ЯКІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

УДК 004. 415.2.045

А.А. Орехова, В.С. Харченко
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

НОРМАТИВНАЯ БАЗА И ОЦЕНКА КАЧЕСТВА ЧЕЛОВЕКО-МАШИННЫХ ИНТЕРФЕЙСОВ ИУС АЭС НА ОСНОВЕ SAFETY CASE МЕТОДОЛОГИИ

Проанализированы проблемы, связанные с обеспечением безопасности человеко-машинных интерфейсов информационно-управляющих систем АЭС. Предложен подход для оценки безопасности ЧМИ ИУС АЭС, основанный на методологи Safety Case. Представлена профилеобразующая база требований к качеству ЧМИ. Описан пример оценки качества ЧМИ.

Проаналізовано проблеми, пов'язані із забезпеченням безпеки людино-машинних інтерфейсів інформаційно-керуючих систем АЕС. Розглянуто підхід для оцінки безпеки ЛМІ ІКС АЕС, заснований на методології Safety Case. Запропонована профілеутворювальна база вимог до якості ЛМІ. Наданий приклад якості ЛМІ.

The problems associated with safety of human-machine interfaces, information and control systems in NPP are analyzed.. An approach to assess the safety HMI I&C system NPP, based on Safety Case methodology is proposed. The profile of standards for HMI quality requirements is presented. An example of HMI quality assessment is described.

Ключевые слова: человеко-машинный интерфейс, информационно-управляющие системы, АЭС, качество, безопасность

Введение.

Проблема безопасности и качество человеко-машинных интерфейсов

Модернизация и продление ресурса реакторов атомных электростанций (АЭС) требует разработки и внедрения новых информационно-управляющих систем (ИУС) [1–3]. Их безопасность зависит от качества человеко-машинных интерфейсов (ЧМИ). Для предотвращения ошибок операторов ЧМИ необходимо проектировать с учетом требований к безопасности ИУС. Современные подходы к проектированию ЧМИ ориентированы на пользователя, его цели и задачи. В процессе проектирования ЧМИ этап оценки качества занимает центральное место и обязан выполняться после каждого этапа проектирования. Известные методы оценки ЧМИ слабо формализованы и ориентированы, главным образом, на оценку эффективности, производительности и субъективной удовлетворенности пользователя. В то же время для критических приложений, таких как ИУС АЭС, важным направлением исследований является разработка моделей, методов, инженерных методик, а также инструментальных средств оценки безопасности ЧМИ.

Безопасность оценивает уровень риска, вреда людям, бизнесу, программному обеспечению, собственности или окружающей среде. В стандарте ISO 9126-4 безопасность определяется как субхарактеристика качества в использовании программных систем [4].

Анализ материалов конференций ICONE18 (Китай,2010) и NPIC-HMIT (США, 2008,2010) [5,6], других источников показал, что актуальными в области ЧМИ в настоящее время являются: исследования человеческого фактора с целью уменьшения вероятности ошибок и повышения качества и эффективности работы; оценка действий операторов и влияния цифровых систем на его работу; анализ человеческой надежности; оценка интерфейсов на основе анализа результатов работы операторов; оценка работоспособности интерфейса на основе мо-

дели человеческих познавательных процессов; анализ минимального оборудования необходимого оператору для выполнения действий, связанных с риском и учетом оценки возможных последствий; разработка правил и контрольных списков для экспертной оценки критических функций безопасности, рискованно важных задач, критических человеческих действий.

При оценке безопасности ИУС АЭС, других критических систем и их программного обеспечения получил распространение подход, основанный на методологии Safety Case (MSC), методы и средства, реализации которой проанализированы в [7]. Она предполагает комплексную, трассированную от детализированных требований до документированных по определенному шаблону результатов оценку безопасности системы и ее ПО «под ключ».

Эта оценка поддерживается специальными инструментальными средствами. Как показывает анализ публикаций, вопросы оценки влияния качества ЧМИ на безопасность в рамках MSC в известных работах не рассматривался.

Цель данной работы – адаптация известной модели оценки, базирующейся на Safety Case методологии и принципах, изложенных в [7], а также постановка задачи оценивания безопасности ЧМИ путем нечеткого многокритериального анализа вариантов [8,9].

Для достижения этой цели необходимо решить следующие задачи:

– определить и исследовать сценарии задач оператора, наиболее важных для безопасности АЭС;

– изучить отношение между задачей и риском в контексте выполняемых сценариев;

– проанализировать механизмы, посредством которых может повышаться риск в условиях отвлечения и снижения осведомленности оператора о ситуации;

– определить показатели, которые наилучшим образом позволят оценить безопасность ЧМИ;

– выбрать наиболее эффективные методы для оценки безопасности ЧМИ на различных этапах жизненного цикла.

1 Методология оценки безопасности

1.1 Исходные положения. Следует подчеркнуть, что уже на начальном этапе проектирования необходимо выбрать критерии, которые позволят оценить наиболее удачную концепцию ЧМИ с точки зрения безопасности при ее использовании в реальных условиях. Оценка безопасности на основе методологии Safety Case подразумевает формальное представление доказательств, доводов и предположений, направленных на обеспечение гарантии того, что система отвечает требованиям безопасности, и требования безопасности являются адекватными [10].

На начальном этапе анализа проекта внимание должно быть уделено логическим аргументам, которые будут использованы, чтобы продемонстрировать, что система безопасна в использовании. Это может быть выполнено, например, с помощью построения структуры целей, как показано на рис. 1.

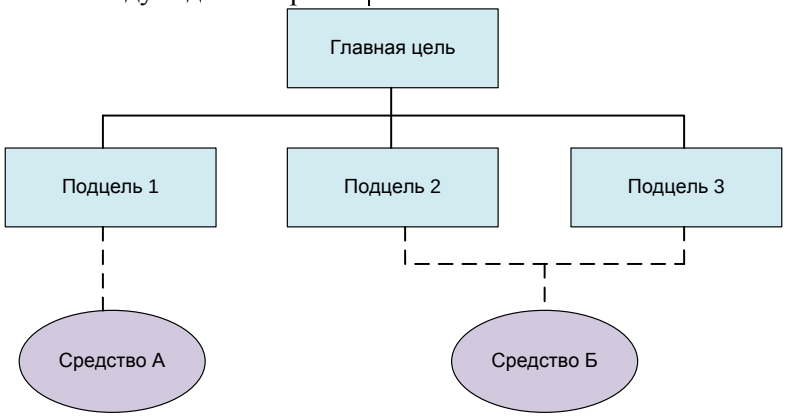

Рис. 1. Структура целей

Цель (которая может быть интерпретирована как проверка требования) делится на подцели до тех пор, пока не будут определены средства, которые могут продемонстрировать, что подцель достигнута. Эти средства затем используются для проверки безопасности в процессе разработки системы.

