литературным данным [1, 2] при числе циклов «включено-выключено» $F \geq 1$ цикл/ч преобладают отказы, обусловленные цикличностью работы. Поэтому вопрос о достоверности результатов расчёта надёжности весьма актуален в случае циклического режима работы ЭУ, особенно при числе циклов $F \rightarrow 1$ цикл/ч и более.

При разработке метода расчёта эксплуатационной надёжности элементов для циклического режима работы использованы источники [2, 3]. Принят во внимание экспериментальный график изменения отношения интенсивности отказов элемента при циклическом режиме работы к интенсивности отказов при непрерывном режиме в зависимости от частоты включения F (цикл/ч). Обсуждается модель, аппроксимирующая экспериментальный график, и подходы к определению коэффициентов модели в зависимости от группы аппаратуры. На основе модели получена формула учёта циклического режима работы элемента при расчёте надёжности ЭУ.

Литература

1. *Никулин С.М.* Надёжность элементов радиоэлектронной аппаратуры. М., 1979.

2. Шишмарёв В.Ю. Надёжность технических систем: учебник для студ. высш. учеб. заведений. М., 2010.

3. *Klass P.J.* Cycling tests increase reliability factors. «Aviation Week», Sept. 1960, 5, Vol. 3, № 10.

ЗАЩИТА ИНФОРМАЦИИ В ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЁННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Е.В. Новиков, Д.А. Мельниченко

Современные системы управления технологическими процессами и мониторинга состояния промышленных предприятий становятся все более сложными, объединяя в единое целое объекты, удаленные друг от друга на сотни километров.

Проблемам защиты данных в этих системах не всегда уделяется должное внимание. Например, широко используются информационные технологии, имеющие достаточно хорошо известные уязвимости. Прежде всего, это стандартная операционная система Windows, протоколы IP, HTTP, XML, Ethernet, NET, коммутационное оборудование и средства передачи данных, включая модемы, мультиплексоры, коммутаторы, маршрутизаторы.

Собственно информационные технологии при этом давно используют методы противодействия внешним и внутренним угрозам, в то время как в сложных информационно-управляющих системах эти методы далеко не всегда применяются. Иногда это и объективно объяснимо, т.к. требования безопасности могут входить в конфликт с алгоритмами работы систем управления, особенно функционирующих в режиме реального времени. Так в системе мониторинга состояния химически опасных объектов критическим параметром является время реакции оператора и в период анализа ситуации и принятия решения его не должны отвлекать сообщения о, например, возможном вирусном заражении.

Вместе с тем, такие вирусные атаки могут привести в сложных системах управления техническими процессами к большому материальному ущербу, а иногда и иметь катастрофические последствия.

Исходя из изложенного выше, можно утверждать, что при проектировании сложных территориально распределенных систем управления обязателен этап анализа потенциальных угроз, оценки степени их опасности в терминах «риск-ущерб» и разработки методов защиты информации в создаваемых системах.

ПРИНЦИПЫ КОРРЕКТИРОВКИ ПОКАЗАНИЙ МОЩНОСТИ ЯДЕРНОЙ ЭНЕРГЕТИЧЕСКОЙ УСТАНОВКИ

С.М. Сацук

Прогресс в области информационных технологий предоставляет инженеру, работающему в области ядерной энергетики, возможность для реализации новых прогрессивных проектов ядерной энергетической установки. Система, которая обеспечивает безопасную эксплуатацию реакторной установки (РУ) должна иметь современное оборудование и алгоритмы. В состав такой системы входит большое количество подсистем, которые контролируют соответствующие параметры РУ физически различными способами: СВРК, АКНП и т.д. Одной из подсистем контроля управления и защиты является АКНП. АКНП состоит из нескольких независимых комплектов (двух или трех)