примером несимметричной аутентификации может служить схема Диффи-Хэллмана, представляющая собой совокупность процедуры выработки общего секретного ключа и взаимной аутентификации пользователей сети. **Схема Диффи-Хеллмана** была предложена авторами в середине 70-годов прошлого века и привела к настоящей революции в криптографии и ее практических применениях.

При использовании симметричных криптосистем, для сети, имеющей N абонентов, причем N - достаточно большое число, количество секретных ключей должно быть $\approx \frac{N^2}{2}$. Таким образом, система обеспечивающая сеть ключами является достаточно громоздкой и дорогостоящей. Диффи и Хеллман решили эту проблему за счет использования открытого распределения и вычисления ключей.

Пусть система связи состоит из трех пользователей А, В и С. Для организации системы связи выбирается большое простое число p и некоторое число g, $1 < g < p-1$, такое что все числа из множества $\{1,2,3,..., p-1\}$ могут быть представлены как различные степени $g \bmod p$. Другими словами, g - примитивный элемент поля Галуа $GF(p)$. Числа p и g известны всем пользователям.

Пользователи выбирают числа $k_{зA}$, $k_{зB}$, $k_{зC}$, которые являются закрытыми ключами. Затем пользователи вычисляют открытые ключи:

$$k_{oA} = g^{k_{зA}} \bmod p,\ k_{oB} = g^{k_{зB}} \bmod p,\ k_{oC} = g^{k_{зC}} \bmod p.$$

Пусть пользователь А решил организовать сеанс связи с В. Пользователь А сообщает В по открытому каналу, что он хочет передать ему сообщение. Затем пользователь А вычисляет:

$$Z_{AB} = \left(k_{oB}\right)^{k_{3A}} \bmod p.$$

В свою очередь, абонент В вычисляет число

$$Z_{BA} = \left(k_{oA}\right)^{k_{3B}} \bmod p.$$

$$Z_{AB} = Z_{BA}.$$

Таким образом, пользователи А и В получают одно и тоже число $k = Z_{AB} = Z_{BA}$, являющееся сеансовым ключом, причем это число не передавалось по линии связи.

Рассмотренный протокол не является аутентичным. Пользователи никак не подтверждают подлинность друг друга. Злоумышленник может замаскироваться под одного из пользователей системы, предъявив свой открытый ключ. Рассмотрим аутентичную схему распределения ключей Диффи-Хеллмана.

1) пользователь А вырабатывает случайное число x_A и отправляет пользователю В сообщение

$$g^{x_A} \bmod p;$$

2) пользователь В вырабатывает случайное число x_B и вычисляет

$$g^{x_B} \bmod p,$$

и на своем закрытом ключе создает подпись

$$S_B\left(g^{x_A} \bmod p, g^{x_B} \bmod p\right),$$

сообщения $\left(g^{x_A} \bmod p, g^{x_B} \bmod p\right)$. Затем В вычисляет сеансовый ключ

$$k_{AB} = g^{x_A x_B} \bmod p,$$

зашифровывает подпись на этом ключе и отправляет А сообщение

$$\left\langle g^{x_B} \bmod p; E_{k_{AB}}\left\{S_B\left(g^{x_A} \bmod p, g^{x_B} \bmod p\right)\right\}\right\rangle;$$

3) пользователь А вычисляет сеансовый ключ

$$k_{AB} = g^{x_A x_B} \bmod p$$

с помощью своего секретного ключа создает подпись

$$S_A\left(g^{x_A} \bmod p, g^{x_B} \bmod p\right),$$

зашифровывает ее и отправляет В сообщение

$$\left\langle E_{k_{AB}}\left\{S_A\left(g^{x_A} \bmod p, g^{x_B} \bmod p\right)\right\}\right\rangle.$$

Если проверка подписи В абонентом А завершилась успешно, т.е. А убедился в справедливости равенства

$$S_B^{-1}\left\{D_{k_{AB}}\left(E_{k_{AB}}\left\{S_B\left(g^{x_A} \bmod p, g^{x_B} \bmod p\right)\right\}\right)\right\} = \left(g^{x_A} \bmod p, g^{x_B} \bmod p\right),$$

он может быть уверен в подлинности пользователя В. Если проверка подписи А пользователем В завершилась успешно, т.е. В убедился в справедливости равенства

$$S_A^{-1}\left\{D_{k_{AB}}\left(E_{k_{AB}}\left\{S_A\left(g^{x_A} \bmod p, g^{x_B} \bmod p\right)\right\}\right)\right\} = \left(g^{x_A} \bmod p, g^{x_B} \bmod p\right),$$

он в свою очередь может быть уверен в подлинности пользователя А.

Одним из наиболее эффективных протоколов аутентификации является **протокол Шнорра**.

Пусть p и q - простые числа, такие, что q делит $(p-1)$. Шнорр предлагал использовать p разрядностью не менее 512 битов и q разрядностью не менее 140 битов. Пусть $g \in Z_p$, Z_p - множество целых чисел от 0 до $(p-1)$, такое, что

$$g^q \bmod p = 1, g \neq 1.$$

Протокол Шнорра основан на проблеме дискретного логарифма. В качестве закрытого ключа пользователь выбирает некоторое случайное число $k_з \in Z_p$, а открытый ключ вычисляет $k_o = g^{k_з} \bmod p$.

Схема аутентификации Шнорра состоит в следующем:

1) пользователь А выбирает случайное число $x_A \in Z_p$, вычисляет

$$y_A = g^{x_A} \bmod p,$$

и посылает его пользователю В;

2) пользователь В выбирает случайное t-разрядное число $x_B \in \{0,1,..., (2^t - 1)\}$ и посылает его пользователю А;

3) пользователь А вычисляет

$$s = x_A + k_{3A} x_b \bmod q$$

и посылает его пользователю В;

4) пользователь В проверяет соотношение

$$y_A = g^s (k_{oA})^{x_B} \bmod p,$$

и, если оно выполняется, признает подлинность пользователя А.

Злоумышленник, знающий только открыты ключ k_o, p, q и g не может пройти аутентификацию. Шнорр рекомендовал использовать t разрядностью не менее 72 битов.

Аутентификация объекта. В процессе аутентификации объекта, иногда называемой аутентификацией источника данных, проверяется подлинность идентификатора, представленного с некоторыми данными. В отличие от аутентификации субъекта в этой ситуации пользователю не нужно быть активным участником процесса аутентификации. Данный тип аутентификации (см. рис. 1.20) по сути, ничем не отличается от процедуры контроля целостности.

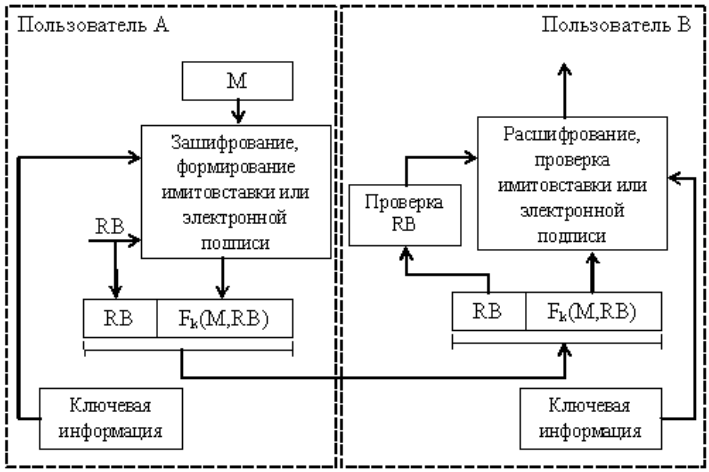

Рисунок 1.20. Схема аутентификации объекта

Для аутентификации объекта применяется шифрование симметричным алгоритмом, выработка имитовставки или электронной подписи. Первые два варианта применяются в том случае, когда пользователь и верификатор доверяют друг другу. Если необходимо иметь возможность доказательства подлинности идентификатора третьей стороне (при условии, что верификатор не имеет возможности изменить массив данных), например, необходима юридическая значимость пересылаемых электронных документов, требуется электронная подпись.

1.5. Имитозащита информации

Информация в каналах обмена данными и управления БАС подвергается случайным и умышленным деструктивным воздействиям. Для обнаружения случайных искажений информации применяются корректирующие коды, которые в некоторых случаях позволяют не только зафиксировать факт наличия искажений информации, но локализовать и исправить эти искажения.

Умышленные деструктивные воздействия чаще всего имеют место при хранении информации в памяти компьютера и при ее передаче по каналам связи. При этом полностью исключить возможность несанкционированных изменений в массивах данных не представляется возможным. Следовательно, крайне важно оперативно обнаружить такие изменения, так как в этом случае ущерб, нанесенный законным пользователям, будет минимальным.

Как правило, целью злоумышленника, навязывающего ложную информацию, является выдача ее за подлинную, поэтому своевременная фиксация факта наличия искажений в массиве данных сводит на нет все усилия злоумышленника.

Под **имитозащитой** понимают не только исключение возможности несанкционированных изменений информации, а совокупность методов, позволяющих достоверно зафиксировать факты изменений, если они имели место.

Для обнаружения искажений в распоряжении законного пользователя (например, получателя информации при ее передаче) должна быть некая процедура проверки $F(x)$, дающая на выходе 1, если в массиве данных x отсутствуют искажения, или 0, если такие искажения имеют место. Идеальная процедура такой проверки должна обладать следующими свойствами [7]:

- невозможно найти такое сообщение x' способом, более эффективным, чем полный перебор по множеству допустимых значений x (такая возможность в распоряжении противника имеется всегда);
- вероятность успешно пройти проверку у случайно выбранного сообщения x' не должна превышать заранее установленного значения.

Учитывая, что в общем случае все возможные значения x могут являться допустимыми, второе требование требует внесения избыточности в

защищаемый массив данных. При этом чем больше разница между размером преобразованного избыточного x' и размером исходного x массивов, тем меньше вероятность принять искаженные данные за подлинные.

На рис. 1.21-1.23 показаны некоторые возможные варианты внесения такой избыточности. В роли неповторяющегося блока данных RB могут выступать метка времени, порядковый номер сообщения и т.п. В роли контрольного кода могут выступать имитовставки или ЭП. **Имитовставкой** принято называть контрольный код, который формируется и проверяется с помощью одного и того же секретного ключа.

Использование блока RB позволяет контролировать целостность потока сообщений, защищая от повтора, задержки, переупорядочивания или их утраты. При использовании в качестве RB порядкового номера получатель, получив $(i+1)$-е сообщение, проверяет равенство $RB_{i+1} = RB_i + 1$, т.е. что его номер на единицу больше номера предыдущего i-го сообщения. При использовании в качестве RB метки времени получатель контролирует, чтобы времена отправки и приема сообщений соответствовали друг другу с учетом задержки в канале связи и разности показаний часов отправителя и получателя.

