АППАРАТНЫЕ ЗАКЛАДКИ В ИНТЕГРАЛЬНЫХ МИКРОСХЕМАХ

О.А. Карманова, И.А. Захаров, В.Р. Стемпицкий

Стремление обеспечения максимальной скорости обработки информации при минимальных массогабаритных параметрах, помехоустойчивости, наталкивается на все больше проблем, связанных с достижением оптимальных свойств конструкций современных интегральных радиоэлектронных устройств (ИРЭУ) и соответствием действующим нормам обеспечения безопасного их использования, бессбойного функционирование устройства. Одной из угрозы безопасной эксплуатации электронного оборудования является не санкционированная или не документированная модификация интегральных схем.

Модификации интегральных схем (ИС), именуемые аппаратными закладками (АЗ), – это устройство скрытно устанавливаемое (внедряемое, встраиваемое) или подключаемое к элементам информационной системы (ТС обработки и передачи информации) в целях получения несанкционированного доступа к информации (т. е. в нужный момент времени обеспечить утечку информации, нарушение ее целостности или блокирование. К остальным элементам, которое способно вмешаться в работу системы [1, с. 16].

Аппаратной закладкой может быть специальная микросхема, выполняющая те же функции, что и программная закладка. Одним из видов аппаратных закладок является радиозакладка. С помощью аппаратной закладки могут перехватываться видеоизображение, выводимое на экран монитора; информация, вводимая с клавиатуры, выводимая на принтер, записываемая на жесткий диск компьютера; записываемая на внешние накопители (flesh-память, USB-накопитель, DVD. CD и др.) [1, с. 16–17].

Вредоносное действие аппаратных закладок является серьезной проблемой безопасности электронных устройств, особенно, если речь идет о выполнении критически важных задач государственного уровня. Несанкционированные аппаратные закладки могут привести к катастрофическим последствиям во время эксплуатации приложений с повышенными требованиями к информационной безопасности, например, в военных структурах, в коммуникационных и национальных инфраструктурах.

Результатом работы аппаратной закладки может быть, как полное выведение системы из строя, так и нарушение ее нормального функционирования, ее изменение или блокирование. Данные ИС могут, также, стать объектами умышленных манипуляций [2, с. 450]. В данной работе авторы исследуют существующие угрозы распространяющихся уязвимых аппаратных компонентов с внедренными в них уязвимостями – аппаратными закладками (аппаратными троянами) в интегральные микросхемы. Систематизируют классификации аппаратных закладок, способы их внедрения, методы выявления и защиты интегральных микросхем от несанкционированного вмешательства.

Литература

1. Дождиков В.Г., Салтан, М.И. Краткий энциклопедический словарь по информационной безопасности. М.: Энергия, 2010. 240 с.

2. Белоус А.И., Солодуха В.А., Шведов С.В. Программные и аппаратные трояны – способы внедрения и методы противодействия. Первая техническая энциклопедия. Книга 2. М.: Техносфера, 2019. 630 с.