На рис. 2 приведена другая нотация, которая также может быть использована для представления обоснования безопасности. Альтернативный метод состоит в использовании диаграммы Утверждение-Аргумент-Доказатель-

ство. В качестве доказательства в этом методе могут выступать, например, результаты некоторых тестов, созданных в процессе разработки для поддержки утверждений нижнего уровня (sub-claims). Эти утверждения затем принимают участие, как аргументы, демонстрирующие правильность утверждения верхнего уровня.

Важно, чтобы план создания Safety Case был составлен в самом начале процесса проектирования. Это позволит определить, во-первых, какие необходимо собрать доказательства и, во-вторых, что необходимо использовать для их поддержки на различных этапах жизненного цикла. Одной из проблем является выбор глубины и строгости доказательств. Некоторые пункты доказательств могут быть более убедительными, чем другие, и это необходимо учитывать при оценке эффективности обоснования безопасности в целом.

Safety Case отчет должен содержать все сведения, необходимые для оценки безопасности системы. Чем выше требования к безопасности, тем более высокий уровень детализации будет необходим. Качественный Safety Case предоставляет информацию в таком объеме и виде, который сделает работу эксперта комфортной с точки зрения достоверности, доступности и удобства использования.

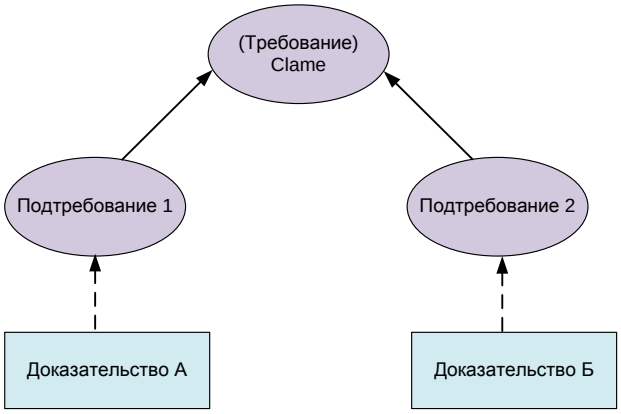

Рис. 2. Диаграмма «требование-аргумент-доказательство»

Типичное содержание Safety Case включает:

Описание системы (Definition of the system) – определяет цель оценки, описывает рассматриваемую систему (задачи, функции, структуру и компоненты) и ее взаимодействие с другими системами.

Отчет по управлению качеством (Quality Management Report) – приводит доказательства того, что требования к процессу обеспечения качества были выполнены.

Отчет по управлению безопасностью (Safety Management Report) – он свидетельствует о том, что действия, определенные в плане обеспечения безопасности, были выполнены. Он должен включать в себя результаты различных анализов безопасности, а также список всех определенных опасностей (журнал опасности).

Технический отчет по безопасности (Technical Safety Report) – он объясняет технические принципы, которые обеспечивают безопасность. Он должен включать отчеты по проверке каждого компонента, включая ЧМИ.

Смежные Safety Cases (Related Safety Cases) – документ содержит ссылки на любые Safety Cases для других жизненно важных систем, которые связаны с рассматриваемой системой.

Выводы должны быть представлены в форме анализа того, почему деятельность, осуществляемая разработчиком, и система атрибутов, являются достаточными.

Для адаптации все элементы Safety Case должны быть определены в рамках процесса проектирования, разработки и производства, применяемых для ЧМИ ИУС АЭС.

1.2 Концептуальная модель оценки. На рис. 3 приведена концептуальная модель системы оценки безопасности ЧМИ ИУС АЭС [9].

Решение проблем оценки безопасности ЧМИ ИУС АЭС носит комплексный характер и непосредственно связано с моделированием и анализом процесса проектирования, требований технического задания, учета контекста использования и дизайна. Модель безопасности ЧМИ строится путем анализа (профилирования) нормативной базы. Выбор методов оценки напрямую зависит от профиля безопасности и этапа жизненного цикла ЧМИ. Результаты оценки непосредственно влияют на повышение

безопасности ЧМИ ИУС АЭС.