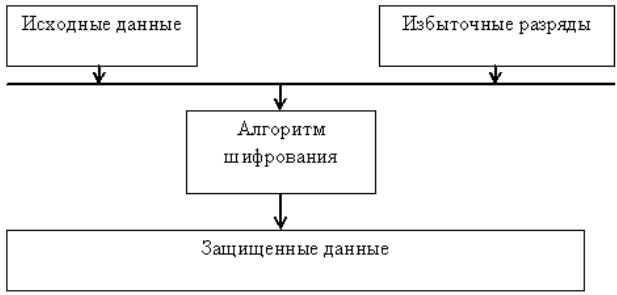

Рисунок 1.21 Схема контроля целостности с использованием шифрования

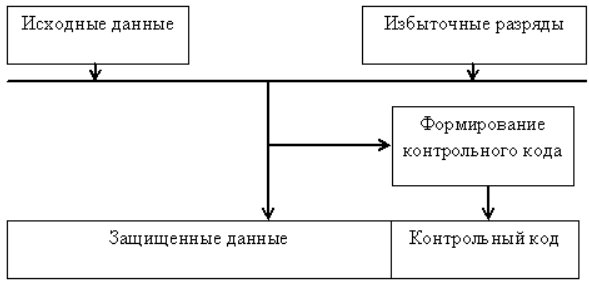

Рисунок 1.22 Схема контроля целостности с контрольным кодом

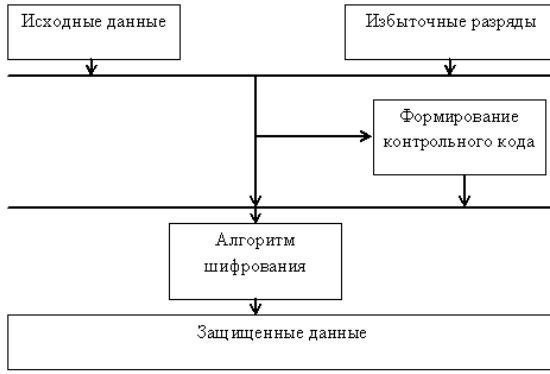

Рисунок 1.23 Схема контроля целостности с контрольным кодом и шифрованием

Целостность потока сообщений можно также контролировать, используя шифрование со сцеплением сообщений (см. рис. 1.24).

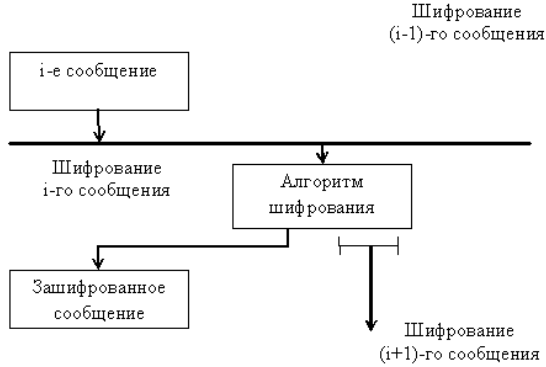

Рисунок 1.24. Контроль целостности потока сообщений

Самый естественный способ преобразования информации с внесением избыточности - это добавление к исходным данным контрольного кода s фиксированной разрядности N, вычисляемого как некоторая функция от этих данных:

$$x' = (x, s) = (x, f(x)), \ |s| = N.$$

В этой ситуации выделение исходных данных из преобразованного массива x' суть простое отбрасывание контрольного кода s. Проверка же целостности заключается в вычислении для содержательной части x' полученного массива данных контрольного кода $s' = f(x')$, и сравнении его с переданным значением s. Если они совпадают, сообщение считается подлинным, в противном случае ложным:

$$F(x') = \begin{cases} 1, & s = f(x'), \\ 0, & s \neq f(x'). \end{cases}$$

Функция $f(\cdot)$ формирования контрольного кода должна удовлетворять следующим требованиям:

- она должна быть вычислительно необратимой, т.е. подобрать массив данных под заданный контрольный код можно только путем полного перебора по пространству возможных значений x;
- у злоумышленника должна отсутствовать возможность сформировать ложный массив данных (или ложное сообщение) x' и снабдить его корректно вычисленным контрольным кодом $s' = f(x')$.

Второе свойство можно обеспечить двумя способами: либо сделать функцию $f(\cdot)$ зависимой от некоторого секретного параметра (ключа), либо пересылать контрольный код отдельно от защищаемых данных.

Простейшим примером кода s является контрольная сумма блоков массива данных. Например, если $X = X_1 X_2 X_3 ... X_t$, то

$$s = f(X) = \sum_{i=1}^{t} X_i (\mathrm{mod}\, 2^n).$$

где n - разрядность.

Однако такое преобразование непригодно для имитозащиты, так как контрольная сумма не зависит от взаимного расположения блоков, а самое главное, соответствующее преобразование не является криптографическим. Процедура подбора данных под заданную контрольную комбинацию чрезвычайно проста. Пусть некий массив данных $X = X_1 X_2 X_3 ... X_t$ имеет контрольную сумму s. Тогда для внесения не обнаруживаемых искажений противнику достаточно дополнить произвольный ложный массив

$$X' = X'_1 X'_2 X'_3 ... X'_t,$$

еще одним блоком

$$X'_{t'+1} = s - \sum_{i=1}^{t'} X'_i (\mathrm{mod}\, 2^n).$$

Можно выделить два основных криптографических подхода к решению задачи защиты информации от несанкционированных изменений данных:

- формирование с помощью функции шифрования E_k блочного шифра **кода аутентификации сообщений MAC** (Message Authentication Code);

• формирование с помощью необратимой функции сжатия (*хеш-функции*) информации **кода обнаружения манипуляций с данными MDC** (Manipulation Detection Code).

В табл. 1.1 приведена сравнительная характеристика указанных двух подходов [5-7]. Главное различие между кодами MAC и MDC заключается в том, что в первом случае для формирования контрольного кода требуется секретная информация, а во втором - нет.

Таблица 1.1. Сравнительная характеристика MAC и MDC

Параметр	MAC	MDC
Используемое преобразование	Функция шифрования блочного шифра	Хеш-функция
Секретная информация	Секретный ключ	Нет
Возможность для противника вычислить контрольный код	Отсутствует	Присутствует
Хранение и передача контрольного кода	Вместе с защищаемыми данными	Отдельно от защищаемых данных
Дополнительные условия	Требует предварительного распределения ключей	Необходим аутентичный канал для передачи контрольного кода
Области использования	Защита при передаче данных	Защита при разовой передаче данных, контроль целостности хранимой информации

Код аутентификации сообщений. Формирование кода MAC с использованием функции шифрования блочного шифра официально закреплено во многих государственных стандартах шифрования. Имитовставка ГОСТ 28147-89 является классическим примером кода MAC. Код аутентификации сообщений может формироваться в режимах CBC или CFB, обеспечивающих зависимость последнего блока криптограммы от всех блоков открытого текста. В случае использования преобразования E_k для выработки контрольного кода требования к нему несколько отличаются от требований при его использовании для шифрования: во-первых, не требуется свойство обратимости; во-вторых, его криптостойкость может быть снижена (например, за счет уменьшения числа раундов шифрования как в ГОСТ 28147-89). Действительно, в случае выработки кода MAC преобразование всегда выполняется в одну сторону, при этом в распоряжении злоумышленника есть только зависящий от всех блоков открытого текста контрольный код, в то время как при шифровании у него имеется набор блоков криптограммы, полученных с использованием одного секретного ключа.

Существует вариант построения кода MAC на основе использования секретного ключа и функции хеширования, при котором хешированию подвергается результат конкатенации секретного ключа и исходного сообщения, поэтому, как и в классическом случае у злоумышленника, не

знающего ключа, отсутствует возможность вычислить контрольный код. Для повышения безопасности подобного алгоритма получения MAC создана схема вложенного MAC, в которой хеширование выполняется дважды. В американском стандарте FIPS 198 вложенный MAC назван HMAC (hashed MAC). В американском стандарте FIPS 113 определена схема формирования кода аутентификации сообщений, названная CMAC.

Код обнаружения манипуляций с данными. Код MDC есть результат действия хеш-функции. Иначе говоря, MDC — это хеш-образ сообщения X, к которому применили хеш-функцию, т.е. $s = h(X)$. Схема формирования кода MDC, обладающего гарантированной стойкостью, равной стойкости используемого шифра, может быть следующей:

1) массив данных X разбивается на блоки фиксированного размера, равного размеру ключа $|k|$ используемого блочного шифра, т.е.

$$X = X_1 X_2 X_3 ... X_t,$$
$$|X_1| = |X_2| = |X_3| = ... = |X_{m-1}| = |k|,\ 0 < |X_t| < |k|;$$

2) если последний блок X_t неполный, он дополняется каким-либо образом до нужного размера $|k|$;

3) вычисляется хеш-образ

$$s = h(X) = E_{X_t}(..E_{X_3}(E_{X_2}(E_{X_1}(s_0)))),$$

где s_0 - синхропосылка.

Задача подбора массива данных $X' = X'_1 X'_2 X'_3 ... X'_t$ под заданный контрольный код s эквивалентна системе уравнений, которую необходимо решить для определения ключа для заданных блоков открытого и закрытого (в режиме простой замены) сообщений. Однако в рассматриваемой ситуации нет необходимости решать всю систему

$$E_{X'_1}(s_0) = s_1, E_{X'_2}(s_1) = s_0, ..., E_{X'_t}(s_{X'-1}) = s,$$

достаточно решить одно уравнение

$$E_{X'_i}(s_{i-1}) = s_i,$$

относительно X'_i, остальные блоки массива X могут быть произвольными. Но и эта задача в случае использования надежной функции E_k вычислительно неразрешима.

К сожалению, приведенная схема формирования MDC не учитывает наличия так называемых **побочных ключей** шифра. Если для $k' \neq k$ справедливо

$$E_{k'}(X_i) = E_k(X_i),$$

где X_i - некоторый блок открытого текста, то такой код k' и является побочным ключом, т.е. ключом, дающим при шифровании блока X_i точно такой же результат, что и истинный ключ k.

Обнаружение противником побочного ключа при дешифровании сообщения не является особым успехом, так как с вероятностью, близкой к 1, на этом найденном побочном ключе он не сможет правильно расшифровать другие блоки закрытого текста, учитывая, что для различных блоков побочные ключи в общем случае также различны. В случае выработки кода MDC ситуация прямо противоположна: обнаружение побочного ключа означает, что противник нашел такой ложный блок данных, использование которого не изменяет контрольного кода [7].

Для уменьшения вероятности навязывания ложных данных в результате нахождения побочных ключей, при преобразовании применяются не сами блоки исходного сообщения, а результат их расширения по некоторому алгоритму. Под **расширением** понимается процедура получения блока данных большего размера из блока данных меньшего размера.

CRC-код. Идеальным средством защиты информации от случайных искажений являются CRC- коды (cyclic redundancy code). Достоинствами CRC-кодов являются [7]:

- высокая достоверность обнаружения искажений, доля обнаруживаемых искажений не зависит от длины массива данных и составляет $1-2^N$, где N - разрядность контрольного кода;
- зависимость контрольного кода не только от всех бит анализируемой информационной последовательности, но и от их взаимного расположения;
- высокое быстродействие, связанное с получением контрольного кода в реальном масштабе времени;
- простота аппаратной реализации и удобство интегрального исполнения;
- простота программной реализации.

К сожалению, простое условие пропуска искажений делает CRC-коды принципиально не пригодными для защиты от умышленных искажений информации.

Сущность процесса контроля целостности с использованием CRC-кодов заключается в следующем. Генератор CRC-кода инициализируется фиксированным начальным значением. Чаще всего в качестве начального заполнения используется либо код «все 0», либо код «все 1». Учитывая, что от начального состояния генератора достоверность метода не зависит, все дальнейшие рассуждения выполняются в предположении, что исходное состояние устройства - нулевое. Анализируемая двоичная последовательность преобразуется в короткий (обычно шестнадцати- или тридцатидвухразрядный) двоичный код - CRC-код. Значение полученного CRC-кода сравнивается с эталонным значением, полученным заранее для

последовательности без искажений. По результатам сравнения делается вывод о наличии или отсутствии искажений в анализируемой последовательности.

