АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

А. Л. Труханович, Н. А. Ращеня, В. О. Хилинский

Белорусский государственный университет, г. Минск, Беларусь
E-mail: atrukhanovich@bsu.by

Для подготовки специалистов в области информационной безопасности разработан и изготовлен аппаратно-программный комплекс, позволяющий организовать эффективный процесс изучения основных принципов создания устройств защиты информации, способов генерации ключевой информации, изучения алгоритмов криптографического преобразования данных.

Ключевые слова: алгоритм; криптография; защита информации; АПК.

Современная компьютерная безопасность основывается на комплексе мер предотвращения несанкционированного доступа (НСД) к ресурсам ПК. Одних программных мер недостаточно, чтобы надежно защитить ПЭВМ от вредоносного программного обеспечения или доступа с целью получения информации с жесткого диска. Аппаратно-программные решения позволяют более надежно защитить информацию обрабатываемую и хранимую на компьютере.

На сегодняшний день остро стоит вопрос в обучении специалистов, способных разрабатывать аппаратно-программные решения защиты от НСД. Для более качественного обучения студентов разработан и создан аппаратно-программный комплекс (АПК) «Крипто-Лаб» для изучения белорусских стандартов шифрования.

АПК «Крипто-Лаб» выполнен на базе персональной электронно-вычислительной машины (ПЭВМ) и включает аппаратно-программное устройство и программное обеспечение.

В аппаратную часть входит устройство, способное хранить ключевую информацию, реализовывать криптографические преобразования и генерировать случайную числовую последовательность (СЧП). Изделие имеет следующие характеристики:

- PCI-интерфейс для питания и взаимодействия с ПЭВМ;
- цифровой процессор, память программ и энергонезависимое ОЗУ для обеспечения решения задач пользователя;
- модуль генерации случайной числовой последовательности (СЧП) на физическом источнике шума (полупроводниковый диод).

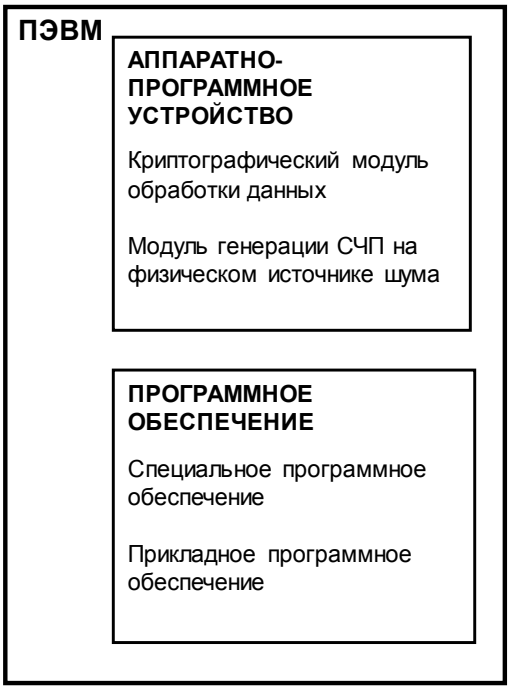

Рис. 1. Структура АПК «Крипто-Лаб»

В программную часть входит материал, позволяющий обучающемуся получить информацию об алгоритмах и других способах НСД, получить визуальное отображение работы того или иного алгоритма шифрования, при помощи программных средств реализовать защиту информации на собственном профессиональном компьютере (ПК). Программное обеспечение имеет следующие основные функциональные возможности:

- реализацию криптографических преобразований данных по ГОСТ 28147-89 [1], СТБ 34.101.31-2011 [2], СТБ 1176.1-99 [3], СТБ 1176.2-99[4] в аппаратно-программное устройство (АПУ) и ПЭВМ;
- функционирование АПУ под управлением операционной системы Windows XP/7;
- выполнение в ПЭВМ криптографических функций, реализованных в АПУ;
- выгрузку СЧП из АПУ;
- генерацию СЧП на системном (состояние, процессы и события операционной системы ПЭВМ) источнике шума;
- генерацию псевдослучайных числовых последовательностей;
- статистическую обработку числовых последовательностей;
- пошаговое выполнение в ПЭВМ криптографических преобразований данных по ГОСТ 28147-89 [1], СТБ 34.101.31-2011 [2], СТБ 1176.1-99 [3], СТБ 1176.2-99 [4];

– интерфейс пользователя для работы с АПК «Крипто-Лаб» и визуализации результатов статистической обработки числовых последовательностей и пошагового выполнения криптографических преобразований.

Комплекс позволяет выполнять следующие практические работы:

7. «Изучение аппаратно-программного комплекса «Крипто-Лаб»».

