ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Предлагаемое учебное пособие необходимо для усвоения материала, преподаваемого по дисциплинам «Алгоритмы кодирования и шифрования информации», «Основы кодирования и шифрования информации» и «Методы и технические средства защиты информации». Материал пособия составлен в соответствии с требованиями стандарта по следующим направлениям подготовки специалистов: «Специальные радиотехнические системы», «Инфокоммуникационные технологии и системы специальной связи», «Радиоэлектронные системы и комплексы». В основу пособия положены основополагающие принципы построения цифровых систем связи.

Для успешного усвоения разделов дисциплины необходимы знания, полученные студентами при изучении предшествовавших дисциплин, касающихся высшей математики, информатики, теории электросвязи, цифровых устройств в связи. Материал дисциплины будет использоваться для изучения специальных дисциплин, в которых цифровая обработка сигналов на базе сигнальных процессоров имеет первоочередное значение.

Цель преподавания дисциплины:

– обеспечить студентов навыками ориентации в специфических особенностях защищенной передачи информации в радиотехнических системах;

– сформировать у студентов системы научных понятий и научно упорядоченных базовых представлений об основах построения, параметрах и характеристиках аппаратно-программных шифраторов в цифровых системах связи;

– обеспечить студентов владением основами построения и расчета характеристик устройств радиотехнических систем средствами LabVIEW.

В результате изучения дисциплины студенты должны:

- освоить принципы построения цифровых скремблеров/дескремблеров и их основные функции;
- освоить принципы построения и функционирования криптографических систем на базе аппаратных шифраторов;
- освоить навыки проектирования цифровых систем защищенной передачи сигналов с помощью алгоритмических средств LabVIEW.

Для проведения исследований, касающихся криптографической безопасности радиотехнических систем различного назначения, используются персональный компьютер и среда графического программирования LabVIEW фирмы National Instruments. Для построения виртуальных приборов аппаратно-

программных шифраторов в LabVIEW, начиная с 2011 г., существует специальная библиотека Crypto-Tools, но в данном учебном пособии приведены оригинальные решения, отличные от приведенных в указанной бибилиотеке приборов.

Для ознакомления с реализацией приведенных виртуальных приборов LabVIEW требуются основные навыки работы с этим средством проектирования, а также знание основ цифровой схемотехники, знание основ алгоритмов шифрования и кодирования информации.

В первом разделе приведено описание цифровых скремблеров и их особенностей, указано их применение в цифровых системах связи и изложены принципы построения их моделей в виртуальных приборах LabVIEW. Во втором разделе представлено описание классического блочного алгоритма шифрования DES и приведена реализация виртуального прибора LabVIEW DES-шифратора. В третьем разделе изложены принципы построения цифровой стеганографической системы передачи информации, описаны примеры реализации виртуальных приборов стегосистем, реализующих метод наименьшего значащего бита и гибридный метод формирования стегоконтейнера в пакетах закодированных сообщений в каналах с помехами для сетевой стеганографии. Четвертый раздел посвящен сравнительному анализу некоторых хеш-функций и практической реализации моделей на основе использования MD5-хэша в виртуальных приборах LabVIEW.

РАЗДЕЛ 1

1. ВИРТУАЛЬНЫЕ ПРИБОРЫ МОДЕЛЕЙ ЦИФРОВЫХ СКРЕМБЛЕРОВ/ДЕСКРЕМБЛЕРОВ

1.1. Цель

Изучить основные особенности и принципы построения цифровых скремблеров для осуществления программной реализации виртуальных приборов в среде LabVIEW.

1.2. Краткие теоретические сведения

В средствах цифровой радиосвязи, где применимы методы криптографии, получившие широкое распространение, обеспечивая достаточно высокую степень защиты информации от несанкционированного доступа, также используются алгоритмы цифрового скремблирования, находящие применение при реализации методов потокового шифрования.

Известно, что цифровое скремблирование производит преобразование структуры цифрового потока без изменения скорости передачи с целью получения свойств случайной последовательности. Скремблер осуществляет защиту информации от несанкционированного доступа и ускоряет процесс выделения тактовой частоты для осуществления дескремблирования данных при приеме.

Скремблеры и дескремблеры реализуют на основе генераторов псевдослучайных последовательностей битов (ГПСП), выполненных с использованием М-разрядных сдвиговых регистров с цепями обратной связи, отличающихся периодом генерируемых последовательностей битов.

Известны много разновидностей систем скремблер-дескремблер, двумя видами которых являются системы с неизолированными и изолированными от канала связи ГПСП (рис. 1.1, 1.2) [1,2]. Скремблеры с изолированными и с неизолированными генераторами ПСП могут быть реализованы в виде самосинхронизирующихся и с начальной установкой.

При потере синхронизма между скремблером и дескремблером время его восстановления не превышает числа тактов, зависящего от разрядности регистра сдвига ГПСП скремблера. На приемной стороне выделение информационной последовательности происходит сложением по модулю два принятой

скремблированной последовательности с псевдослучайной последовательностью ГПСП.