CRC-код часто называют **сигнатурой** *(signature*). Однако этот термин следует признать неудачным, создающим ненужную путаницу, так как термин *signature* может означать также и ЭП.

Процесс получения CRC-кода можно рассматривать как процедуру наложения псевдослучайной последовательности, формируемой регистром сдвига с линейной обратной связью (LFSR), на входную анализируемую последовательность.

Рассмотрим схему генератора CRC-кода, показанную на рис. 1.25. Входной анализируемой двоичной последовательности

$$A = a_0 a_1 a_2 ... a_i ... a_{m-1},\ a_i \in \{0,1\},\ i = \overline{0,(m-1)},$$

Можно поставить в соответствие многочлен $A(x)$ степени $(m-1)$. Тогда процесс получения CRC-кода эквивалентен делению многочлена $A(x)$ входной последовательности на характеристический многочлен $\varphi(x) = \Phi(x^{-1})x^N$ степени N генератора CRC-кода. В качестве характеристического многочлена чаще всего выбирается примитивный многочлен. Для случая, представленного на рис. 1.25 $\varphi(x) = x^4 + x + 1$.

Если

$$A(x) = \varphi(x)Q(x) + R(x),$$

где $Q(x)$ и $R(x)$ - соответственно частное и остаток от деления, то коэффициенты многочлена $Q(x)$ появляются на выходе триггера q_{N-1}, а коэффициенты многочлена $R(x)$ остаются в регистре генератора после прохождения всей последовательности A. Иначе говоря, CRC-код s в точности равен коду остатка R.

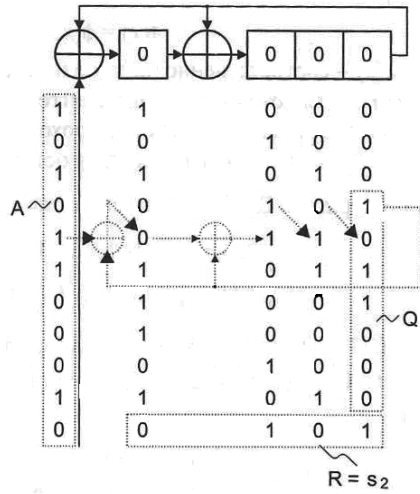

Рисунок 1.25. CRC-генератор

Работа генератора CRC-кода описывается системой линейных уравнений

$$\begin{cases} q_0(t+1) = \alpha_N q_{N-1}(t) \oplus a_t, \\ q_i(t+1) = \alpha_{N-i} q_{N-1}(t) \oplus q_{i-1}(t), i = \overline{1, N-1}, \end{cases}$$

где $q_i(t)$ и $q_i(t+1)$ - состояние j-го разряда (триггера) соответственно в моменты времени t и $t+1$, $t = \overline{0,m}$, $j = \overline{0, N-1}$. В матричной форме уравнение работы CRC-генератора имеет вид

$$\begin{bmatrix} q_0(t+1) \\ q_1(t+1) \\ .... \\ q_{N-1}(t+1) \end{bmatrix} = \begin{bmatrix} 0 & 0 & ... & \alpha_N \\ 1 & 0 & ... & \alpha_{N-1} \\ ... & ... & ... & ... \\ 0 & ... & 1 & \alpha_1 \end{bmatrix} \times \begin{bmatrix} q_0(t) \\ q_1(t) \\ ... \\ q_{N-1}(t) \end{bmatrix} + \begin{bmatrix} a_t \\ 0 \\ ... \\ 0 \end{bmatrix},$$

или

$$\mathbf{q}(t+1) = T_2 \mathbf{q}(t) \oplus \mathbf{a}(t),$$

где

$$\mathbf{q}(t)=\begin{bmatrix} q_0(t) \\ q_1(t) \\ ... \\ q_{N-1}(t) \end{bmatrix},\ \mathbf{q}(t+1)=\begin{bmatrix} q_0(t+1) \\ q_1(t+1) \\ ... \\ q_{N-1}(t+1) \end{bmatrix},\ \mathbf{a}(t)=\begin{bmatrix} a \\ 0 \\ ... \\ 0 \end{bmatrix},\ s=\mathbf{q}(m)=\begin{bmatrix} q_0(m) \\ q_1(m) \\ ... \\ q_{N-1}(m) \end{bmatrix}.$$

Таким образом, для CRC-генератора как линейного устройства справедлив принцип суперпозиции, который гласит: реакция линейного устройства на сумму двух входных воздействий равна сумме реакций на каждое воздействие в отдельности.

Пусть $A=a_0a_1a_2...a_i...a_{m-1}$ - анализируемая двоичная последовательность, $B=b_0b_1b_2...b_i...b_{m-1}$ - правильная последовательность (без искажений), e - последовательность, полученная в результате сложения по модулю 2 соответствующих элементов последовательностей A и B, т.е. для любого элемента последовательности e справедливо

$$e_i=a_i\oplus b_i, i=\overline{0,(m-1)}.$$

Единичные биты последовательности e соответствуют искаженным битам последовательности B, поэтому последовательности e логично назвать **последовательностью** или **вектором ошибок**. При отсутствии искажений

$$\forall i=\overline{0,(m-1)}, e_i=0.$$

Пусть $A(x)$, $B(x)$ и $e(x)$ - многочлены; S_A, S_B, S_e - CRC-коды соответственно последовательностей A, B и e. Искажения в последовательности A будут пропущены, если $S_A=S_B$. Имеем $A=B\oplus e$, откуда, применяя принцип суперпозиции, получаем равенство

$$s_A=s_B\oplus s_e.$$

Таким образом, необходимым и достаточным условием пропуска искажений является равенство $s_e=0$, которое имеет место, когда многочлен $e(x)$ нацело делится на многочлен $\varphi(x)$.

Пусть N-разрядность CRC-кода и $e\neq 0$, т.е. в анализируемой последовательности длиной m есть искажения. Рассмотрим достоверность метода, т.е. условия, при которых $S_e=0$. При $m\le N$ контрольный код не может быть нулевым, так как первая единица, попавшая в регистр генератора, не успевает выйти из него до конца формирования CRC-кода и не может быть уничтожена из-за сложения с битом обратной связи. Таким образом, при длине входной последовательности, меньшей или равной

разрядности CRC-кода, для $\forall e \neq 0$ справедливо $s_e \neq 0$, т.е. число не обнаруживаемых искажений равно $N_e = 0$. При $m = N + 1$, когда степень многочлена меньше или равна N, существует только один многочлен $e(x)$, нацело делящийся на многочлен $\varphi(x)$, это $e(x) = \varphi(x)$, а значит, в этом случае $N_e = 1$. При $m = N + 2$, существуют уже три многочлена $e(x)$, степени меньшей или равной $N + 1$, нацело делящиеся на многочлен $\varphi(x)$, это $e(x) = \varphi(x)$, $e(x) = \varphi(x) \times x$, $e(x) = \varphi(x) \times (x + 1)$, а значит, $N_e = 1$. В общем случае при $N > 1$ справедливо

$$N_e = 2^{m-N} - 1.$$

Учитывая, что общее число искажений в последовательности длиной m равно $2^m - 1$, для доли P_d обнаруживаемых искажений получаем соотношение

$$P_d = 1 - \frac{2^{m-N} - 1}{2^m - 1}.$$

На практике $m >> N$, а значит $2^m >> 1$, $2^{m-N} >> 1$,

$$P_d = 1 - \frac{2^{m-N}}{2^m} = 1 - 2^{-N}$$

Таким образом, доля обнаруживаемых искажений не зависит от длины анализируемой последовательности, а определяется лишь разрядностью контрольного кода.

2. МЕТОДЫ ЗАЩИТЫ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ ОТ РАДИОЭЛЕКТРОННОГО ПОДАВЛЕНИЯ

2.1. Классификация методов защиты от помех

Рассмотрим, какие различия между сигналом и помехой могут быть использованы в целях защиты БАС от активных помех [6,9,10,49]:

1. Могут быть применены различия в спектральном составе сигнала и помехи, которые реализуются с помощью различных фильтрующих схем. Методы защиты:

- перестройка по несущей частоте РЛС;
- оптимальная фильтрация сигналов.

2. Используются различия во временной структуре сигналов и помех, которые сами по себе представляют частный случай различий в спектрах. Методы защиты – селекция импульсных сигналов по:

- длительности;
- частоте следования;
- временному интервалу;
- временному коду.

3. Используются различия в амплитудах сигналов и помех. Методы защиты с помощью схем селекции по амплитуде и при компенсационном методе.

4. Различия в пространственном положении цели и источника помех. Методом защиты является уменьшение уровня побочного излучения и приема по боковым и задним лепесткам диаграммы направленности антенн БАС.

5. Различия в поляризационной структуре сигнала и помех, учитывая, что помехи имеют круговую или эллиптическую поляризацию, а волна, отраженная от цели, является плоскополяризованной.

С точки зрения воздействия активных помех на системы БАС методы защиты можно разделить на две основные группы:

- методы препятствующие попаданию помехи в приемную систему и устройство обработки сигнала. К ним относятся следующие виды селекции сигналов: пространственная, частотная, поляризационная.

- методы борьбы с помехами, проникшими в приемную систему. Их действие основано на различии параметров сигнала цели и помехи по спектральным характеристикам, по частоте повторения и длительности, по амплитуде и т.д. Для борьбы с помехами такие отличительные признаки могут специально вводится в сигнал для повышения эффективности защиты (например, поляризация волн, временная расстановка импульсов, тип модуляции и т.д.).

2.2. Частотная и фазовая селекция

Частотная селекция основана на различии спектров сигналов и помех. Частотная селекция рассматривается как одно из основных средств помехозащиты от преднамеренных активных и пассивных помех. Основой принципа частотной селекции является известное из радиотехники выражение спектральной функции сигнала на выходе линейного четырехполюсника:

$$\dot{S}_{вых}(\omega) = \dot{K}(j\omega)\dot{S}_{вх}(\omega)$$

Если выбрать частотную характеристику четырехполюсника, пропускающую только спектр полезного сигнала, то можно устранить влияние помех, находящихся вне полосы приема

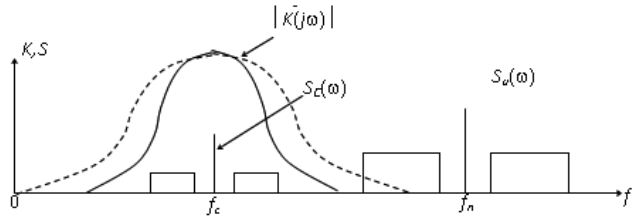

Рисунок 2.1. Частотная селекция

Рассмотрим некоторые варианты частотной и фазовой селекции.

Изменение рабочей частоты РТС

Известны несколько способов изменения несущей частоты.

- использование двух приемо-передающих каналов, настроенных на различные частоты f_1 и f_2. Каналы работают попеременно. Переключение проводится вручную оператором или автоматически с помощью анализатора электронно-магнитной обстановки (ЭМО), фиксирующего наличие помехи в приемном канале.

- относительно медленное непрерывное изменение рабочей частоты РТС по заданному закону, например, $f_c=f_0(1+k\sin\Omega t)$, где Ω - низкая частота, k - коэффициент, определяющий девиацию частоты.

- частота изменяется скачкообразно от одного значения к другому, но на каждой из выбранных частот ведется достаточно долго.

- наиболее перспективно и уже используется, быстрое изменение частоты по случайному закону (например, в системах цифровой связи – расширение спектра, в системах наблюдения – изменение частоты от импульса к импульсу).

