

УДК 62-503.5

Компьютерный вирус как разновидность враждебной неисправности в системе управления орбитальной группировкой космических аппаратов

Ашарина Ирина Владимировна^(*)

asharinairina@mail.ru

SPIN-код: 1002-9349

АО «НИИ «Субмикрон», Москва, Россия

Аннотация. Описаны физические причины появления неисправностей враждебного (византийского) вида в бортовых вычислителях орбитальной группировки (ОГ) космических аппаратов (КА). Рассмотрены особенности компьютерных вирусов с точки зрения их влияния на вычислители информационно-управляющих систем как физические неисправности. Определены способы парирования неисправностей, вызванных компьютерным вирусом.

Ключевые слова: информационно-управляющая система, сбое- и отказоустойчивость системы, резервирование, орбитальная группировка, враждебная неисправность

Введение. Одним из способов обеспечения сбое- и отказоустойчивого выполнения целевой задачи в необслуживаемых информационно-управляющих систем (ИУС) космического базирования [1] является репликация этой задачи с использованием динамической избыточности, обеспечивающей системное самообнаружение проявившихся неисправностей, их самоидентификацию по месту проявления и типу (сбой, программный сбой, отказ), самовосстановление целевой работы сбившихся бортовых вычислителей (БЦВМ) КА, саморе конфигурацию системы, состоящую в изоляции отказавших БЦВМ и включения вместо них с запасных БЦВМ [2].

Причины появления неисправностей враждебного вида в БЦВМ ОГ КА. Случайное воздействие внешних факторов. К негативным воздействиям в космосе относятся: 1) высокие либо низкие температуры окружающей среды, вызывающие перегрев или замерзание устройства; 2) электромагнитное излучение, негативно влияющее на работу радио-электронного оборудования (РЭО); 3) радиационные характеристики открытого космоса, приводящие к сбоям и отказам РЭО, которые не всегда удается парировать, не прибегая к процедуре взаимного информационного согласования (ВИС) [1].

Ошибка шины PCI. Шина PCI (Peripheral Component Interconnect) является универсальным интерфейсом, применяемым в большинстве электронных устройств [3]. Основные характеристики работы микросхем характеризует крутизна фронтов. Проблема возникает если для тактирования нескольких соединенных между собой устройств используется сигнал с большим временем нарастания [3], тогда может возникнуть перекося тактовых импульсов, но такая неисправность легко обнаруживается. Ситуация усложняется при

нарушениях в драйвере устройства выдачи сигнала, приводящие к его ослаблению. Физически это проявляется как появление паразитного сопротивления. При недостаточной мощности устройства выдачи сигнала фронт сигнала оказывается все более пологим. Это приводит к тому, что в определенный момент времени приема сигнала его значение в начале передающего тракта может оказаться равным «1», а в конце равным «0». В средних точках значение сигнала будет находиться в зоне неопределенности и случайным образом может оказаться равным как «0», так и «1».

Целенаправленное злонамеренное воздействие внешнего источника.

При работе любого передающего устройства на него может воздействовать внешний сигнал, целью которого часто является не уничтожение источника, а искажение передаваемого им сигнала, что способно вызвать более серьезные последствия. Такой сигнал в виде кратковременного импульса способен привести к сбою и последующему восстановлению передающего устройства. Тогда разные приемники передаваемого целевого сигнала получают разную информацию, что соответствует определению враждебной неисправности [1, 2]. К этому же классу причин можно отнести заражение компьютерным вирусом БЦВМ КА, при котором зараженная БЦВМ может вести себя преднамеренно враждебно, не имея физических неисправностей. В этом случае необходимо как можно быстрее обнаружить проблему, поскольку, в отличие от остальных случаев проявления враждебных неисправностей, возможно заражение других БЦВМ ОГ КА.

Заключение. При неисправностях, вызванных появлением компьютерных вирусов, при отсутствии физического повреждения БЦВМ в реконфигурации, сопровождающейся заменой неисправной БЦВМ на резервную (при наличии), нет необходимости. Требуются лишь антивирусные восстановительные процедуры с последующим втягиванием восстановленной БЦВМ в целевую работу. Поскольку ситуация аналогична идентификации программного сбоя, характеризующегося как последовательность сбоев в двух подряд идущих целевых циклах выполнения задачи, предлагается следующая последовательность действий: 1) блокировка зараженной БЦВМ по возможности передачи любых данных; 2) запуск антивирусной программы с внешнего по отношению к ней устройства; 3) подача команды на запись данных в заданную область памяти восстанавливаемой БЦВМ; 4) подача команды на чтение данных из заданной области памяти восстанавливаемой БЦВМ; 5) передача считанных данных во все восстанавливающие БЦВМ ОГ КА; 6) команда для восстановленной БЦВМ на выполнение программы, размещенной в ее памяти в процессе восстановления.

Список источников

- [1] Ашарина И.В., Гришин В.Ю., Орлов А.В. Сбое- и отказоустойчивая система управления орбитальной группировкой космических аппаратов. *Академические чтения по космонавтике, посвященные памяти академика С.П. Королёва и других вы-*

дающихся отечественных ученых — пионеров освоения космического пространства: сб. тез. Москва, Изд-во МГТУ им. Н.Э. Баумана, 2026.

- [2] Лобанов А.В., Сиренко В.Г. Распределенные методы системного диагностирования многомашинных вычислительных систем. *Автоматика и телемеханика*, 2000, вып. 8, с. 165–172.
- [3] Петров С.В. *Шины PCI, PCI Express. Архитектура, дизайн, принципы функционирования*. Санкт-Петербург, БХВ-Петербург, 2006, 416 с.