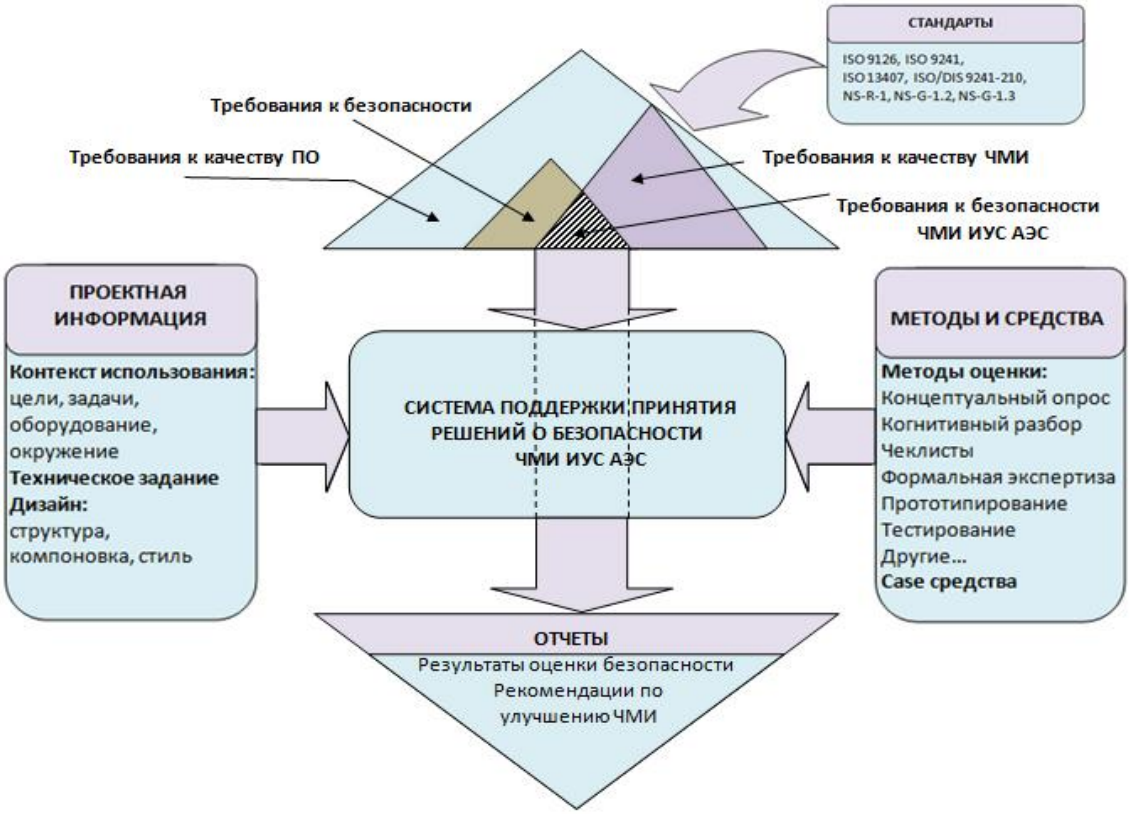

Рис. 3. Концептуальная модель системы оценки безопасности ЧМИ ИУС АЭС

3 Анализ нормативной базы в области качества ЧМИ и удобства использования (usability, юзабилити)

Стандарты, связанные с юзабилити, можно классифицировать с учетом следующих признаков [11]:

– возможность поддержки проектирования, ориентированного на пользователя;

– процесс, используемый для разработки продукта;

– пользовательский интерфейс и взаимодействие;

– использование продукта (эффективность, продуктивность, удовлетворенность в определенном контексте использования).

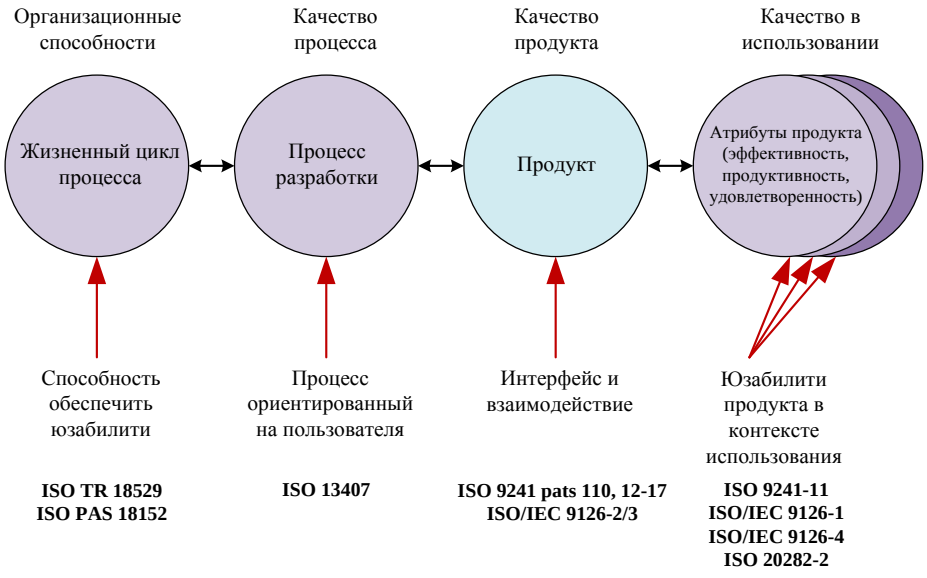

Рис. 4. Классификация стандартов юзабилити

В стандарте ISO 13407 описан процесс проектирования интерактивных систем, ориентированных на пользователей. Этот стандарт содержит рекомендации по организации проектирования интерфейсов и органичному встраиванию этого процесса в общий жизненный цикл производства ПО. В стандарте приведены методы юзабилити, необходимые для определения контекста использования продукта, выявления требований пользователей и заказчиков к системе, прототипирования и тестирования удобства использования продукта.

Дальнейшим развитием нормативной базы стал стандарт ISO/DIS 9241-210 (Human-centered design for interactive systems) – эргономика взаимодействия человека и компьютера, который имеет статус обязательного. Он регламентирует процессы разработки интерфейсов программных систем и ориентирован на удобство использования для пользователей самых различных слоев населения. В этом стандарте более выражен цикл разработка-оценка. Этап оценки занимает решающее место. Вместо понятия “user” появилось “human”, включающее в себя не только пользователя в привычном понимании, но и “customer” – покупателя, заказчика и клиента.

4 Разработка профилеобразующей базы стандартов ЧМИ ИУС АЭС

Существует несколько общепринятых стандартов, которые применяются в проектировании интерфейсов. Некоторые из них имеют рекомендательный характер, в то время как другие обязательны. К ним, прежде всего, относятся стандарты серии ISO/IEC 9126 [4] и серия ISO 9241 [12]. Однако в этих стандартах аспект безопасности или не рассматривается вообще (ISO 9241) или рассматривается на этапе использования (ISO/IEC 9126). Поэтому для ЧМИ ИУС АЭС необходимо также учитывать требования стандартов в области атомной энергетике. На рис. 5 приведена разработанная профилеобразующая база стандартов для оценки качества и безопасности ЧМИ ИУС АЭС, а в табл. 1 – указаны ключевые стандарты.

