УДК 681.3.06

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ФОРМИРОВАНИЯ И ИССЛЕДОВАНИЯ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Александр Потий, Евгений Попович, Юрий Горбенко, Виталий Вервейко
Харьковский государственный технический университет радиоэлектроники

Аннотация: **Рассматривается задача создания программных и аппаратных компонентов генераторов случайных и псевдослучайных чисел, встраиваемых в системы защиты информации, описываются компонентные модели генераторов случайных и псевдослучайных чисел, приводится пример реализации элементов модели.**

Summary: **Considers a creation task of program and hardware components of generators of accidental and psevdoaccidental numbers, built in information defense systems, describe the componental generators models of accidental and psevdoaccidental numbers, leads a realization example by model element.**

Ключевые слова: **Системы защиты информации, генераторы случайных и псевдослучайных чисел.**

Введение

Безопасность большинства криптографических систем зависит от способов формирования и использования ключей, паролей и параметров. Предельные характеристики стойкости достигаются в случае, если ключи и параметры выбираются случайно, равновероятно и независимо из полного пространства. Для выполнения этих условий используются генераторы случайных и псевдослучайных последовательностей.

Генераторы случайных и псевдослучайных последовательностей могут быть реализованы аппаратно или программно. Аппаратные генераторы реализуются в виде отдельных устройств, подключаемых к аппаратной платформе. Программные генераторы основываются на программируемой среде операционных систем. Для создания программных и аппаратных компонентов генераторов, встраиваемых в систему, необходимо построить компонентную модель генераторов и реализовать элементы этой модели.

I Компонентная модель генераторов (RNG/PRNG Model)

Генераторы случайных и псевдослучайных чисел - это аппаратные, программные или программно-аппаратные устройства или системные компоненты, предназначенные для формирования последовательностей случайных или псевдослучайных чисел. Генераторы реализуются в виде отдельных компонентов, встраиваемых в систему. Под системой понимается программный или аппаратный ресурс, на основе которого создается система защиты информации. Генератор, подключенный, инициализированный и функционирующий в системе, предоставляет функции генерации последовательностей случайных и псевдослучайных чисел использующему его программному или аппаратному компоненту системы защиты информации. Компонентная модель генератора представлена на рис. 1.

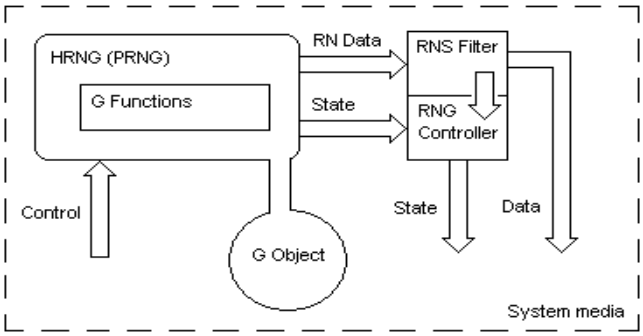

Рисунок 1 - Компонентная модель генератора.

Интерфейс генератора, встраиваемого в систему, должен, соответствовать интерфейсу системы и обеспечивать возможность создания, передачи и приема следующих потоков данных:

- управления функционированием генератора;
- выходных последовательностей;
- о состоянии генератора.

ISBN 966-622-022-9

Управление генератором осуществляется системой, которая формирует данные из среды системы (system media). Под управлением этих данных генератор формирует выходные последовательности, информирует систему о своем состоянии, выдает данные о состоянии и параметрах выполнения функции генерации. Информация о состоянии генератора при выполнении функции генерации содержит также данные о параметрах формируемой последовательности. Выходная последовательность (Random Numbers Data – RN Data) и информация о состоянии генератора (Generator State – G State) поступают на фильтр выходной последовательности (Random Numbers Sequence Filter – RNS Filter) и на контроллер состояния генератора (Generator Controller - G Controller).

Фильтр выходной последовательности выполняет фильтрацию (контроль) выхода генератора на основе анализа статистических параметров последовательности. Контроллер генератора получает информацию о состоянии генератора и о параметрах выходной последовательности и по полученным данным формирует информацию о состоянии генератора, передаваемую в среду системы. Фильтр, кроме определения параметров последовательности, анализирует их и в зависимости от результатов анализа пропускает или не пропускает выходную последовательность генератора в среду системы, формируя необходимую информацию для контроллера.

Таким образом, генератор представляется в системе базовым объектом генератора – компонентом (программными функциями или аппаратным устройством), выполняющим функции генерации последовательностей случайных или псевдослучайных чисел. Кроме того, для представления генератора в качестве системного ресурса используется системный объект генератора.

Компонентные модели аппаратных и программных генераторов в системе имеют одинаковую общую структуру, но отличаются особенностями представления объекта и ресурса генератора в системе.

