Информационная безопасность систем микропроцессорной централизации

Рассматривая информационную безопасность систем микропроцессорных централизаций, прежде всего следует отметить, что категория обрабатываемой в них информации – открытая, следовательно, угроза утечки информации не является актуальной. Таким образом, в качестве основной будем рассматривать угрозу нарушения технологии обработки информации.

Рассмотрим подробнее порядок обеспечения и доказательства информационной безопасности в части недекларированых возможностей и несанкционированного доступа. Доказательством соответствия требованиям по НДВ может служить соответствующий сертификат. На данный момент существует 35 аккредитованных ФСТЭК испытательных лабораторий и девять сертифицирующих органов, обеспечивающих проведение требуемых проверок.

В случае с несанкционированным доступом на сегодняшний день возникают вопросы, связанные с отсутствием соответствующей нормативной базы, определяющей требования и регламентирующей порядок проведения аттестации систем. Требования по функциональной безопасности, в свою очередь, не отражают требований к
реакции систем на несанкционированные воздействия.

При этом на примере системы микропроцессорной централизации EBILock 950 отметим, что реализованные алгоритмы функциональной безопасности обеспечивают перевод в безопасное состояние при нарушении технологии обработки информации.

Информационная безопасность
системы МПЦ EBILock 950

Ядром системы EBILock 950 является специализированный управляющий компьютер. В состав системы также входит исполнительная часть – система объектных контроллеров и автоматизированные рабочие места, реализующие интерфейс управления системой и наблюдения за ее функционированием. Информационная безопасность системы МПЦ EBILock 950 обеспечивается за счет применения закрытых локальных физических сетей, не имеющие прямых связей с сетями общего пользования.

Для замены программного обеспечения центрального процессора требуется физический доступ к оборудованию МПЦ и знание паролей доступа. Исполнительные элементы системы – объектные контроллеры имеют программное обеспечение, записанное в ПЗУ, что также не может быть изменено без физического доступа к контроллеру, что в обязательном порядке фиксируется системой.

В отличие от релейных и релейно-процессорных систем в МПЦ EBILock 950 нет возможности изменения взаимозависимостей и случайных ошибок на действующем объекте из-за вмешательства персонала путем перепаек, установки перемычек и т.п. действий.

Следует отметить, что за 13 лет эксплуатации не зафиксировано ни одного случая несанкционированного воздействия на систему! В 2004 году система МПЦ EBILock 950 была сертифицирована на отсутствие недекларированых возможностей.

Основанием для выдачи сертификата послужили сертификационные испытания лаборатории ООО «Центр безопасности информации» и экспертное заключение Гостехкомиссии России.

В сентябре 2012 года с учетом развития функциональных возможностей системы была проведена повторная сертификация в ФСТЭК России. Сертификат был выдан на основании сертификационных испытаний лаборатории ФГУП «ЗащитаИнфоТранс» и экспертного заключения ОАО «НИИАС».

В части защиты от несанкционированного доступа следует отметить, что на сегодняшний день ни одна компания на сети РЖД, поставляющая системы СЦБ, не имеет доказательств соответствия требованиям по несанкционированному доступу в первую очередь по причине отсутствия самих требований.

Дальнейшие шаги

Дальнейшими направлениями деятельности по обеспечению информационной безопасности объектов СЦБ и анализу системы на соответствие требованиям информационной безопасности является разработка нормативной
базы по оценке возможностей несанкционированного доступа.

Система МПЦ EBILock 950 разработка компании ООО «Бомбардье Транспортейшн (Сигнал)» – первая, на базе которой формируются требования по обеспечению информационной безопасности в части несанкционированного доступа, что в дальнейшем может послужить основой требований для других микропроцессорных систем СЦБ.

ООО «Бомбардье Транспортейшн (Сигнал)» включено в состав рабочей группы ОАО «РЖД» по организации и проведению работ в области информационной безопасности микропроцессорных систем ЖАТ. В план работ группы входит подготовка отчетных материалов, рекомендаций по обеспечению безопасности информации, предложений по внесению в нормативную документацию по информационной безопасности микропроцессорных систем ЖАТ.

Эффективным решением поставленных задач может быть только сотрудничество всех заинтересованных сторон: заказчика, поставщиков, сертифицирующих органов, а также испытательных и экспертных центров.