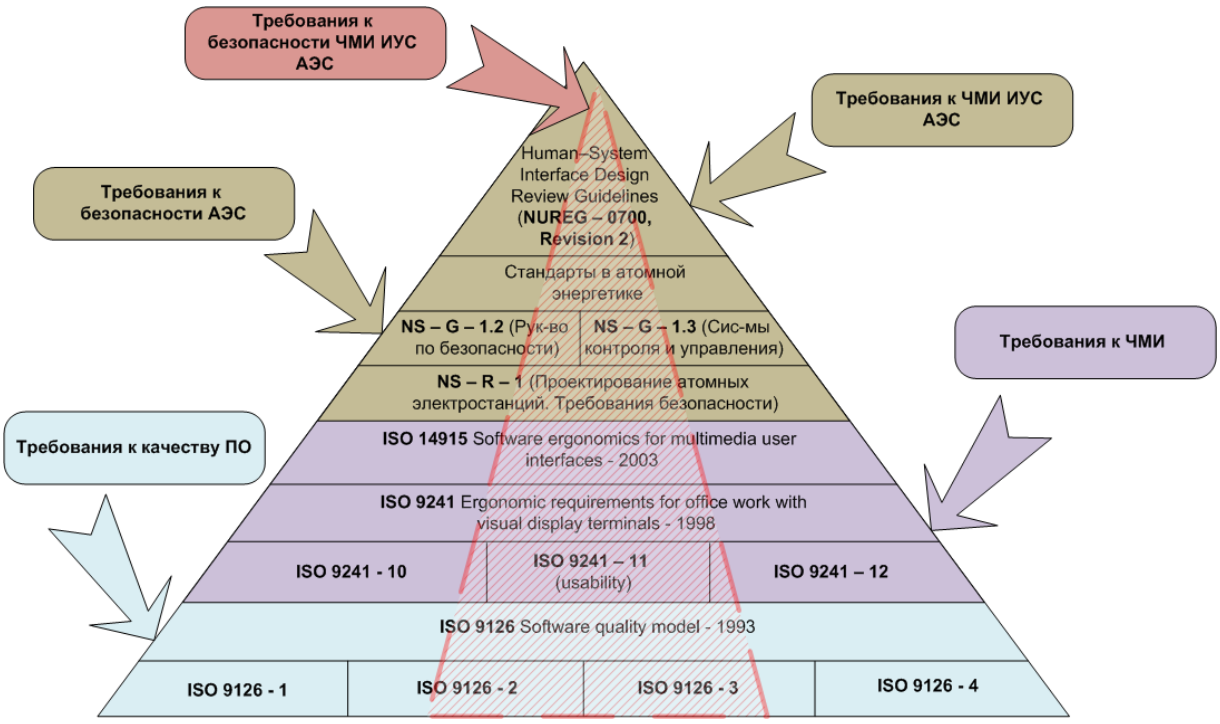

Рис. 5. Профилеобразующая база стандартов ЧМИ ИУС АЭС

Таблица 1
Международные документы высшего уровня иерархии

Наименование документа	**Содержание**
NS-R-1 Проектирование атомных электростанций. Требования безопасности	Роль человеческого фактора Человеко-машинный интерфейс Организация пультов управления Применение компьютеризованных систем защиты.
NS-G-1.2 Оценка безопасности и независимая проверка для атомных электростанций. Руководство по безопасности	Даны рекомендации по оценке безопасности в процессе проектирования, а также рекомендации по независимой проверке оценки безопасности АЭС в целом.
NS-G-1.3 Системы контроля и управления, важные для безопасности атомных электростанций	Материалы по проектированию систем контроля и управления АЭС, включая все элементы таких систем, а также интерфейсы оператора

Требования к программному обеспечению ИУС АЭС приведены в следующих международных нормативных документах:

– МЭК 60880 Изд.2: 2006 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Аспекты программного обеспечения компьютерных систем, выполняющих функции категории А»;

– МЭК 62138 Изд.1: 2004 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Аспекты программного обеспечения для компьютерных систем, выполняющих функции категории В или С»;

– IEEE 1012-1998 «Верификация и валидация программных средств»;

национальных нормативных документах:

– НП 306.5.02/3.035 – 2000 Требования по ядерной и радиационной безопасности к ИУС, важных для безопасности АЭС;

а также в нормативных документах бывшего СССР и РФ:

– ГОСТ 28195-89 «Оценка качества программных средств. Общие положения»;

– ГОСТ Р ИСО/МЭК 12207-99. Информационные технологии. Процессы жизненного цикла программных средств;

– ГОСТ 29075-9 «Системы ядерного приборостроения для атомных станций. Общие требования»;

– РД-03-17-2001 «Положение об аттестации программных средств, применяемых при обосновании безопасности объектов использования атомной энергии».

В стандарте NS-G-1.2 «Оценка безопасности и независимая проверка для атомных электростанций. Руководство по безопасности» [13] имеется ряд требований имеющих отношение к человеко-машинному интерфейсу.

Требование 1. Следует, чтобы проект станции облегчал работу операторов и способствовал выполнению ими оптимальных действий в режимах нормальной эксплуатации и при авариях. Это необходимо обеспечивать, уделяя внимание проекту станции, подготовке эксплуатационных процедур и подготовке всего эксплуатационного персонала.

Требование 2. Систематический учет человеческого фактора и разработку человеко-машинного интерфейса следует включать в процесс проектирования на раннем этапе и продолжать до его окончания.

Требование 3. Следует выявлять предписанные эксплуатационному персоналу действия по обеспечению безопасности, Включая действия, выполняемые операторами, ответственными за контроль и управление станцией и реагирование на отказы, а также действия по техническому обслуживанию, испытанию и калибровке.

Требование 4. Для действий по обеспечению безопасности следует выполнять анализ задач, чтобы оценить нагрузку на операторов, обусловленную необходимостью принятия решений и выполнения действий. В результате анализа задач следует определять проектные требования к человеко-машинному интерфейсу, объему необходимой информации и управления, разработке эксплуатационных процедур и программам подготовки персонала.

Требование 5. Следует обеспечить объем информации и управления, достаточные, чтобы позволить операторам:

– выполнять действия в режимах нормальной эксплуатации, такие как изменение мощности реактора;

– оперативно оценивать общее состояние

станции при нормальной эксплуатации, ожидаемых нарушениях нормальной эксплуатации и авариях;

– контролировать состояние реактора и всего оборудования станции;

– выявлять важные для безопасности изменения состояния станции;

– подтверждать выполнение предусмотренных проектом действий автоматики по обеспечению безопасности;

– определять необходимость и выполнять предписанные действия.

Требование 6. Оператору следует предоставлять информацию о параметрах систем и оборудования станции, достаточную, чтобы подтвердить выполнение требуемых действий по обеспечению безопасности и убедиться в том, что эти действия привели к желаемому результату.

Требование 7. Рабочие зоны и условия работы персонала на площадке следует проектировать в соответствии с принципами эргономики, обеспечивая надежное и эффективное выполнение задач. Особое внимание следует уделять системам отображения данных, компоновке панелей.