II Компонентная модель объекта аппаратного генератора (HRNG)

Аппаратные платформы компьютерных или других систем позволяют встраивать или подключать к системе дополнительные аппаратные компоненты (устройства). В качестве таких компонентов используются и аппаратные датчики случайных чисел. Устройства аппаратных датчиков, реализованные в соответствии со спецификацией логического и аппаратного интерфейса, поддерживаемого системой, подключаются к ней в качестве периферийных устройств.

Подключение устройств аппаратных датчиков к компьютеру позволяет использовать их в компьютерных системах защиты информации. Современные компьютерные системы и сети основываются на аппаратных компонентах персональных компьютеров. Реализация стандартизированных спецификаций логических и электрических интерфейсов и слотов расширения позволяет интегрировать аппаратные датчики в любую компьютерную систему.

Аппаратные датчики подключаются к системным шинам ввода/вывода (слотам расширения) или к стандартным интерфейсам системной платы. Управление функционированием датчика может выполнять базовая система ввода/вывода (Basic Input Output System - BIOS), ядро операционной системы (Kernel) или процессы, выполняемые в операционной системе (Processes). Для реализации элементов управления созданы дополнительные программные компоненты, встраиваемые в состав стандартных компонентов операционных систем. Компонентная модель встраивания аппаратного датчика случайных чисел в компьютерную систему с операционной системой приведена на рис. 2.

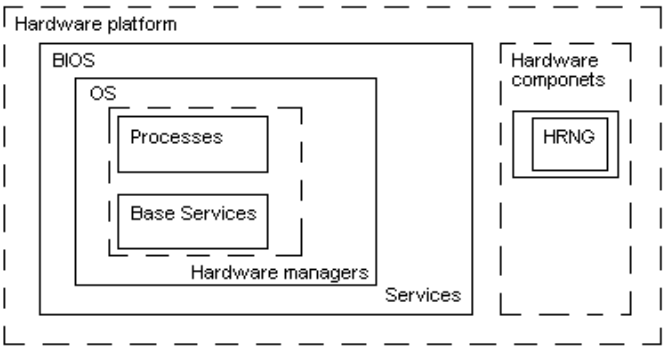

Рисунок 2 - Компонентная модель встраивания и функционирования аппаратного датчика случайных чисел в компьютерной системе

Базовая система ввода/вывода имеет прямой доступ ко всем аппаратным компонентам компьютерной

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

системы. Память системы содержит программы инициализации и работы с аппаратными ресурсами стандартных компонентов, к которым при подключении через стандартный интерфейс относятся и аппаратные датчики. Поэтому программы системы позволяют работать с датчиками случайных чисел, как со стандартными устройствами – через обычные интерфейсы и слоты. Создание нестандартных устройств требует нестандартного реконфигурирования системы, добавления в нее новых аппаратных компонентов и элементов управления. Это значительно усложнило бы реализацию таких компонентов.

Ядро операционной системы, как и базовая система ввода/вывода, имеет полный доступ ко всем аппаратным ресурсам системы. Поэтому управляющие программы (драйвера устройств – device drivers) могут управлять функционированием устройств аппаратных датчиков непосредственным программированием и конфигурированием компонентов системы, представляющих устройства генераторов. Использование функций и менеджеров ядра позволяют поддерживать разные конфигурации аппаратных ресурсов, реализующих датчики случайных чисел, встраивать и использовать их в системе.

Менеджеры аппаратных ресурсов и другие элементы управления доступны процессам через базовые сервисы, реализованные в операционной системе. Некоторые операционные системы позволяют процессам иметь непосредственный доступ к конфигурированию системы, настройке и управлению аппаратными средствами.

Для подключения аппаратного генератора к системе компонент генератора реализован в виде стандартного устройства, используемого в аппаратной платформе системы. Для обеспечения функционирования аппаратного генератора созданы программные элементы управления в операционной системе. В аппаратных и программных компонентах генераторов отдельные элементы компонентной модели аппаратного генератора могут быть реализованы как в аппаратной, так и в программной части.

Функции генерации и базовый объект генератора представляются в его аппаратной части. Системный ресурс такого генератора определяется в операционной системе как логический объект аппаратного устройства с элементами программного управления функциями и системным объектом генератора.

Фильтр выходных последовательностей реализуется в аппаратной части или в программных элементах управления. Контроллер состояния генератора включает в себя часть функций аппаратных компонентов генератора и платформы, а также программных компонентов операционных систем: базовой системы ввода/вывода, менеджеров и драйверов ядра. Драйверы аппаратных генераторов встраиваются в операционную систему и выполняют функции менеджера объектов генератора и управления объектами ресурсов, которыми представлены аппаратные компоненты генераторов в операционной системе. Совмещение программных и аппаратных элементов обеспечивает надежность и эффективность функционирования аппаратных датчиков случайных чисел в системе.

