

МАЛОГАБАРИТНЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С USB-ИНТЕРФЕЙСОМ

Научно-исследовательское учреждение «Институт прикладных физических проблем имени А.Н.Севченко» Белорусского государственного университета.
Минск, Республика Беларусь. rashchenia@bsu.by

Разработан аппаратно-программный генератор случайных числовых последовательностей (СЧП) «Ключ-ВС» с USB-интерфейсом, обеспечивающий формирование СЧП на физическом источнике шума и ее выгрузку в ПЭВМ со скоростью не менее 5 Мбит/с в виде двоичной последовательности по статистическим свойствам близкую (не хуже 10^{-5}) к последовательности независимых равновероятных испытаний.

Надежность и безопасность средств криптографической защиты информации определяется безопасностью и качеством используемых в них ключей. Для формирования криптографических ключей гарантированного качества применяют генераторы случайных числовых последовательностей (ГСЧП). При этом генерируемые случайные числа должны быть равномерно распределены на всем диапазоне и независимы. Обеспечение равновероятности и независимости на заданном уровне достигается применением ГСЧП, использующих для генерации случайных чисел недетерминированные физические процессы.

Разработан аппаратно-программный ГСЧП с USB-интерфейсом «Ключ-ВС».

Структурная схема

ГСЧП «Ключ-ВС» выполнен в виде аппаратно-программного устройства, в состав которого входят следующие основные модули:

- схема обработки шумового сигнала;
- программируемая логическая интегральная схема (ПЛИС);
- USB-мост;
- блоки стабилизации и преобразования напряжения;
- датчик температуры;
- блок индикации.

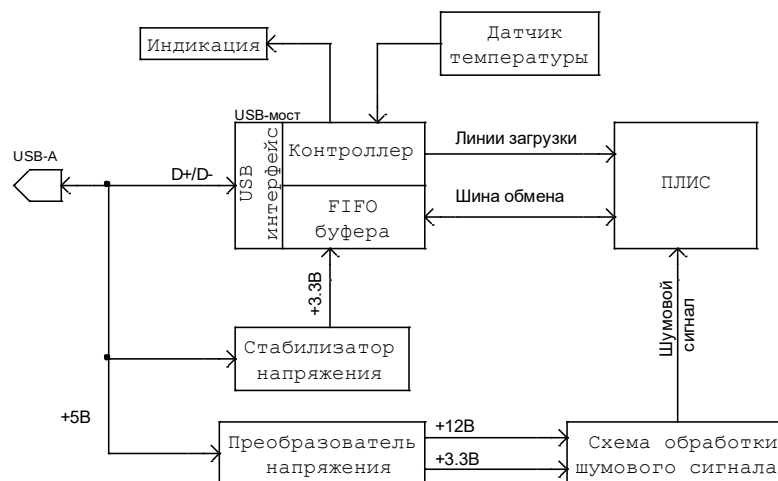


Рисунок 1 – Структурная схема ГСЧП «Ключ-ВС»

Схема обработки шумового сигнала обеспечивает получение аналогового шумового сигнала с физического источника шума (полупроводникового шумового диода) и его преобразование в цифровую форму.

ПЛИС выполняет обработку оцифрованного аналогового шумового сигнала, обеспечивая получение первичной СЧП. Она также обеспечивает функции интерфейса обмена с USB-мостом.

USB-мост обеспечивает реализацию внешнего интерфейса изделия с целевой ПЭВМ. Для обмена данными между ПЛИС и ПЭВМ используются FIFO-буфера моста USB. Кроме того, USB-мост включает контроллер, который обеспечивает выполнение функций управления режимами работы моста USB, а также загрузку в ПЛИС конфигурационных данных.

Модули стабилизации и преобразования напряжения обеспечивают электропитание ГСЧП «Ключ-ВС» от USB-порта целевой ПЭВМ, включая организацию всех режимов электропитания (плюс 3,3 В, плюс 5 В, плюс 12 В), необходимых для функционирования аппаратных и аппаратно-программных компонент устройства.

Датчик температуры обеспечивает измерение температуры и во взаимодействии с контроллером моста USB позволяет обеспечить контроль температурного режима эксплуатации ГСЧП «Ключ-ВС».

Блок индикации предназначен для визуального отображения основных режимов функционирования устройства в целях обеспечения удобства его эксплуатации. Его наличие позволяет оператору визуально определять состояние устройства (работоспособно, не функционирует, находится в состоянии ошибки или обмена данными и т.д.). На аппаратном уровне индикация обеспечивается применением светодиода.

