КОМПЛЕКС ДЛЯ ИЗУЧЕНИЯ РАСПРОСТРАНЕНИЯ СИГНАЛОВ И ЗАЩИТЫ ПЕРЕДАВАЕМЫХ ДАННЫХ НА НЕЛИЦЕНЗИРУЕМОЙ ЧАСТОТЕ

Л.Ю. Левченко, А.П. Борисов
Алтайский государственный технический университет
им. И.И. Ползунова, г. Барнаул

В настоящее время информация является одной из наиболее важнейших ценностей нашего мира. Утечка информации может нанести существенный вред ее владельцу, в связи с этим необходимо ее защищать соответствующим образом. Поэтому актуальна проблема повышения качества практической подготовки студентов направления «Информационная безопасность» На данный момент на рынке представлено мало обучающих комплексов, предназначенных для изучения беспроводной передачи информации, особенно в нелицензируемых частотах. Поэтому возникла потребность в создании такого комплекса.

Для дальнейшего трудоустройства студент направления «Информационная безопасность» должен овладеть такими навыками как:

1. знание современных стандартов шифрования;
2. опыт работы с техническими и программными средствами шифрования [1].

Комплекс, изображенный на рисунке 1, поможет студентам приобрести данные навыки.

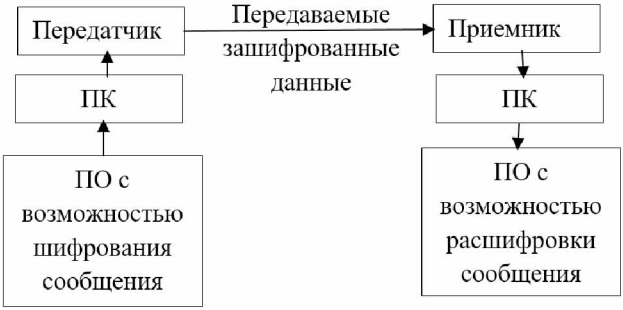

Рис. 1. Общий вид разработанного комплекса’

Для создания обучающего комплекса используются программно-аппаратное средство Arduino, радиомодуль SI4432 и

радиоудлинитель. У Arduino есть ряд преимуществ над иными микроконтроллерами [2]:

1. свободно распространяемое программное обеспечение (среда разработки Arduino);
2. Arduino IDE основан на языке C++. Есть возможность заменить любую высокоуровневую команду или библиотеку для Arduino на аналогичную C++;
3. широкий программный функционал позволяет реализовать практически любое устройство.

Схема обучающего комплекса представлена на рисунках 2-3.

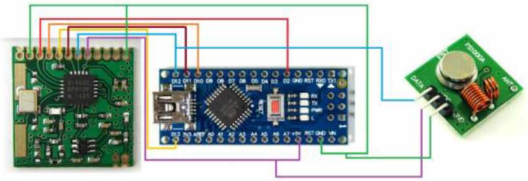

Рис. 2. Схема передатчика

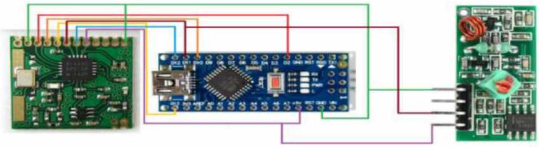

Рис. 3. Схема приемника

Устройство передает информацию на частоте 433 МГц. С помощью обучающего комплекса студенты будут изучать передачу информации в зашифрованном виде, а также исследовать дальность распространения сигналов.

Принцип работы обучающего комплекса со стороны пользователя [3]:

Для корректной работы устройства при передаче информации пользователь должен выполнить несколько действий. Во-первых, выбрать радиомодуль, который он использует при передаче информации. Во-вторых, выбрать COM-порт, к которому будет подключено устройство. Для того чтоб передать данные необходимо открыть порт на запись. Информация будет передаваться в зашифрованном виде, поэтому пользователь должен выбрать тип шифрования из предложенного списка. Можно использовать

несколько видов шифрования одновременно или не использовать шифрование вообще.

Принцип приема сообщения очень похож на принцип передачи. Пользователь также должен выбрать радиомодуль, COM-порт и открыть порт на чтение, а также выбрать виды шифрования, которые использовались при передаче. Прием информации происходит автоматически. Расшифрованная информация появится в текстовом поле.

Главная задача шифрования — это сохранить конфиденциальность, целостность и идентифицируемость, передаваемой информации. Существует два вида шифрования: симметричный и ассиметричный. При симметричном шифровании и отправитель, и получатель использует один и тот же ключ. При ассиметричном шифровании существует открытый ключ (для получателя) и закрытый ключ (для отправителя). В обучающем комплексе будут применяться несколько методов шифрования. Рассмотрим подробнее данные алгоритмы шифрования

Алгоритм AES (рисунок 4) является симметричным алгоритмом шифрования. Значение длины ключа должно быть не менее 4 символов. Допустимо использование любых символов, как в ключе, так и в шифруемом сообщение.

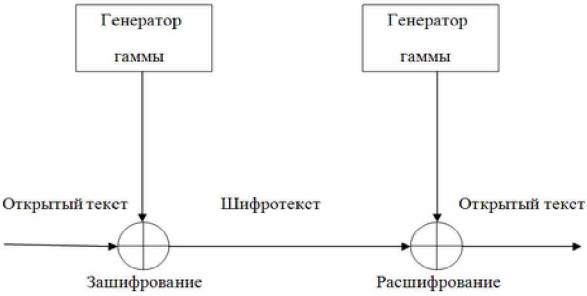

Рис. 4. Алгоритм AES.

Алгоритм RSA (рисунок 5) является асимметричным алгоритмом шифрования. Пользователь сначала должен сгенерировать открытый ключ, который применяется при приеме сообщений. Открытый ключ состоит из открытого модуля и публичной экспоненты. Закрытый ключ состоит из закрытого модуля, этот ключ хранится только у отправителя сообщения. Для

корректной работы в программе есть проверка преобразования данных.

Рис. 5. Алгоритм RSA

В заключение хочется сказать, что в настоящее время очень важно развитие учебно-лабораторных комплексов для студентов подготовки студентов направления «Информационная безопасность». Данный обучающий комплекс поможет студентам изучить беспроводную передачу информации, шифрование информации.

Библиографический список

11. Редакция журнала «Information Security» Специалист информационной безопасности // Журнал «Information Security/Информационная безопасность» № 4, 2013, с. 12

12. Максимов А.И., Борисов А.П. Разработка комплекса средств беспроводной передачи информации на базе микроконтроллеров Arduino // Использование цифровых средств обучения и робототехники в общем и профессиональном образовании: опыт, проблемы, перспективы [Текст]: сборник научных статей II Международной научно-практической конференции, Барнаул, 5-6 ноября 2015 г. – Барнаул : Изд-во Алт. Ун-та, 2015, С.107-110

13. Белый С.С., Борисов А.П. Повышение качества проведения лабораторных работ при помощи устройства передачи данных по радиоканалу // Влияние науки на инновационное развитие: сборник статей Международной научно - практической конференции (28 февраля 2017 г., г. Екатеринбург). - Уфа: МЦИИ ОМЕГА САЙНС, 2017, с.22-24