ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ЯДЕРНЫХ ЭЛЕКТРОСТАНЦИЙ

В.Н. Путилин

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Кибербезопасность АЭС означает защиту технологического процесса от несанкционированного доступа и обеспечивается за счет эффективного управления системам АСУ ТП, решающими задачи надежного регулирования основного технологического процесса. При этом информация о ходе технологического процесса в АСУ ТП не представляется «в чистом виде», а поступает через систему защиты, которая для устранения искажений и сохранения конфиденциальности требует внедрения в технические средства АСУ ТП соответствующих программных или технических механизмов [1].

Особенностью структуры и алгоритмов работы технических средств защиты информации является согласование с принятой на АЭС структурой глубокоэшелонированной защиты, в которой каждый уровень защиты имеет свою подсистему информационной безопасности и обеспечивает определенную эффективность защиты барьеров от характерных для данного уровня воздействий и определенного типа атаки. Поэтому у АЭС, как и у любого крупного промышленного объекта автоматизации, можно выделить пять контуров кибербезопасности со своими техническими средствами.

В первом находятся все датчики, подключенные к программно-логическим контроллерам (ПЛК). Второй контур (шлюзовой) осуществляет сбор информации с ПЛК и ее передачу в сеть системы верхнего блочного уровня (СВБУ). В третьем контуре находится СВБУ, с которой взаимодействует оператор, управляющий технологическим оборудованием АЭС. В четвертом контуре с данными СВБУ работают технологи, отвечающие за конкретную подсистему АЭС. Пятый контур – контур внешнего доступа, сопряженный с кризисным центром, в который поступает информация о состоянии АЭС через протокол удаленного доступа без возможности управления.

АСУ ТП атомной электростанции находится в изолированной сети и отключена от внешних сетей, поэтому нелегитимное подключение к АЭС полностью контролируется системой безопасности АЭС, работающая на строго заданных алгоритмах.

Правильней говорить о «недекларированных возможностях» (НДВ) к вмешательству в рабочий процесс отдельных уровней защиты. НДВ могут быть везде. В процессоре, в контроллере, в сервере, в маршрутизаторе, коммутаторе и планшете. НДВ могут быть

в более высокоуровневом ПО, в операционных системах, прошивках оборудования, в ПО непосредственного управления техническими средствами.

В заключение можно отметить, что особенность задачи состоит в том, что технические средства защиты информации в системе безопасности должны развиваться в направлении полного контроля НДВ на каждом из уровней соответствующего технологического процесса. Отказы и повреждения технических и программных средств должны приводить к появлению сигналов на щитах управления (БПУ, РПУ и др.) и вызывать действия, направленные на обеспечение безопасности АЭС.

Реализация системы информационной безопасности АСУ ТП представляет собой комплексную задачу. Все указанные факторы в совокупности влияют на общую защищенность системы АСУ ТП и применяемые технические средства должны обеспечивать такое состояние подсистем и комплексов АСУ ТП АЭС, при котором риски нарушения технологического процесса из-за кибератак на АСУ ТП АЭС минимизированы

Список литературы

1. Путилин, В. Н. Задача обеспечения информационной безопасности атомных электростанций / В. Н. Путилин // Технические средства защиты информации: тез. докл. XX Белорусско-российской науч.-техн. конф., Минск, 7 июня 2022 г. – С. 82–83.