АСПЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

А. Ю. Павлин, Н. Н. Акимов, А. В. Жулин[1]

Филиал РФЯЦ-ВНИИЭФ «НИИИС им. Ю. Е. Седакова», г. Нижний Новгород
[1]НГТУ им. Р. Е. Алексеева, г. Нижний Новгород

Вопросам обеспечения безопасности автоматизированной системы управления технологическими процессами (АСУ ТП) в настоящее время уделяется пристальное внимание на государственном уровне [1]. Например, указ Президента РФ № 620 от 22.12.2017 г. «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

Разработаны нормативно-методические документы в области информационной безопасности, к которым относятся методические документы государственных органов России и стандарты информационной безопасности.

К методическим документам государственных органов России относятся:

− доктрина информационной безопасности РФ;

− приказы и руководящие документы федеральной службы по техническому и экспортному контролю (ФСТЭК) (Гостехкомиссии России);

− приказы федеральной службы безопасности;

Стандарты информационной безопасности, среди которых выделяют:

− международные стандарты;

− государственные (национальные) стандарты РФ;

− рекомендации по стандартизации;

− методические указания.

Авторы документа «Доктрина информационной безопасности Российской Федерации» [2], введенной Указом Президента РФ от 05.12.2016 № 646 учли текущую ситуацию в мире информационных технологий и не обошли стороной проблему компьютерных атак, направленных на промышленную сферу [3].

К приоритетам РФ в сфере информационной безопасности отнесено:

– «Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время»;

– «Развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности»;

– «Содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также защиту суверенитета Российской Федерации в информационном пространстве».

Анализ нормативной базы по кибербезопасности АСУ ТП атомной электростанции (АЭС) показал, что существующие стандарты в рамках принципов и подходов к информационной безопасности можно считать результатом доработки существующих методик, учитывающих специфику АСУ ТП. Сами же стандарты можно разделить на общие стандарты, учитывающие специфику промышленных систем, в частности наличие таких элементов, как автоматизированная система управления и различные датчики, и отраслевые стандарты, учитывающие особенности конкретной отрасли [4].

Современные АСУ ТП представляют собой сложные компьютеризированные системы, отличающиеся большой разветвленностью, большим числом и разнотипностью оборудования, сложностью алгоритмов управления. Многообразие функций АСУ ТП, интегрированность с объектом управления, очевидно, приводит к многообразию угроз и потенциальной опасности при нарушении кибербезопасности АСУ ТП АЭС. Вместе с развитием АСУ ТП развиваются и совершенствуются угрозы кибербезопасности, устанавливаются новые требования по защищенности АСУ ТП:

– нормативная документация РФ – Приказ ФСТЭК № 31 от 14 марта 2014 г., федеральный закон № 187 от 26 июля 2017 г., Приказ ФСТЭК № 235 от 21.12.2017 г., Приказ ФСТЭК № 239 от 25.12.2017 г.;

– стандарты международной электротехнической комиссии (МЭК/IEC) – IEC 61513:2011, IEC 60880:2006, IEC 62645:2014, IEC 62859:2016, проект IEC 63096;

– документы международного агентства по атомной энергии – NSS 17, NST036, NST037, NST038, NST045, NST047.

Основное внимание предлагается уделить методологии определения рисков от возможного намеренного вмешательства в систему управления с целью нанесения вреда для потенциально опасного промышленного объекта.

В настоящее время предложен ряд подходов к оценке рисков информационных систем, используемых в промышленности, в том числе:

– оценка критических эксплуатационных угроз и уязвимостей (OCTAVE – Operationally Critical Threat and Vulnerability Evaluation) [5];

– метод анализа и управления рисками Центрального агентства по вычислительной технике и телекоммуникациям (CRAMM – Central Computer and Telecommunications Agency Risk Analysis and Management Method) [6];

– консультативный, целевой и бифункциональный анализ рисков (COBRA – Consultative, Objective and Bifunctional Risk Analysis [7];

– консультативный и целевой анализ рисков (CORAS – Consultative and Objective Risk Analysis) [8, 9];

– основанная на модели, методология оценки рисков для систем, критичных по безопасности (model-based risk assessment methodology for security-critical systems).

