УДК 004.056

А.В. ТРИФОНЕНКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ПРИНЦИПЫ РАЗРАБОТКИ ПРОГРАММНЫХ СРЕДСТВ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ АЭС

В атомной энергетике контролирующие организации предъявляют чёткие требования к критически важному для безопасности программному обеспечению. В данной работе изучена общая структура требований к программным средствам, важным для безопасности атомных электростанций, на примере международных стандартов, требования проанализированы в контексте современного рынка информационных технологий, рассмотрены частные примеры программного обеспечения, отвечающего стандартам, с целью формирования новых практик и стандартов в различных сферах информационных технологий.

Современный рынок информационных технологий перенасыщен решениями для разработки программного обеспечения (ПО). Всё больше программных систем разработки проектируется с учётом необходимости предотвращения ошибок, вызываемых человеческим фактором.

Существующие своды принципов и рекомендаций к разработке ПО, выработанные крупными инженерными компаниями, направлены, в основном, на оптимизацию масштабирования, сокращение затрат на подготовку специалистов, зависят от конкретного языка программирования, применяемого фреймворка или архитектуры программной системы. Принципы, разработанные отдельными специалистами в индустрии, разрозненны, и не всегда применимы к произвольному программному проекту.

С целью выявления универсальных практик, подходящих для разработки отказоустойчивого ПО, было решено изучить стандарты, применяемые в сферах, где безопасность и отказоустойчивость имеют высшую ценность [1] по сравнению с отдельными потребительскими свойствами, а также в которых на этапе проекта предполагается закладывать значительные средства на обеспечение безопасности и отказоустойчивости ПО.

Требования к разработке программных средств, важных для безопасности атомной электростанции (АЭС), сформулированы Международной электротехнической комиссией (МЭК) в стандартах IEC 60880 и 62138. Аналогичные российские стандарты зафиксированы Росстандартом, как ГОСТ Р МЭК 60880-2010 [2] и 62138-2021 [3], и

являются переводными версиями соответственных документов МЭК. Разделы этих документов регламентируют многие аспекты проектирования, написания и трансляции программных средств [4], некоторые из которых могут представлять интерес для разработчиков ПО, применяемого и в менее критичных с точки зрения безопасности и отказоустойчивости сферах.

Общие требования к проектам программного обеспечения, согласно стандарту, предусматривают поэтапное следование процессам управления проектом, обеспечения и контроля качества ПО, управления конфигурацией, обеспечения защищённости и верификации ПО.

Кроме того, стандарт описывает принципы выбора языков программирования, программных инструментов и вспомогательных средств, предупреждения отказов и изготовления документации.

Были выделены и отдельно рассмотрены некоторые частные примеры требований стандартов, для них был проведён сравнительный анализ с известными мировыми практиками и принципами разработки ПО. Также требования соотнесены с принципами работы современных языков программирования и известных фреймворков. Приведены некоторые примеры реализации рассмотренных стандартов в атомной отрасли [5].

Список литературы

1. Development of Safety-Critical Systems. Architecture and Software. / G. Karmarkar, A. Wakankar, A. Kabra, P. Pandya. – Кам, Швейцария: Springer, 2023. – 498 с. – ISBN: 978-3-031-27900-3. – DOI: https://doi.org/10.1007/978-3-031-27901-0.

2. ГОСТ Р МЭК 60880-2010. Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А. – М.: Стандартинформ, 2011. – 90 с.

3. ГОСТ Р МЭК 62138-2021. Программное обеспечение систем контроля и управления атомной станции, выполняющих функции безопасности категории В и С. – М.: Российский институт стандартизации, 2022. – 46 с.

4. J. Lahtinen и др. Comparison between IEC 60880 and IEC 61508 for Certification Purposes in the Nuclear Domain // Computer Safety, Reliability, and Security29th International Conference: . Proceedings, Vienna, Austria, September 2010. – Вена, Австрия, 2010. – С. 55–67. – ISSN 0302-9743. – DOI: https://doi.org/10.1007/978-3-642-15651-9_5.

5. SimInTech: среда динамического моделирования технических систем / Б.А. Карташов, Е.А. Шабаев, О.С. Козлов, А.М. Щекатуров. – М.: ДМК-Пресс, 2017. – 424 с. – ISBN: 978-5-97060-482-3.