Шибаев Станислав Сергеевич – e-mail: sshib75@mail.ru; лаборатория оптоэлектроники; с.н.с.; к.т.н.

Помазанов Александр Васильевич – e-mail: pav_tsure@mail.ru; кафедра информационной безопасности телекоммуникационных систем; профессор; к.т.н.

Volik Denis Petrovich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: DVLbest@mail.ru; 2, Shevchenko street, Taganrog, 347922, Russia; phone: +78634312482; the department of radioengineering electronics.

Shibaev Stanislaw Sergeyevich – e-mail: sshib75@mail.ru; laboratory of optoelectronics; senior scientist; cand. of eng. sc.

Pomazanov Alexandr Vasilievich – e-mail: pav_tsure@mail.ru; the department of telecommunication systems information security; professor; cand. of eng. sc.

УДК 681.3.016

В.Т. Корниенко

ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНЫХ ПРИБОРОВ LABVIEW В УЧЕБНОМ ПРОЦЕССЕ ДЛЯ СКРЕМБЛИРОВАНИЯ ЦИФРОВОГО ПОТОКА ДАННЫХ

Целью работы является представление лабораторного практикума на основе технологии виртуальных приборов LabVIEW для выполнения скремблирования цифрового потока данных. Проанализированы разновидности систем скремблер-дескремблер с неизолированными и изолированными от канала связи генераторами псевдослучайных последовательностей бит. Рассмотрены приложения скремблирования цифрового потока данных в системах условного доступа цифрового телевещания и в системах видеонаблюдения при передаче видео высокой четкости с использованием цифрового последовательного интерфейса HD-SDI. Приведена структура скремблер-дескремблер интерфейса SDI и для нее в качестве примера рассмотрены лицевая и диаграммная панели виртуального прибора LabVIEW. В результате проделанной работы были созданы виртуальные приборы, осуществляющие цифровое скремблирование текстовых сообщений, речевых сигналов, jpeg-изображений, а также библиотечные модули (вложенные виртуальные приборы) для осуществления скремблирования разными способами. В итоге использование новых информационных технологий в инженерном образовании позволило реализовать лабораторный практикум для исследования принципов построения цифровых скремблеров.

Скремблер; дескремблер; регистр сдвига с линейной обратной связью; система условного доступа; цифровой последовательный интерфейс; виртуальный прибор LabVIEW; лабораторный практикум.

V.T. Kornienko

APPLICATION OF LABVIEW VIRTUAL DEVICES IN EDUCATIONAL PROCESS FOR SCRAMBLING OF DIGITAL DATA FLOW

The design of LabVIEW's virtual devices of digital scrambler is considered. The purpose of this abstract is the representation of a laboratory practical work on the basis of technology of virtual devices LabVIEW for performance of a digital data flow scrambling. The versions of scrambler systems with generators of pseudo-casual bit sequences which are not isolated and isolated from the communication channel are analyzed. The applications of a digital flow scrambling given in systems of conditional access of a digital video broadcasting and in systems of video registration are considered by transfer of a video of high clearness with use of the digital consecutive interface HD-SDI. The structure scrambler-descrambler of the interface SDI is given and for

it as an example are considered the front and diagram panel of the LabVIEW's virtual device. As a result of the virtual devices researches which are carrying out digital scrambling of the text messages, speech signals, jpeg-images, and also library modules for scrambling realization by different ways were created. As a result of use of new information technologies in engineering education has allowed to realize a laboratory practical work for research of digital scrambler construction principles.

Digital scrambler; LabVIEW; virtual device; pseudorandom numbers generators; conditional access system.

Изучение разделов ряда дисциплин на радиотехническом факультете ЮФУ сопровождается использованием студентами в лабораторных экспериментах технологий создания виртуальных приборов в среде LabVIEW, позволяют изучить принцип действия и характеристики сложных технических систем передачи информации, обеспечивающих защиту данных, и получить практические навыки в построении алгоритмических моделей технических средств [1].

