УДК 004.052.3

АНАЛИЗ РИСКА ВЫВОДА ЗНАЧИМОГО ОБЪЕКТА КИИ ИЗ СТРОЯ В УСЛОВИЯХ РЕАЛИЗАЦИИ УГРОЗЫ ПЕРЕХВАТА УПРАВЛЕНИЯ АСУ ТП

Пермякова М.А. Университет ИТМО
Научный руководитель – к.т.н., доцент Бибиков С.В.
Университет ИТМО

При создании комплексных систем безопасности значимых объектов критической информационной инфраструктуры необходимо проводить анализ рисков функциональной и информационной безопасности, обусловленных возможными отказами аппаратных средств. Одним из потенциальных рисков является перехват управления на уровне физических устройств, являющийся результатом успешной реализации угрозы осуществления нарушителем несанкционированного доступа к информационной инфраструктуре за счёт получения права управления входящей в её состав автоматизированной системы управления технологическими процессами путём эксплуатации уязвимостей её программного обеспечения или слабостей технологических протоколов передачи данных.

При проектировании комплексных систем безопасности значимых объектов критической информационной инфраструктуры необходимо соблюдать выполнение требований, направленных на обеспечение функционирования систем управления в штатном режиме, при котором обеспечивается выполнение целевых функций в условиях воздействия угроз безопасности информации, а также на снижение рисков незаконного вмешательства в процессы функционирования.

Риск-ориентированный подход к обеспечению безопасности рассматривается как совокупность непрерывных процессов, которые необходимо поддерживать на всех стадиях жизненного цикла системы. Стандарты в области управления рисками и функциональной безопасности задают требования к проектированию наложенных систем управления кибербезопасностью автоматизированных систем управления и SCADA-систем, а также к проектированию систем с уже заложенными и интегрированными мерами безопасности. Проектируемая система должна поддерживать непрерывный жизненный цикл процессов безопасности на всех стадиях существования объекта защиты, включающий в себя постоянный пересмотр уже обработанных рисков, идентификацию и анализ новых, анализ эффективности принятых компенсационных мер и изменяющегося пространства рисков и угроз на заданном временном интервале.

Одной из методик оценки рисков на всем жизненном цикле системы является методика HAZOP (Hazard and Operability Study), направленная на обнаружение потенциальных опасностей и проблем работоспособности автоматизированной системы управления на протяжении ее жизненного цикла. На первом этапе перечисляются все потенциальные причины, которые могут привести к нарушению штатного функционирования системы, к останову критического технологического процесса или системы в целом. Затем подробно описываются все возможные последствия. При оценке последствий важно учитывать существующие системы защиты и их параметры функционирования. Завершающим этапом является определение уровня риска, присущего каждой опасности. Если вероятность возникновения опасности высока, а тяжесть последствий мала, риск можно расценивать как средний. С другой стороны, если вероятность возникновения опасности низкая, а тяжесть последствий высока, риск расценивается как высокий.

При количественной оценке риска, обусловленного опасностью, определенной в ходе анализа HAZOP, необходимо установить количественные критерии и учесть прочие

производственные риски, которым подвергается система в течение заданного временного интервала.

Для снижения риска перехвата управления автоматизированной системы при проектировании систем безопасности определяются функции безопасности, реализуемые соответствующими средствами защиты информации, а также функции, встроенные в специализированное программное обеспечение промышленного назначения.

Результаты, полученные в ходе анализа рисков, дают возможность оценить эффективность проектируемых систем безопасности, а также степень их соответствия четырехуровневой концепции кибербезопасности автоматизированных систем управления технологическими процессами, согласно стандарту ISA/IEC 62443-4-1-2018.