

ОЦЕНКА КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АЭС: АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ СОВЕРШЕНСТВОВАНИЯ

Жарко Е.Ф.

Институт проблем управления им. В.А. Трапезникова РАН, Москва, Россия
zharko@ipu.ru

Аннотация. В статье рассматривается роль программного обеспечения (ПО) в обеспечении безопасности и эффективности функционирования атомных электростанций (АЭС). Анализируются актуальные проблемы оценки качества ПО для систем, важных для безопасности АЭС. Обсуждаются перспективные направления совершенствования процессов оценки качества.

Ключевые слова: АЭС, программное обеспечение, качество ПО, безопасность, верификация, валидация, стандарты.

Введение

Атомная энергетика, являясь одним из ключевых компонентов глобальной энергетической инфраструктуры, предъявляет высокие требования к надежности и безопасности. В этом контексте программное обеспечение (ПО), интегрированное в системы контроля, управления и защиты атомных электростанций (АЭС), приобретает статус критически важного элемента, от которого напрямую зависит не только эффективность производственных процессов, но и ядерная и радиационная безопасность объектов. Корректность функционирования, надежность и защищенность данного ПО напрямую детерминируют безопасность эксплуатации ядерных установок, эффективность предотвращения инцидентов и аварийных ситуаций, а также минимизацию их потенциальных радиологических и экономических последствий. По мере усложнения технологических процессов на АЭС, увеличения объемов обрабатываемой информации и расширения функциональности цифровых систем, зависимость от работы программных комплексов возрастает.

Актуальность проблемы оценки качества ПО для атомной энергетике экспоненциально возрастает в свете нескольких взаимосвязанных факторов. *Во-первых*, наблюдается ужесточение нормативных требований к безопасности, обусловленное как анализом предыдущих инцидентов в целом атомной отрасли, так и стремлением к достижению максимально возможного уровня защищенности. *Во-вторых*, современные информационно-управляющие системы АЭС характеризуются значительным увеличением сложности, гетерогенностью компонентов, использованием распределенных архитектур и необходимостью интеграции с системами различных поколений. *В-третьих*, увеличение киберугроз, направленных на объекты критической информационной инфраструктуры, ставит перед разработчиками и эксплуатирующими организациями новые вызовы в обеспечении информационной (компьютерной) безопасности программных продуктов. Эти факторы в совокупности формируют сложную научно-техническую задачу, требующую глубокого анализа и разработки адекватных методологических подходов к оценке качества ПО. Существующие подходы к верификации и валидации ПО, хотя и основаны на стандартах, могут не в полной мере соответствовать динамично меняющимся условиям и нарастающей сложности цифровых систем. Это порождает необходимость в непрерывном совершенствовании методологических основ, инструментальных средств и процедур оценки качества ПО, предназначенного для использования в критически важных системах АЭС.

1. Классификация программного обеспечения систем, важных для безопасности АЭС

Неотъемлемым элементом обеспечения ядерной и радиационной безопасности АЭС является строго регламентированный подход к разработке, внедрению и эксплуатации ПО, задействованного в системах, выполняющих функции безопасности или влияющих на их выполнение. Основопологающим этапом, определяющим уровень предъявляемых требований к качеству ПО и объему процедур его оценки, является классификация. Данная классификация детерминирует строгость регламентов на всех этапах жизненного цикла ПО, включая спецификацию требований, проектирование, кодирование, верификацию, валидацию, управление конфигурацией и сопровождение.

Программное обеспечение, применяемое на АЭС, классифицируется по степени его влияния на безопасность, что соответствует принципу дифференцированного подхода к обеспечению качества [1]. Международное агентство по атомной энергии (МАГАТЭ) в своих руководящих документах, таких как серия норм безопасности (например, IAEA Safety Standards Series No. SSG-39 [2]), предлагает методологические основы для такой классификации. В частности, SSG-39 рекомендует

классифицировать системы контроля и управления (СКУ) по категориям безопасности, что напрямую транслируется и на их программные компоненты. Типично выделяются категории А, В, и С (или аналогичные, например, классы 1, 2, 3), где принадлежность к категории определяется исходя из анализа последствий отказа данной системы или функции, выполняемой ПО.

Категория А (или Класс 1): К этой категории относится ПО, выполняющее функции, отказ которых может непосредственно привести к возникновению проектной аварии, нарушению пределов безопасной эксплуатации реакторной установки или невозможности выполнения первоочередных действий по управлению аварией. ПО данной категории реализует критически важные функции безопасности (например, срабатывание аварийной защиты реактора, активация систем аварийного охлаждения активной зоны).

Категория В (или Класс 2): Включает ПО, отказ которого не приводит напрямую к тяжелым последствиям, но может способствовать развитию неблагоприятных событий, усложнить выполнение функций безопасности системами категории А, или привести к нарушению нормальных условий эксплуатации, требующему вмешательства систем безопасности. Примерами могут служить ПО систем нормальной эксплуатации, или системы диагностики, предоставляющие информацию для принятия решений оперативным персоналом в условиях, предшествующих аварийным.

Категория С (или Класс 3): Относится ПО, отказ которого имеет минимальное или косвенное влияние на безопасность АЭС. Сюда могут входить вспомогательные системы, системы мониторинга параметров, не являющихся критическими для безопасности, или информационно-вычислительные системы общестанционного уровня, не связанные напрямую с управлением технологическими процессами, важными для безопасности.