Требование 8. Человеко-машинный интерфейс следует проектировать так, чтобы предоставлять операторам исчерпывающую, но легко воспринимаемую информацию для принятия правильных решений и выполнения необходимых действий.

Требование 9. Необходимость срочных действий оператора следует сводить к минимуму. Допустимое время для таких действий следует определять на основе поддающегося обоснованию подхода наилучших оценок.

Требование 10. Для всех действий оператора в анализе задач следует показывать, что оператор имеет достаточно времени для решений и действий, что информация, необходимая для принятия решений, представлена просто и однозначно.

Требование 11. Следует обеспечивать малую чувствительность к ошибкам персонала. Насколько практически возможно следует обеспечивать снижение последствий ошибочных действий. Для этой цели следует тщательно устанавливать приоритет между действиями оператора и автоматическим срабатыванием систем безопасности.

Требование 12. Следует разрабатывать инструкции для всех действий, выполняемых персоналом, включая нормальную эксплуатацию станции и ее восстановление из состояний нарушения и аварий, в том числе тяжелых. ориентированы. Инструкции следует по мере возможности проверять путем выполнения обходов по месту, использования макетов и тренажеров.

5 Принципы проектирования ЧМИ ИУС АЭС

5.1 Основные принципы. Руководство NUREG-0700 [14] предлагает руководящие принципы и рекомендации, необходимые для выполнения оценки качества ЧМИ:

а) руководящие принципы для основных элементов ЧМИ: дисплеи, пользовательский интерфейс взаимодействия, управления и контроля;

б) руководящие принципы для рассмотрения шести систем: сигнализации, отображения, управления, компьютерных процедур, автоматизированной системы поддержки оператора и система связи;

в) рекомендации для обзора рабочих станций и рабочих мест;

г) руководящие принципы для поддержки ЧМИ.

Дизайн ЧМИ должен поддерживать работу персонала по выполнению основной задачи - мониторинга и контроля АЭС, без чрезмерной рабочей нагрузки, связанной с использованием ЧМИ (оконной манипуляцией, отображением выбора, навигации и т.п.). ЧМИ также должен поддерживать распознавание, толерантность (терпимость) и восстановление от любых человеческих ошибок.

Принципы проектирования, содержащиеся в этом документе, представляют общие характеристики ЧМИ, необходимые для поддержки работы персонала. Хотя эти принципы не являются подробным обзором руководящих принципов, они служат нескольким целям. Во-первых, они использовались для разработки многих детальных руководящих принципов этого обзора. Во-вторых, они могут быть использованы для поддержки в проведении оценки аспектов ЧМИ, которые не очень хорошо определяются подробными руководящими принципами.

Таким образом, они могут быть использованы, например, при рассмотрении новых конструкций ЧМИ, когда формат отображения не определен в руководящих принципах. Приведенные ниже 18 принципов делятся на четыре категории: общие принципы, основная задача, вторичная задача, и задача поддержки (табл. 2). Категории и принципы описаны ниже.

Безопасность персонала - дизайн должен свести к минимуму возможность травм и воздействия вредных материалов.

Таблица 2
Высокоуровневые принципы проектирования ЧМИ ИУС АЭС

Категория	**Принцип**
Основные принципы	Безопасность персонала Когнитивная совместимость Физиологическая совместимость Простота конструкции Согласованность
Проектирование с основной задачи	Понимание ситуации Целевая совместимость Пользовательская модель совместимости Структура элементов ЧМИ Логическая/Явная структура Своевременность Совместимость управления/Отображения Обратная связь
Вторичная задача	Когнитивная нагрузка Нагрузка ответа (реакции)
Задача поддержки	Гибкость Руководства и поддержка пользователя Толерантность и управление ошибками

Когнитивная совместимость - роль оператора должна состоять из целенаправленных и значимых задач, которые позволяют персоналу поддерживать хорошую осведомленность об АЭС и поддерживать уровень нагрузки, который не настолько высокий, чтобы негативно повлиять на производительность, но достаточной для поддержания бдительности.

Физиологическая совместимость – дизайн интерфейса должен отражать рассмотрение физиологических характеристик человека, включая визуальное/слуховое восприятие, биомеханику (достижения и движения), характеристики управления и антропометрии.

Простота конструкции – ЧМИ должны представлять простой дизайн в соответствии с требованиями задач.

Согласованность – должна быть высокая степень согласованности между ЧМИ, процедурами и обучающими системами. В ЧМИ пути системных функций всегда должны быть согласованы, отражать высокую степень стандартизации, и быть в полном соответствии с процедурами и подготовкой кадров.

5.2 Проектирование основной задачи. Это принципы поддержки основных задач оператора в процессе мониторинга, принятия решений и управления для поддержания безопасной эксплуатации.

Понимание ситуации - информация, представленная пользователям ЧМИ должна быть правильно, быстро и легко понята и поддерживаться на высоком уровне с целью осведомленности пользователей о статусе системы.

Целевая совместимость – система должна отвечать требованиям пользователей для выполнения своих задач (в том числе, безопасное завершение работы, осмотр, техническое обслуживание и ремонт).

Данные должны быть представлены в форматах соответствующих задач (включая, необходимость доступа к подтверждающим данным или необработанным данным в случае отображения более высокого уровня).

Не должно быть ненужной информации или вариантов контроля.

Пользовательская модель совместимости - все аспекты системы должны быть совместимы с ментальными (психическими) моделями пользователей (понимание и ожидание поведения системы осуществляется путем подготовки кадров, использования процедур и опыта).

Все элементы системы должны быть совместимы с установленными допущениями, т.е. должны быть выражены в привычной форме, пригодной с функциональной точки зрения, а не абстрактно или в формах, требующих дополнительной интерпретации.

Структура элементов ЧМИ – структура всех аспектов ЧМИ (от элементов в отдельных дисплеях до отдельных рабочих станций и всей комнаты управления) должна быть основана на требованиях пользователя и должна отражать общие принципы организации по важности, частоте и порядке использования. Информация

критических функций безопасности должна быть доступна всем, работающим в команде, для обеспечения ее распознавания и сведения к минимуму поиска данных и ответных мер.

