УДК 004.056

В.Г. ИВАНЕНКО[1], Н.Д. ИВАНОВА[2]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*Российский университет транспорта (МИИТ), Москва*

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП

Цель исследования: формирование предложений к алгоритму анализа рисков информационной безопасности (ИБ) АСУ ТП. На основании национальных и международных нормативно-методических документов и практики обеспечения информационной безопасности в статье определен перечень факторов и характеристик рисков ИБ АСУ ТП, что позволяет проводить анализ рисков на основании результатов уже проведенного анализа безопасности АСУ ТП. В результате разработан алгоритм анализа рисков ИБ АСУ ТП, ориентированный на объекты защиты и их уязвимости.

При формировании подхода к анализу рисков информационной безопасности (ИБ) автоматизированных систем управления технологическим процессом (АСУ ТП) важно учесть, что обеспечение ИБ АСУ ТП должно быть ориентировано на защиту функциональных компонентов, выполняемых ими функций, а также на защиту самого технологического объекта управления.

На основе анализа определений государственных и международных стандартов можно выделить два основных фактора риска: величина тяжести последствий от наступления опасного события и вероятность его наступления. В свою очередь, фактор вероятности наступления нежелательного события может быть характеризован по параметрам уязвимостей системы и ее компонентов и потенциала нарушителя.

Тяжесть последствий от успешной реализации угрозы ИБ на АСУ ТП может характеризоваться классом защищенности АСУ, в соответствии с приказом ФСТЭК России № 31 [1] определяемого степенью возможного ущерба от нарушения целостности, доступности, конфиденциальности информации, обрабатываемой в АСУ ТП. Также для АСУ ТП, являющихся объектами критической информационной инфраструктуры, тяжесть последствий от успешной реализации угрозы ИБ может характеризоваться с помощью показателей критериев значимости объектов КИИ РФ.

Уязвимости АСУ ТП могут характеризоваться метриками из стандарта Common Vulnerability Scoring System (CVSS) [2], являющимся открытым стандартом оценки уязвимостей.

Для определения характеристик потенциала нарушителя может быть использован стандарт ГОСТ Р ИСО/МЭК 18045-2013 [3], который предлагает методику определения потенциала нападения нарушителя, ориентированную на имеющиеся в системе уязвимости, что согласуется с определенным ранее подходом.

В общем случае предлагаемый алгоритм анализа рисков АСУ ТП включает следующую последовательность действий. После проведенной идентификации рисков оценка последствий от реализации угроз ИБ производится на основании ранее проведенного категорирования уязвимых объектов защиты. В рамках анализа ущерб из-за отказов компонентов определяется тяжестью ущерба отказа соответствующей системы согласно положениям Постановлением Правительства № 127 [4] в части категорирования объектов КИИ, заключающимся в присвоении определенной категории значимости объектам по результатам анализа «сверху-вниз». Для каждого компонента АСУ ТП на основании ранее проведенной идентификации рисков ИБ АСУ ТП формируется перечень уязвимостей и проводится их анализ на основании метрик стандарта CVSS [2]. Далее для каждой уязвимости оцениваются необходимые возможности нарушителя для ее успешной эксплуатации в соответствии со стандартом ГОСТ Р ИСО/МЭК 18045-2013 [3]. В результате проведенного анализа рисков ИБ АСУ ТП КИИ формируется сопоставление объектов защиты, уязвимостей и возможностей нарушителей, а также определяются их характеристики.

Предлагаемый подход к анализу рисков ориентирован на объекты защиты и их уязвимости, что позволяет реализовать детальный анализ рисков в условиях неопределенности видов возможных нарушителей и их мотивов.

Список литературы

1. Приказ ФСТЭК от 14.03.2014. № 31. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14- marta-2014-g-n-31 (дата обращения: 14.09.2023).

2. Common Vulnerability Scoring System version 3.1: Specification Document. – URL: https://www.first.org/cvss/specification-document/ (дата обращения: 14.09.2023).

3. ГОСТ Р ИСО/МЭК 18045-2013. – Введ. 28.08.2013. – URL: https://gostexpert.ru/data/files/18045-2013/65454.pdf (дата обращения: 14.09.2023).

4. Постановление Правительства Российской Федерации от 08.02.2018 № 127. – URL: http://publication.pravo.gov.ru/Document/View/0001201802130006 (дата обращения: 14.09.2023).