Национальные регламенты и стандарты, такие как российские Нормы и Правила в атомной энергетике (НП), например, НП-001-15 [3] и НП-026-16 [4], также устанавливают жесткие требования к классификации систем и, соответственно, их программного обеспечения по влиянию на безопасность. Эти документы детализируют критерии отнесения элементов АС к классам безопасности и определяют соответствующие требования к их надежности и качеству.

Критичным для безопасности (часто соответствующим высшей категории А или Классу 1) считается ПО, отказ которого с высокой вероятностью или детерминированно может привести к нарушению одного или нескольких фундаментальных принципов обеспечения безопасности: управление цепной реакцией деления, отвод тепла от ядерного топлива и удержание радиоактивных веществ в установленных границах. К такому ПО относятся, например, программные модули систем управления и защиты реактора (СУЗ), включая алгоритмы формирования сигналов аварийной и предупредительной защиты; программы управления системами аварийного и планового расхолаживания; программное обеспечение систем контроля и управления системами безопасности (например, системами аварийного электроснабжения, системами локализации аварий); а также программы систем контроля радиационной обстановки, критически важные для оценки последствий и принятия решений в аварийных ситуациях.

Важно отметить, что классификация ПО не является статичной и может пересматриваться в случае модификации программного продукта, изменения его роли в системе или при получении новых данных о надежности и потенциальных последствиях отказа. Процесс классификации является основой для применения градуированного подхода к обеспечению качества: чем выше категория безопасности ПО, тем более строгие методы и средства должны применяться при его разработке, верификации, валидации и аттестации, включая требования к независимости экспертов, полноте тестирования, формальным методам доказательства корректности и документированию. Таким образом, корректная и обоснованная классификация ПО является краеугольным камнем в обеспечении безопасности эксплуатации АЭС.

2. Требования к качеству ПО для систем безопасности АЭС

Программное обеспечение, функционирующее в составе систем, важных для безопасности АЭС, подчиняется строгим и многоаспектным требованиям к качеству. Эти требования детерминируются потенциально катастрофическими последствиями отказов такого ПО и регламентируются международными (МАГАТЭ, МЭК) и национальными нормативными документами. Фундаментальным принципом является применение градуированного подхода, согласно которому строгость требований к качеству ПО и глубина его оценки коррелируют с классификацией системы по влиянию на безопасность. Ключевые атрибуты качества, рассматриваемые как императивы при разработке и эксплуатации такого ПО, включают:

- **Надежность (Reliability):** Данный атрибут определяет способность ПО безотказно выполнять специфицированные функции в заданных условиях эксплуатации на протяжении установленного интервала времени или для определенного числа операций. В контексте систем безопасности АЭС надежность ПО трансформируется в требование высокой степени уверенности в его предсказуемом и детерминированном поведении. Это подразумевает не только отсутствие явных дефектов кодирования, но и минимизацию вероятности проявления скрытых ошибок, способных привести к невыполнению или некорректному выполнению функций безопасности. Количественные показатели надежности ПО, где это применимо, должны быть обоснованы и соотнесены с общими целями безопасности АЭС, в том числе с результатами вероятностного анализа безопасности. Достижение требуемого уровня надежности обеспечивается совокупностью мер, включая формализацию требований, строгое следование методологиям разработки, статическое и динамическое тестирование, а также анализ предшествующего опыта эксплуатации аналогичных систем.
 - **Отказоустойчивость (Fault Tolerance):** Отказоустойчивость ПО характеризует его способность сохранять полную или частичную работоспособность, либо корректно переходить в предопределенное безопасное состояние при возникновении отказов взаимодействующих аппаратных компонентов, внешних систем или при обнаружении внутренних ошибок самого ПО. Для систем безопасности АЭС важно, чтобы ПО обладало механизмами обнаружения, локализации и нейтрализации последствий отказов. Это может достигаться за счет использования принципов резервирования (например, многоверсионное программирование, каналы с идентичным ПО на резервированном оборудовании), самодиагностики, алгоритмов восстановления после сбоев, а также реализации стратегий «безопасного отказа», гарантирующих перевод системы в состояние, не угрожающее безопасности станции.
 - **Корректность функционирования (Correctness):** Корректность представляет собой степень соответствия реализованного поведения ПО его функциональным и нефункциональным спецификациям, а также предписанным требованиям безопасности. Это включает точность выполнения алгоритмов и вычислений, правильность реализации логических условий и переходов состояний, а также своевременность реакции на управляющие воздействия и внешние события. Особое значение придается полноте и непротиворечивости исходных спецификаций. Для подтверждения корректности программных модулей могут применяться формальные методы верификации, доказывающие соответствие реализации математически строгим спецификациям, наряду с исчерпывающим тестированием, охватывающим все предусмотренные сценарии работы и граничные условия.
 - **Защищенность (Security and Safety assurance against unauthorized access and errors):** Данный комплексный атрибут охватывает как аспекты информационной безопасности (*cybersecurity*), так и аспекты предотвращения непреднамеренных ошибок, способных инициировать опасные сценарии.
 - **Информационная безопасность (Security):** Направлена на обеспечение целостности, доступности и, при необходимости, конфиденциальности программного кода, данных и управляющих команд от несанкционированного доступа, модификации или деструктивного воздействия, включая кибератаки. Меры по обеспечению информационной безопасности включают управление доступом, аутентификацию, шифрование, обнаружение вторжений, а также разработку ПО с учетом принципов безопасного кодирования.
 - **Защита от непреднамеренных ошибок (Safety assurance against errors):** Подразумевает наличие в ПО механизмов, предотвращающих или минимизирующих последствия ошибок оперативного персонала, сбоев при вводе данных или некорректного взаимодействия с системой. Это достигается путем тщательного проектирования пользовательских интерфейсов, реализации проверок вводимых данных на допустимость и правдоподобность, а также использования систем поддержки принятия решений.
- Помимо указанных атрибутов самого ПО, требования предъявляются к процессам его жизненного цикла. Регламентация охватывает все стадии: от инициации проекта, формирования и анализа требований, проектирования архитектуры и детального проектирования, кодирования и тестирования модулей, интеграции компонентов, комплексного тестирования системы до ввода в эксплуатацию, сопровождения (включая управление изменениями и исправление дефектов), модернизации и, в конечном итоге, вывода из эксплуатации. Центральное место в процессах жизненного цикла занимают:
- **Верификация и валидация (V&V):** Систематические процессы, проводимые на каждом этапе жизненного цикла с целью подтверждения того, что разрабатываемый продукт (требования, проект, код) соответствует своим спецификациям (верификация) и что конечный продукт удовлетворяет