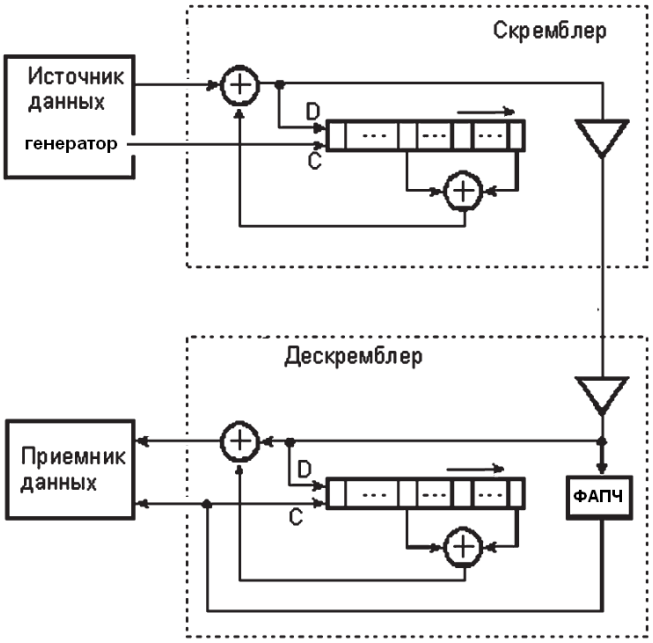

Рис. 1.1. Система скремблер-дескремблер на основе неизолированных ГПСП

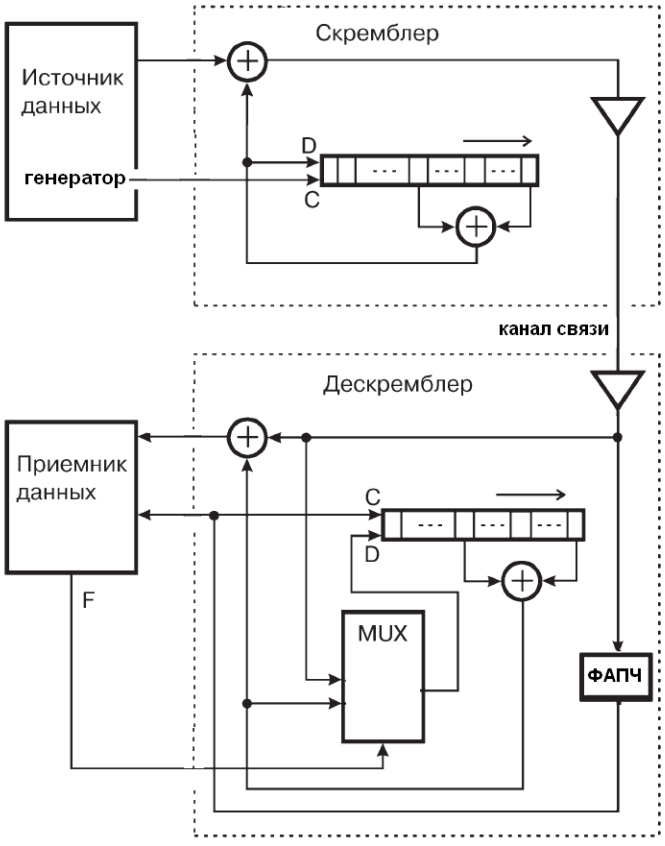

Рис. 1.2. Система скремблер-дескремблер на основе изолированных ГПСП

Недостатками самосинхронизирующихся скремблеров-дескремблеров является свойство размножения ошибок и периодичность выходной последовательности. Влияние ошибочно принятого бита проявляется k раз, где k – число обратных связей, поэтому в регистре сдвига число k не должно превышать 2. Для предотвращения периодичности выходной последовательности в скремблере и дескремблере предусматриваются дополнительные схемы контроля, выявляющие и нарушающие периодичность [2].

Отсутствие эффекта размножения ошибок и необходимость специальной защиты от длинных повторяющихся серий нулей или единиц делают способ скремблирования с принудительной установкой эффективнее, но цена этого – затраты на решение задачи взаимной синхронизации системы скремблер-дескремблер.

Скремблированная последовательность битов по каналу связи поступает в дескремблер, где с помощью генератора с фазовой автоподстройкой частоты из входного сигнала выделяется тактовый сигнал, который передается на синхронизирующие входы регистра сдвига ГПСП и приемника данных. Синхронизация достигается автоматически после заполнения регистров одинаковыми данными. В системе с изолированными генераторами, показанной на рис. 1.2, ошибки, поступающие из канала связи, не размножаются, так что такая система более устойчива к неблагоприятным последовательностям битов. Начальная кодовая синхронизация системы с изолированными генераторами, как показано на рис.1.2, осуществляется с использованием аппаратных средств дескремблера – мультиплексора MUX и программно-управляемого выхода приемника данных, на котором формируется управляющий сигнал F. При нормальной работе системы приемник данных постоянно поддерживает на выходе сигнал F = 0. На выход мультиплексора передается сигнал с выхода элемента «исключающее ИЛИ» ГПСП, который изолирован от внешних воздействий со стороны канала связи. Когда в потоке данных нет обусловленного протоколом обмена разделения на информационные кадры, тогда приемник формирует сигнал F = 1, что переключает мультиплексор к подаче на вход регистра сдвига ГПСП сигнала скремблированных данных, как в системе с неизолированными генераторами [2].

Простейшим генератором ПСП является линейный регистр сдвига (ЛРС) с функцией обратной связи в виде сумматора по модулю 2 некоторых битов регистра. Перечень этих битов, называемый отводной последовательностью, только при определенных состояниях циклически пройдет через все $2^n - 1$ внутренних состояний, имея максимальный период, и позволяет получить на

выходе ГПСП М-последовательность. Для того чтобы ГПСП имел максимальный период формируемой последовательности бит, многочлен, образованный из отводной последовательности

$$p(x)=a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + 1,$$

должен быть примитивным в поле двоичных чисел [2]. Степень многочлена является длиной сдвигового регистра.

Значения ненулевых коэффициентов a_i i= 1, k определяют выводы разрядов регистра сдвига для подачи на вход сумматора по модулю два, коэффициент a_0 всегда равен 1 по определению.

Линейные регистры сдвига с обратной связью для реализации важного принципа повышения криптоустойчивости шифров – распространения влияния одного элемента шифра на другие элементы, должны использовать большое количество предшествующих элементов при формировании очередного элемента линейной рекуррентной последовательности (ЛРП). Наиболее эффективными в этом случае являются генераторы составных ЛРП (СЛРП) на базе ЛРС, которые обладают следующими особенностями:

- объединение нескольких ЛРП, полученных от ЛРС с различными длинами и различными многочленами обратной связи, позволяет достичь высокого уровня *диффузии* – рассеянии статистических особенностей потока данных по широкому диапазону статистических характеристик зашифрованного сообщения, так как значение каждого бита данных влияет на значения многих элементов зашифрованного сообщения и соответственно любой элемент зашифрованного сообщения зависит от множества элементов потока данных;
- составной генератор будет иметь максимальную длину периода, если длины сдвиговых регистров будут взаимно простыми числами, а все многочлены обратной связи являться примитивными;
- ключ шифрования определяет начальные состояния ЛРС.

Известны такие базовые генераторы составных ЛРП на базе ЛРС как комбинационный генератор СЛРП (рис.1.3), генератор Геффа (рис.1.4), генератор переменного шага (рис.1.5) – разновидность генераторов, основанных на управлении синхросигналом, и ряд других ГПСП. Для повышения криптостойкости необходимо усложнять способ комбинирования исходных ПСП в составную. Так в генераторе Геффа три генератора ПСП объединяются нелинейным образом – два генератора ПСП являются входами мультиплексора,

а третий ГПСП подключен к адресному входу мультиплексора и своей последовательностью управляет последним.