III Компонентная модель объекта программного генератора (PRNG)

Операционные системы дают возможность создания любых программных компонентов, в том числе и программных генераторов псевдослучайных чисел. Основой построения программных генераторов являются программные методы формирования последовательностей псевдослучайных чисел. При программной реализации функции генерации содержатся в программном объекте – исполняемом модуле – в формате, поддерживаемом операционной системой, или набором программ в памяти системы.

Функционирующий программный генератор представлен образом исполняемого модуля и объектом генератора в адресном пространстве системы. Процесс функционирования генератора представляет собой системный ресурс, управляемый операционной системой. Процесс использует базовые сервисы операционной системы в реализации программного генератора, а также включает в себя менеджер объектов генераторов, созданных в системе. Таким образом, функционирование программного генератора зависит от функционирования операционной системы, а также ее базовых сервисов.

Объект генератора включает в себя экземпляр функций генерации и данные о текущем состоянии генератора. Объект генератора создается и хранится в безопасной памяти. Фильтр выходной последовательности генератора входит в состав компонентов генерации или функционирует в виде отдельного программного компонента. Часть функций контроллера генератора включаются непосредственно в состав генератора, а часть создаются в фильтре и в самой операционной системе. Компонентная модель встраивания программного генератора псевдослучайных чисел в операционную систему приведена на рис. 3.

Таким образом, программный генератор, создаваемый на основе программной среды операционной системы, учитывает особенности построения отдельных элементов используемой операционной системы. Объекты генератора и модули с функциями генерации представлены как стандартные программные компоненты, что позволяет использовать разные уровни встраивания в операционную систему.

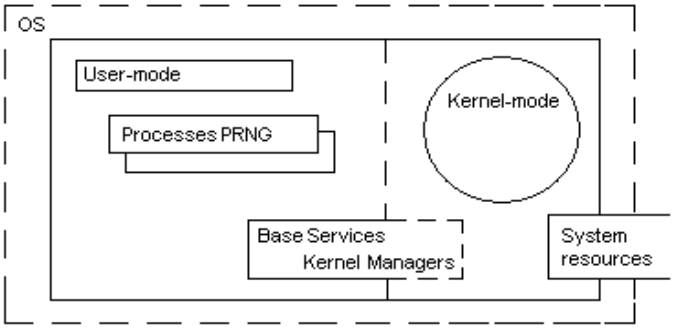

Рисунок 3 - Компонентная модель встраивания программного генератора псевдослучайных чисел в операционную систему.

IV Реализация объектной модели генераторов СЧ и ПСЧ

В соответствии с описанной компонентной моделью генераторов на основе аппаратного датчика случайных чисел «Гряда-1» и алгоритма генерации псевдослучайных чисел, описанного в стандарте ANSI X9.17 [3], были разработаны программные компоненты для подключения и встраивания в системы защиты информации. Программные системные компоненты разработаны для платформ Win32®. Хотя отдельные элементы могут функционировать и в других 32-разрядных операционных системах.

Аппаратный датчик случайных чисел «Гряда-1» подключается к системе через ISA-слот и представляется в пространстве адресов портов ввода/вывода регистром данных BASE=348h – R (16-битный порт вывода), и регистром состояния BASE+2 (34Ah) – R (16-битный регистр состояния). Через порт данных происходит чтение 16-битного случайного числа, а старший бит порта состояния определяет готовность сформированного числа. После чтения числа из входного порта данных повторное чтение числа невозможно, а бит готовности регистра статуса сбрасывается в неактивный уровень. После формирования устройством нового числа и записи его в выходной буфер линия состояния готовности выставляется в активный уровень.

Программирование устройства и прямое обращение процессов из пользовательского режима к портам ввода/вывода допускается только в операционных системах Win9x. В технологии WinNT2000® такой возможности операционная система не предоставляет. Поэтому для использования функций аппаратного генератора в операционных системах WinNT2000® разработан драйвер устройства, который позволяет работать с генератором на уровне ядра операционной системы.

Аппаратный датчик «Гряда-1» не имеет внутренних средств контроля параметров выходной последовательности, поэтому фильтр выхода генератора реализован программно в драйвере устройства. Функции контроллера разделены между аппаратными и программными компонентами системы, а также драйвером устройства. В программных реализациях компонентов генерации случайных и псевдослучайных чисел обычно реализуются три интерфейсные функции: открыть генератор, прочитать из генератора и закрыть генератор.