Известно, что скремблирование цифрового потока данных производит преобразование его структуры без изменения скорости передачи с целью получения свойств псевдослучайной последовательности, обеспечивая защиту информации от несанкционированного доступа и ускоряя процесс выделения тактовой частоты при осуществлении дескремблирования на приемной стороне. Цифровые скремблеры и дескремблеры реализуются на основе генераторов псевдослучайных последовательностей битов (ПСП), выполненных с использованием М-разрядных сдвиговых регистров с цепями обратной связи и отличающихся периодом генерируемых последовательностей битов. Известны многие разновидности систем скремблер-дескремблер, одними из которых являются системы с неизолированными и изолированными от канала связи генераторами ПСП [2], самосинхронизирующиеся и с начальной установкой. При потере синхронизма между скремблером и дескремблером время его восстановления не превышает числа тактов, зависящего от разрядности регистра сдвига генератора ПСП скремблера. Недостатками самосинхронизирующихся скремблеров-дескремблеров является свойство размножения ошибок и периодичность выходной последовательности, которые устраняются использованием в регистре сдвига числа отводных разрядов не более двух и применением дополнительных схем контроля, выявляющих и нарушающих периодичность [3].

Приложения цифрового скремблирования имеют место в цифровых системах телевещания с условным доступом (DVB CA), в сетях сотовой связи (алгоритм шифрования A5), в системах видеонаблюдения (стандарты SMPTE цифровых последовательных интерфейсов SDI HD-SDI).

Так, например, в системе условного доступа цифрового телевещания производится скремблирование/дескремблирование мультиплексированного потока видео, звука, данных, а зашифрованные сообщения управления доступом и условного доступа передаются в цифровом потоке без скремблирования [4]. Оборудование таких систем использует обобщенный алгоритм скремблирования (CSA), криптостойкий алгоритм одноключевого блочного шифрования/расшифровки (AES-128) и двухключевой ассиметричный алгоритм шифрования/расшифровки кодового слова дескремблера (RSA) [5, 6, 7]. Известные стримеры систем условного доступа обеспечивают, например, скорости передачи видеоданных MPEG2 через последовательный высокоскоростной интерфейс ASI для CSA – 10 Мб/с и для AES-128 – 40 Мб/с [8].

Для систем видеонаблюдения при передаче 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. 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 [9].

На рис. 1 показана структура скремблер-дескремблер интерфейса SDI. Например, стандарт SMPTE имеет следующие спецификации для цифровых последовательных интерфейсов SDI и HD-SDI: SMPTE 259M, регламентирующий передачу цифрового потока видео для композитного сигнала NTSC на 143 Мбит/с и PAL 177 Мбит/с, передачу телевизионных сигналов форматов 525/625 со скоростями 270 Мбит/с и 360 Мбит/с; SMPTE 292M, описывающий новый формат передачи HDTV со скоростью 1,458 Гбит/с [9].

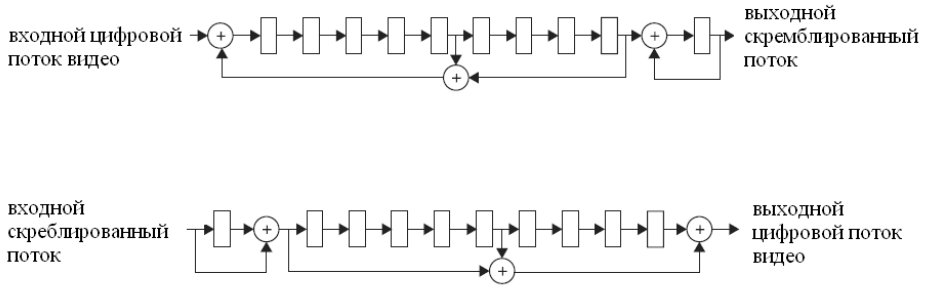

Рис. 1. Система скремблер-дескремблер интерфейса SDI

Известен также подход для скремблирования цифрового видео потока на основе матриц Судоку, который по ряду показателей не уступает перечисленным выше аналогам скремблирования [10].