Если несущая частота сигналов изменяется случайно от импульса к импульсу в пределах полосы Δf_{PTC}, плотность распределения частот постоянна и закон распределения интервала между скачками симметричен, то математическое ожидание модуля разности частот двух следующих друг за другом импульсов равно $M_{|f_i-f_{i+1}|}=\dfrac{\Delta f_{PTC}}{2}$.

Этот способ хорошо защищает от активных маскирующих помех и от прицельных шумовых помех. При использовании заградительных по всей полосе помех он неэффективен, но для заградительной помехи должна быть больше мощность.

Например: в настоящее время в радиолокационных системах наблюдения используется быстрая перестройка частоты от (0,03 до 0,2)f_0. Тогда для РЛС с длиной волны λ=10 см (f_0=3000МГц) перестройка на 5% от f_0 составляет Δf_{PTC}=150 МГц при полосе пропускания приемника РЛС (имеется в виду УПЧ) $\Delta f_{УПЧ}$=1,5 МГц, отношение $\Delta f_{PTC}/\Delta f_{УПЧ}$=100.

Т.е. при прочих равных условиях мощность передатчика заградительных помех должна быть в 100 раз больше по сравнению с мощностью передатчика прицельных помех.

Быстрая настройка частоты в широких пределах является мерой борьбы с непреднамеренными помехами одного частотного поддиапазона. Если эффективная полоса приемника РТС равна $\Delta f_{эфф}$, эффективное значение ширины спектра излучаемого сигнала - Δf_c и полоса перестройки Δf_{PTC} (причем $\Delta f_{PTC} >> N_{PTC}\,\Delta f_{эфф}$ и $\Delta f_{PTC} >> N_{PTC}\,\Delta f_c$, N_{PTC} - число РТС БАС в одном частотном диапазоне) то вероятность $P_{пом}$ попадания сигналов соседних РТС БАС в приемный канал каждой из них будет равна

$$P_{пом} = \frac{\Delta f_{эфф} + \Delta f_c}{\Delta f_{PTC}}\left(N_{PTC} - 1\right).$$

При этом предполагается, что для возникновения непреднамеренных помех достаточно совпадения хотя бы крайних частот j –го сигнала с шириной спектра Δf_{cj} и полосы пропускания i–го приемника $\Delta f_{эффi}$.

При Δf_c =2МГц, $\Delta f_{эфф}$=2Δf_c =2МГц, Δf_{PTC}=500 МГц (5% от f_0=10000МГц) и N_{PTC}=10 получим $P_{пом}$=0,1. Т.е. в среднем только десятая часть цикла будет сопровождаться непреднамеренными помехами.

Для защиты от заградительной помехи методом частотной селекции целесообразна перестройка на частоту, обеспечивающую минимальную мощность помехи. Этот способ защиты основан на использовании неравномерного распределения частотной плотности мощности помех в диапазоне возможной перестройки несущей частоты РТС.

Использование системы автоматического слежения за частотой (АСЧ) для защиты от помех

Системы АСЧ могут функционировать при наличии опорного сигнала (там, где рядом имеется передатчик, например РЛС, система мобильной связи и т.д.) так и в отсутствии опорного сигнала (т.е. происходит подстройка по принимаемому радиосигналу).

Эти системы представляют собой систему автоматического поиска и захвата базовым элементом которым является частотный дискриминатор с петлей обратной связи.

Остановимся подробнее на устройстве фазовой системы слежения за частотой и фазой (ФАПЧ). Действие таких систем основано на использовании фазовых детекторов для различения фаз или частот входных колебаний. Снижение мешающего действия помех с помощью фазовой системы АСЧ основано не на уменьшении полосы УПЧ РПУ (как это имеет место в случае применения частотных систем АСЧ), а на фильтрующем устройстве этой системы и обработке сигнала близкой к когерентной.

На фазовую систему АСЧ можно смотреть как на устройство, осуществляющее синхронное детектирование. Для выполнения этой операции в СД требуется опорный сигнал, совпадающий по фазе с входным сигналом. Опорным сигналом может служить напряжение следящего генератора системы ФАПЧ.

При синхронном детектировании АМ сигнала отсутствует подавление сигнала шумом практически при любом уровне шума. Пусть на СД вместе с сигналом $V_c(t)$ действует нормальный узкополосный шум $n(t)$

$$V_{вх}(t) = U_c(t)\cos\omega_c t + n(t).$$

Представим шум в виде двух случайных процессов

$$n(t) = A(t)\cos\omega_c t + B(t)\sin\omega_c t,$$

где $A(t) = U_м(t)\cos\theta(t)$; $B(t) = U_м(t)\sin\theta(t)$ - нормальные шумы с той же дисперсией, что и $n(t)$; $U_м(t)$, $\theta(t)$ – медленно изменяющиеся случайные процессы.

При опорном напряжении $V_{оп}(t) = U_{оп}\cos\omega_c t$ выходное напряжение после СД с интегратором

$$V_{сд} = K_{сд}\left[U_c(t)\cos\omega_c t + n(t)\right]U_{оп}\cos\omega_c t = \frac{1}{2}K_{сд}U_c(t) + \frac{1}{2}K_{сд}A(t) - U_{оп}.$$

Благодаря синхронному детектированию квадратичная составляющая $B(t)$ в выходном напряжении отсутствует, а отношение сигнал/шум на выходе сохраняется тем же, что и на входе, поскольку дисперсии процессов $A(t)$ и $n(t)$ одинаковы.

Использование СД с фазовой системой АСЧ иллюстрируется схемой рис. 2.2.

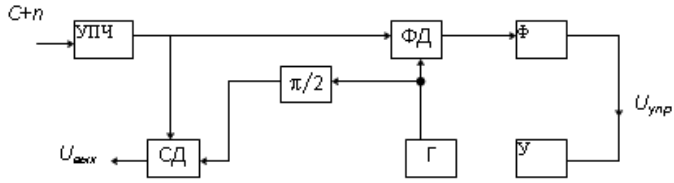

Рисунок 2.2 - СД с фазовой системой АСЧ

В состав фазовой схемы АСЧ входит фазовый детектор ФД, фильтр низких частот Ф, устройство управления частотой У и следящий генератор Г. Здесь следящий генератор осуществляет слежение за частотой сигнала ω_c, поступающего с выхода УПЧ РПУ.

Если ω_c – величина постоянная (или медленно меняется в сравнительно небольших пределах) и начальная частота $\omega_{ГО}$ (при нулевом управляющем напряжении $U_{упр}$) совпадает с частотой сигнала $\omega_c = \omega_{ГО}$, можно показать, что в этом случае между напряжением сигнала и генератора Г устанавливается разность фаз $\Delta\varphi = \frac{3}{2}\pi \pm 2k\pi$.

После поворота фазы на $\pi/2$ напряжение генератора подается в качестве опорного на СД. На сигнальный вход СД поступает сигнал с выхода УПЧ.

Для подавления узкополосных помех (непрерывные помехи, модулированные узким спектром, импульсы большой длительности) применяются режекторные фильтры. Полоса этих фильтров выбирается в соответствии с полосой помехи.

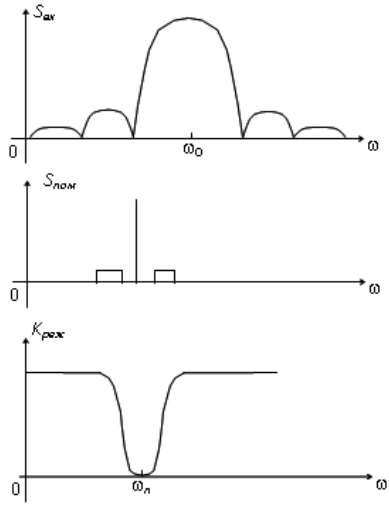

Рисунок 2.3. Применение режекторных фильтров

Отдельную группу приемных систем с повышенной помехозащищенностью по отношению к импульсным помехам составляют «следящие фильтры». Область их применения ЧМ и ФМ сигналы.

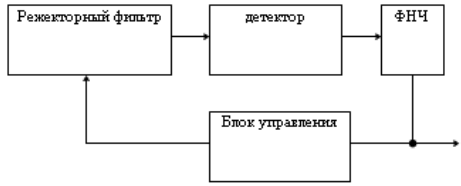

Рисунок 2.4. Схема фильтра

Управляющее напряжение, поступающее с выхода частотного детектора, через фильтр нижних частот и блок управления, воздействует на реактивные параметры следящего фильтра, изменяя его настройку в нужном направлении. За счет узкополосности следящего фильтра в цепи связи (ФНЧ) появляется возможность уменьшения уровня помех на следящем фильтре при практической неискаженности полезной информации ЧМ сигнала. В этом случае система реализует прием «активного спектра» сигнала, значительно более узкого по сравнению с полным спектром, определяемым Фурье-преобразованием. Пороговый выигрыш приема со следящей

настройкой практически определяется соотношением эффективных полос широкополосного приема и приема со следящей настройкой.

Использование частотной селекции в широкополосных системах связи

Широкополосные системы связи (ШСС) или системы, использующие для кодирования информации шумоподобные сигналы (ШПС), известны давно [1]. Одним из важнейших достоинств ШСС, обеспечивших их стремительное развитие, является высокая устойчивость по отношению к широкому классу помех, как искусственного, так и естественного происхождения. Помехоустойчивость ШСС определяется отношением мощности сигнала и мощности помехи на выходе согласованного фильтра (коррелятора):

$$q^2 = \frac{P_C}{P_П} \cdot 2 \cdot B$$

где P_C и $P_П$ - мощность сигнала и мощность помехи на входе приемного устройства (ПУ); $B=FT$ - база используемого ШПС.

Соотношение означает, что при фиксированных значениях P_C и $P_П$ на входе ПУ ШСС, повысить отношение сигнал/помеха на выходе ПУ можно только увеличивая базу используемого шумоподобного сигнала.

Для фазоманипулированных ШПС, фаза которых принимает только два значения - 0 и π, база сигнала равна числу элементов порождающей его кодовой последовательности N. Среди ШПС с небольшими базами наиболее известны сигналы Баркера и M-последовательности.

Для защиты ШСС от помех, уровень которых превышает обеспечиваемый базой допустимый запас помехоустойчивости, применяют дополнительные методы подавления. Указанные методы можно разделить на две группы - режекция пораженной части спектра ШПС и компенсация помехи в ПУ путем создания ее копии с последующим вычитанием созданной копии помехи из входного сигнала. Реализация дополнительных методов защиты осуществляется, в основном, цифровым способом на промежуточной или видеочастоте ПУ. При этом полагают, что входные сверхвысокочастотные (СВЧ) каскады ПУ преобразуют входную смесь полезного сигнала, шума и помех линейно, не внося значительных искажений в принимаемый сигнал.

Одним из вариантов защиты входных каскадов ШСС от мощной УП может быть ее режекция в спектре полезного сигнала на СВЧ с помощью режекторного фильтра, а если помех несколько, то с помощью блока режекторных фильтров.

На рисунке 2.5 показана блок-схема входных каскадов ШСС с включенным в нее режекторным фильтром.

