любых новых устройств вне зависимости от прав пользователя, ведущего в данный момент сеанс работы.

Проведя исследование, определив возможные угрозы и уязвимости было принято решение о создании устройства, обеспечивающего защиту от программных кейлоггеров, работающих в операционной системе. На базе микроконтроллера Arduino организованы приём событий от физической клавиатуры, модификация этих данных и последующая передача операционной системе. Подготовленное программное обеспечение, работающее в операционной системе, в свою очередь, проводит обратную модификацию и передаёт введённые пользователем данные в защищаемое приложение. Таким образом, данные, которые поступят в кейлоггер, будут находиться в модифицированном виде.

БЕЗОПАСНОСТЬ BLUETOOTH УСТРОЙСТВ

В.А. Кузьменко

Цель исследования — оценить безопасность передачи данных по Bluetooth.

В процессе исследования было выявлено следующее:

– передача данных по Bluetooth защищается PIN кодом на устройствах, поддерживающих Bluetooth версии 2.0 и выше.

– данные шифруются 128-битным AES алгоритмом на устройствах, поддерживающих Bluetooth версию 4.0 и выше.

– устройства инициируют пересопряжение, если на частоту, в которой они работают, начинает влиять неизвестный пользователь. Однако если нет свободных частот в диапазоне Bluetooth, то имеется возможность «подслушать» ключ сопряжения и методом подбора взломать PIN код.

Таким образом, сформирована рекомендация пользователям: в случае использования технологии Bluetooth для передачи данных, требующих шифрование, необходимо самостоятельно осуществлять шифрование таких данных.

Также в ходе исследования было разработано приложение, обеспечивающее безопасность рабочего места персонального компьютера на основе контроля наличия рядом ключевого Bluetooth устройства. Данное приложение позволяет также удаленно подавать команды управления с мобильного телефона на компьютер в зашифрованном виде. При разработке приложения использовалось программно-аппаратное средство для построения систем автоматики и робототехники — Arduino.

АППАРАТНЫЕ РЕАЛИЗАЦИИ ОПЕРАЦИЙ УМНОЖЕНИЯ В ПОЛЯХ ГАЛУА ПРИ ПОСТРОЕНИИ ЭЛЕМЕНТОВ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Е.В. Листопад

При построении современных систем на кристалле (в том числе для криптографической защиты информации) часто возникают задачи реализации арифметических операций в полях Галуа. От эффективности их реализации (в первую очередь, операций умножения) существенно зависят характеристики создаваемых систем. Поля Галуа характеризуются двумя параметрами: число двоичных разрядов, необходимых для представления символа, и генерирующий полином, определяющий порядок следования элементов поля [1].

Рассмотрим аппаратные реализации умножения элементов поля с числом двоичных разрядов равным 16. Умножение в поле подразумевает выполнение двух стадий: логическое умножение и приведение по модулю генерирующего полинома. Выполнение данных стадий возможно в следующих вариантах:

1. Выполнение приведения по модулю после умножения одного из множителей на каждый бит, каждую пару бит или каждые 4 бита второго множителя. Вся операция умножения будет выполнена за 16, 8 или 4 такта процессора соответственно.

2. Выполнение приведения по модулю (на 2-м такте) после перемножения элементов поля (на 1-м такте). Вся операция умножения будет выполнена за 2 такта.

3. Выполнение приведения по модулю на том же такте, что и перемножение элементов поля. Вся операция умножения будет выполнена асинхронно за 1 такт.

Лучшие соотношения показателей быстродействия и аппаратных затрат кристалла имеет вариант реализации умножения за 2 такта процессорного времени.