потребностям пользователя и предназначенному использованию в реальных условиях эксплуатации (валидация). Для ПО систем безопасности часто требуется независимая верификация и валидация (IV&V).

- **Управление конфигурацией** (*Configuration Management*): Процесс идентификации компонентов ПО и аппаратных средств, контроля изменений этих компонентов, регистрации и отслеживания статуса изменений, а также аудита конфигурации для обеспечения ее целостности и соответствия документации.
- **Документирование** (*Documentation*): Создание и поддержание в актуальном состоянии полного комплекта документации, описывающей все аспекты ПО и его жизненного цикла, включая спецификации требований, проектную документацию, исходный код с комментариями, планы и отчеты по тестированию, руководства пользователя и по эксплуатации.
- **Обеспечение прослеживаемости** (*Traceability*): Возможность отслеживания связей между требованиями, элементами проекта, кодом, тестовыми случаями и результатами тестирования в обоих направлениях. Прослеживаемость является ключевым инструментом для анализа влияния изменений и оценки полноты покрытия требований.

Соблюдение этих строгих требований к качеству ПО и процессам его жизненного цикла является фундаментальной предпосылкой для обеспечения безопасной и надежной эксплуатации АЭС. Это требует высокой квалификации разработчиков, применения передовых методологий и средств разработки, а также формирования соответствующей культуры безопасности на всех уровнях организации, вовлеченной в создание и эксплуатацию ПО для АЭС.

3. Методики и подходы к оценке качества ПО

Оценка качества программного обеспечения, предназначенного для использования в системах контроля и управления (СКУ) АЭС, представляет собой сложную, многоаспектную задачу, требующую применения комплексного и строго регламентированного методологического аппарата. Фундаментом для такой оценки служит иерархическая система международных и национальных стандартов, определяющих требования к жизненному циклу ПО и критерии его соответствия.

Ключевыми международными стандартами, устанавливающими нормативы для ПО систем, важных для безопасности (СВБ), являются:

- **IEC 60880:2006** [5], определяющий наиболее строгие требования к ПО, отказ которого может привести к тяжелым последствиям.
- **IEC 62138:2018** [6], регламентирующий требования к ПО систем с менее критичными, но все же важными для безопасности функциями.
- **IEEE Std 7-4.3.2** [7], который дополняет стандарты МЭК, фокусируясь на критериях для компьютерных систем, используемых в системах безопасности.

В Российской Федерации разработана и внедрена система национальных стандартов, например, серия ГОСТ Р МЭК, которые гармонизированы с вышеуказанными международными документами, обеспечивая единство подходов и требований на национальном уровне. Эти стандарты формируют нормативную базу, определяющую как процессы разработки, так и методы оценки качества конечного программного продукта.

Методологическая база оценки качества ПО для АЭС включает в себя совокупность взаимодополняющих подходов, направленных на всестороннее исследование программных артефактов и процессов их создания:

- **Формальные методы.** Данная группа методов основана на использовании математически строгих нотаций для описания спецификаций требований, архитектуры и алгоритмов ПО, а также для формального доказательства их корректности и соответствия заданным свойствам, включая свойства безопасности. Применение формальных методов, таких как аксиоматическая семантика, теория моделей или абстрактная интерпретация, позволяет с высокой степенью достоверности верифицировать критически важные аспекты поведения ПО. Несмотря на значительную трудоемкость и необходимость высокой квалификации специалистов, роль формальных методов неуклонно возрастает, особенно при разработке и аттестации программных модулей, отнесенных к наивысшим классам безопасности, где цена ошибки недопустимо высока [8].
- **Верификация и Валидация (V&V).** Процессы верификации и валидации являются неотъемлемой частью жизненного цикла ПО СВБ и осуществляются на всех его этапах.
 - **Верификация** представляет собой процесс подтверждения того, что разрабатываемое ПО на каждом этапе жизненного цикла соответствует требованиям, определенным на предыдущем

этапе, и спецификациям данного этапа. Иными словами, верификация отвечает на вопрос: «Правильно ли мы создаем продукт?». Ключевыми активностями верификации являются инспекции, формальные технические обзоры, сквозные проверки, анализ трассируемости требований, а также статический анализ.

