ЗАДАЧА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

В.Н. Путилин

Задача обеспечения информационной безопасности и кибербезопасности – обеспечение непрерывности, безопасности и эффективности технологических и производственных процессов АЭС.

Решением рассмотренных проблем можно считать использованием моделей информационной безопасности, построенной на основе модели МАГАТЭ, которая определяет, как основной элемент информацию, представленную в цифровой форме, и системы, используемые для ее обработки и хранения на уровне технологического управления, т. е. АСУ ТП АЭС.

Кибербезопасность АСУ ТП АЭС, как составная часть информационной безопасности АЭС, заключается в поддержании значений рисков для АЭС (экономических, экологических, социальных), связанных с возможным нарушением (умышленным и не умышленным) доступности, целостности или конфиденциальности информации (программ, данных и их потоков) в АСУ ТП АЭС, в заданных пределах.

При этом АСУ ТП имеет достаточно большое количество уязвимых мест, способных привести к нарушению корректной работы технологического процесса

и реализации угроз несанкционированного доступа к информации в системах диспетчерского управления и сбора данных, отдельных интерфейсах управления автоматизированными комплексами разного назначения, элементах телеметрических систем управления производством. АСУ ТП может быть реально защищена только при решении задач защиты на всех возможных уровнях, угрозы для которых принято определять в виде трех основных групп: угрозы техногенного характера; угрозы антропогенного характера; угрозы несанкционированного доступа.

Техногенные угрозы рассматриваются как физическое влияние на компоненты АСУ ТП. К антропогенным относятся ошибки персонала, преднамеренные и непреднамеренные действия людей, занятых обслуживанием АСУ ТП, ошибки в организации работ с компонентами АСУ ТП. Угрозы несанкционированного доступа для АСУ ТП возникают при взаимодействии компонентов АСУ ТП с локальной вычислительной сетью предприятия при необходимости передачи информации о состоянии технологической среды и управления воздействиями на технологические объекты.

В заключении можно отметить, что особенность задачи состоит в том, что информация, как предмет, безопасность которого определяется, должен быть определен как по внутренней структуре, так и по внутренним свойствам и связям с внешними устройствами, которые необходимы для формирования требований к его безопасности.

Реализация системы информационной безопасности АСУ ТП представляет собой комплексную задачу. Все указанные факторы в совокупности влияют на общую защищенность системы АСУ ТП. Это и отказ даже от минимальных мер безопасности, и использование Windows, как основной операционной системы для рабочих станций и серверов, и слабая дисциплина сотрудников, а также тот факт, что на каждом из этапов жизненного цикла должны быть определен свой набор мероприятий по выделению актуальных угроз и объектов защиты в АСУ ТП.

Литература

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