Перечисленные методы и алгоритмы скремблирования цифрового потока данных положены в основу лабораторного практикума с использованием среды LabVIEW для создания виртуальных приборов [11]. Созданы виртуальные лабораторные приборы: цифрового скремблера на основе изолированных генераторов ПСП, цифрового скремблера на основе неизолированных генераторов ПСП, упрощенной модели обобщенного алгоритма скремблирования (CSA), упрощенной модификации алгоритма шифрования A5, цифрового скремблера стандарта SDI.

Для примера рассмотрим алгоритм формирования SDI-скремблера. Например, лицевая панель виртуального прибора для осуществления скремблирования приведена на рис. 2, а упрощенная диаграммная панель – на рис. 3. На лицевую панель прибора выведены все необходимые органы управления и индикации скремблера. Из приведенной на рис. 2 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 после-

довательностью бит генератора формирования NRZ кода. Полученный в результате преобразований строковый массив данных выводится в виде строки скремблированного текстового сообщения.

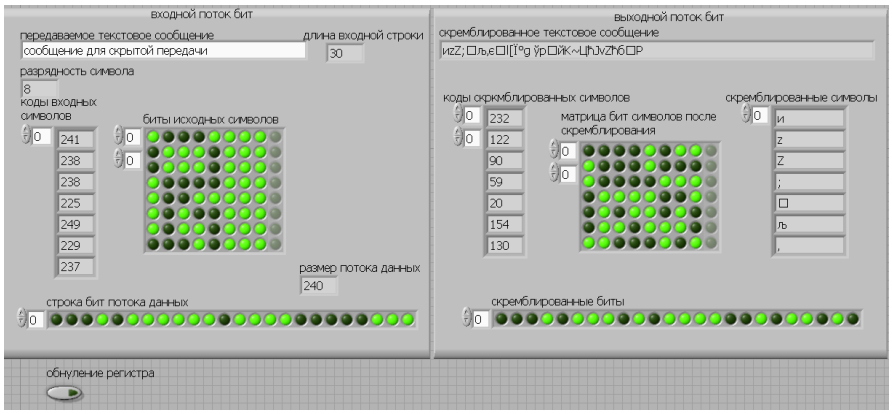

Рис. 2. Лицевая панель виртуального прибора цифрового скремблера текстового сообщения

В результате проделанной работы были созданы виртуальные приборы, осуществляющие цифровое скремблирование текстовых сообщений, речевых сигналов, jpeg-изображений, а также библиотечные модули (вложенные виртуальные приборы) для осуществления скремблирования с изолированными ГПСП, с неизолированными ГПСП, с самосинхронизацией, с начальной установкой, в которых ГПСП могут быть реализованы в виде моделей генератора Геффа, генератора на нелинейных фильтрах, генератора переменного шага, сжимающего генератора. Разработанные библиотечные модули позволяют реализовать соответствующие системы скремблер-дескремблер и исследовать их характеристики в результате лабораторного эксперимента.

Таким образом, использование новых информационных технологий в инженерном образовании позволило реализовать лабораторный практикум для исследования принципов построения цифровых скремблеров передаваемых сообщений.

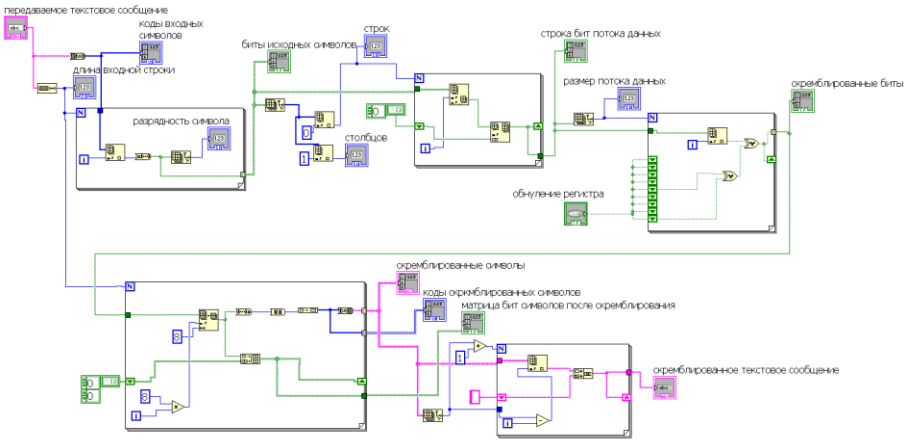

Рис. 3. Диаграммная панель виртуального прибора цифрового скремблера текстового сообщения