- **Валидация** – это процесс подтверждения того, что разработанное ПО соответствует своему назначению, то есть удовлетворяет требованиям конечного пользователя и выполняет поставленные задачи в предполагаемых условиях эксплуатации, включая обеспечение требуемого уровня безопасности. Валидация отвечает на вопрос: «Создаем ли мы правильный продукт?». Основным инструментом валидации является динамический анализ, включая всестороннее тестирование.

Деятельность по V&V документируется в соответствующих планах и отчетах, обеспечивая прозрачность и контролируемость процессов оценки [9, 10].

- **Статический анализ.** Этот метод включает анализ исходного кода, объектного кода и сопутствующей документации без фактического выполнения программы. Целью статического анализа является выявление потенциальных дефектов, аномалий, уязвимостей (например, переполнение буфера, некорректное управление памятью), отклонений от стандартов кодирования и метрик сложности кода. Для проведения статического анализа широко применяются специализированные программные инструменты – статические анализаторы кода, которые могут автоматически обнаруживать множество типовых ошибок и проблемных конструкций. Важным аспектом является квалификация используемых инструментов статического анализа в соответствии с требованиями стандартов.
- **Динамический анализ.** Динамический анализ предполагает исследование поведения ПО непосредственно во время его выполнения на целевой или моделирующей платформе. Центральным компонентом динамического анализа является тестирование, которое в контексте ПО для АЭС носит исчерпывающий и многоуровневый характер:
 - **Модульное (компонентное) тестирование:** проверка корректности функционирования отдельных программных модулей или компонентов в изоляции.
 - **Интеграционное тестирование (Интеграционные испытания):** проверка взаимодействия между модулями и компонентами системы.
 - **Системное тестирование:** проверка соответствия всей интегрированной системы исходным функциональным и нефункциональным требованиям, включая требования безопасности и надежности.
 - **Приемочное тестирование (Приемочные испытания):** формальный процесс, демонстрирующий заказчику и регулирующим органам, что система соответствует всем специфицированным требованиям и готова к эксплуатации.
 - **Регрессионное тестирование:** проводится после внесения изменений в ПО или его окружение для подтверждения того, что модификации не привели к появлению новых дефектов или повторному возникновению устраненных ранее.

Особое внимание при динамическом анализе уделяется достижению максимальной полноты покрытия кода (например, покрытие операторов, ветвей, условий) и покрытия требований. Для этого разрабатываются детальные тестовые сценарии и используются различные методики тест-дизайна (например, анализ граничных значений, классы эквивалентности, и т.д.). Тестирование может проводиться в эмулированной или симулированной среде, а также с использованием технологии «аппаратно-программного тестирования» [11].

- **Аудит качества ПО.** Аудит представляет собой независимую систематическую проверку процессов разработки, эксплуатации ПО, а также всей сопутствующей документации на предмет их соответствия установленным требованиям, стандартам, планам и процедурам. Аудиты могут быть внутренними (проводимыми силами самой организации) или внешними (проводимыми заказчиком, регулирующими органами или независимыми аккредитованными организациями). Результаты аудитов служат основой для принятия решений о соответствии ПО, выявления областей для улучшения и подтверждения эффективности системы менеджмента качества разработчика.

Интегрированное применение перечисленных методик и подходов, подкрепленное строгим соблюдением процедур управления конфигурацией, управления изменениями и управления документацией, позволяет сформировать убедительные доказательства того, что ПО для АЭС обладает требуемым уровнем качества и способно безопасно выполнять свои функции в течение всего жизненного цикла.

4. Проблемы и вызовы современной практики оценки качества

Современная практика оценки качества программного обеспечения, предназначенного для применения в системах контроля, управления и защиты АЭС, сталкивается с комплексом взаимосвязанных проблем и вызовов. Эти вызовы обусловлены как спецификой самой атомной отрасли, характеризующейся высочайшими требованиями к безопасности и надежности, так и общими тенденциями развития информационных технологий.