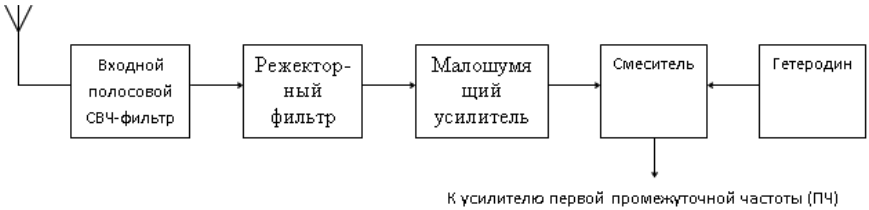

Рисунок 2.5. Схема входных каскадов ШСС

Спектр фазоманипулированного ШПС, образованного М - последовательностью длиной 63 элемента, показан на рис. 2.6. КФ этого сигнала, по отношению к КФ неискаженного ШПС приведена на рис. 2.7. Нетрудно видеть, что форма основного пика КФ меняется незначительно, уменьшается лишь его амплитуда. Похожие результаты получены в [6], согласно которым режекция не более чем четверти спектра ШПС, не вызывает существенных искажений КФ, лишь уменьшает амплитуду основного пика.

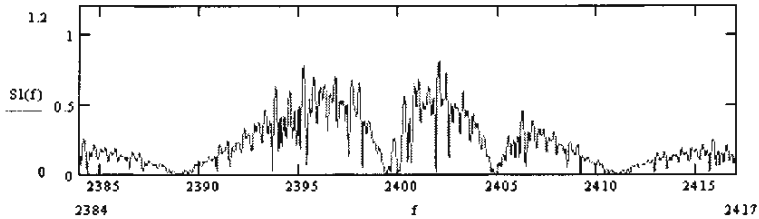

Рисунок 2.6. Спектр фазоманипулированного ШПС, прошедшего через два режекторных фильтра

Чтобы выяснить максимальное число $N_{\text{МАКС}}$ мощных УП, которые могут быть подавлены описанным способом, необходимо знать ширину спектра полезного сигнала ΔF, ширину полосы режекции каждого включенного фильтра на ДР Δf_i, которая должна превышать ширину спектра помехи $\Delta F_{УП}$. В этом случае

$$N_{МАКС} = \frac{1}{4}\frac{\Delta F}{\Delta f_i}$$

при $\Delta f_i \le \Delta F_{УП}$.

Для более точного определения $N_{МАКС}$ в каждом конкретном случае необходимо задаться величиной порога обнаружения, которая зависит от принятого в системе критерия обнаружения.

Рассмотрение способа определения типа помехи, действующей на ШСС, выходит за рамки данной статьи. Высказанные здесь предположения справедливы в том случае, когда на ШСС действуют только мощные УП,

ширина спектра которых значительно меньше ширины спектра полезного сигнала $\Delta F_{УП} << \Delta F$, а мощность значительно превышает границы динамического диапазона ПУ $P_{УП} >> P_{МАКС.ПУ}$.

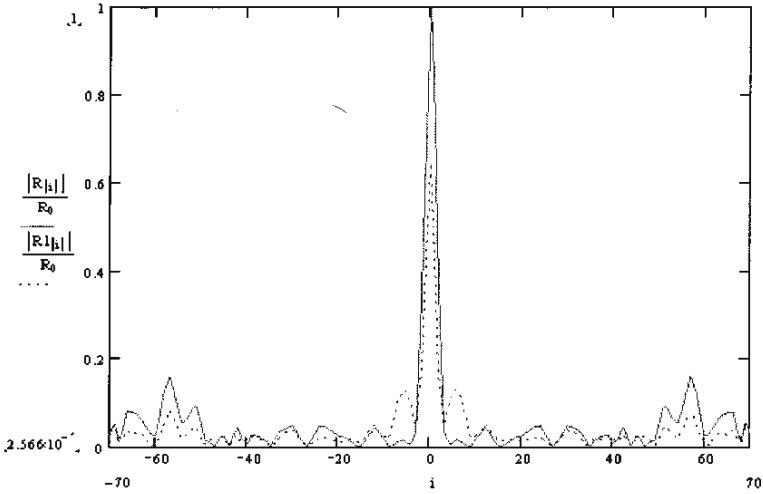

Рисунок 2.7. Корреляционная функция ШПС (неискаженного сплошная линия, искаженного – пунктирная линия)

Таким образом:

1. Защиту широкополосных систем от воздействия узкополосных помех, мощность которых превышает границы динамического диапазона приемного устройства, необходимо осуществлять во входных каскадах ПУ, до малошумящего усилителя и смесителя.

2. Для защиты ШСС от мощных нестационарных УП можно использовать перестраиваемые режекторные СВЧ фильтры на диэлектрических резонаторах.

3. Максимально возможное количество УП, которые могут быть подавлены указанным способом, зависит от ширины спектра полезного ШПС, ширины полосы режекции каждого фильтра на ДР и величины порогового уровня основного пика корреляционной функции, при котором происходит обнаружение полезного сигнала, принятого в конкретной системе.

2.3. Амплитудная селекция

Учитывая то, что обычно амплитуда сигнала и помехи существенно отличается, одним из наиболее распространенных методов защиты от помех является использование амплитудной селекции.

Селекция сигналов при ограничении их снизу

Этот вид селекции применяется в тех случаях, когда амплитуда полезного сигнала существенно превышает амплитуду помехи. Селекция осуществляется амплитудным селектором (АС), представляющим собой ограничитель снизу или ждущий генератор импульсов (см. рис.).

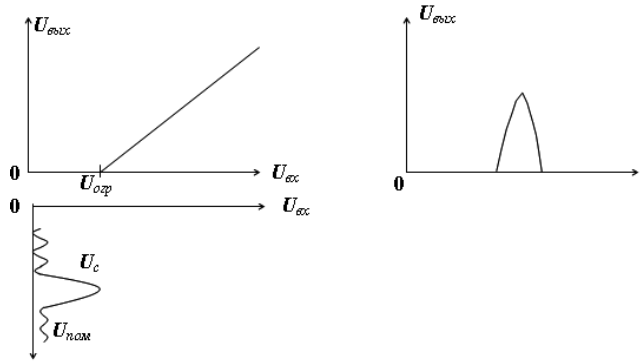

Рисунок 2.8. Принцип амплитудной селекции сигналов при ограничении их снизу

Применительно к высокочастотным сигналам такую селекцию можно назвать селекцией при ограничении по минимуму. Применяя раздельное ограничение высокочастотного колебания снизу и сверху, и затем, суммируя выходные напряжения ограничителей, можно «вырезать» все помехи $|U_n(t)| < U_{огр}$.

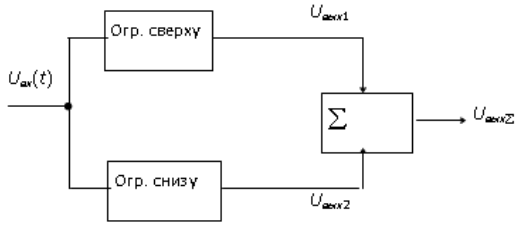

Рисунок 2.9. Схема амплитудной селекции (ограничение сверху и снизу)

При использовании ждущего генератора импульсов (мультивибратор, блокинг-генератор) в качестве селектора пороговый уровень представляет собой запирающее напряжение.

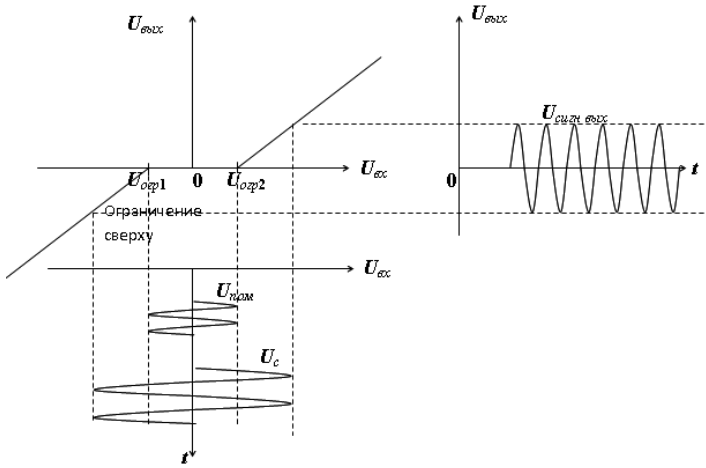

Рисунок 2.10. Принцип амплитудной селекции сигналов при ограничении их снизу и сверху

Селекция импульсов по уровню (бланкирование)

Селекция такого вида целесообразна в тех случаях, когда амплитуда полезного сигнала существенно меньше амплитуды помехи либо амплитуды сигналов колеблются вблизи какого-то уровня.

а) Для селекции импульсов малой амплитуды совместно используются ограничитель снизу и логическая схема запрета. Функциональная схема селекторного устройства изображена на рис. 2.11.

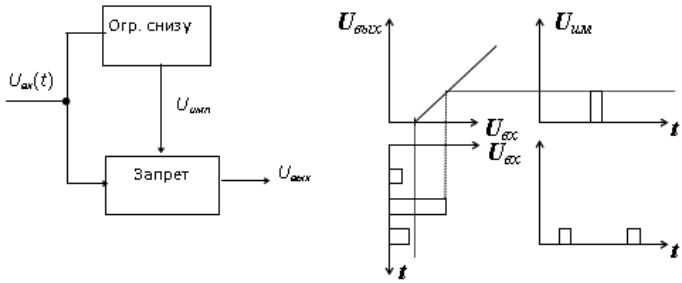

Рисунок 2.11. Схема селекторного устройства и принцип работы

Через ограничитель снизу проходят те импульсы, амплитуда которых превышает пороговый уровень. С выхода ограничителя импульсы с амплитудой $U_{имп}$ поступают к запрещающему входу схемы «Запрет». Ко второму входу (информационному) подводят входное напряжение. Напряжение на вход поступает только тогда, когда отсутствует напряжение на запрещающем входе. Итак, пройдут только импульсы $U_c<U_{огр}$.

б) Можно использовать селектирующее устройство, которое пропускает только такие импульсы, амплитуда которых не выходит за заданные границы $U_{огр1}<U_c<U_{огр2}$.

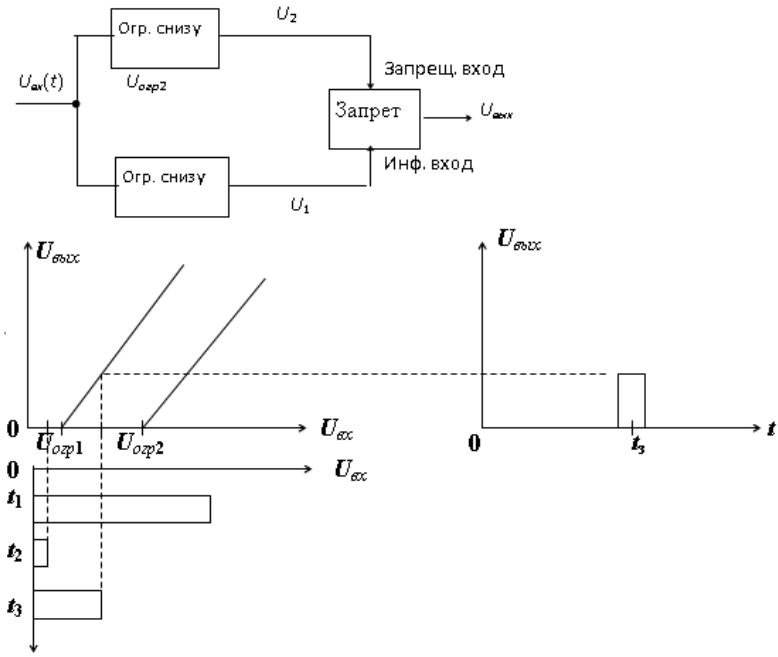

Рисунок 2.12. Схема селектирующего устройства и принцип работы

Входное напряжение пропускается через два ограничителя снизу, имеющие уровни ограничения $U_{огр1}$ и $U_{огр2}$. Если $U_{вх}<U_{огр1}$ и $U_{огр2}$, то импульсы не проходят через селектор, т.к. нет напряжения на информационном входе. При $U_{вх}>U_{огр2}$ импульсы не проходят, т.к. есть напряжение на запрещающем входе. И только если $U_{огр1}<U_{вх}<U_{огр2}$ на выходе будет импульс сигнала.