Функция открытия контекста аппаратного генератора выполняет создание системного объекта, определяющего генератор в системе, а также технологическое тестирование генератора. Создание и инициализация объекта генератора выполняется средствами операционной системы. Технологическое тестирование реализовано на основе федерального стандарта США FIPS 140-1 [1, 2]. Оно обеспечивает выполнение загрузочных тестов в момент инициализации генератора и контроль текущей работоспособности устройства. К загрузочным тестам аппаратных модулей отнесены тесты проверки критических функций модуля в аппаратных и программных компонентах, а также статистическое тестирование выхода аппаратного генератора. Для контроля текущей работоспособности устройства используется ограниченный набор тестов, аналогичных загрузочным.

Фильтр выходной последовательности использует для статистического тестирования последовательностей случайных бит набор статистических тестов. Стандарт FIPS 140-1 определяет четыре статистических теста. Согласно методике статистического тестирования отдельная битовая строка длиной 20000 битов, получаемая с выхода генератора случайных чисел, проверяется по каждому из четырех тестов. Если какой-нибудь из тестов не пройден, то фильтр выдает контроллеру информацию о том, что генератор не прошел тест. Решение о прохождении теста принимается на основе проверки попадания вычисляемых значений статистических параметров в доверительную область, рассчитанную для заданного уровня

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

значимости. Функция открытия контекста генератора может быть выполнена успешно, если объект генератора успешно создан в системе и выполнены загрузочные тесты устройства.

Функция генерации последовательности случайных чисел (или чтение из генератора), используя созданный при открытии объект генератора, выполняет чтение последовательности данных из устройства. Затем получаемые блоки случайных данных фильтруются в драйвере устройства. Фильтр блоков случайных данных построен на основе методики статистического тестирования стандарта FIPS 140-1. Если статистические параметры полученных данных не удовлетворяют рассчитанным доверительным интервалам, то блок отбрасывается и выполняется повторное чтение нового блока из генератора.

В процессе работы с аппаратным генератором необходимо выполнять техническое тестирование генератора. Такую возможность предоставляет функция открытия контекста генератора.

Функция закрытия контекста аппаратного генератора выполняет удаление объекта генератора из системы, очистку системных ресурсов, занимаемых генератором, то есть непосредственное закрытие и удаление контекста аппаратного датчика.

Программная реализация алгоритма генерации псевдослучайных чисел, описанного в стандарте ANSI X9.17, включает в себя аналогичные программные компоненты, используемые в программной модели аппаратного генератора. Работа с программным генератором построена на тех же функциях, что и элементы управления аппаратным датчиком.

Функция открытия контекста программного генератора выполняет создание объекта генератора, содержащего его параметры: ключи алгоритма шифрования ГОСТ 28147-89 и текущие параметры генерации. Объект генератора создается в безопасной памяти (технология безопасной памяти). Параметры, содержащиеся в объекте, используются в процессе генерации.

Функция генерации выполняет программное формирование последовательности случайных чисел с использованием созданного объекта программного генератора. Как и в случае аппаратного генератора сформированные блоки случайных данных фильтруются программным фильтром.

Функция закрытия контекста программного генератора выполняет удаление объекта генератора из безопасной памяти. При этом параметры генератора удаляются.

Заключение

Реализованные компоненты аппаратных и программных генераторов встроены в системы защиты информации для компьютерных систем на основе программных платформ Win32®. Основная часть элементов управления реализована программно и функционирует в пользовательском режиме (user-mode), кроме драйверов аппаратных генераторов, работающих в режиме ядра (kernel-mode).

Все программные и аппаратные компоненты корректно встраиваются в аппаратную платформу и операционную систему. Встроенные компоненты функционируют стабильно, обеспечивая выполнение возложенных на них функций. Параметры выходных данных генераторов постоянно контролируются фильтрами и контроллерами. Корректность инициализации генераторов обеспечивает выполнение загрузочных тестов. Статистические параметры тестирования проверены и проанализированы на этапе отладки. Правильность и стабильность функционирования элементов управления обеспечивает постоянный контроль над качеством выходных последовательностей.

Литература: 1. FIPS PUB 140-1. Cryptographic modules security requirements // NIST, 1993. 2. А. Менезис, П. ван Оршот, С. Ватсон. Прикладная криптография // CRC Press, 1996. Глава 5. 3. ANSI X9.17. "American National Standard for Financial Institution Key Management (Wholesales)" American Bankers Association, 1985.

УДК 681.325

ПРИНЦИПЫ ПОСТРОЕНИЯ И ИСПОЛЬЗОВАНИЯ АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ СЕРИИ “ГРЯДА”

Михаил Бондаренко, Иван Горбенко, Андрей Свинарев, Александр Столяр, Виктор Лапин
Харьковский государственный технический университет радиоэлектроники

Аннотация: **Рассматриваются проблемные вопросы проектирования, разработки, испытания и эксплуатации аппаратных средств защиты информации на примере устройств серии «Гряда».**