Назначение и основные технические характеристики

ГСЧП «Ключ-ВС» предназначен для генерации и вывода в ПЭВМ СЧП на физическом источнике шума.

Область применения ГСЧП «Ключ-ВС» – системы и аппаратно-программные комплексы криптографической защиты информации, изготовления ключевой документации, сертификационные и доверительные центры инфраструктуры на публичных ключах, лабораторные и научные исследования.

ГСЧП «Ключ-ВС» обеспечивает:

- генерацию СЧП с использованием физического источника шума на полупроводниковом диоде и ее вывод в ПЭВМ;
- самотестирование работоспособности;
- тестирование работоспособности по команде оператора;
- контроль качества СЧП по команде оператора;
- контроль температуры на поверхности платы (внутри корпуса) устройства (при включенном электропитании ПЭВМ);
- функционирование под управлением операционной системы (ОС) семейства Windows;
- визуальную индикацию режимов функционирования.

ГСЧП «Ключ-ВС» выполнен в виде аппаратно-программного устройства, помещенного в защитную оболочку (металлический корпус) и предназначенного для использования в составе ПЭВМ.



Рисунок 2 – Внешний вид ГСЧП «Ключ-ВС»

Основные технические характеристики ГСЧП «Ключ-ВС»:

- скорость генерации СЧП не менее 5 Мбит/с;
- взаимодействие с ПЭВМ через интерфейс USB 2.0;
- электропитание от USB порта ПЭВМ +5 В;

- формирование и выгрузка в ПЭВМ СЧП в виде двоичной последовательности по статистическим свойствам близкой (не хуже 10^{-5}) к последовательности независимых равновероятных испытаний;
- встроенный датчик температуры;
- блокировка выгрузки СЧП при выходе температуры на поверхности платы (внутри корпуса) устройства за заданный диапазон (от плюс 5 до плюс 60 °С);
- встроенный светодиод для визуальной индикации режимов функционирования;
- статистическое тестирование качества выгруженной в ПЭВМ СЧП в соответствии с тестами, определенными в FIPS 140-1 [1].

Полученные с ГСЧП «Ключ-ВС» выборки СЧП (1000 подвыборок по 10^6 бит) успешно проходят тестирование с использованием пакета тестов NIST [2].

Программное обеспечение

Программное обеспечение (ПО) ГСЧП «Ключ-ВС» включает специальное ПО (СПО) и прикладное ПО (ППО).

СПО ГСЧП «Ключ-ВС» состоит из:

- программы контроллера моста USB – обеспечивает функционирование устройства на шине USB, а также загрузку в ПЛИС конфигурационных данных;
- программы-файла конфигурации ПЛИС – обеспечивает функции интерфейса обмена с мостом USB и цифровой обработки шумовых сигналов.

ППО ГСЧП «Ключ-ВС» состоит из:

- драйвера – обеспечивает функционирование устройства под управлением ОС семейства Windows;
- библиотеки функций – предоставляет разработчику пользовательских программ интерфейс работы с устройством под управлением ОС семейства Windows;
- пользовательского ПО – предоставляет интерфейс пользователя для работы с устройством под управлением ОС семейства Windows.

Пользовательское ПО обеспечивает следующие основные функциональные возможности:

- просмотр характеристик ГСЧП «Ключ-ВС»;
- тестирование ГСЧП «Ключ-ВС»;
- получение и сохранение в файл СЧП с ГСЧП «Ключ-ВС»;
- проверку качества СЧП;
- ведение журнала событий.

Контроль качества сгенерированной (выгруженной) СЧП осуществляется путем выполнения статистических тестов. При этом имеется возможность выбора режима тестирования: выполнить все доступные или только выбранные статистические тесты.

Во время работы пользовательского ПО обеспечиваются:

- визуальная индикация режимов и результатов выполнения команд оператора;
- выдача сообщений об ошибках, возникающих при работе оператора с ГСЧП «Ключ-ВС», включая ошибки при тестировании работоспособности устройства.

В ППО изделия реализована возможность переключения на английский язык интерфейса оператора.

Список литературы

1. Security requirements for Cryptographic Modules. FIPS 140-1. – U.S. Department of Commerce. 1994.
2. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Numbers, revision 1a.