РАЗДЕЛ I. ТЕЛЕКОММУНИКАЦИИ

Артамонов В.А.

Скрытый канал передачи информации за счет ЭМИ интерфейса USB

Академия ФСО России

(Россия, Орел)

doi:10.18411/sciencepublic-12-05-2020-01

idsp: sciencepublic-12-05-2020-01

Развитие инфокоммуникационных систем и технологий привело к созданию нового класса угроз информационной безопасности, подразумевающих использование скрытых каналов передачи информации, противодействие которым с помощью традиционных средств обеспечения безопасности трудно осуществимо. Под скрытым каналом следует понимать непредусмотренный разработчиком инфокоммуникационных технологий канал передачи информации, который может быть задействован для нарушения политики безопасности. Одним из таких каналов является скрытый канал передачи информации за счет ЭМИ интерфейса USB.

Прикладной уровень протокола USB вводит определение термина «конечная точка», согласно которому возможна передача данных только в одном направлении. Конечная точка OUT может переносить данные с главного компьютера на устройство (например, при записи файла на USB-носитель). Конечная точка IN может переносить данные с устройства на хост-компьютер (например, при получении видеопотока с веб-камеры USB).

Сигнал на линейном выходе USB представляет собой импульсную последовательность, при этом основные параметры импульсов в этой последовательности, такие как длительность и скважность, зависят от передаваемых по интерфейсу данных. В качестве линейного кода в шине USB используется код NRZI. Это значит, что передача нулевого бита соответствует изменению уровня сигнала в шине, а передача единицы соответствует отсутствию изменения уровня сигнала. Вставка бит используется для того, чтобы не потерять синхронизацию при монотонном единичном сигнале. Суть этой вставки заключается в том, что после каждых 6 подряд единиц вставляется нулевой бит. Временное представление сигнала USB изображено на рисунке 1.

Рис. 1 – Временное представление сигнала в шине USB

Было обнаружено, что передача последовательности битов «0» на USB-устройство генерирует детектируемое излучение в диапазоне от 240 МГц до 480 МГц. Осуществляя передачу определенной битовой последовательности, сформированной по закону изменения скрытно передаваемых данных, по шине USB, возможно реализовать модуляцию электромагнитного излучения (ЭМИ) интерфейса. При этом в спектре ЭМИ появляются дискретные составляющие, находящиеся в узкой полосе частот. За счет узкополосности этих составляющих возможно детектирование ЭМИ на довольно больших расстояниях.

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