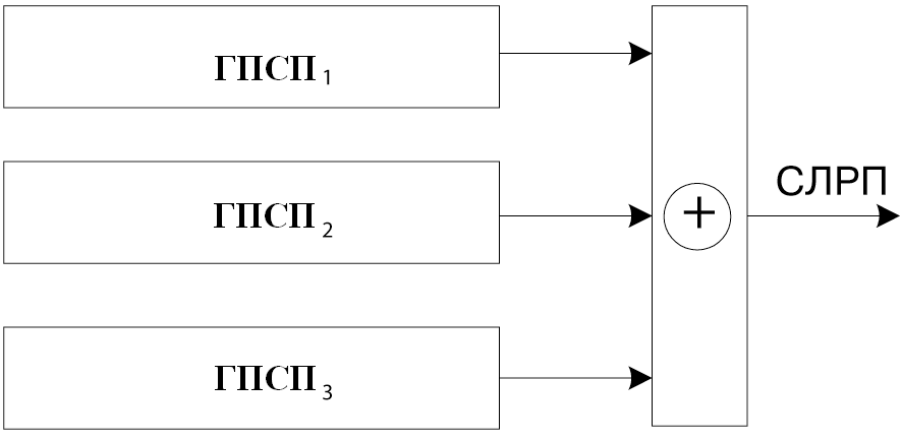

Рис. 1.3. Комбинационный генератор СЛРП

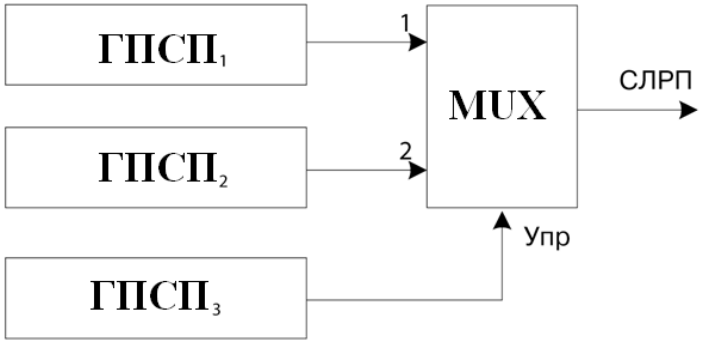

Рис. 1.4. Генератор Геффа

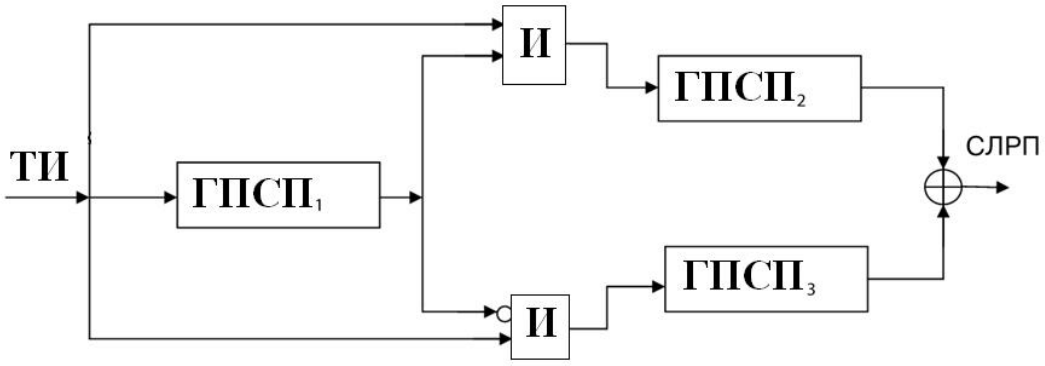

Рис. 1.5. Генератор переменного шага

Если в ранее рассмотренных нелинейных комбинациях генераторов перемещение данных во всех регистрах сдвига с обратной связью

контролируется одним синхросигналом, то основой функционирования генератора переменного шага является внесение нелинейности в работу путём управления синхросигналом одного регистра выходной последовательностью другого ЛРС. Первый генератор $ГПСП_1$ синхронизован внешним синхросигналом тактовой последовательности импульсов (ТИ) и если на его выходе в текущий момент времени присутствует единичное состояние, то на второй $ГПСП_2$ подаётся синхросигнал, сдвигая данные на один разряд, а третий $ГПСП_3$ данные не сдвигает, т.е повторяет свой предыдущий выходной бит. Если же на выходе $ГПСП_1$ присутствует ноль, то на $ГПСП_3$ подаётся синхросигнал, а $ГПСП_2$ повторяет свой предыдущий выходной бит. Выходная последовательность битов генератора с переменным шагом является результатом операции побитового суммирования по модулю 2 выходных последовательностей регистров $ГПСП_2$ и $ГПСП_3$. Для увеличения криптостойкости генератора с переменным шагом необходимо, чтобы длины регистров сдвига были выбраны как попарно простые близкие числа.

Применение алгоритмов потокового шифрования [4-7] на основе скремблирования широко используется в системе безопасности GSM-связи (см. рис.1.6), основу которой составляют три алгоритма:

A3 – алгоритм аутентификации, основанный на хэш-функции;

A8 – алгоритм генерации сеансового ключа для потокового шифрования информации в канале связи между сотовым телефоном и базовой станцией после аутентификации;

A5 – алгоритм шифрования потока цифровой речевой информации (в зависимости от применения используются разновидности алгоритма: A5/1, A5/2, A5/3, …).

Смарт-карты мобильных станций содержат алгоритмы A3 и A8, а в самом телефоне алгоритмом A5 зашит в ASIC-чип. На базовых станциях центр аутентификации использует алгоритмы A3-A8 для идентификации мобильного абонента и генерации сеансового ключа, а также ASIC- чип с A5.

Согласно *алгоритму A3* с помощью заложенной в SIM-карте информации в результате взаимного обмена данными между подвижной станцией и базой осуществляется полный цикл аутентификации и разрешается доступ абонента к сети. Процедура проверки базой подлинности абонента реализуется посредством передачи базой случайного номера (RAND) на подвижную станцию, затем, определения мобильным абонентом значения отклика (SRES), используя полученный случайный номер RAND и ключ аутентификации пользователя (Ki), по алгоритму A3: SRES = f1(Ki, RAND), и отсылке подвижной станцией

вычисленного значения хэша SRES на базу для сверки принятого значения SRES с аналогичным значением SRES, вычисленным в центре аутентификации. Если оба значения совпадают, то подвижная станция осуществляет передачу сообщений, а если нет, тогда связь прерывается.

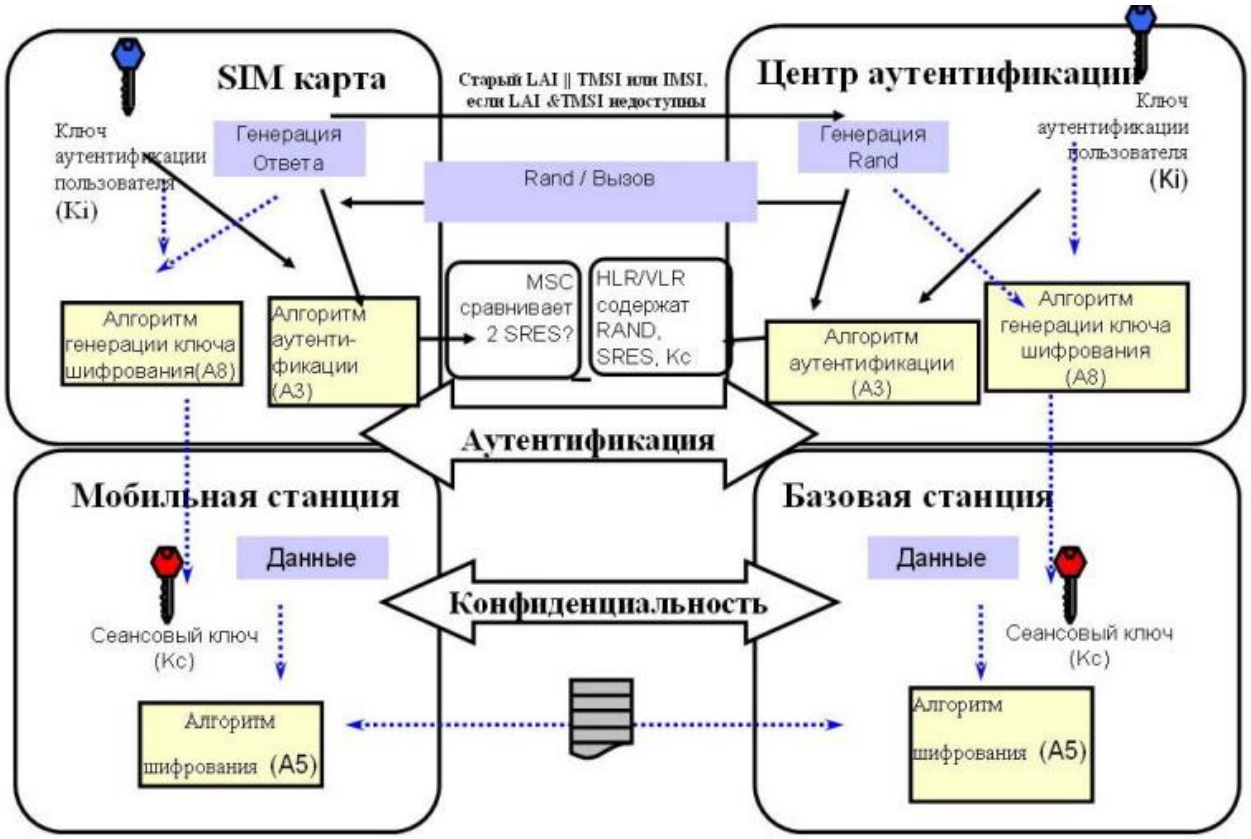

Рис. 1.6. Структура системы безопасности GSM-связи

Алгоритм формирования ключей шифрования A8 хранится как в модуле SIM на мобильной станции, так и в центре аутентификации и обеспечивает секретность передаваемой по радиоканалу информации. После приема случайного номера RAND подвижная станция вычисляет, кроме отклика SRES, также и сеансовый ключ шифрования (Кс), используя RAND, ключ аутентификации пользователя Ki по алгоритму A8: Кс = f2(Ki, RAND). Ключ шифрования Кс не передается по радиоканалу.

