ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ УПРАВЛЯЮЩИХ СИСТЕМ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

С.В. Дробот, В.Н. Русакович, С.М. Сацук

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

Автоматизированная система управления технологическими процессами АЭС (АСУ ТП АЭС) играет основную роль в обеспечении безопасной эксплуатации одного из наиболее сложных объектов управления, каким является АЭС. Управляющие системы современных АЭС, которые проектировались и сооружались уже в 21 веке, от аналоговых методов и средств управления перешли к цифровым (дискретным) методам и средствам. Цифровые технологии используются и при модернизации существующих АЭС. Однако использование компьютерной техники и цифровых технологий в управляющих системах АЭС, как называется АСУ ТП АЭС в нормативных правовых актах (НПА), регулирующих ядерную безопасность в Республике Беларусь, сделало эти системы уязвимыми для кибератак. Исторически при проектировании управляющих систем АЭС не уделялось должного внимания компьютерной безопасности в связи с тем, что аналоговые системы являются неуязвимыми для кибератак из-за их жесткой реализации, а также в связи с отсутствием коммуникации с внешними сетями и системами.

Кибератаки на управляющие системы АЭС, использующие цифровые технологии, могут поставить под угрозу ядерную безопасность АЭС и привести к неприемлемым радиологическим последствиям. В связи с чем ряд документов МАГАТЭ [1, 2] определяют необходимость защиты компьютерных систем, включая управляющие системы, объектов использования атомной энергии. Технические руководящие материалы [3], опубликованные в 2018 году в Серии изданий МАГАТЭ по физической ядерной безопасности, содержат рекомендации по применению мер, обеспечивающих компьютерную безопасность в отношении управляющих систем АЭС, на всех этапах их жизненного цикла от проектирования до модернизации. Документ 2020 года [4], изданный в Серии МАГАТЭ по ядерной энергии, включает описание большого числа методов защиты управляющих систем АЭС от кибератак для всех этапов жизненного цикла, а также рассматривает их основные достоинства и недостатки.

Анализ НПА по обеспечению ядерной и радиационной безопасности Республики Беларусь показывает необходимость актуализации их в части установления требований по обеспечению компьютерной безопасности управляющих систем АЭС с целью их гармонизации с документами МАГАТЭ.

Список литературы

1. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). IAEA Nuclear Security Series No. 13. Recommendations. – Vienna, IAEA, 2011. 57 p.

2. Computer Security Techniques for Nuclear Facilities. IAEA Nuclear Security Series No. 17-T (Rev. 1). Technical Guidance. Vienna, IAEA, 2021. 140 p.

3. Computer Security of Instrumentation and Control Systems at Nuclear Facilities. IAEA Nuclear Security Series No. 33-T. Technical Guidance. – Vienna, IAEA, 2018. 58 p.

4. Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants. IAEA Nuclear Energy Series No. NR-T-3.33. Technical Reports. Vienna, IAEA, 2020. 72 p.