В данной работе изучаются принципы построения аппаратной части устройства защиты информации на базе предложенного оборудования. Изучается структурная схема устройства. В комплекс входит цифровой сигнальный микропроцессор, позволяющий осуществлять криптографические преобразования. На устройстве присутствует энергонезависимая память, которая оснащена батарейным питанием, и служит для хранения важной или ключевой информации. Так же устройство имеет буфер обмена, для получения и выдачи информации. На плате присутствуют шумовые диоды, которые способны выдавать случайную числовую последовательность, используя физические процессы.

8. «Случайная числовая последовательность»

При изучении СЧП надо знать, какими способами можно сформировать качественную последовательность, научится генерировать последовательность при помощи программных алгоритмов и других различных физических явлений, изучить способы проверки полученной числовой последовательности на качество. В комплексе предусмотрено формирования последовательности при помощи алгоритмов (псевдослучайная последовательность), с использованием шумовых диодов (через регистры доступа к устройству и через буфер обмена с памятью) и на основе внутреннего ресурса ПЭВМ. Так же реализованы и описаны основные тесты качества СЧП (проверка цепочек нулей и единиц, проверка длинных цепочек).

9. «Генерация и работа с ключевой информацией на АПК «Крипто-Лаб»»

Ключевая информация (КИ) – это наиболее важный блок программно-аппаратного комплекса. В работе предложено изучить возможные виды ключевой информации: ключи для шифрования, ключи для установления соединения и прочее. Есть возможность изучить способы генерации ключей. Рассматриваются способы контроля целостности КИ. Есть возможность исследования надежности хранения ключей в разных областях памяти устройства. Также приведены способы уничтожения критической информации при НСД.

10. «Алгоритм криптографического преобразования данных ГОСТ28147-89»

Изучение наиболее распространенного блочного алгоритма ГОСТ28147-89 [1] - одна из ключевых задач при подготовке специалиста по защите информации. Комплекс позволяет детально изучить алгоритм в разных режимах работы, получить визуальное отображение всех шагов алгоритма, что позволяет более глубоко понять смысл преобразования. Изучив основу алгоритма, комплекс предоставляет возможность непосредственного использования алгоритма как в аппаратной, так и в программной реализации.

11.«Алгоритм криптографического преобразования данных СТБ 34.101.31-2011».

Созданный и сертифицированный в Беларуси алгоритм СТБ 34.101.31-2011 [2] важен для изучения подготовки специалиста по защите информации. В работе предложено визуальное отображения всех шагов криптопреобразования. Изучаются всевозможные режимы работы алгоритма. Производится анализ режимов с целью понимания для чего нужны разные режимы.

12.«Изучение ассиметричных алгоритмов шифрования»

Рассматриваются алгоритмы, основанные на работе с большими числами или использование эллиптических кривых. Рассматриваются способы реализации и возможности внедрения алгоритмов в аппаратную часть устройства. Производится анализ и делаются выводы о возможностях использования подобных алгоритмов в различных системах.

13.«Алгоритм криптографического преобразования данных СТБ 1176.1-99.(функция хеширования)»

Изучается Белорусский стандарт получения криптостойкой функции хеширования. Производится пошаговая визуализация способов построения функции и хеш-последовательности. Изучаются требования, которым должна удовлетворять полученная последовательность.

14.«Алгоритм криптографического преобразования данных СТБ 1176.2-99.(Электронная Цифровая Подпись)»

В работе продемонстрирована пошаговая визуализация формирования ЭЦП посредством алгоритма СТБ 1176.2-99 [4]. Производится анализ работы с подписью, устанавливаются способы вычленения измененного документа. Рассматриваются возможные программные и аппаратные реализации ЭЦП. Анализируются способы работы.

Изучив аппаратно-программный комплекс «Крипто-Лаб» и проделав вышеперечисленные практические работы, специалист получает базовые знания, необходимые при разработке и создании устройств для защиты от несанкционированного доступа к информации.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Государственный стандарт СССР ГОСТ28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм Криптографического преобразования.". 1996. 26 с.
2. Государственный стандарт СТБ 34.101.31-2011 "Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности.". 2011. 30 с.
3. Государственный стандарт СТБ 1176.1-99 "Информационная технология. Защита информации. Функция хэширования.". 2000. 16 с.
4. Государственный стандарт СТБ 1176.2-99 "Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи.". 2000. 16 с.

ФИЗИЧЕСКИЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЦИФРОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А. Л. Труханович, Н. А. Ращеня, М. И. Новик

Белорусский государственный университет, Минск, Беларусь
E-mail: atrukhanovich@bsu.by

Разработан аппаратно-программный генератор случайных числовых последовательностей (СЧП) 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 (не хуже 10^{-5}) близкую к последовательности независимых равновероятных испытаний.

Ключевые слова: алгоритм; СЧП; физический источник шума; генератор.

Случайная числовая последовательность широко используется при формировании различных параметров для криптографических алгоритмов. При этом генерируемые случайные числа должны быть равномерно распределены на всем диапазоне и независимы. Обеспечение качества случайной последовательности на заданном уровне достигается применением генераторов, использующих недетерминированные физические процессы.

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.