Алгоритм A5 описан в стандарте GSM 03.20 и используется для шифрования голосовых данных и конфиденциальных сигнальных сообщений на участке подвижная станция – базовая станция [6-7]. В нем применена более криптостойкая система регистров переменного тактирования с различными длинами и функциями обратной связи. Псевдослучайная последовательность формируется с помощью ГПСП, реализуемом на основе трёх линейных регистров

сдвига с обратной связью, имеющих разрядности 19, 22 и 23 бита соответственно, что в сумме дает 64-битный сеансовый ключ шифрования в GSM, как показано на рис.1.7 при реализации *алгоритма A5/1*.

Многочлены обратных связей соответственно для первого, второго и третьего регистров сдвига имеют вид:

$P_1(x)=X^{19} + X^{18} + X^{17} + X^{14} + 1,$

$P_2(x)=X^{22} + X^{21} + 1,$

$P_3(x)=X^{23} + X^{22} + X^{21} + X^{8} + 1.$

Сдвигами управляет специальная схема, организующая на каждом шаге смещение как минимум двух регистров, что приводит к их неравномерному движению. В каждом регистре есть отводы от разрядов бит синхронизации: в первом регистре это 8 разряд ($R_{1\,8}$), во втором – 10 разряд ($R_{2\,10}$) и в третьем – 10 разряд ($R_{3\ 10}$). Биты синхронизации служат для формирования мажоритарной функции управления тактированием регистров сдвига $F = R_{1\,8}$ AND $R_{2\,10}$ OR $R_{1\,8}$ AND $R_{3\ 10}$ OR $R_{2\ 10}$ AND $R_{3\ 10}$. Таким образом, управление тактированием осуществляет сдвиг только тех регистров, у которых бит синхронизации равен F, т.е. сдвигаются регистры, синхробит которых принадлежит большинству.

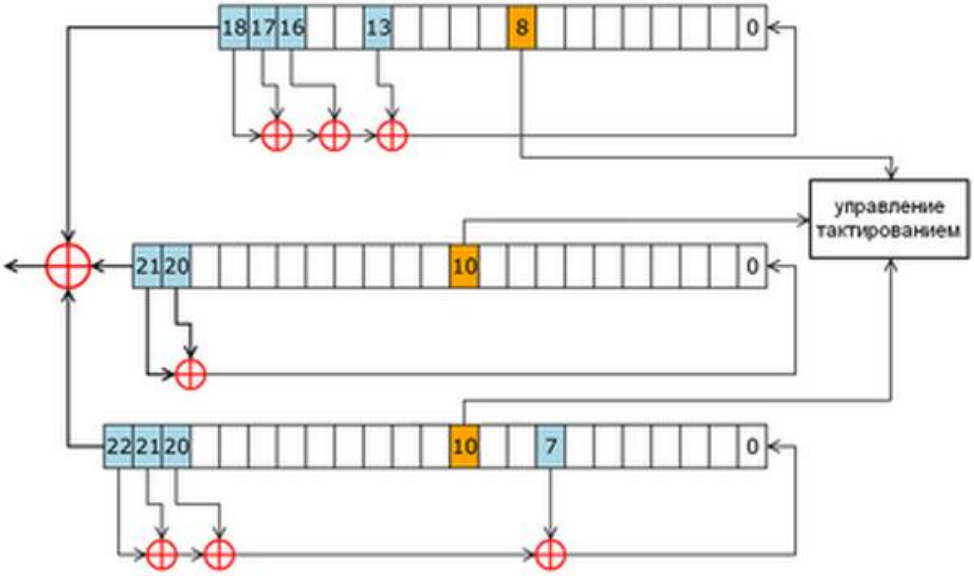

Рис. 1.7. Структура ГПСП, реализующего алгоритм шифрования A5/1

Каждый выходной бит последовательности формируется как результат операции суммирования по модулю 2 (XOR) выходных бит регистров.

Передача данных осуществляется разбивкой на кадры по 114 бит. Перед инициализацией регистры обнуляются, на вход ГПСП поступают сеансовый ключ K размером 64 бита, сформированный с помощью алгоритма A8, и номер кадра

Fn длительностью 22 бита. Далее последовательно выполняются такты инициализации и рабочие такты шифрования.

Инициализация включает в себя 64 такта, при которых очередной бит ключа суммируется по модулю 2 (XOR) с младшим битом каждого регистра, при этом происходит сдвиг регистров на каждом такте, далее осуществляются аналогичные 22 такта, только операция XOR производится с номером кадра, а также 100 тактов с управлением сдвигами регистров, но без генерации последовательности.

В процессе рабочих 228 (114 + 114) тактов формируется псевдослучайная последовательность бит ГПСП с управлением тактированием регистров сдвига и происходит потоковое шифрование передаваемого кадра (первые 114 бит) и дешифрование (последние 114 бит) принимаемого.

Далее инициализация производится заново, используя новый номер кадра, и процесс повторяется.

В модификации *алгоритма A5/2* добавлен ещё один регистр сдвига (рис.1.8), управляющий движением остальных, разрядностью 17 бит (R4), в которых биты 3, 7, 10 являются битами синхронизации. Формируемая мажоритарная функция оперирует с битами синхронизации управляющего регистра сдвига $F = R_{4\,3}$ AND $R_{4\,7}$ OR $R_{4\,3}$ AND $R_{4\,10}$ OR $R_{4\,7}$ AND $R_{4\,10}$. При этом происходит сдвиг первого регистра, если $R_{4\,10} =$ F, второго регистра, если $R_{4\,3} =$ F и третьего регистра, если $R_{4\,7} =$ F.

Каждый выходной бит последовательность формируется как результат операции суммирования по модулю 2 (XOR) старших бит регистров и мажоритарных функций от определённых битов регистров: в первом регистре это 12, 14, 15 разряды, во втором – 9, 13, 16 разряды и в третьем – 13, 16, 18.

Изменения в процессе передачи данных для модификации алгоритма A5/2 касаются только инициализации, во время которой в течение 64+22 тактов заполняются сеансовым ключом и номером кадра как первые три регистра, так и четвертый регистр сдвига. Далее следует один такт для заполнения единицами 3, 7 и 10 разрядов синхронизации четвертого регистра сдвига и 99 тактов с управлением сдвигами регистров, но без генерации последовательности.

Модификация *алгоритма A5/3* также называется алгоритмом Касуми, за основу которого взят шифр MISTY.