Применительно к опасным промышленным объектам, к которым относится АЭС, целесообразно рассматривать проблемы безопасности как проблемы надежности сложных человеко-машинных систем по отношению к здоровью и жизни людей, состоянию окружающей среды, материальному ущербу. Проблема кибербезопасности может рассматриваться как частный (специфический) случай проблемы обеспечения надежности/безопасности объектов. Таким образом, логично применить известные методы для качественного и количественного анализа кибербезопасности из теории надежности, такие как «Анализ дерева событий», представленный на рис. 1 и «Анализ дерева неисправностей», представленный на рис. 2.

Следует отметить, что поскольку срок службы энергоблока АЭС составляет более 30 лет с возможностью его продления, а также оборудование и система управления подвергаются периодической замене и модификации, то анализ защищенности от киберугроз необходимо проводить на всем жизненном цикле системы.

Несмотря на то, что современная АЭС является изолированной от внешнего мира системой и содержит большой набор средств защиты, как любая сложная система имеет конечную вероятность возникновения нештатных ситуаций в случае преднамеренного воздействия на нее. Комплексная система безопасности должна обеспечивать защиту всех элементов АСУ ТП и не приводить к снижению уровня надежности, установленного в техническом задании на систему. Для решения данной проблемы необходимо совершенствование нормативной базы, совершенствование культуры безопасности и продолжение проведения исследований в данном актуальном направлении.

