Тема 1.5 Безопасность микропроцессорных систем

Некоторые встроенные системы находят массовое применение, например, устройства RFID. Встроенные системы являются привлекательной целью для создателей вредоносного кода из-за своей распространённости и относительной беззащитности. Постепенно злоумышленники пытаются создать вредоносный код для встроенных систем (например, RFID-вирус, Cabir). Этот процесс пока затрудняется разнородностью встроенных устройств, отсутствием доминирующего ПО и ограниченной функциональностью некоторых видов устройств. С другой стороны, задача антивирусных компаний и исследователей компьютерной безопасности осложнена теми же обстоятельствами, а также маломощностью встроенных систем, зачастую не позволяющей пользоваться распространённым антивирусным ПО.

При передаче сигнала через любой канал связи возможно возникновение ошибок, которые могут приводить к искажению переносимой информации. Существует много методов для исправления подобных ошибок, но прежде чем исправлять, необходимо эти ошибки обнаружить. Для этого также существуют определенные методы, основанные на избыточности передаваемой информации, что позволяет не только выявлять наличие факта искажения информации, но и в ряде случаев устранять эти искажения. Наиболее известные из методов обнаружения ошибок передачи данных являются:

1. Посимвольный контроль четности, называемый также поперечным, подразумевает передачу с каждым байтом дополнительного бита, принимающего единичное значение по четному или нечетному количеству единичных битов в контролируемом байте. Посимвольный контроль четности прост как в программной, так и в аппаратной реализации, но его вряд ли можно назвать эффективным методом обнаружения ошибок, так как искажение более одного бита исходной последовательности резко снижает вероятность обнаружения ошибки передачи. Этот вид контроля обычно реализуется аппаратно в устройствах связи.
2. Поблочный контроль четности, называемый продольным. Схема данного контроля подразумевает, что для источника и приемника информации заранее известно, какое число передаваемых символов будет рассматриваться ими как единый блок данных. В этой схеме контроля для каждой позиции разрядов в символах блока (поперек блока) рассчитываются свои биты четности, которые добавляются в виде обычного символа в конец блока. По сравнению с посимвольным контролем четности поблочный контроль четности обладает большими возможностями по обнаружению и даже корректировке ошибок передачи, но все равно ему не удается обнаруживать определенные типы ошибок.
3. Вычисление контрольных сумм. В отличие от предыдущих методов для метода контрольных сумм нет четкого определения алгоритма. Каждый разработчик трактует понятие контрольной суммы по-своему. В простейшем виде контрольная сумма — это арифметическая сумма двоичных значений контролируемого блока символов. Но этот метод обладает практически теми же недостатками, что и предыдущие, самый главный из которых — нечувствительность контрольной суммы к четному числу ошибок в одной колонке и самому порядку следования символов в блоке.
4. Контроль циклически избыточным кодом — CRC (Cyclical Redundancy Check). Это гораздо более мощный и широко используемый метод обнаружения ошибок передачи информации. Он обеспечивает обнаружение ошибок с высокой вероятностью. Кроме того, этот метод обладает рядом других полезных моментов, которые могут найти свое воплощение в практических задачах.