Логическая/явная структура – все аспекты системы (форматы, терминология, последовательность, группировка, и поддержка принятия решений оператора) должна отражать очевидную логику, основанную на требованиях задачи. Отношения каждого отображения, управления и обработки данных для общей задачи/функции должны быть ясными. Структура интерфейса и связанная с ней навигация должны быть сделаны легкой для пользователей, чтоб можно было понять, где они находятся в пространстве данных и должна позволить им получить быстрый доступ к данным, не видимым в настоящее время. Ход работы системы и структурированность должны быть ясными для пользователя.

Своевременность – проектирование системы должно принимать во внимание когнитивные возможности пользователей, а также связанные с процессом ограничения времени. Скорость информационного потока и требования контроля за исполнением, которые являются слишком быстрыми или слишком медленными, могут привести к снижению производительности.

Совместимость управления/отображения – отображение должны быть совместимым с вводимыми данными и контролем требований.

Обратная связь – система должна предоставлять полезную информацию о состоянии системы, допустимых операциях, ошибках и восстановлении после ошибки, опасных операциях, и достоверности данных.

5.3 Вторичная задача. На данном этапе реализуются принципы минимизации второстепенных задач, которые не направлены на достижение целей, которые соответствуют основной задаче. Выполнение второстепенных задач отвлекает от основных задач. Примеры вторичной задачи - навигация по дисплеям, манипулирование окнами и доступ к данным.

Когнитивная нагрузка – информация, представленная системой должна быстро восприниматься и пониматься. Система должна минимизировать требования для вычислений или преобразований в уме и использовать напоминания. Исходные данные должны быть представлены непосредственно, в удобной форме.

Нагрузка ответа (реакции) – система должна требовать минимальное количество действий для получения результата. Кроме того, система не должна требовать ввода избыточных данных, повторного ввода информации, имеющейся уже в системе, или информации, которую система может генерировать по уже поступившим данным.

5.4 Задача поддержки. Эти принципы адресованы характеристикам ЧМИ, которые поддерживают его использование персоналом.

Гибкость – система должна предоставить пользователю несколько способов для совершения действий, а отображение и контроль должен быть отформатирован в конфигурации наиболее удобной для задачи.

Руководства и поддержка пользователя - система должна обеспечить эффективную "Помощь". Информативные, легкие в использовании рекомендации должны быть предоставлены в он-лайн и офф-лайн режимах, чтобы помочь пользователю понять, как работать с системой.

Толерантность и управление ошибками – отказоустойчивый дизайн должен предоставляться везде, где сбой может привести к повреждению оборудования, травмам персонала, или непреднамеренной работе с критически важным оборудованием. Система должна вообще быть сконструирована таким образом, чтобы ошибки пользователя не имели серьезных последствий. Система должна предлагать простые, понятные уведомления об ошибке и простые, эффективные методы для восстановления.

6 Методики оценки ЧМИ

6.1 Модель оценки качества ЧМИ. Базовая модель процесса оценки, определенная в стандарте ISO 9126-4, показана на рис. 6.

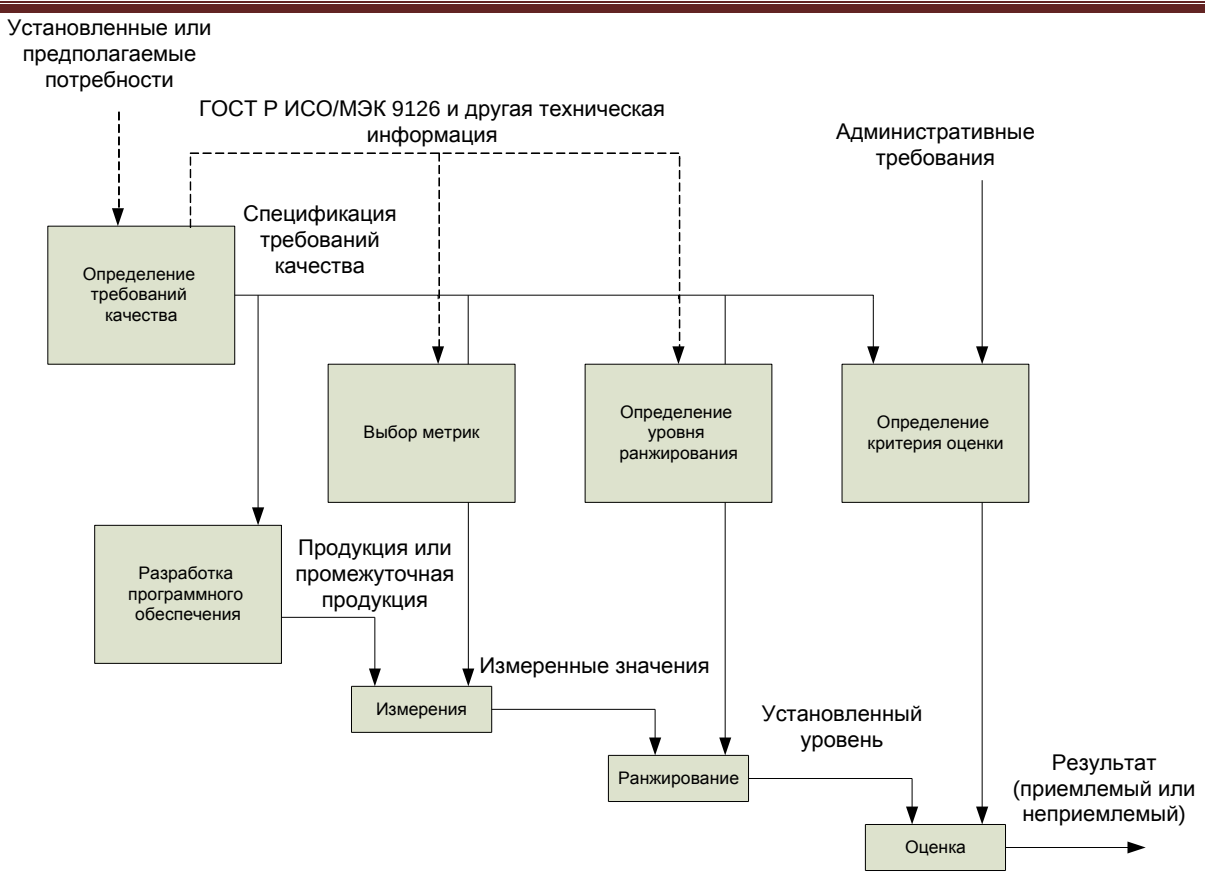

Рис. 6. Модель процесса оценки (ISO/IEC 9126)

Основными этапами процесса оценки являются:

– разработка требований для оценки;
– определение критериев оценки;
– выбор метрик;
– измерение характеристик качества;
– ранжирование;
– оценка результата (сравнение с критериями и требованиями).