Приложения цифрового скремблирования находят свое применение не только в системах мобильной радиосвязи, но и в системах цифрового телевизионного вещания в приемниках цифрового телевидения и системах кабельного телевидения, а также в системах видеонаблюдения (стандарты SMPTE цифровых последовательных интерфейсов SDI HD-SDI).

Так обобщенный алгоритм скремблирования – Common Scrambling Algorithm (CSA2) (утвержден институтом европейских телекоммуникационных стандартов - European Telecommunications Standards Institute (ETSI) и европейским союзом телерадиовещания – European Broadcasting Union (EBU)) обеспечивает защиту MPEG контента пользователей телевизионной сети. В системах условного доступа цифрового телевещания криптостойкость обеспечивается использованием комбинации методов скремблирования и шифрования [8-11]. Здесь мультиплексированный поток видео, звука и данных передается скремблированным, в то время как зашифрованные сообщения управления доступом (ECM) и условного доступа (EMM) передаются в цифровом потоке без скремблирования [8-11].

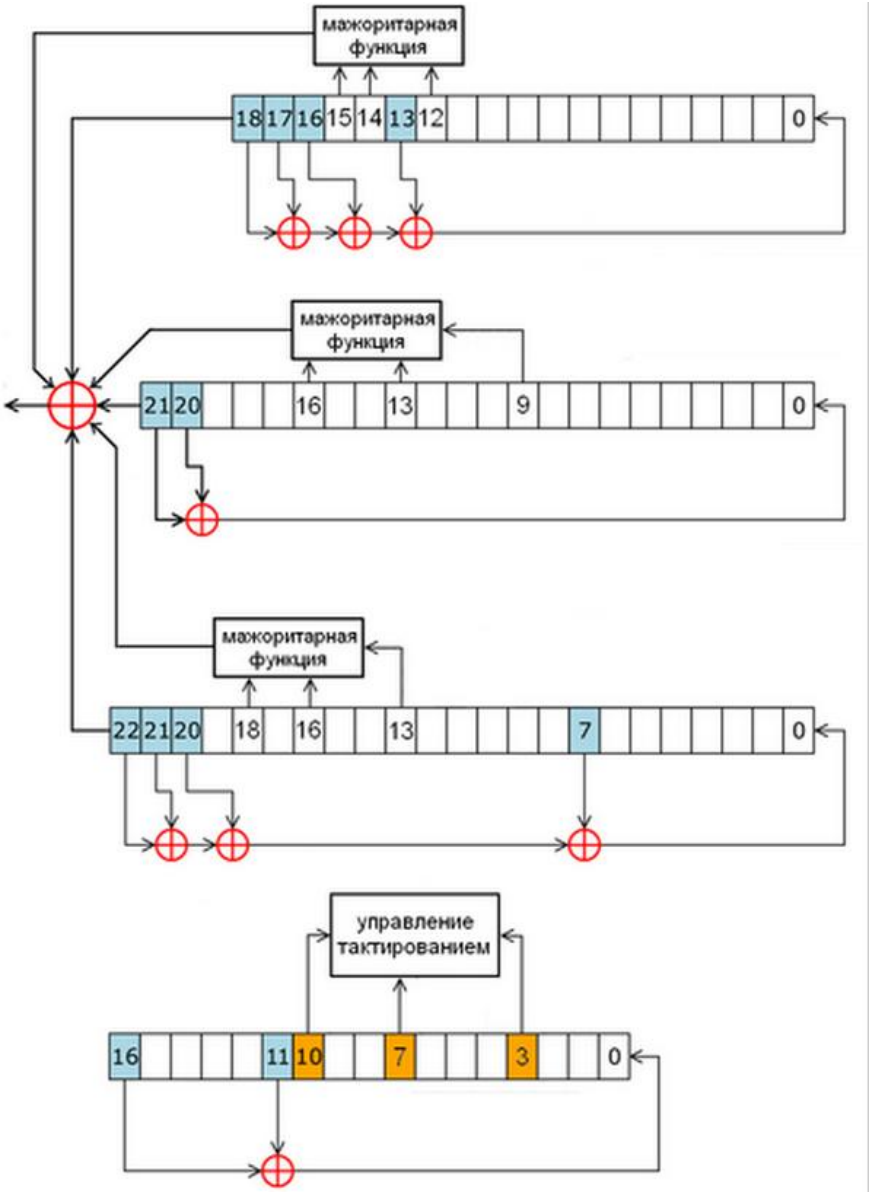

Рис. 1.8. Структура ГПСП, реализующего алгоритм шифрования A5/2

Современная система условного доступа представляет собой комплекс программно-аппаратных средств, формирующих несколько взаимосвязанных между собой подсистем: подсистемы обслуживания абонентов и управления подпиской; подсистемы генерации и управления ключами; подсистемы скремблирования и шифрования транспортного потока; подсистемы безопасности аппартно-программного обеспечения декодера. Оборудование таких систем использует обобщенный алгоритм скремблирования (CSA), криптостойкий алгоритм одноключевого блочного шифрования/дешифровки (DES или AES-128) и двухключевой ассиметричный алгоритм шифрования/дешифровки кодового слова дескремблера (RSA) [8-11].

Потоковый алгоритм скремблирования-дескремблирования реализован в оборудовании DVB-скремблеров, DVB-мультиплексоров, DVB-стримеров с типовыми характеристиками: максимальная тактовая частота 300 МГц, пропускная способность 500 Мбит/с, размер ключа – 64 бита. Известные стримеры систем условного доступа обеспечивают, например, скорости передачи видеоданных MPEG2 через последовательный высокоскоростной интерфейс ASI для CSA – 10 Мб/с [10], т.е. операция мультиплексирования потока видео, звука, данных, зашифрованных сообщений управления доступом и условного доступа снижают скорость передачи. Обобщенный алгоритм скремблирования-дескремблирования CSA выглядит как каскадное соединение потокового и блочного шифраторов, каждый из которых использует 64-битный ключ [11].

Архитектура системы условного доступа при скремблировании потока данных в спутниковом цифровом вещании приведена на рис.1.9, а при дескремблировании – на рис.1.10.

Для систем видеонаблюдения при передачи видео высокой четкости используется цифровой последовательный интерфейс HD-SDI, обеспечивающий номинальную скорость передачи данных 1,485 Гбит / с и использующийся для передачи несжатого, незашифрованного цифрового видеосигнала по коаксиальным или оптоволоконным линиям связи. В стандарте регламентируется передача потока 8- или 10-разрядных слов по одному каналу в последовательном коде. Полоса последовательного канала при передаче 8-разрядных цифровых видеосигналов составит 27 МГц х 8 = 216 МГц, а для 10-разрядного – 27 МГц х 10 = 270 МГц.