- **Экстремально высокая цена ошибки и требование «нулевой терпимости» к дефектам.** Любой отказ или некорректное функционирование ПО в системах, важных для безопасности АЭС, потенциально способен инициировать развитие аварийных ситуаций с катастрофическими последствиями. Это детерминирует необходимость достижения высокого уровня надежности, сопоставимого с принципом «нулевой терпимости» к дефектам в компонентах, непосредственно влияющих на ядерную и радиационную безопасность. Следовательно, процессы верификации и валидации ПО должны обеспечивать максимальную тщательность, полноту покрытия и использование наиболее строгих методов анализа, включая, где это применимо, формальные методы доказательства корректности.
- **Имманентная сложность и масштаб современных информационно-управляющих систем (ИУС) АЭС.** ИУС АЭС представляют собой сложные, многоуровневые, распределенные и зачастую гетерогенные человеко-машинные системы. Они характеризуются значительным объемом программного кода, большим количеством взаимодействующих компонентов, сложными алгоритмами управления технологическими процессами в реальном времени и интенсивными информационными потоками. Всесторонняя оценка качества таких систем затруднена экспоненциальным ростом пространства состояний, сложностью моделирования всех возможных сценариев взаимодействия и выявления скрытых дефектов, проявляющихся только при специфических комбинациях входных данных и состояний системы. Это создает серьезные вызовы для методик тестирования, отладки и анализа покрытия.
- **Длительный жизненный цикл ПО и проблемы обеспечения долгосрочной поддержки.** Программное обеспечение на АЭС проектируется и эксплуатируется на протяжении десятилетий, что значительно превышает типичные сроки жизни ПО в других отраслях. Это порождает комплекс проблем, связанных с необходимостью поддержания его актуальности, функциональной совместимости с модернизируемым технологическим оборудованием и обновляемыми программно-аппаратными платформами. Особую остроту приобретают вопросы управления конфигурацией, регрессионного тестирования при внесении изменений, управления старением как программных, так и аппаратных компонентов, а также обеспечения кибербезопасности на протяжении всего эволюционирующего жизненного цикла.
- **Гетерогенность технологического ландшафта и интеграционные вызовы.** На действующих АЭС зачастую одновременно эксплуатируются как унаследованные системы, разработанные несколько десятилетий назад с использованием устаревших технологий и парадигм программирования, так и современные цифровые платформы, основанные на сервисно-ориентированных архитектурах, технологиях промышленного интернета вещей и элементах искусственного интеллекта. Интеграция этих разнородных систем, обеспечение их корректного взаимодействия и выработка унифицированных подходов к оценке качества представляют собой нетривиальную инженерную и методологическую задачу.
- **Ограничения существующих методов и средств автоматизации оценки качества.** Несмотря на значительный прогресс в разработке инструментальных средств статического и динамического анализа кода, средств автоматизированного тестирования и моделирования, многие аспекты оценки качества ПО для АЭС по-прежнему требуют значительного объема труда высококвалифицированных экспертов. Это особенно актуально для верификации сложных нефункциональных требований (например, к производительности в реальном времени, отказоустойчивости, безопасности), а также для анализа уникальных, нетиповых архитектурных решений. Полностью автоматизировать процесс доказательства соответствия ПО всем требованиям безопасности для критически важных систем зачастую невозможно или экономически нецелесообразно, что подчеркивает сохраняющуюся роль экспертных оценок.
- **Трудоемкость процессов документирования и подтверждения соответствия требованиям регуляторов.** Формирование полного, корректного, непротиворечивого и прослеживаемого комплекта нормативно-технической, проектной, эксплуатационной и тестовой документации, однозначно доказывающего соответствие ПО всем установленным требованиям, является

чрезвычайно трудоемким и ресурсозатратным процессом. Обеспечение прослеживаемости требований от исходных спецификаций до конкретных модулей кода и тестовых случаев требует высокой дисциплины и применения специализированных инструментов управления требованиями и конфигурациями. Любые неточности или пробелы в документации могут стать препятствием для лицензирования и ввода систем в эксплуатацию.

- **Дефицит и специфика квалификации экспертных кадров (человеческий фактор).** Разработка, верификация, валидация и экспертиза ПО для АЭС требуют от специалистов уникального сочетания компетенций: глубоких знаний в области ядерной физики и технологий, специфики технологических процессов АЭС, современных методов программной инженерии, стандартов безопасности и регулирования в атомной отрасли. Подготовка таких специалистов является длительным и дорогостоящим процессом, и их дефицит является существенным ограничивающим фактором. Кроме того, сохраняется риск человеческой ошибки на всех этапах жизненного цикла ПО, что обуславливает необходимость внедрения многоуровневых систем контроля, независимой верификации и валидации (IV&V), а также постоянного повышения квалификации персонала.

Таким образом, эффективное решение указанных проблем требует комплексного подхода, сочетающего совершенствование методологической базы оценки качества, разработку и внедрение передовых инструментальных средств, развитие нормативно-правовой базы, а также целенаправленную подготовку и привлечение высококвалифицированных специалистов.

5. Передовые технологии и перспективные направления развития

Совершенствование методологии и инструментария оценки ПО для АЭС неразрывно связано с интеграцией передовых информационных технологий и развитием существующих подходов. Эти инновации призваны повысить объективность, полноту и эффективность процессов верификации и валидации, а также снизить трудоемкость и вероятность человеческой ошибки.

Одним из наиболее перспективных направлений является **использование искусственного интеллекта (ИИ) и машинного обучения (МО)**. Интеграция технологий ИИ и МО открывает перспективы для существенной автоматизации трудоемких этапов тестирования, включая интеллектуальную генерацию тестовых сценариев на основе моделей поведения системы или исторических данных о дефектах, а также автоматизированный анализ результатов выполнения тестов с классификацией сбоя. Алгоритмы МО могут применяться для выявления аномалий в поведении программных систем в реальном времени или при анализе лог-файлов, что особенно актуально для систем мониторинга и диагностики АЭС. Предиктивная оценка качества, основанная на анализе метрик кода, процесса разработки и данных о предыдущих дефектах, позволяет проактивно идентифицировать модули с высоким риском и концентрировать на них усилия по тестированию. Анализ больших объемов эксплуатационных данных и логов функционирования ПО с применением МО может способствовать выявлению скрытых паттернов и корреляций, указывающих на потенциальные проблемы или области для улучшения. При этом особое внимание должно уделяться вопросам интерпретируемости и валидации моделей ИИ, применяемых в системах важных для безопасности, для обеспечения доверия к их результатам и соответствия требованиям безопасности.