Существует много методов и методик, которые применяются в процессе проектирования для оценки качества интерфейсов (табл. 3). Их анализ приведен в работах [15-18]. Наибольшее распространение получили методы экспертной оценки [19].

6.2 Задача оценивания безопасности ЧМИ. Анализ критериев безопасности показал, что они имеют, как правило, качественный и интервальный характер. Значения большинства из них могут быть описаны лингвистическими переменными [16]. Поэтому задача оценки безопасности и выбора лучшего с точки зрения критерия безопасности варианта ЧМИ ИУС АЭС может быть сформулирована, как задача нечеткого многокритериального анализа вариантов [8]. Пусть варианты ЧМИ заданы множеством $P=\{P_1,P_2,...,P_k\}$, а критерии безопасности – множеством $G=\{G_1,G_2,...,G_n\}$, тогда задача многокритериального анализа состоит в упорядочивании элементов множества P по критериям из множества G. Вариант ЧМИ $P_j \in P$ оценивают по критерию $G_i \in G$ числом $\mu_{G_i}(P_j)$ в диапазоне $[0,1]$. Чем больше число $\mu_{G_i}(P_j)$, тем лучше вариант P_j по критерию G_i, $i=\overline{1,n}$, $j=\overline{1,k}$. Тогда, критерий G_i можно представить нечетким множеством $\tilde{G}_i$ на универсальном множестве вариантов P [12,16]:

$$\tilde{G}_i=\left\{\frac{\mu_{G_i}(P_1)}{P_1},\frac{\mu_{G_i}(P_2)}{P_2},...,\frac{\mu_{G_i}(P_k)}{P_k}\right\}, \quad (1)$$

где $\mu_{G_i}(P_j)$ – степень принадлежности элемента P_j нечеткому множеству $\tilde{G}_i$. Находить степени принадлежности нечеткого множества (1) удобно методом построения функций принадлежности на основе парных сравнений. При использовании этого метода необходимо сформировать матрицы парных сравнений вариантов по каждому критерию. Общее количество таких матриц равно количеству критериев. Наилучшим вариантом будет тот, который одновременно лучший по всем критериям. Нечеткое

решение $\tilde{D}$ находится как пересечение частных критериев (формула 3).

Таблица 3
Методы оценки качества интерфейсов

Методы оценки ЧМИ	**Степень автомат.**			**Этапы ЖЦ**		
Экспертиза компонентов	+			+	+	
Эвристическое исследование	+			+	+	
Фокусные группы	+			+	+	+
Макетирование	+			+	+	
Анализ конкурентов	+			+	+	+
Мысли вслух	+			+	+	
Протоколы самоотчета	+					+
Опросники	+					+
Обзоры	+			+		
Карточная сортировка	+			+	+	+
Контрольные листы	+				+	+
Мозговой штурм	+			+		
Параллельный дизайн	+			+	+	
Шаблоны	+			+		
Стилевые правила	+			+		
Диаграммы сходства	+			+	+	+
Анализ задач	+			+		
Плюралистическая проработка	+			+		
Контекстное исследование	+					+
Руководства по дизайну	+				+	+
Степень автоматизации 1.Ручные 2. Автоматизированные 3. Автоматические						
Этапы ЖЦ 1. Формирование требований 2. Тестирование 3. Проектирование. и реализация						

Согласно с полученным нечетким множеством $\tilde{D}$, наилучшим вариантом следует считать тот, у которого наибольшая степень принадлежности:

$$D = \arg\max(\mu_D(P_1), \mu_D(P_2), \dots, \mu_D(P_k))$$

.

При неравновесных критериях степени принадлежности нечеткого множества $\tilde{D}$ находят по формуле:

$$\mu_D(P_j) = \min_{i=\overline{1,n}}(\mu_{G_i}(P_j))^{\alpha_i},\ j = \overline{1,k} \quad (2)$$

где α_i - коэффициент относительной важности критерия $G_i, \alpha_1 + \alpha_1 + \dots + \alpha_n = 1$

$$\tilde{D} = \tilde{G_1} \cap \tilde{G_2} \cap \dots \cap \tilde{G_n} = \left\{ \frac{\min\limits_{i=1,n} \mu_{G_i}(P_1)}{P_1}, \frac{\min\limits_{i=1,n} \mu_{G_i}(P_2)}{P_2}, \dots, \frac{\min\limits_{i=1,n} \mu_{G_i}(P_k)}{P_k} \right\} \quad (3)$$

Широкое распространение для нахождения рангов критериев на основе матрицы парных сравнений получил метод, Саати. Этот поход заключается в отыскании приближениях значений вектора рангов, как среднегеометрических величин каждой строки матрицы парных сравнений. Полученные таким образом среднегеометрические значения собственного вектора нормализуются делением на сумму средних геометрических.

6.3 Отчет по оценке безопасности.

Результаты оценки безопасности представляются в виде отчета (см.шаблон табл.4).