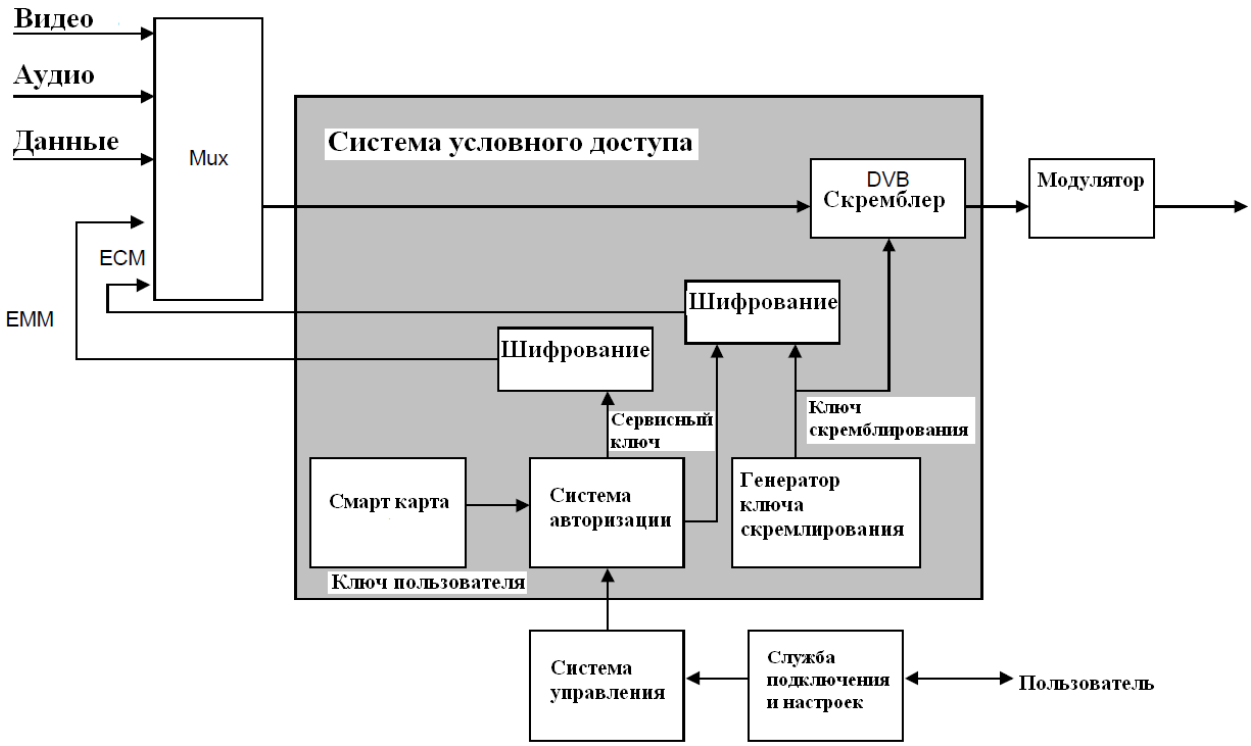

Рис. 1.9. Структура системы условного доступа при скремблировании потока данных

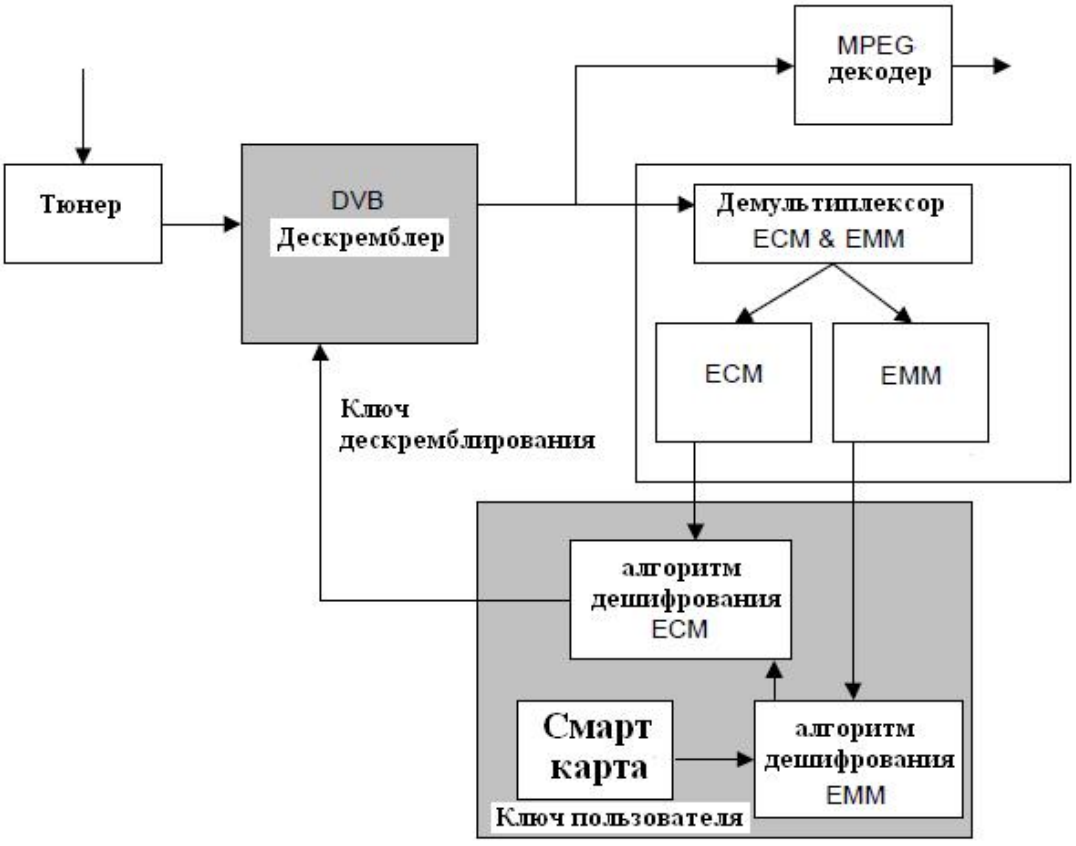

Рис. 1.10. Структура системы условного доступа при дескремблировании потока данных

Передаче сигнала в канал связи предшествует скремблирование, оптимизирующее спектр передаваемого сигнала и обеспечивающее выделения тактовой частоты на стороне приемника. Младший бит каждого слова в последовательном потоке передается первым, при этом реализован код NRZI, не чувствительным к полярности сигналов. В данном стандарте используется комбинационный генератор ПСП на основе полиномиальной последовательности типа $p_1(x) \oplus p_2(x)$, где: $p_1(x) = x^9 + x^4 + 1$ – образующий многочлен, обеспечивающий скремблированный NRZ-сигнал; $p_2(x) = x+1$ – образующий многочлен, обеспечивающий скремблированную NRZI последовательность, не чувствительную к полярности сигналов [8-11].

1.3. Задания для самостоятельной проработки

1. Создать виртуальный прибор цифрового скремблера с самосинхронизацией.
2. Создать виртуальный прибор цифрового скремблера с начальной предустановкой.
3. Создать виртуальный прибор цифрового комбинационного генератора СЛРП.
4. Создать виртуальный прибор генератора Геффа.
5. Создать виртуальный прибор генератора переменного шага.
6. Создать виртуальный прибор цифрового скремблера с управлением тактированием регистров сдвига, согласно алгоритму A5/1.
7.* Создать виртуальный прибор цифрового дескремблера с самосинхронизацией.
8.* Создать виртуальный прибор цифрового дескремблера с начальной предустановкой.

1.4. Рекомендации к выполнению экспериментального задания

Для создания диаграммной панели виртуального прибора необходимо использовать среду LabVIEW и ее библиотеку Programming с соответствующими разделами работы с файлами File I/O, со строками String и матрицами Array.

Для создания виртуального прибора для осуществления заданного вида цифрового скремблирования в качестве примера рассмотрим алгоритм формирования М-последовательности с периодом 1023 с характеристическим многочленом с коэффициентами 10000001001 [5], реализованный в ГПСП скремблера. Упрощенная лицевая панель виртуального прибора для

осуществления скремблирования приведена на рис.1.11, а упрощенная диаграммная панель – на рис.1.12. На лицевую панель прибора выведены все необходимые органы управления и индикации скремблера.

