УДК 621.039-78

ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

В.Н. Путилин

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

Аннотация. Техническое обеспечение информационной безопасности АЭС зависит от множества факторов. Основным из них является тот факт, что набор мероприятий по выделению актуальных угроз и объектов защиты в АСУ ТП и технические средства защиты информации в системе безопасности должны развиваться в направлении полного контроля технических и программных средств на каждом из уровней соответствующего технологического процесса. На основе информации о текущем состоянии системы, применяемых методах и мерах безопасности, функциональных особенностях технических средств и т.д. определяется текущий уровень безопасности для каждой зоны.

Ключевые слова: АЭС; информационная безопасность; уровень защиты; АСУ ТП; меры безопасности; несанкционированный доступ; кибербезопасность.

TECHNICAL IMPLEMENTATION OF THE TASK OF INFORMATION SECURITY OF NUCLEAR POWER PLANTS

V.N. Putilin

Educational Institution "Belarusian State University of Informatics and Radio Electronics", Minsk, Belarus

Abstract. Technical support of NPP information security depends on many factors. The main one is the fact that the set of measures to identify current threats and objects of protection in APCS and technical means of information protection in the security system should develop in the direction of complete control of technical and software means at each level of the corresponding technological process. Based on information about the current state of the system, applied methods and safety measures, functional features of equipment, etc., the current safety level for each zone is determined.

Keywords: NPP; information security; protection level; security measures; unauthorized access; cybersecurity.

Введение

Обеспечение непрерывности, безопасности и эффективности технологических и производственных процессов атомных станций в настоящее время происходит с использованием моделей информационной безопасности, построенной на основе модели МАГАТЭ (рис. 1).

В этой модели основным элементом является информация, представленная в цифровой форме, и системы, используемые для ее обработки и хранения на уровне технологического управления, т.е. АСУ ТП АЭС.

Большое количество уязвимых мест в АСУ ТП может 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.

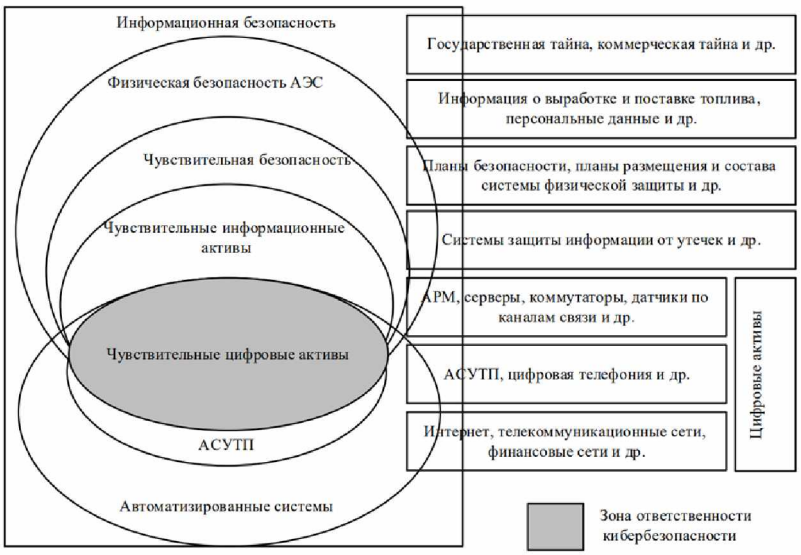

Рис. 1. Общая модель взаимодействия информационной и кибербезопасности для атомной промышленности

Fig. 1. General model of interaction between information and cyber security for the nuclear industry

Особенность модели заключается в поддержании в заданных пределах значений рисков (экономических, экологических, социальных), связанных с возможными (умышленными и неумышленными) нарушениями доступности, целостности или конфиденциальности информации (алгоритмов, данных и сигналов) в АСУ ТП АЭС.

Основная часть

Реализация системы информационной безопасности АСУ ТП представляет собой комплексную задачу. 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].

В общем случае можно говорить, что «недекларированные возможности» (НДВ) к вмешательству в рабочий процесс на отдельных уровнях защиты 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.

АСУ ТП атомной электростанции отключена от внешних сетей и поэтому нелегитимное подключение к АЭС должно полностью контролироваться системой безопасности АЭС, работающая на строго заданных алгоритмах.

Реальная защита АСУ ТП возможна только при решении задач защиты в виде трех основных групп на всех возможных уровнях, угрозы для которых принято определять в виде:

– угрозы техногенного характера, как физическое влияние на компоненты АСУ ТП;

– угрозы антропогенного характера (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.

Структура принятой на АЭС глубокоэшелонированной защиты построена так, что каждый уровень защиты имеет свою подсистему информационной безопасности и обеспечивает определенную эффективность защиты барьеров от характерных для данного уровня воздействий и определенного типа атаки.

Для каждой выделенной зоны проводится идентификация и классификация активов, анализ уязвимостей и угроз, моделирование нарушителей и детальная оценка рисков. На основе информации о текущем состоянии системы, применяемых методах и мерах безопасности, функциональных особенностях технических средств и т. д. определяется текущий уровень безопасности для каждой зоны.

Соответственно для АЭС, как для любого крупного промышленного объекта автоматизации, можно выделить пять контуров кибербезопасности со своими техническими средствами [2].

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.

Заключение

В заключение можно отметить, что особенность задачи состоит в том, что технические средства защиты информации в системе безопасности должны развиваться в направлении полного контроля технических и программных средств 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.

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 использованных источников

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

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

References

1. General Safety Provisions for Nuclear Power Plants (NP FS) - Minsk: Ministry of Emergency Situations of the Republic of Belarus. 2009. – 28 p.

2. V.N. Putilin. The task of ensuring information security of nuclear power plants//Technical means of information protection: tez. doc. XX Belarusian-Russian scientific and technical conf., Minsk, June 7, 2022. P. 82-83.

Сведения об авторах

Путилин В.Н., канд. техн. наук, доц., доцент кафедры электроники, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». putilin@bsuir.by.

Information about the authors

Putilin V.N., Cand. Sci., Associate Professor of the Electronics Department, Educational Institution "Belarusian State University of Informatics and Radio Electronics". putilin@bsuir.by.