Таблица 4

Технический отчет по безопасности

Объект оценки	Шифр интерфейса
Цель оценки	Проверка основных принципов
Категория функции (задачи)	**Категория А:** используется для обозначения тех функций, которые играют основную роль в достижении или поддержании безопасности АЭС с целью предотвращения развития аварий до недопустимых последствий
Технические принципы (характеристика)	**Название принципа:** когнитивная совместимость **Содержание:** роль оператора должна состоять из целенаправленных и значимых задач, которые позволяют персоналу поддерживать хорошую осведомленность с АЭС и поддерживать уровень нагрузки, который не настолько высокий, чтобы негативно повлиять на производительность, но достаточной для поддержания бдительности.
Субхарактеристики	Отсутствуют
Метрика	**Название метрики:** User health and safety **Содержание:** влияние на здоровье и безопасность пользователей **Шкала:** Высокая - низкая **Источник:** Стандарт ISO/IES 9126-4
	Название метрики: Психофизиологическая цена деятельности **Содержание:** Степень усталости, утомления, болезненных ощущений и т.д., возникающие при работе с продуктом **Шкала:** Высокая - низкая **Источник:** USABILITYLAB (нестандартная)
Методы	**Название метода:** когнитивный разбор (Экспертная оценка) **Содержание:** эксперты, участвующие в оценке, конструируют сценарии по спецификациям или раннему прототипу, и затем входят в роль пользователя, работающего с интерфейсом, следуя этим сценариям — осуществляют прогон по интерфейсу.
Информация об эксперте	Фамилия, имя, отчество Опыт эксперта
Дата проведения оценки	18.06.11
Выводы	Выводы эксперта о степени соответствии объекта требованию. Обоснование полноты и достаточности проверки

Выводы

Проведенный анализ нормативной базы для ЧМИ, прежде всего, ИУС АЭС, позволил

выделить группы требований, среди которых основными являются требования к проектированию и оценке ЧМИ, а также требования к безопасности ЧМИ.

В основу оценки безопасности ЧМИ положена методология Safety Case. Ее элементами являются уточнение требований с учетом полученной профилеобразующей базы, выделение субпрофиля требований к безопасности ЧМИ, выбор методов (методики) оценки и их реализация, формирование итоговой оценки. Дальнейшие исследования целесообразно направить на детализацию методики и разработку инструментальных средств оценки качества и безопасности ЧМИ.

Список литературы

1. Харченко В.С. Новые информационные технологии и безопасность информационно-управляющих систем АЭС / Харченко В.С., Ястребенецкий М.А., Скляр В.В. // Ядерная и радиационная безопасность.- 2003.– Т. 6.– № 2.– С. 19-28.

2. Ястребенецкий М.А. Новым энергоблокам АЭС Украины – новые информационные и управляющие системы / Ястребенецкий М.А., Васильченко В.Н. и др. // Ядерная и радиационная безопасность. - 2004. – 7, № 4.– С. 5-12.

3. Скляр В.В. Особенности и оценка безопасности программного обеспечения информационных и управляющих систем АЭС Украины / Скляр В.В., Харченко В.С., Ястребенецкий М.А. // Ядерные измерительно-информационные технологии. – 2006. – № 1 (17). – С. 3-18.

4. Information Technology — Software Product Quality: ISO/IEC 9126, 19.11.1999. – 308 с.

5. Danying Gu. Study on a methodology of human factor engineering operating experience review for

nuclear power plant / Danying Gu, Shuhui Zhang, Zhonghe Ning // Proceedings of the 18th International Conference on Nuclear Engineering ICONE18 May 17-21, 2010, Xi'an, China.

6. Орєхова А.О., Харченко В.С. Аналіз вимог до інтерфейсів інформаційно-управляючих систем АЄС // Вісник ХНТУ ім. П.Василенка. Технічні науки. Випуск 102. "Проблеми енергозабезпечення та енергозбереження в АПК України". – Харків: ХНТУСГ, 2010. – с.109-111.

7. Andrashov A., Kharchenko V., Netkachova K.,et.al. Safety Case-Oriented Assessment of Critical Software: Several Principles and Elements of Techniques. Monographs of System Dependability. Dependability of Networks, Wroclaw, OWPW, 2010. – p. 11-25.

8. Штовба С.Д. Проектирование нечетких систем средствами MATLAB. – М.: Горячая линия – Телеком,2007. – 288 с.

9. Орехова А.А., Харченко В.С. Оценка безопасности человеко-машинных интерфейсов информационно-управляющий систем АЭС на основе нечеткого многокритериального анализа вариантов //

Обчислювальній інтелект. Матеріали І-ї Міжнародної науково-технічної конференції . – Черкаси:Маклаут, 2011. – с. 219-220.

10. Fowkes M., Ward D.D., Jesty P., Recommended methodology for preliminary safety analysis of the HMI of an IVIS concept or design, HASTE Deliverable 4 v1.01 October, 2005.

11. Bevan, N. International Standards for HCI and Usability. International Journal of Human-Computer Studies, 55 (4), 2006.

12. Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11. Guidance on usability: ISO 9241, First edition, 15.03.1998. – 28 с.

13. Оценка безопасности и независимая проверка для атомных электростанций. Руководства / Серия норм МАГАТЭ по безопасности № NS-G-1.2 МАГАТЭ: Вена, 2004. – 99 с.

14. Human-System Interface Design Review Guidelines, NUREG-0700, U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research Washington, 2002, 659 p.

15. Гордеев А.А., Гордеева Д.В., Гончаренко А.А. Оценка качества удобства в использовании бизнес-критических Веб-сервисов, Радіоелектронні і комп'ютерні системи, 2009, №7 (41), С. 38-40.

16. Орехова А.А. Анализ критериев и методов проектирования безопасных интерфейсов информационно-управляющих систем // МНТК " ІКТМ-2010": Тези доповідей. Том 2. – Харків: Національний аерокосмічний університет "Харківській авіаційний інститут", 2010. – с. 219.

17. Скляр В.В. Оценка качества и экспертиза программного обеспечения / В.В. Скляр; под ред. В.С. Харченко. – Х.: Нац. аэрокосм. ун-т "ХАИ", 2008. – 204 с.

18. Харченко В.С. Методы моделирования и оценки качества и надежности программного обеспечения / Харченко В.С., Скляр В.В., Тарасюк О.М. // – Х.: 2004. – 159с.

19. Гнатієнко Г.М., Снитюк В.Є. Експертні технології прийняття рішень: Монографія. – К.: ТОВ «Маклаут», 2008. – 444 с.

Сведения об авторах:

Харченко Вячеслав Сергеевич - доктор технических наук, профессор, заведующий кафедрой «Компьютерные системы и сети» Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», заслуженный изобретатель Украины. Научные интересы: надежность и безопасность информационно-управляющих систем для критических приложений.

E-mail: v.kharchenko@khai.edu

Орехова Анастасия Александровна – аспирант кафедры «Компьютерные системы и сети», Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ». Научные интересы: качество человеко-машинных интерфейсов систем важных для безопасности.

E-mail: nastya.orehova@rambler.ru

Статья поступила в редакцию 07.09.2011 г.