Использование накопления сигнала

Метод накопления представляет собой частный случай метода согласованной фильтрации, при которой обеспечивается максимальное отношение мощностей полезного сигнала и помехи, если помеха – белый шум. Однако, метод накопления, независимо от формы полезного сигнала, реализуется с помощью сумматора или интегратора, именуемых накопителями.

Сущность метода накопления при использовании сумматора сводится к тому, что в течение заданного времени $T_н$ в смеси $U_{вх}(t)$ сигнала и помехи берется заранее установленное количество отсчетов. Значения $U_{вх}(t)$ в точке отсчета суммируется, а затем на основании суммарного сигнала решающее

(пороговое) устройство дает ответ о наличии или отсутствии сигнала в смеси $U_{вх}(t)$.

Если это интеграл, то $U_{вых}(t)=\frac{1}{T_н}\int_0^{T_н}U_{вх}(t)dt$. Если накопитель реагирует на n отсчетов, то сигнал $U_{вых}(t)$ на выходе сумматора равен $U_{вых}(t)=\sum_{i=0}^{n}(U_c+U_i)=nU_c+\sum_{i=1}^{n}U_i$, где U_i – значение помехи в момент времени t_i (i=1,2,…,n), соответствующие фиксации i – го импульса сигнала.

В случае белого шума, т.к. случайные величины U_1, U_2, … U_n взаимно не коррелированы, то при нулевом математическом ожидании функции $U_i(t)$ дисперсия помехи $\sigma_U^2=n\sigma_{U_n}^2$. Здесь $\sigma_{U_n}^2$ - дисперсия случайной функции $U(t)$. Тогда отношение квадрата амплитуды $n^2U_c^2$, которую имеет полезный сигнал, к дисперсии помехи на выходе сумматора $q_н=\frac{nU_c^2}{\sigma_{U_n}^2}$. Если бы накопления не было, то $q=\frac{U_c^2}{\sigma_{U_n}^2}$, т.е. выигрыш в n раз! При наличии взаимной корреляции между U_1, U_2, … U_n отношение $\frac{q_н}{q}<n$.

Если полезный сигнал характеризуется непрерывной функцией времени, то в состав накопителя вместо сумматора включают интегратор.

Итак, увеличение отношения сигнал/помеха при методе накопления достигается увеличением времени, в течение которого принимается решение о наличии сигнала.

2.4. Амплитудно-частотная селекция

При амплитудно-частотной селекции выделение сигналов в присутствии помех основывается на использовании их различий по амплитуде и по частоте одновременно.

Система ШОУ (широкая-ограничитель-узкая)

Типичной системой является ШОУ. Это устройство широко используется в радиосвязи для борьбы с импульсными помехами большой амплитуды и малой длительности.

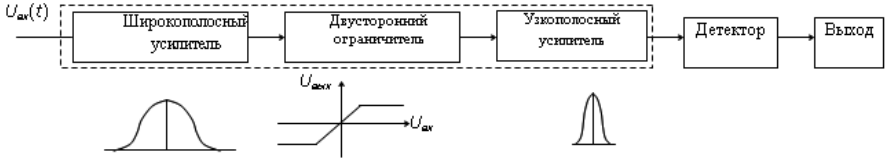

Рисунок 2.13. Система ШОУ

Широкая $\Delta f_ш$ и узкая Δf_y полосы пропускания усилителей симметричны относительно центральной частоты входного напряжения. Полоса пропускания Δf_y согласуется с полосой, занимаемой спектром сигнала $\Delta f_y \approx \Delta f_c$. Полоса $\Delta f_ш$ выбирается с учетом возможной длительности τ_n помеховых импульсов $\Delta f_ш \le \frac{1}{\tau_n}$, $\Delta f_ш >> \Delta f_y$, т.к. среднее значение ширины спектра помехи существенно больше ширины спектра сигнала.

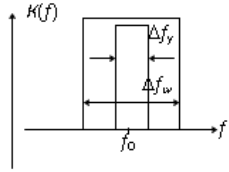

Рисунок 2.14. Выбор полосы пропускания

Уровень ограничения устанавливается в соответствии с амплитудой сигнала $V_c(t)$ на выходе широкополосного усилителя.

Чтобы обеспечить оптимальное соотношение между уровнем ограничения и амплитудой сигнала, предусматривается возможность управления порогом ограничения и усилением широкополосного усилителя.

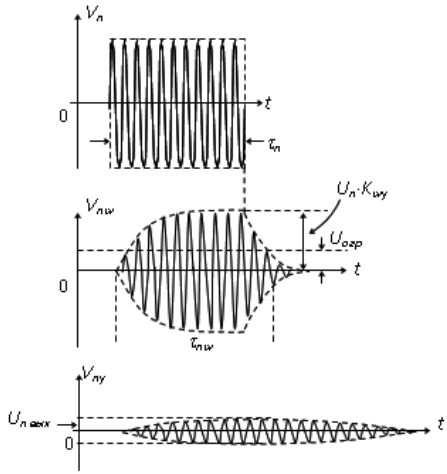

Рисунок 2.14.

На вход приемника воздействует ВЧ импульс помехи $V_n(t)$ с прямоугольной огибающей, длительностью τ_n и амплитудой U_n.

На выходе широкополосного усилителя образуется импульс $V_{nш}(t)$ с экспоненциальными фронтами. Длительность фронта этого импульса определяется длительностью импульса на входе τ_n (напомним, что полоса $\Delta f_ш$

выбирается с учетом τ_n и равна $\Delta f_ш \le \frac{1}{\tau_n}$), и длительностью среза полосой пропускания $\Delta f_ш$.

С помощью ограничителя резко уменьшается амплитуда, а, следовательно, и энергия импульсной помехи. На выходе двустороннего ограничителя помеха представляет собой импульс с трапецеидальной огибающей, амплитудой $U_{огр}$ и длительностью $\tau_{пш}$.

На выходе узкополосного усилителя короткий помеховый импульс растягивается, т.к. $\tau_y \sim 1/\Delta f_y$.

$$U_{п\,вых} = K_y U_{огр}\left[1 - \exp\left(-\frac{\tau_{пш}}{\tau_y}\right)\right].$$

$$U_{с\,вых} = K_ш K_y K_c$$

Мешающее действие помехи резко снижается, если перед выходным устройством обеспечить превышение сигнала над помехой в 2÷3 раза. Система ШОУ может повысить отношение сигнал/помеха на порядок (если $\tau_y >> \tau_{пш}$, то $\exp\left(-\frac{\tau_{пш}}{\tau_y}\right) \to 1$).

Выше был рассмотрен случай прихода сигнала и помехи в разные моменты времени. Теперь обратимся к оценке воздействия импульсной помехи на непрерывно существующий сигнал. Примем следующее условие

$$\Delta f_y << \Delta f_ш << \frac{1}{\tau_n},$$

т.е. будем считать, что широкая полоса пропускания значительно меньше эффективного значения спектра помехи.

Оценим увеличение отношения сигнал/помеха в этих условиях. Будем считать, что

$$V_c(t) = U_c \cos\omega_0 t \qquad -\infty < t < \infty$$

$$V_n(t) = \begin{cases} U_n \cos(\omega_0 t + \pi) & 0 \le t \le \tau_n \\ 0 & t \notin 0, \tau_n \end{cases}$$

$$\left(\frac{U_c}{U_n}\right)_{вх} << 1$$

Взят наиболее «опасный» случай совпадающих частот сигнала и помехи

$$V_n(t) = K_ш U_c \cos\omega_c t + K_ш U_n \left(1 - e^{-\frac{t}{\tau_ш}}\right) \cos(\omega_0 t + \pi)$$

$$U_{ш\,\max} = K_ш \left[U_n \left(1 - e^{-\frac{\tau_n}{\tau_ш}}\right) - U_c \right]$$

,

в момент $t=\tau_n$. При $\tau_n << \tau_ш$, раскладывая в ряд $e^{-\frac{\tau_n}{\tau_ш}}$ имеем $U_{ш\,\max} \approx K_ш (3U_n \tau_n \Delta f_ш - U_c)$.

Итак, после окончания импульса помехи имеет место последействие, определяемое помехой

$$V_ш(t) = K_ш (3U_n \tau_n \Delta f_ш - U_c) e^{-\frac{t}{\tau}} \cdot \cos(\omega_0 t + \pi)$$

уменьшилось до порога ограничения, т.е. $K_ш (3U_n \tau_n \Delta f_ш - U_c) e^{-\frac{\tau_{пш}}{\tau_ш}} = U_{огр}$.

Следовательно $\tau_{пш} = \tau_ш e_n \left[3\tau_n \Delta f_ш \left(\frac{U_n}{U_c}\right)_{вх} - 1 \right]$. На выходе ограничителя при отсутствии помехи действует только сигнал $V_{огр\,с}=U_c \cos\omega_0 t$.

Когда разность амплитуд помехи и сигнала превышает пороговый уровень, то выходное напряжение имеет фазу помехи $V_{огр\,п}=U_{огр}\cos(\omega_0 t+\pi)$.

При прохождении этого напряжения через узкополосный усилитель, этот импульс «растягивается», и его амплитуда

$U_{п\,вых} = 2K_y U_{огр} \left(1 - e^{-\frac{\tau_{пш}}{\tau_y}}\right)$, т.к. $\tau_{пш} << \tau_y$, то $U_{п\,вых} \approx 2U_{огр} K_y \frac{\tau_{пш}}{\tau_y}$.

Таким образом:

1. Система ШОУ, эффективно подавляющая импульсные помехи, несколько ухудшает отношение сигнал/шум.

2. Серьезным недостатком системы ШОУ является возникновение перекрестных искажений при одновременном попадании в широкую полосу входного усилителя полезного сигнала и сигнала мощной мешающей станции, частота которой существенно отличается от f_0.

$$V_{вх}(t) = U_c \cos\omega_0 t + U_n \cos\omega_n t;\ U_c << U_n,\ |\omega_0 - \omega_n| > 2\pi f_y.$$

Обозначим $\omega_0 - \omega_n = \Omega$ и проведем замену $\cos\omega_0 t = \cos(\omega_n + \Omega)t = \cos\omega_n t \cdot \cos\Omega t - \sin\omega_n t \sin\Omega t$. Получим $V_{вх}(t) = (U_c \cos\Omega t + U_n)\cos\omega_n t - U_c \sin\Omega t \sin\omega_n t$. Множители при $\cos\omega_n t$ и

$\sin\omega_n t$ можно рассматривать как медленно меняющиеся функции времени (т.к. $\Omega<<\omega_n$). Тогда можно записать

$$V_{вх}(t)=U(t)\cos[\omega_n t+\varphi(t)],$$

где

$$U(t)=\sqrt{(U_c\cos\Omega t+U_n)^2+U_c^2\sin^2\Omega t},$$

$$\varphi(t)=arctg\frac{U_c\sin\Omega t}{U_n+U_c\cos\Omega t}\approx\frac{U_c}{U_n}\sin\Omega t.$$

Предполагая, что уровень ограничения ниже наименьшего значения огибающей, результирующего колебания, получим на выходе ограничителя

$$V_{вых}(t)=U_{огр}\cos\left(\omega_n t+\frac{U_c}{U_n}\sin\Omega t\right).$$

Т.е. на выходе ограничителя образуется ФМ колебание, спектр которого при $\frac{U_c}{U_n}<<1$, включает три составляющие ω_n, $\omega_n+\Omega=\omega_0$, $\omega_n-\Omega=2\omega_n-\omega_0$. Через узкополосный усилитель пройдет только одна составляющая с частотой ω_0 и амплитудой $U_{вых}=U_{огр}\frac{U_c}{U_n}$, что и обусловливает ее зависимость от амплитуды помехового сигнала.