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Корниенко В.Т. Шеверева А.В*. Использование виртуальных приборов LabVIEW для анализа работы цифровых скремблеров. Практика и перспективы развития партнерства в сфере высшей школы // Материалы четырнадцатого международного научно-практического семинара. г. Донецк, 15-18 апреля 2013 г. В 3-х томах. Т. 2. – Донецк: ДонНТУ, 2013. – С. 89-93.
2. *Шевкопляс Б.* Скремблирование передаваемых данных // Схемотехника. – 2004. – № 12. – С. 24-27.
3. *Шевкопляс Б.* Скремблирование передаваемых данных // Схемотехника. – 2005. – № 2. – С. 32-35.
4. *Boucqueau J.M, Verians X*. “Next Generation Conditional Access Systems for Satellite Broadcasting," ESA Contract 16996/02/NL/US Octalis 2003.
5. *Афанасьев А.В*. Гибридная защита от несанкционированного доступа мультимедийного вещания в сетях передачи данных: Сборник трудов МГТУ им. Н.Э. Баумана. – М., 2004.
6. Support for use of the DVB Scrambling Algorithm version 3 within digital broadcasting systems. DVB Document A125. July 2008.
7. DVB CSA2 Descrambler Core. CLP-42 Product Brief Elliptic Technologies Inc.62 Steacie Drive, Suite 201. Ottawa, ON, Canada.
8. *Самрин А.* Стандарты цифровых видеоинтерфейсов // Компоненты и технологии. – 2006. – № 2.
9. *Ralf-Philipp Weinmann, Kai Wirt*. Analysis of the DVB Common Scrambling Algorithm. Technical University of Darmstadt. Department of Computer Science. Darmstadt, Germany. October 12, 2004.
10. *Yue Wu, Sos Agaian, Joseph P. Noonan.* Sudoku Associated Two Dimensional Bijections for Image Scrambling. A paper draft submitted to ieee transactions on multimedia.
11. *Бутырин П.А., Васьковская Т.А., Каратаев В.В., Материкин С.В.* Автоматизация физических исследований и эксперимента: компьютерные измерения и виртуальные приборы на основе LabVIEW7. – М.: ДМК-пресс, 2005.

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Корниенко Владимир Тимофеевич – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: vlad_korn65@mail.ru; г. Таганрог, ул. Дзержинского, 170, кв. 53; тел.: +79515271225; кафедра радиотехнических и телекоммуникационных систем; к.т.н.; доцент.

Kornienko Vladimir Timofeevich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: vlad_korn65@mail.ru; 170, Dzerginsky street, fl. 53, Taganrog, Russia; phone; +79515271225; the department of radio engineering and telecommunication systems; cand. of eng. sc.; associate professor.

УДК 621.396.6

Т.А. Суанов

МОДЕЛИРОВАНИЕ ВЫСОКОСКОРОСТНЫХ ЛИНИЙ ПЕРЕДАЧИ В МНОГОСЛОЙНЫХ ПЕЧАТНЫХ ПЛАТАХ

Представлен этап предтопологического моделирования в маршруте проектирования высокоскоростных многослойных печатных плат с помощью системы автоматизированного проектирования Mentor Graphics Expedition-PCB.

Приведены результаты моделирования печатных линий передачи с целью выявления проблем обеспечения целостности сигналов и электромагнитной совместимости. Рассмотрены длинные линии передачи, требующие согласования, представлены временные диаграммы сигналов в несогласованных и согласованных линиях передачи при разных способах согласования. Исследованы линии передачи с взаимной электромагнитной связью на