Рис. 2 – Спектр сигнала в шине USB при реализации скрытого канала

Для цифровой модуляции данных возможно использование двоичной частотную манипуляцию (B-FSK). Как правило, при частотной манипуляции данные передаются посредством изменения частоты несущей, так что разные частоты соответствуют разным значениям входных данных. В двоичной форме FSK частота несущего сигнала варьируется между двумя значениями, соответствующими двоичному 0 или 1.

Фактическая передача данных выполняется путем записи файла, сформированного по закону изменения скрытно передаваемых данных с учетом используемого вида модуляции, в произвольный блок данных на устройстве USB. Процесс передачи не требует специальных привилегий (например, root или admin). Требуется только разрешение на создание файла на съемном устройстве. Такие файлы часто создаются процессами для сохранения файлов и хранения временных данных или для обработки промежуточных результатов.

Таким образом, за счет создания программ, способных создавать файлы, содержание которых промодулировано скрытно передаваемыми данными, с учетом особенностей линейного кода NRZI интерфейса USB возможна реализация скрытого канала передачи информации.

1. M. Guri. GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies // Ben-Gurion University of the Negev Cyber Security Research Center, 2015.
2. Markus G. Kuhn. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations // Ben-Gurion University of the Negev Cyber Security Research Center, 1998.
3. M. Guri. USB: Air-Gap Covert-Channel via Electromagnetic Emission from USB // Ben-Gurion University of the Negev Cyber Security Research Center, 2016.

Головач Е.С.

**Реализация программно-аппаратного комплекса защиты информации,
обрабатываемой на средствах вычислительной техники от несанкционированного
доступа**

*Академия ФСО России
(Россия, Орел)*

doi:10.18411/sciencepublic-12-05-2020-02

idsp: sciencepublic-12-05-2020-02

В настоящее время информационные системы применяются во всех областях деятельности человечества и силовых структур, поэтому, увеличивается количество угроз информационной безопасности. Основной угрозой безопасности информации

является утечка защищаемой информации посредством несанкционированного доступа к объектам информатизации и (или) информационным ресурсам. Несанкционированный доступ может осуществляться как лицами, не допущенными на объекты информатизации (внешние нарушители), так лицами, умеющими на это право (внутренние нарушители). Наибольшую опасность предоставляют внутренние нарушители, ввиду их осведомленности о структуре и принципах построения системы связи.

Большинство средств вычислительной техники используют систему аутентификацию, основанную на подтверждении прав доступа с помощью пароля. Пароль может устанавливаться как для разрешения запуска системы в целом, то есть при запуске *BIOS*, так и на доступ к файлам пользователей (ввод логина и пароля пользователя для входа в *Windows*). При этом практика показывает, что надежность установленного пароля, в первую очередь, зависит от человеческого фактора. Простые пароли, которые легко запомнить пользователю (даты рождения, имена родственников, часто употребляемые слова и т.п.), менее устойчивы к взлому. И наоборот, сложные пароли хотя и устойчивы к взлому, но большинству людей их непросто запомнить, это в свою очередь ведет к повышению вероятности, что пользователь запишет пароль и перехватить его будет проще. Поэтому, требуется разработка устройства аутентификации, способного в должной мере обеспечить выполнение всех требований по безопасности обрабатываемой информации и удобства использования.

Самым перспективным вектором развития систем аутентификации является использование в качестве идентификационного фактора биометрические признаки человека. В настоящее время все чаще применяются устройства, основанные на сканировании отпечатков пальцев, радужной оболочки глаза или геометрии руки. Большинство биометрических признаков являются уникальными для каждого человека, что дает возможность их повсеместного применения. Невозможность утраты без стороннего физического воздействия и сложность подделки таких признаков обеспечивает высокую надежность устройств аутентификации. Используемые средства защиты информации имеют низкий коэффициент ошибочных отказов и подтверждений.

На сегодняшний день одним из самых перспективных направлений является применение сканера отпечатков пальцев, так как оно сочетает в себе низкую стоимость средств, легкую собираемость идентификационного признака и высокую надежность.

Разрабатываемое средство защиты информации должно удовлетворять следующим требованиям:

1. Функциональные: обеспечение решения требуемой совокупности задач по защите, удовлетворение всем требованиям по защите.
2. Эргономические: минимизация помех пользователям, удобство для персонала системы защиты.
3. Экономические: минимизация затрат на систему, максимальное использование серийных средств.
4. Технические: комплексное использование средств, оптимизация архитектуры.
5. Организационные: структурированность всех компонентов, простота эксплуатации.

Исходя из требований, предъявляемых к разрабатываемому программно-аппаратному комплексу (ПАК), функциональная схема устройства аутентификации будет иметь вид, представленный на рисунке 1.