Система ШПУ (широкая, прерыватель, узкая)

Для устранения этого недостатка используется система ШПУ, у которой вместо амплитудного ограничителя используется управляемый прерыватель.

Рисунок 2.15. Система ШПУ

Принимаемое излучение анализируется с помощью схемы выделения помехи. Если входное напряжение имеет характеристики импульсной помехи, то указанная схема вырабатывает управляющее напряжение, которое приводит к запиранию РПУ на время действия помехи. При наличии полезного сигнала (импульсного или непрерывного) РПУ открыт.

Селектор помехи ШОР (широкая, ограничитель, режекция)

Эта система может использоваться в качестве схемы выделения помехи в ШПУ.

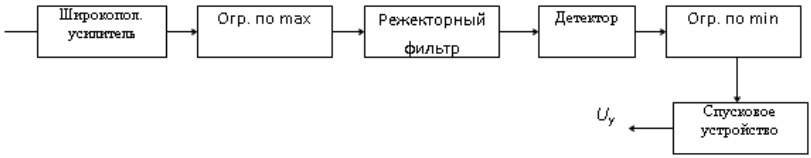

Рисунок 2.16. Селектор помехи ШОР

Через широкополосный усилитель сигнал и помехи проходят без искажения формы огибающей. Ограничитель уравнивает амплитуды выходных напряжений вне зависимости от флуктуаций сигнала и помех на входе РПУ. С помощью режекторного фильтра (РФ) вырезается область частот, соответствующая спектру полезного сигнала с частотой f_0. После ограничителя и РФ амплитуда напряжения помехи будет существенно превышать амплитуду сигнала вне зависимости от картины на входе. ВЧ колебание детектируется. Затем ограничитель по min не пропустит на выход относительно малое напряжение полезного сигнала. Выходным устройством является спусковое устройство (типа блокинг-генератора), которое запирает РПУ.

Схема ШОР эффективно работает при относительно низких частотах следования помех (десятки-сотни Герц).

2.5. Временная селекция

Временная селекция полезных импульсных сигналов на фоне помех основана на отличии селектируемых импульсов от импульсов помех по временному положению (фазе), частоте повторения и длительности.

Селекция импульсов по временному положению

Временная селекция достигается благодаря использованию автоматической системы, осуществляющей слежение за временным положением импульсов селектируемой последовательности – системы автоматической временной селекции по временному положению.

Удобно различать две группы таких систем в зависимости от того, имеются ли в месте приема опорные импульсы или они отсутствуют. Типичная система первой группы – система АСД в импульсной РЛС. Типичная система второй группы – дальномерно-разностная радионавигационная система.

Система АСД представляет собой замкнутую систему регулирования. На рисунке приведена функциональная схема системы АСД.

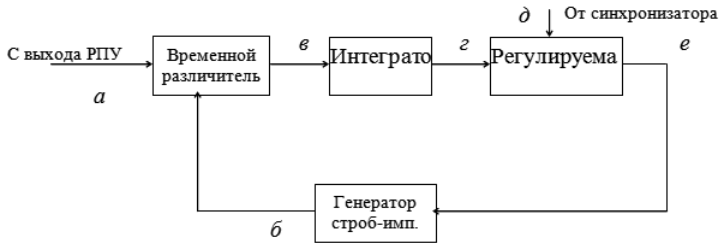

Рисунок 2.17. Функциональная схема системы АСД

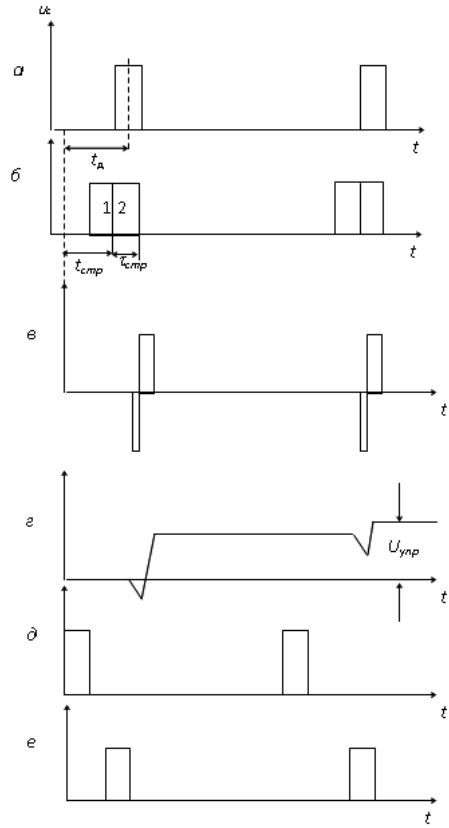

Рисунок 2.18. Временные диаграммы работы системы АСД

На один вход временного различителя поступают эхо-импульсы с РПУ (*а*), на второй – два стробирующих импульса (*б*), вырабатываемых специальным генератором.

Временной различитель представляет собой две схемы совпадения. На одну схему совпадения подается первый (опережающий) строб 1, на вторую – строб 2. Кроме того, на эти схемы поступают сигналы с выхода РПУ.

На выходе каждой схемы возникают импульсы, длительность которых зависит от степени «перекрытия» соответствующего строба отраженным от цели сигналом. Полярности этих импульсов противоположны (рис. 2.18, *в*). После интегрирования выходных импульсов схем совпадения получается напряжение (рис. 2.18, *г*), которое поступает на устройство регулируемой задержки и выполняет роль управляющего напряжения. На выходе регулируемой задержки получаются импульсы, задержанные относительно синхронизирующих на время $t_{стр}$ (рис. 2.18, *е*), определяемое управляющим напряжением $U_{упр}$. В генераторе стробирующих импульсов (ГСИ) из этого напряжения формируется первый строб. Второй строб получается с помощью линии задержки, входящей в состав ГСИ.

При изменении расстояния до цели эхо-сигнал переместится относительно стробов, что вызовет, в свою очередь, перемещение стробов, восстанавливающее первое, т.е. симметричное расположение их относительно эхо-сигнала. Информацию о дальности содержит напряжение на выходе интегратора. Т.к. при сопровождении стробы совпадают с сигналом цели, то представляется возможность работать с нормально запертым приемником, открывая его при помощи этих стробов, на короткое время, когда приходит эхо-сигнал. Благодаря этому повышается помехозащищенность БАС.

Селекция импульсов по частоте повторения

При точно известном (и почти постоянном) периоде повторения импульсов $T_и$ можно использовать схему с каскадами совпадений, действующую по разомкнутому циклу.

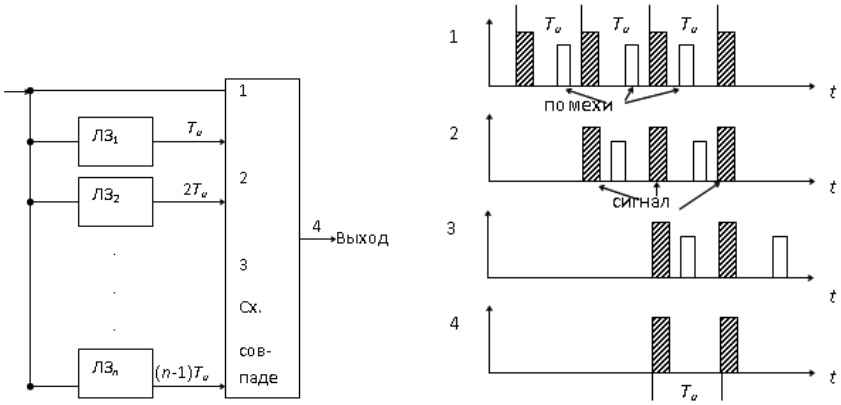

Рисунок 2.19. Селекция по частоте повторения

Сигнал на выходе схем совпадения появляется только в том случае, когда частота повторения входных импульсов равна (или кратна) времени задержки. Диаграмма работы схемы для трехимпульсной схемы совпадений дана на рис., откуда видно, что на выход проходят только импульсы с периодом, равным $T_и=t_з$, а хаотически следующие импульсы помех отсеиваются.

Селекция импульсов по длительности

С точки зрения помехозащиты, интерес представляют селекторы импульсов определенной длительности. Функциональная схема приведена на рис.

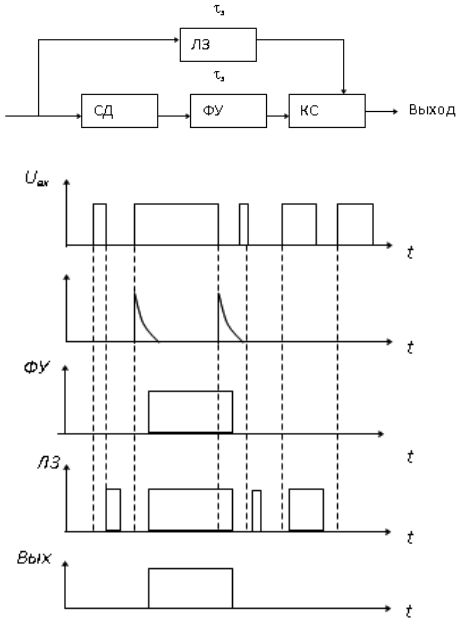

Рисунок 2.20. Селекция по длительности

Входная последовательность поступает на селектор длительности (СД), который пропускает на выход импульсы выбранной длительности. Из этих импульсов в формирующем устройстве (ФУ) образуется стандартный импульс, длительность которого соответствует заданной для селекции. Затем следует каскад совпадения (КС), который пропускает отселектированный импульс. Линия задержки (ЛЗ) предназначена для задержки входных импульсов на время, равное временной задержке в формирующем устройстве (ФУ). Такая схема обеспечивает неискаженную передачу селектируемого импульса.

Функциональная схема селектора длительности может быть представлена в виде линии задержки ЛЗ на длительность селектируемого

импульса, фазоинвертора (ФИ), сумматора Σ, дифференцирующей цепи (ДЦ) и ограничителя (Огр). (рисунок 2.21). Как видно из рис. 2.22 на выходе ограничителя импульс будет только в том случае, когда длительность $\tau_{и1}$ импульсов будет равна времени задержки $t_з$ в лини и ЛЗ.