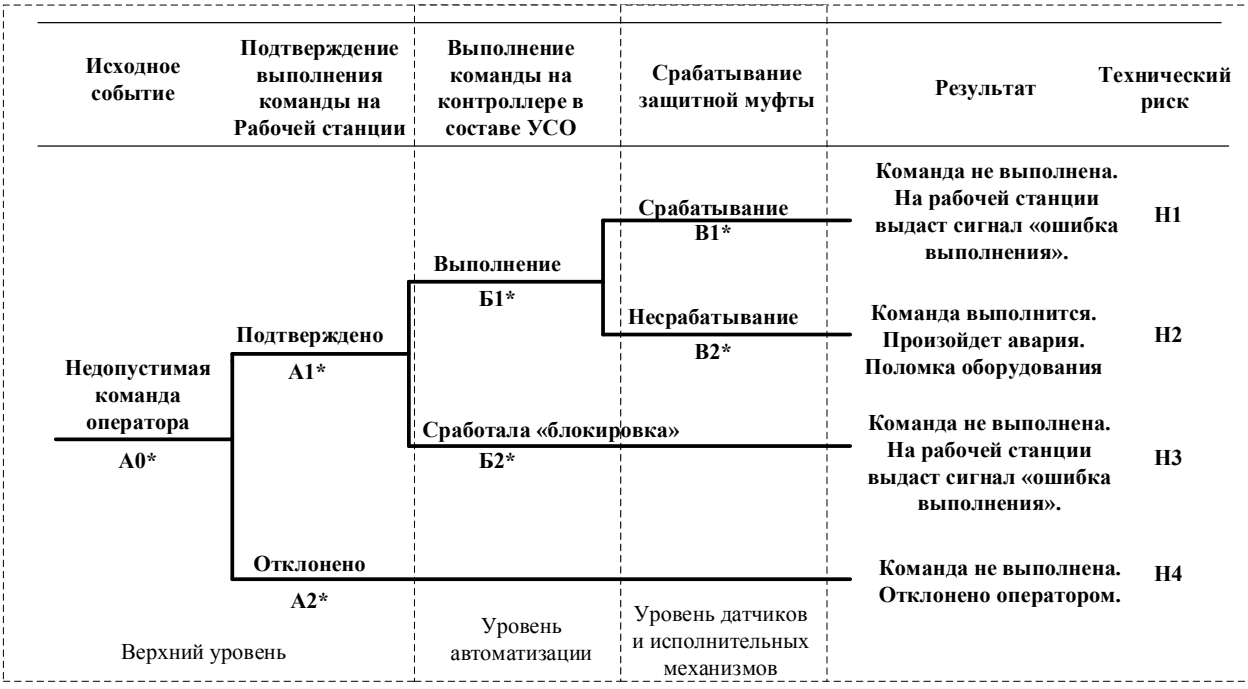

Рис. 1. Структура дерева событий применительно к оценке кибербезопасности

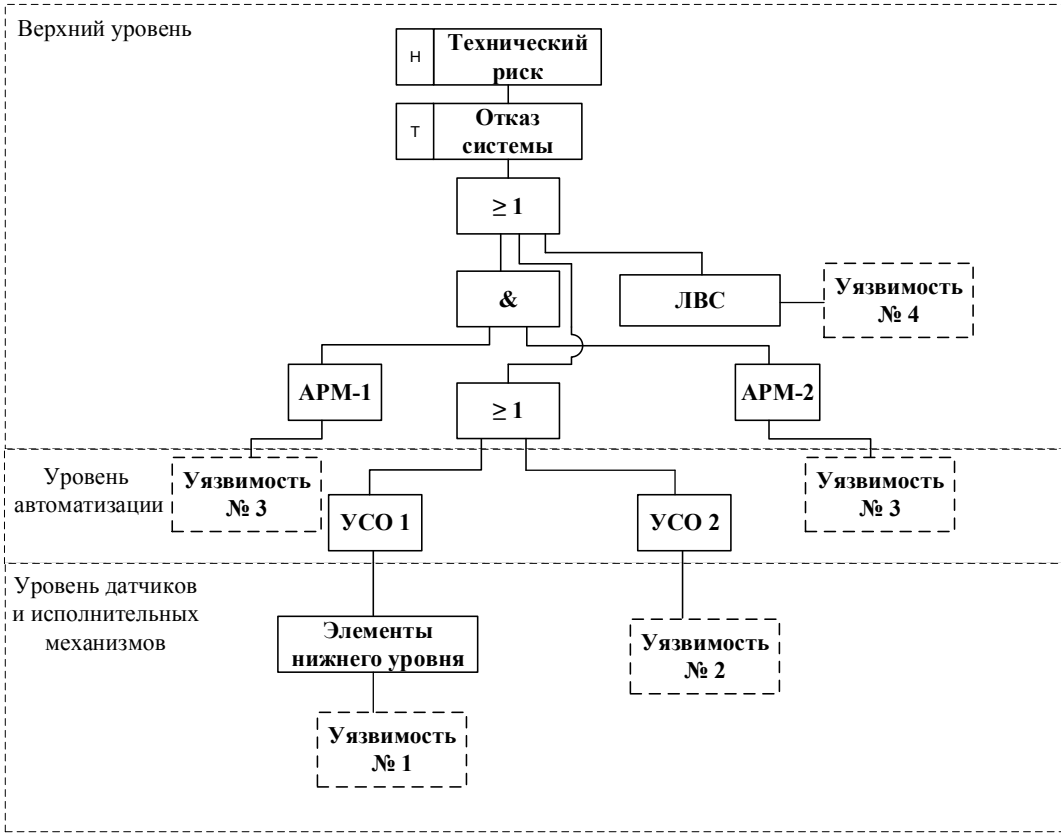

Рис. 2. Структура дерева неисправностей применительно к оценке кибербезопасности: АРМ – автоматизированное рабочее место; ЛВС – локальная вычислительная сеть; УСО – устройство связи с объектом

Литература

1. Дмитриев С. М., Акимов Н. Н., Кольцов В. А. Аспекты обеспечения кибербезопасности АСУ ТП АЭС // Информационно-измерительные и управляющие системы. 2017. № 8 (15). С. 7–13.

2. «Доктрина информационной безопасности Российской Федерации», введенная Указом Президента РФ от 05.12.2016 № 646.

3. Анализ положений Доктрины информационной безопасности РФ. [Электронный ресурс] Режим доступа: https://www.securitylab.ru/analytics/485289.php

4. Душа И. Ф., Зуйков А. В., Духвалов А. П. Информационная безопасность АСУ ТП КВО: нормативно-правовое обеспечение, текущая ситуация // Информационная безопасность. 2014. № 10. С. 100–104.

5. Alberts C, Dorofee A, Stevens J,Woody C. Introduction to the OCTAVE approach. Software Engineering Institute; 2003.

6. Yazar Z. A qualitative risk analysis and management tool – CRAMM. SANS Institute; 2002.

7. RiskWorld. <http://www.riskworld.net/>. [accessed 16.10.15]. RISI. Industry attacks growing. October 14. <http://www.isssource.com/risi-industry-attacks-growing>; 2013 [accessed 23.01.15].

8. Aagedal J., Braber D., Dimitrakos T., Gran B., Raptis D., Stolen K. Model-based risk assessment to improve enterprise security. In: Proceedings of the sixth international enterprise distributed object computing conference. 2002. P. 51–62 EDOC'02.

9. Stolen K., den Braber F., Dimitrakos T., Fredriksen R., Gran B., Houmb S., et al. Model-based risk assessment – the CORAS approach. In: 1st iTrust workshop. 2002.