Дальнейшее **развитие формальных методов** также остается ключевым направлением. Формальные методы, основанные на строгом математическом аппарате, предоставляют наиболее высокий уровень гарантий корректности ПО относительно его спецификаций. Несмотря на их доказанную эффективность, широкое применение сдерживается сложностью и трудоемкостью. Перспективным направлением является повышение уровня автоматизации процессов формальной верификации, например, через развитие более мощных алгоритмов проверки моделей и символического выполнения, а также создание интуитивно понятных и интегрированных в общую среду разработки инструментальных средств. Целью является расширение области применения формальных методов от наиболее критичных модулей к более широкому спектру компонентов ПО автоматизированных систем управления технологическими процессами (АСУ ТП) АЭС, что позволит на ранних этапах разработки доказывать отсутствие определенных классов ошибок.

Существенный потенциал заложен в **моделировании и симуляции**, в частности, в применении методологии **модельно-ориентированной системной инженерии (МОСИ) и концепции цифровых двойников**. МОСИ позволяет создавать формализованные модели системы, включая ее ПО, на ранних этапах жизненного цикла. Такие модели служат основой для ранней верификации требований, анализа архитектурных решений и автоматической генерации части кода или тестовых сценариев, способствуя «сдвигу влево» активностей по обеспечению качества. Дальнейшее развитие этой концепции – создание цифровых двойников объектов АЭС и их систем управления. Цифровые двойники

обеспечивают возможность проведения всесторонних испытаний ПО в виртуальной среде, максимально приближенной к реальным условиям эксплуатации, включая симуляцию отказов оборудования и нештатных ситуаций. Это позволяет не только верифицировать ПО в контексте всей системы, но и валидировать его поведение в динамике, существенно снижая риски на этапе ввода в эксплуатацию и при модернизации.

Продолжается совершенствование методов **углубленного статического и динамического анализа кода**. Традиционные методы являются неотъемлемой частью процесса оценки качества, однако сложность современного ПО требует разработки и внедрения более изощренных инструментальных средств. Это включает развитие техник символьного и конколического выполнения для генерации тестовых данных, покрывающих сложные пути исполнения, продвинутые методы анализа потоков данных и управления для выявления уязвимостей типа «гонка состояний», «переполнение буфера» или «некорректная обработка входных данных». Особое внимание уделяется анализу на предмет соответствия стандартам безопасного кодирования и выявления потенциальных киберуязвимостей, что критически важно для защиты АСУ ТП от внешних и внутренних угроз.

Важным аспектом является заимствование и адаптация зарубежного опыта. Атомная отрасль является глобальной, и многие вызовы в области обеспечения качества и безопасности ПО являются общими для разных стран. Активное изучение, критический анализ и адаптация международных стандартов (например, серии IEC 61508 “*Functional safety of electrical/electronic/programmable electronic safety-related systems*”, IEC 60880 [5], ISO/IEC/IEEE 29119 “*Software and systems engineering – Software testing*”, ISO/IEC 25000 “*Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE)*”) и лучших практик, накопленных в других высокотехнологичных отраслях с повышенными требованиями к надежности (например, аэрокосмическая, медицинская), является значимым фактором совершенствования подходов. При этом необходима тщательная адаптация с учетом национальной нормативной базы, специфики используемых технологических платформ и организационных особенностей предприятий атомной отрасли.

Наконец, адаптация практик непрерывной интеграции и поставки (*CI/CD*) с усиленными мерами безопасности (*DevSecOps*) представляет собой перспективное направление для повышения эффективности и оперативности процессов разработки и оценки качества ПО. Методологии *CI/CD*, доказавшие свою эффективность в коммерческой разработке, требуют существенной адаптации для применения в условиях строгих регламентов атомной отрасли. Речь идет о внедрении практик *DevSecOps*, где задачи обеспечения качества и безопасности интегрируются на всех этапах жизненного цикла ПО, начиная с самых ранних. Это подразумевает максимальную автоматизацию процессов сборки, всестороннего тестирования (включая статический анализ безопасности – *SAST*, динамический анализ безопасности – *DAST*, интерактивный анализ безопасности – *IAST*), верификации и валидации, с обязательным применением строгих процедур контроля конфигурации, управления изменениями и исчерпывающего документирования каждого этапа. Такой подход позволяет не только ускорить циклы разработки и обновления ПО, но и обеспечить непрерывный мониторинг его качества и безопасности, оперативно реагируя на выявленные несоответствия.

Комплексное внедрение и развитие указанных направлений способно качественно трансформировать процессы оценки ПО для АЭС, обеспечивая требуемый уровень надежности и безопасности критически важных систем.

6. Практические рекомендации по совершенствованию оценки качества ПО для АЭС

Для повышения эффективности и обеспечения должной глубины оценки качества программного обеспечения, применяемого на атомных электростанциях, представляется целесообразным реализация комплекса взаимосвязанных мер, направленных на совершенствование существующих подходов и внедрение передовых практик. Данные рекомендации охватывают нормативно-методологические, кадровые, технологические, организационные и культурные аспекты.