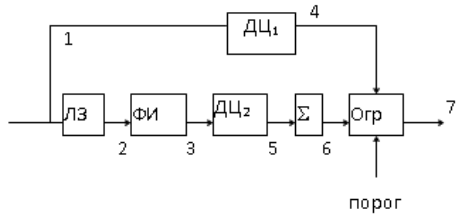

Рисунок 2.21. Функциональная схема селектора длительности

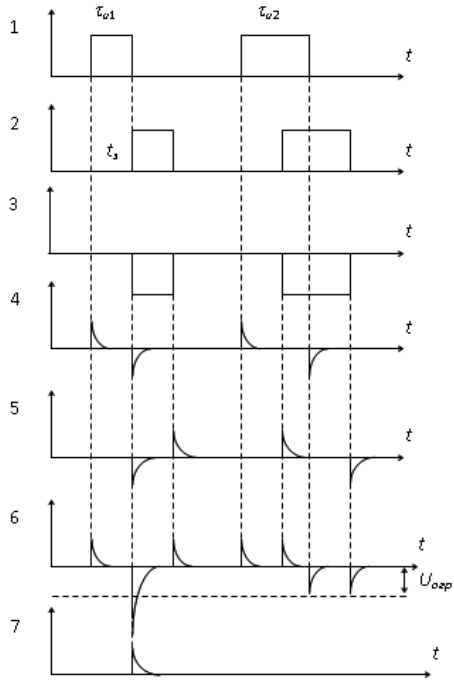

Рисунок 2.22. Временные диаграммы работы селектора длительности

Литература

1. Козлов С.Н. Защита информации. Устройства несанкционированного съема информации и борьба с ними. – М.: Академический проект, 2017.
2. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. Учеб.пособие. – М.: Изд. дом Гос. Ун-та – Высшей школы экономики, 2011.
3. Мельников В.П., Куприянов А.И., Схиртладзе А.Г. Защита информации. – М.: Образовательный издательский центр «Академия», 2014.
4. Болелов Э.А. Криптографические методы защиты информации. Ч. 1. Симметричные криптосистемы. – М.:МГТУ ГА, 2011.
5. Болелов Э.А. Криптографические методы защиты информации. Ч. 2. Асимметричные криптосистемы. – М.:МГТУ ГА, 2012.
6. Информационная безопасность телекоммуникационных систем. Технические аспекты. Учеб.пособие / В.Г. Кулаков, М.В. Гаранин, А.В. Заряев и др. – М.: Радио и связь, 2004.
7. Болелов Э.А., Акмайкин Д.А., Петров В.И., Антонов А.А., Малисов Н.П., Губерман И.Б. Основы защиты информации на транспорте: учебник. / под ред. Болелова Э.А.- М.: ИД Академии Жуковского, 2021. – 240 с.
8. Афанасьев А.А., Веденьев Л.Т. Воронцов А.А. и др.; под ред. Шелупанова А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2009.
9. Кулаков В.Г., Андреев А.Б., Заряев А.В. и др. Защита информации в телекоммуникационных системах. – Воронеж: Воронежский институт МВД России, 2002.
10. Информационная безопасность и защита информации на железнодорожном транспорте: учебник: в 2 ч. / А.А. Корниенко и др.; под ред. А.А. Корниенко. - М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2014.
11. Макаренко С. И., Тимошенко А. В. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 2. Огневое поражение и физический перехват // Системы управления, связи и безопасности. 2020. № 1. С. 147-197. DOI: 10.24411/2410-9916-2020-10106.
12. Еремин Г. В., Гаврилов А. Д., Назарчук И. И. Малоразмерные беспилотники – новая проблема для ПВО // Отвага [Электронный ресурс]. 29.01.2015. № 6 (14). – URL: http://otvaga2004.ru/armiya-i-vpk/armiya-i-vpk-vzglyad/malorazmernye-bespilotniki/ (дата доступа 16.10.2019).
13. Бойко А. Системы обнаружения и нейтрализации беспилотников // RoboTrends [Электронный ресурс], 2019. – URL:

http://robotrends.ru/robopedia/sistemy-obnaruzheniya-i-nyaytralizacii-bespilotnikov (дата обращения 14.04.2020).
14. Демьянович М. А. Использование беспилотных летательных аппаратов в преступных целях: методы противодействия и борьбы // Правопорядок: история, теория, практика. 2019. № 2 (21). С. 108-112.
15. Аниськов Р. В., Архипова Е. В., Гордеев А. А., Пугачев А. Н. К вопросу борьбы с незаконным использованием беспилотных летательных аппаратов коммерческого типа // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2017. № 9-10 (111-112). С. 71-75.
16. Федоров Е. Война с дронами. Саудовский голиаф против хуситов // Военное обозрение [Электронный ресурс]. 28.09.2019. – URL: https://topwar.ru/162842-vojna-s-dronami-saudovskij-goliaf-protiv-husitov.html (дата обращения 14.04.2020).
17. Филиппов А. А., Бажин Д. А., Хлобыстов А. Н. Повышение эффективности управления беспилотного летательного аппарата в условиях помех // Информационно-управляющие системы. 2014. № 6 (73). С. 45-50 – URL: https://cyberleninka.ru/article/n/povyshenie-effektivnosti-upravleniya-bespilotnogo-letatelnogo-apparata-v-usloviyah-pomeh (дата обращения: 16.04.2020).
18. Гришин В. А. Системы технического зрения в решении задач управления беспилотными летательными аппаратами // Датчики и системы. 2009. № 2. С. 46-52.
19. Югай Е. Б. Способ и система навигации пассажирского дрона в горной местности // Патент на изобретение RU 2681278 C1, 05.03.2019.
20. Камнев Е. А. Радиоподавление помехозащищенной навигационной аппаратуры потребителей спутниковых радионавигационных систем в интересах объектово-территориальной защиты. Дис. канд. техн. наук по спец. 05.12.14 «Радиолокация и радионавигация». – М.: МАИ (НИУ), 2018. – 160 с.
21. Жук А. П., Орел Д. В. Об оценке помехозащищенности спутниковых радионавигационных систем // Инфокоммуникационные технологии. 2012. Т. 10. № 2. С. 83-88.
22. Казаков А. Е., Водяных А. А. Пути повышения помехозащищенности навигационной аппаратуры потребителей спутниковых навигационных систем // Системи обробки інформації. 2007. № 1 (59). С. 48-51.
23. Кащеев А. А., Кошелев В. И. Оценка эффективности подавления сигналов спутниковых радионавигационных систем преднамеренными помехами // Журнал радиоэлектроники. 2012. № 7. С. 1. – URL: http://jre.cplire.ru/koi/jul12/3/text.pdf (дата обращения: 14.04.2020).
24. Абукраа А. С., Вилькоцкий М. А., Лыньков Л. М. Влияние на помехоустойчивость и точность абонентских приемников спутниковых навигаторов близкорасположенных экранов с учетом условий распространения радиоволн на реальной местности // Доклады БГУИР. 2017. № 3 (105). С. 85-92.

25. Пантенков Д. Г. Результаты математического моделирования помехоустойчивости спутниковых радионавигационных систем при воздействии преднамеренных помех // Успехи современной радиоэлектроники. 2020. № 2. С. 57-68.
26. Рубцов В. Д., Заикин А. А. Сравнительный анализ эффективности различных вариантов комплексной обработки информации в аппаратуре потребителей спутниковых радионавигационных систем и инерциальной навигационной системе // Научный вестник Московского государственного технического университета гражданской авиации. 2010. № 159. С. 128-132.
27. Усов О. С., Хорошко А. Ю., Кванин Л. В. Лазерный высотомер для беспилотных летательных аппаратов вертолетного типа средней и большой дальности (ЛВ-50) // Секрет производства («ноу-хау») № 218.016.804d от 28.08.2018. – URL: https://edrid.ru/rid/218.016.804d.html (дата обращения: 17.04.2020).
28. Фокин Г. А. Позиционирование в условиях отсутствия прямой видимости с использованием цифровых моделей местности // T-Comm: Телекоммуникации и транспорт. 2019. Том 13. № 11. С. 4-13. DOI: 10.24411/2072-8735-2018-10319.
29. Егурнов В. О., Ильин В. В., Некрасов М. И., Сосунов В. Г. Анализ способов противодействия беспилотным летательным аппаратам для обеспечения безопасности защищаемых объектов // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2018. № 1-2 (115-116). С. 51-58.
30. Верба В. С. Авиационные комплексы радиолокационного дозора и наведения. Принципы построения, проблемы разработки и особенности функционирования. Монография. – М.: Радиотехника, 2014. – 528 с.
31. Верба В. С., Меркулов В. И. Теоретические и прикладные проблемы разработки систем радиоуправления нового поколения // Радиотехника. 2014. № 5. С. 39-44.
32. Верба В. С., Меркулов В. И., Самодов И. О. Управление беспилотными летательными аппаратами в составе локальной сети // Информационно-измерительные и управляющие системы. 2014. Т. 12. № 3. С. 7-12.
33. Боев Н. М. Анализ командно-телеметрической радиолинии связи с беспилотными летательными аппаратами // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. 2012. № 2 (42). С. 86-91.
34. Боев Н. М., Шаршавин П. В., Нигруца И. В. Построение систем связи беспилотных летательных аппаратов для передачи информации на большие расстояния // Известия ЮФУ. Технические науки. 2014. № 3 (152). С. 147-158.
35. Боев Н. М., Лебедев Ю. А. Управление энергетической эффективностью совмещенных каналов передачи данных единой системы связи // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. 2013. № 1 (47). С. 11-15.

36. Боев Н. М. Разработка и проектирование бортового антенно-фидерного оборудования малых беспилотных летательных аппаратов // Решетневские чтения. 2011. Т. 1. С. 162-163.
37. Батурин Т. Н., Боев Н. М. Разработка и проектирование бортового усилителя мощности радиосигнала УКВ-диапазона для беспилотного летательного аппарата // Решетневские чтения. 2012. Т. 1. С. 141-142.
38. 76. Лебедев Ю. А., Боев Н. М. Разработка и проектирование малогабаритной системы связи малых беспилотных летательных аппаратов // Решетневские чтения. 2012. Т. 1. С. 155-156.
39. Слюсар В. И. Передача данных с борта БПЛА: Стандарты НАТО // Электроника: Наука, технология, бизнес. 2010. № 3 (101). С. 80-87.
40. Слюсар В. И. Радиолинии связи с БПЛА. Примеры реализации // Электроника: Наука, технология, бизнес. 2010. № 5 (103). С. 56-61.
41. Ананьев А. В., Стафеев М. А., Макеев Е. В. Апробация способа организации связи с использованием беспилотных летательных аппаратов // Труды МАИ. 2019. № 105. С. 14.
42. Ананьев А. В., Катруша А. Н. Контурная антенна ДКМВ-диапазона для беспилотных летательных аппаратов // Антенны. 2017. № 8 (240). С. 45-52.
43. Ананьев А. В., Катруша А. Н. Сравнительная оценка возможностей радиосвязи с беспилотными летательными аппаратами в диапазонах КВ и УКВ для полузакрытых и закрытых трасс распространения радиоволн // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 10. С. 4-9.
44. Ананьев А. В., Змий Б. Ф., Кащенко Г. А. Модернизация бортовых приемо-передающих систем беспилотных летательных аппаратов на основе эволюционного подхода // Радиотехника. 2016. № 8. С. 46-49.
45. Пантенков Д. Г., Ломакин А. А. Оценка устойчивости спутникового канала управления беспилотными летательными аппаратами при воздействии преднамеренных помех // Радиотехника. 2019. Т. 83. № 11 (17). С. 43-50.
46. Самойленко Д. В., Финько О. А., Еремеев М. А. Распределённая обработка и защита информации в группировке комплексов с беспилотными летательными аппаратами // Теория и техника радиосвязи. 2017. № 4. С. 93-100.
47. Самойленко Д. В., Финько О. А. Помехоустойчивая передача данных в радиоканалах робототехнических комплексов на основе полиномиальных классов вычетов // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 3. С. 49-55.
48. Донченко А. А., Чиров Д. С. Обоснование требований к системе связи беспилотных летательных аппаратов средней и большой дальности // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 12. С. 12-16.
49. Палий А. И. Радиоэлектронная борьба. – М.: Военное издательство, 1989. – 350 с.