МЕТОДЫ ОБЕСПЕЧЕНИЯ И ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И УПРАВЛЯЮЩИХ СИСТЕМ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

В.Н. Путилин

Хакерские атаки на компьютерные сети АЭС могут вызвать отключение электричества или поступление вирусного кода, который (как в некоторых известных случаях) не просто делает невозможной выполнение отдельных операций, начиная с простой перезагрузки компьютера, но может блокировать АСУ управления всего цикла производства электроэнергии.

Система безопасности АЭС имеет сложную структуру, состоящую их пяти контуров кибербезопасности. Первый и второй контуры состоят из датчиков, объединенных в локальной сети обработки информации. Третий и четвертый уровни обеспечивают работу операторов оперативного и неоперативного управления, необходимую для управления технологическим оборудованием АЭС и технологов на автоматизированных рабочих местах (АРМ), которые снабжены средствами визуализации технологических процессов, но лишены возможности управления. Пятый контур – контур внешнего доступа для сопряжения с кризисным центром, в который поступает информация о состоянии АЭС через протокол удаленного доступа без возможности управления по автономным изолированным от Интернета каналам связи.

В работе для каждого контура рассмотрены возможности нарушения режима безопасности и пути уменьшения вероятности их возникновения или умышленной реализации, необходимые при разработке моделей угроз, модели нарушителя и соответственно модели защиты. Практически важными и обязательными средствами для уменьшения потенциальной угрозы является: снижение числа уязвимостей еще на этапе проектирования, например, использованием в контурах управления сертифицированных операционных систем на базе Linux, которые исследовать на уязвимости намного проще; получение доступа к USB-портам

компьютеров на АЭС согласно установленным процедурам; учет «недокументированных возможностей» (НДВ) электронных компонентов как знанием исходного кода, так и самостоятельной прошивкой используемых электронных компонентов, а также решением задачи о создании из «недоверенных» компонентов собственной программной платформы, как доверенной системы и верификацией ее модели на симуляторе на предмет расхождения контролируемых параметров.

Литература

1. Общие положения обеспечения безопасности атомных станций (ОПБ АС). – Минск: Министерство по чрезвычайным ситуациям Республики Беларусь, 2009. – 28 с.