- **Совершенствование нормативно-методической базы.** Ключевым направлением является перманентная актуализация и гармонизация национальной нормативно-методической базы с учетом передового международного опыта, в частности, стандартов и руководств МАГАТЭ (например, серии документов по безопасности АЭС, включая аспекты компьютерных систем), МЭК (например, стандарты IEC 60880 [5], IEC 61508, IEC 61513 [12], IEC 62138 [6]), IEEE и других профильных организаций. Необходимо обеспечивать разработку детализированных методических указаний, регламентирующих процедуры оценки специфических атрибутов качества ПО, критически важных для АЭС. К таким атрибутам относятся, прежде всего, кибербезопасность

(включая устойчивость к целенаправленным атакам и непреднамеренным угрозам), надежность (включая отказоустойчивость и восстанавливаемость), функциональная безопасность, а также устойчивость к ошибкам оператора и эргономичность человеко-машинного интерфейса. Особое внимание следует уделить методикам оценки ПО, разработанного с применением новых технологий, таких как искусственный интеллект, машинное обучение или формальные методы.

- **Внедрение и освоение современных инструментальных средств и технологий.** Современный уровень сложности ПО для АЭС требует применения высокотехнологичных инструментальных средств для всестороннего анализа и тестирования. Необходимо освоение и планомерное внедрение программных комплексов для статического (*Static Application Security Testing, SAST*), динамического (*Dynamic Application Security Testing, DAST*) и интерактивного (*Interactive Application Security Testing, IAST*) анализа безопасности кода, систем управления тестированием (*Test Management System, TMS*), средств управления требованиями (*Requirements Management Systems, RMS*) и конфигурацией ПО (*Software Configuration Management, SCM*). Важное значение приобретают технологии автоматизированного тестирования, включая модельно-ориентированное тестирование (*Model-Based Testing, MBT*), фаззинг-тестирование (разновидность выборочного тестирования) для выявления уязвимостей, а также применение инструментов для формальной верификации критически важных алгоритмов и компонентов ПО. Использование интегрированных платформ разработки и тестирования, поддерживающих практики DevSecOps, способствует повышению эффективности и прозрачности процессов.
- **Усиление роли и механизмов независимой экспертизы и аудита.** Принцип независимости является фундаментальным для обеспечения объективности оценки качества ПО, особенно для систем, классифицируемых по высшим категориям безопасности. Необходимо расширение практики привлечения аккредитованных независимых экспертных организаций для проведения верификации, валидации и аудита ПО на всех ключевых этапах его жизненного цикла, начиная с анализа требований и заканчивая приемочными испытаниями и вводом в эксплуатацию. Должны быть разработаны четкие критерии для проведения такой экспертизы, а ее результаты должны иметь определяющее значение при принятии решений о допуске ПО к эксплуатации. Периодический независимый аудит уже эксплуатируемого ПО также является важным элементом поддержания его соответствия требованиям безопасности.
- **Развитие и поддержание культуры безопасности и качества.** Технические и организационные меры не дадут должного эффекта без формирования и поддержания высокого уровня культуры безопасности и качества во всех организациях, вовлеченных в процессы разработки, поставки, внедрения и эксплуатации ПО для АЭС. Эта культура должна базироваться на приверженности руководства принципам безопасности, четком распределении ответственности, поощрении инициативы по выявлению и устранению недостатков, а также на системе открытого информирования об инцидентах и извлечения уроков. Качество и безопасность ПО должны рассматриваться как безусловный приоритет на всех уровнях управления и исполнения.
- **Интеграция процессов обеспечения и контроля качества на ранних этапах жизненного цикла ПО.** Эффективная стратегия оценки качества предполагает смещение акцента с выявления дефектов на поздних стадиях (тестирование готового продукта) на превентивные меры и раннее обнаружение несоответствий. Это требует глубокой интеграции процессов обеспечения и контроля качества, начиная с этапа формирования и анализа требований к ПО, его проектирования и архитектурной разработки. Применение методик верификации требований, статического анализа проектных решений, прототипирования и раннего моделирования позволяет выявлять и устранять потенциальные проблемы на этапах, когда стоимость их исправления минимальна. Практики непрерывной интеграции и поставки (*CI/CD*) с встроенными механизмами контроля качества и безопасности (*Security by Design, Quality by Design*) должны стать стандартом для разработки ПО АЭС.

На рис. 1 показана организация рекомендаций в логические группы (ранние этапы, разработка, интеграция), при этом сквозные принципы пронизывают все уровни. На рис. 2 представлена взаимосвязь между практиками в рамках концепции «смещения влево» с целью повышения доверия, безопасности и надежности ПО. Основная стратегия концепции «Смещение влево» – перенос фокуса и активности на ранние этапы жизненного цикла (Требования, Проектирование). Методы, используемые на ранних этапах, направлены на раннее выявление дефектов и снижение затрат на их исправление. Принципы «Безопасности через проектирование» и «Качество через проектирование» — это сквозные принципы, которые должны быть интегрированы на всех этапах жизненного цикла, но начинают они функционировать с самых ранних фаз жизненного цикла основываясь на требованиях и

архитектуре. Практики непрерывной интеграции и поставки являются механизмом для автоматизации и частой проверки качества и безопасности. Эти практики начинают работать на этапе разработки, но опираются на качественные требования и архитектуру, разработанные на ранних этапах жизненного цикла программного обеспечения, и включают в себя автоматизированные проверки безопасности и качества.