Рисунок 1 – Функциональная схема ПАК

Ядром разрабатываемого комплекса является программируемый микроконтроллер *Arduino*. Плата будет выполнять функции обработки информации, поступающей со сканера отпечатков пальцев, взаимодействия с блоков управления и сигнализации, а также выдачи сигналов управления на модуль реле.

Модуль реле построен на базе твердотельных переключателей и осуществляет коммутацию соответствующих контактов цепей питания НЖМД. Для осуществления физического разделения достаточно разрыва линий питания +5 и +12 В. Переключение контактов реле происходит путем подачи управляющего сигнала на соответствующий вход канала. Всего в состав модуля входит 8 каналов.

Оптический сканер отпечатков пальцев необходим для считывания уникального узора пальца пользователя для формирования базы данных и последующей проверки сканируемых отпечатков с этой базой. После анализа сканер передает информацию на микроконтроллер. База данных сканера рассчитана на 1000 отпечатков. Разрабатываемое устройство рассчитано на использование двух эталонов для стабильного функционирования.

Блок сигнализации и управления состоит из двух светодиодов и двух кнопок и необходим для выдачи световой индикации о режиме работы комплекса и передачи на микроконтроллер команд переключения этих режимов. Всего предусмотрено два режима работы ПАК: режим заполнения базы данных идентификационными признаками пользователей и рабочий режим, в котором происходит проверка подлинности и предоставление доступа.

Поле коммутации выполняет вспомогательную функцию. На нем размещается блок управления и сигнализации и производится разводка контактов *GND* и +5 В для множественного подключения.

Для соединения всех устройств между собой используются стандартные провода, входящие в набор микроконтроллера.

Принцип работы комплекса состоит из двух этапов.

Начальный этап. При первом включении отпечатки пальцев отсутствуют в базе данных сканера. Когда пользователь прикладывает палец к сканеру, происходит чтение отпечатка пальца. Второй пользователь производит ту же операцию. Когда пользователи зарегистрировали свои биометрические признаки, комплекс переходит ко второму этапу работы.

Второй этап. Один из пользователей прикладывает палец к сканеру, происходит сканирование и проверка степени совпадения предъявляемого отпечатка с тем, который записан в базу данных. При успешной проверке сканер посылает соответствующий сигнал на микроконтроллер. Процессор согласно записанному программному коду анализирует, какой сигнал отправить на модуль реле. При поступлении сигнала на модуль реле задействованные контакты переключаются в соответствующее положение. Таким образом, происходит подключение цепей питания НЖМД и кнопки включения/выключения компьютера и осуществляется доступ к хранящейся на нем информации.

Стоит отметить, что подключение носителей происходит только при выключенном компьютере, то есть когда на цепях питания НЖМД отсутствует напряжение. Для этого один из цифровых портов микроконтроллера настроен на контроль наличия напряжения +5 В. Этот порт необходимо подключить к проводнику, который идет от материнской платы компьютера до модуля реле. При наличии напряжения алгоритм переходит в состояния ошибки и выполнение переключений контактов реле, к которым подключены носители информации, не происходит. Коммутируется только провод кнопки питания системного блока.

Программно-аппаратный комплекс позволяет использовать средства вычислительной техники в многопользовательском режиме, когда каждый пользователь имеет доступ только к той информации, к которой он допущен.

1. Смит Р. Э. Аутентификация: от паролей до открытых ключей. : Пер. с англ. – М. : Издательский дом «Вильямс», 2002. – 432 с. : ил. – Парал. тит. англ.
2. Богомолов С.А. Биометрическая аутентификация пользователя. Биб-лиотечка студента. От простого к сложному. Персональный компьютер. – Москва, 2015 – 26 с.
3. Уроки и проекты для Arduino [Электронный ресурс] // iarduino [Сайт]. URL <https://lesson.iarduino.ru>.

Романюк О.В., Егоров И.Ю.

Исследование способов балансировки трафика в транспортной сети с коммутацией пакетов

*Академия ФСО России
(Россия, Орел)*

doi:10.18411/sciencepublic-12-05-2020-03

ids: sciencepublic-12-05-2020-03

Задача управления трафиком с целью обеспечения оптимального использования распределенных ресурсов в мультисервисных сетях связи является одной из значимых. От успешного решения данной задачи в исключительной степени зависит эффективность использования самого ценного ресурса сети – пропускной способности каналов связи. [1]

В настоящее время мировым научным сообществом и производителями сетевого оборудования разработано множество способов, позволяющих осуществлять управление трафиком и балансировку нагрузки в сетях связи. Данные способы основываются, в свою очередь, на различных подходах, каждому из которых присущи