Из приведенной на рис.1.12 упрощенной диаграммной панели цифрового скремблера видно, что передаваемое текстовое сообщение преобразуется в массив кодов символов, которые после преобразования в логический тип данных в виде 8-разрядных кодовых слов побитно смешиваются с псевдослучайной последовательностью бит. Полученный в результате преобразований строковый массив данных выводится в виде строки скремблированного сообщения.

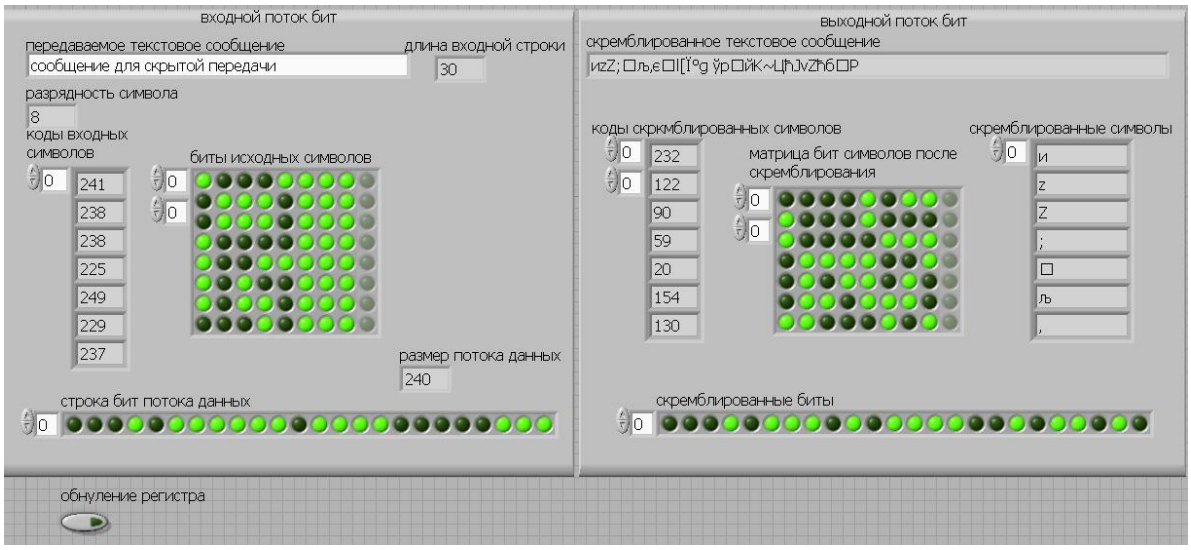

Рис. 1.11. Лицевая панель виртуального прибора цифрового скремблера текстового сообщения

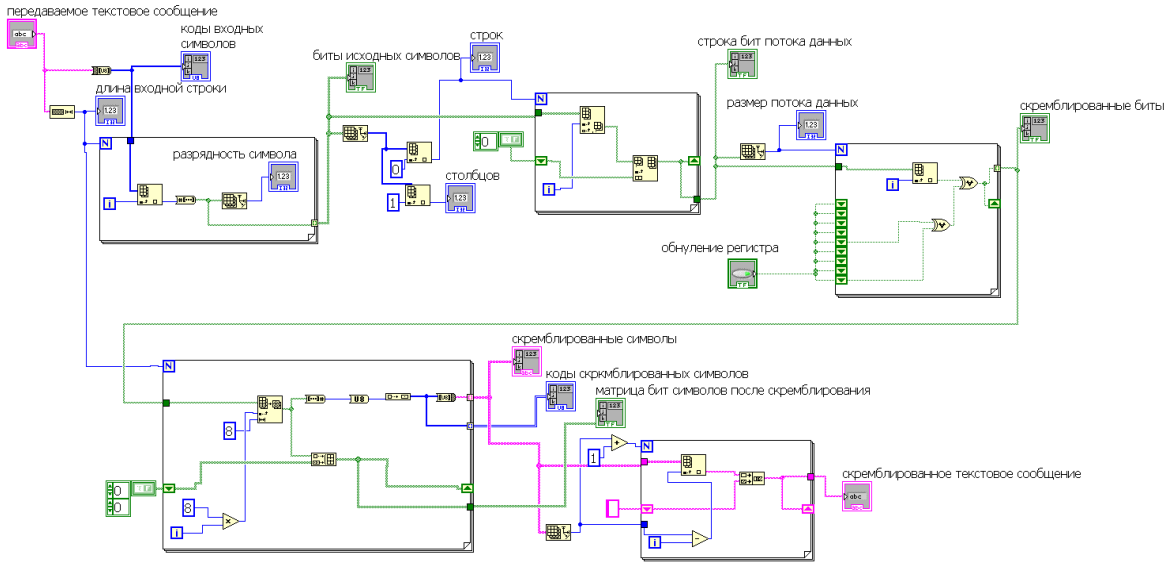

Рис. 1.12. Диаграммная панель виртуального прибора цифрового скремблера текстового сообщения

Рассмотрим пример реализации упрощенной модели скремблера на примере обработки речевого трафика телекоммуникационных сетей [12]. Процесс создания виртуального прибора LabVIEW для эксперимента выполним в несколько этапов.

На первом этапе производится считывание звукового файла речи в формате WAV, отображение временной реализации сигнала и преобразование типов данных. На втором этапе дискретные отсчеты звукового файла представляются в формате с плавающей точкой и формируется поток бит для скремблирования. На третьем этапе осуществляется непосредственно цифровое скремблирование на основе суммирования по модулю два потока бит данных с псевдослучайной последовательностью бит цифрового генератора ПСП. На четвертом этапе происходит преобразование битового скремблированного потока в дискретные отсчеты, а на пятом этапе – отображение скремблированного сигнала и запись его в аудиофайл.

Более детально остановимся на втором этапе при определении формата чисел с плавающей точкой при представлении дискретных отсчетов сигнала в двоичной форме. Такое представление базируется на экспоненциальной форме записи вещественного числа в виде:

$$A = m \times q^n = m \times 2^n$$

где m – мантисса числа

q – основание системы счисления,

n – порядок числа.

Для однозначности представления чисел с плавающей точкой в LabVIEW используется нормализованная форма, при которой мантисса отвечает условию:

$$1 \le |m| < 2.$$

В лабораторных испытаниях при скремблировании речевых сигналов вполне достаточно будет ограничиться для хранения порядка и его знака 4 разрядами, а для хранения мантиссы и ее знака – 10 разрядами. Максимальное значение порядка числа составит $111_2 = 7_{10}$, и, следовательно, максимальное значение числа составит $2^7 = 128$. Минимальное значение порядка числа составит $2^{-7} = 0{,}0078125$. Количество разрядов, отведенных для хранения мантиссы чисел, равное 9 ($2^{10} - 1 = 1023$), определяет точность представления отсчетов сигнала, в данном случае 3 знаков после запятой будет вполне достаточно, и, следовательно, максимальное значение мантиссы ограничено значением 1,999.

Сформированный поток битов данных речевого сигнала, включающий последовательно следующие 14 разрядов порядка и мантиссы для каждого отсчета поступает на цифровой скремблер. Алгоритм работы генератора ПСП скремблера

основан на формировании М-последовательности с периодом 1023 с характеристическим многочленом с коэффициентами 10000001001 [12]. Фрагмент лицевой и диаграммной панелей виртуального прибора представлен на рис.1.13 и 1.14.