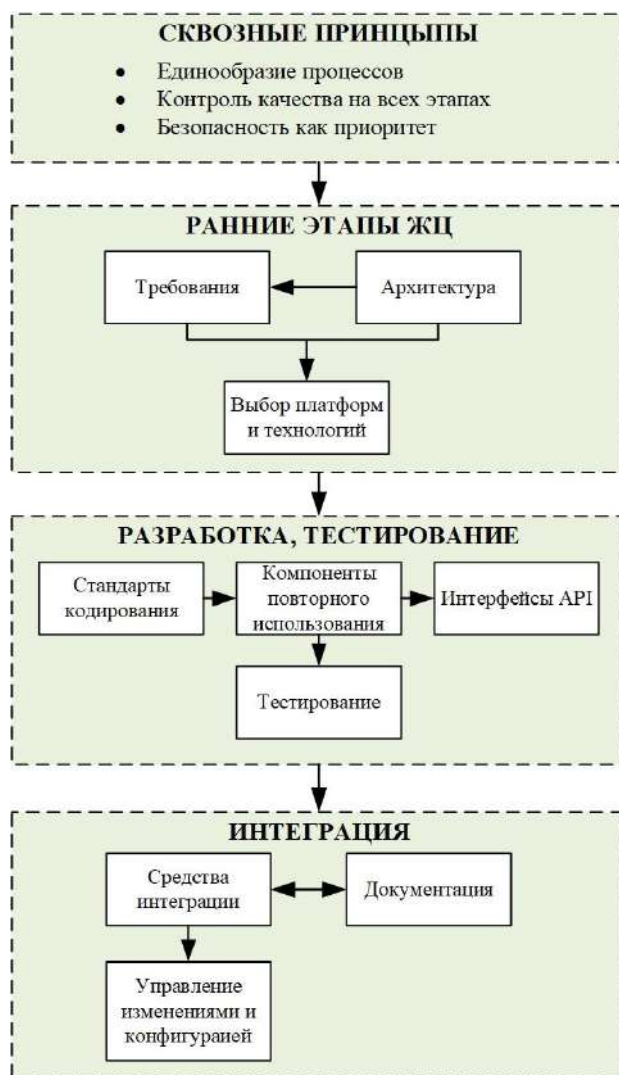


Рис. 1. Организация практик в логические группы



Рис. 2. Взаимосвязь между практиками в рамках концепции «смещения влево»

Наряду с концепцией «смещение влево» существует и комплементарный ему подход «Смещение вправо», который подразумевает тестирование программного обеспечения в реальной производственной среде с участием реальных пользователей. Если концепция «Смещение влево» направлена на предотвращение дефектов, то подход «Смещение вправо» фокусируется на сборе данных о поведении, производительности и надежности программного обеспечения в условиях эксплуатации. Подход «Смещение вправо» позволяет выявлять проблемы, которые невозможно или крайне сложно смоделировать в тестовых окружениях, например, связанные с уникальными конфигурациями оборудования, сетевыми задержками или непредвиденными сценариями использования. Подход «Смещение вправо» важно применять при подготовке требований к модернизации.

7. Заключение

Стоит отметить, что современное обеспечение качества программного обеспечения — это комплексная, многоуровневая дисциплина, интегрированная во все этапы жизненного цикла. Она эволюционировала от простого поиска ошибок к проактивному управлению рисками, оптимизации процессов и внедрению культуры разработки, где качество является общей целью и зоной ответственности.

Реализация предложенных рекомендаций в комплексе позволит существенно повысить уровень доверия к программному обеспечению, используемому в системах управления и контроля на атомных электростанциях, и, как следствие, внести значимый вклад в обеспечение их безопасной и надежной эксплуатации.

Литература

1. *Жарко Е.Ф.* Оценка качества программного обеспечения для систем, важных для безопасности АЭС // Информационные технологии и вычислительные системы. – 2011. – № 3. – С. 38–44.
2. IAEA Safety Standards Series No. SSG-39 – Design of Instrumentation and Control Systems for Nuclear Power Plants. – International Atomic Energy Agency, Vienna, 2016. – 184 p.
3. Общие положения безопасности атомных станций (НП-001-15) // Ядерная и радиационная безопасность. – 2016. – № 1(79). – С. 39–62.
4. Требования к управляющим системам, важным для безопасности атомных станций. НП-026-16 // Ядерная и радиационная безопасность. – 2017. – № 1(83). – С. 27–41.
5. IEC 60880:2006. Nuclear power plants – Instrumentation and control systems important for safety – Software aspects for computer-based systems performing category A functions. – International Electrotechnical Commission, Geneva, SW, 2006. – 217 p.
6. IEC 62138:2018. Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions. – International Electrotechnical Commission, Geneva, SW, 2018. – 106 p.
7. IEEE Std 7-4.3.2-2016. IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations. – IEEE, 2016. – 86 p.
8. *Buzhinsky I., Pakonen A., Vyatkin V.* Explicit-state and symbolic model checking of nuclear I&C systems: A comparison // IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 2017. – P. 5439–5446.
9. IEEE Std 1012-2016. IEEE Standard for System, Software, and Hardware Verification and Validation. – IEEE, 2017. – 260 p.
10. Technical Reports Series № 384 – Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control. – International Atomic Energy Agency, Vienna. 1999. – 126 p.
11. *Panicucci P., Ornati F., Topputo F.* Design of a Low-Aberration Variable-Magnification Optical Stimulator for Vision System Hardware-in-The-Loop Testing // IEEE Transactions on Aerospace and Electronic Systems. – IEEE, 2025. – P. 1–12.
12. IEC 61513:2011. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems. – International Electrotechnical Commission, Geneva, SW, 2011. – 205 p.