Таким образом, в результате работы можно создать виртуальные приборы, осуществляющие цифровое скремблирование текстовых сообщений и речевых сигналов.

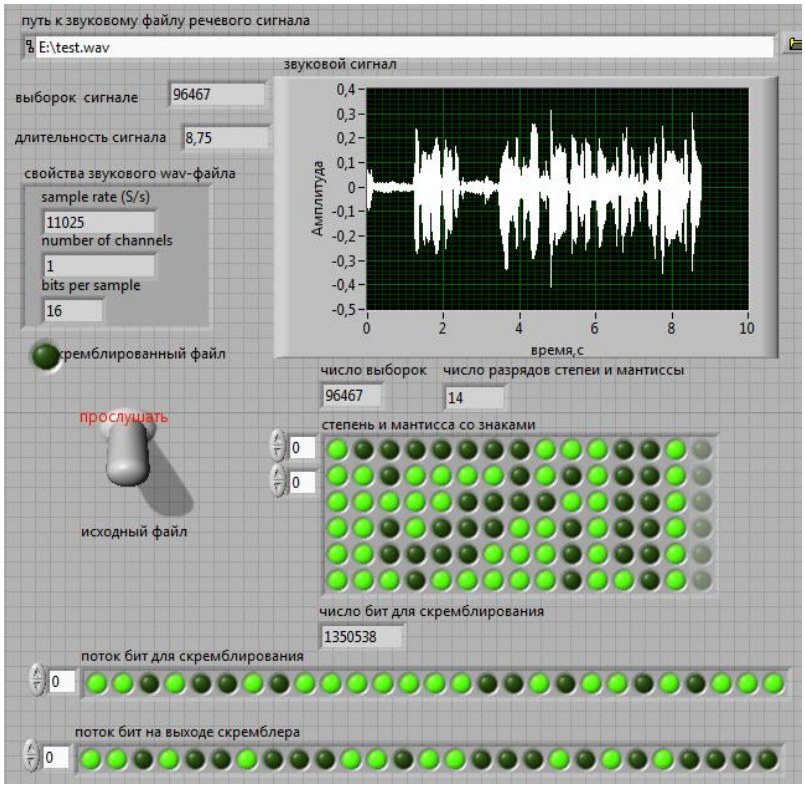

Рис. 1.13. Фрагмент лицевой панели виртуального прибора цифрового скремблера речевого сигнала

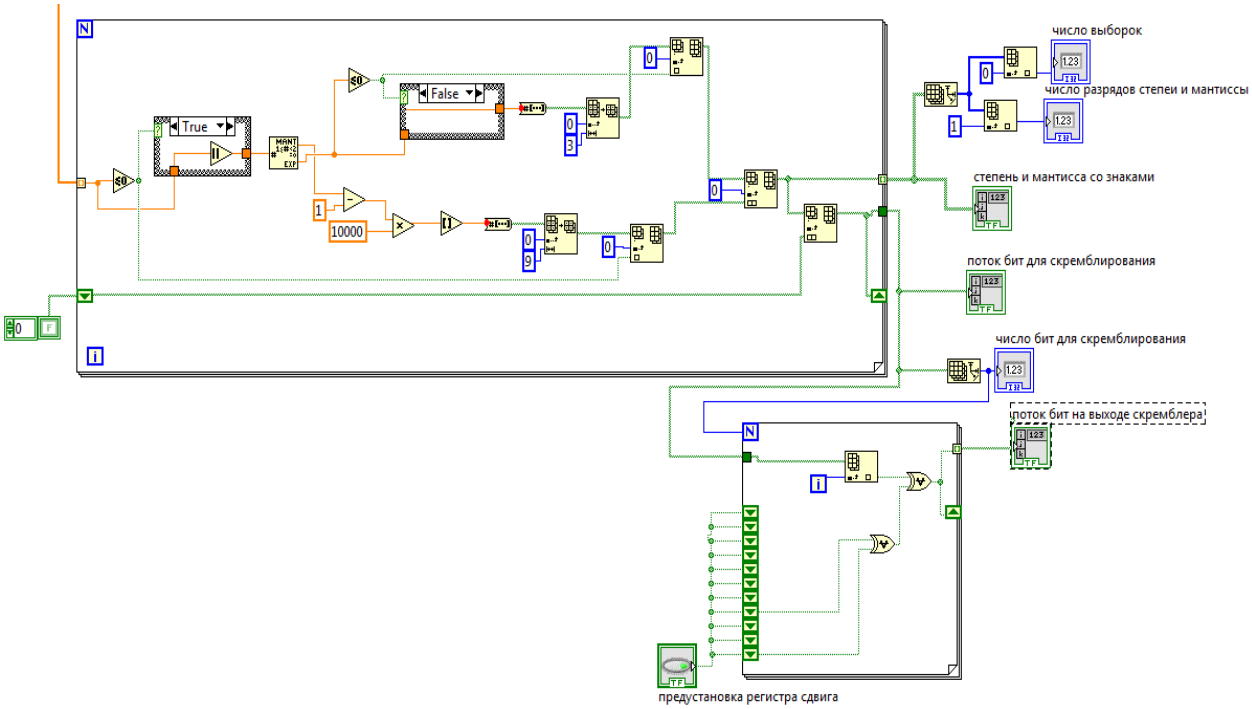

Рис. 1.14. Фрагмент диаграммной панели виртуального прибора цифрового скремблера речевого сигнала

Созданные библиотечные модули (вложенные виртуальные приборы) для осуществления скремблирования с изолированными ГПСП, с неизолированными ГПСП, с самосинхронизацией, с начальной установкой, а также реализация ГПСП в виде моделей генератора Геффа, генератора переменного шага, сжимающего генератора позволяют реализовать соответствующие системы скремблер-дескремблер и исследовать их характеристики в результате лабораторного эксперимента.

Контрольные вопросы для самопроверки

1. Назвать свойства псевдослучайных последовательностей генераторов ПСП цифровых скремблеров.
2. Каким образом можно увеличить период генератора ПСП в цифровом скремблере?
3. Дать сравнительную характеристику цифровых скремблеров с самосинхронизацией и начальной установкой.
4. Пояснить принцип работы системы скремблер/дескремблер с неизолированными генераторами ПСП.
5. Пояснить принцип работы системы скремблер/дескремблер с изолированными генераторами ПСП.

6. Из-за чего происходит нарушение работы скремблера/дескремблера с неизолированными генераторами ПСП.

7. Из-за чего происходит нарушение работы скремблера/дескремблера с изолированными генераторами ПСП?

8. Назвать способы защиты цифровых скремблеров.

9. Назвать особенности генераторов составных ЛРП на базе ЛРС.

10. Пояснить принцип работы комбинационного генератора СЛРП.

11. В чем заключается особенность генераторе Геффа?

12. Пояснить принцип работы генератора переменного шага.

13. Пояснить принцип работы системы безопасности GSM-связи. Какие алгоритмы шифрования в ней используются?

14. Пояснить процесс шифрования голосовых данных в стандарте GSM согласно алгоритму A5/1.

15. Объяснить отличия модификации алгоритма A5/2 от его предшественника.

16. Назвать назначение и особенности обобщенного алгоритма скремблирования.

17. Пояснить принцип работы системы система условного доступа цифрового телевещания.

18. Назвать особенности использования цифрового скремблирования в системах видеонаблюдения.