УДК 004. 415.2.045

А.А. ОРЕХОВА[1], В.Р. ТИЛИНСКИЙ[2], В.С. ХАРЧЕНКО[1]

[1]*Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»*
[2]*ООО «Вестрон», Харьков*

МЕТОДИКА КОМПЛЕКСНОЙ ОЦЕНКИ БЕЗОПАСНОСТИ ЧЕЛОВЕКО-МАШИННОГО ИНТЕРФЕЙСА ИУС КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Предложен подход к оценке безопасности человеко-машинных интерфейсов информационно-управляющих систем АЭС, основанный на методологии Safety Case. Рассматривается модель объекта оценки с учетом человеческого фактора. Предложена нормативная профилеобразующая база для выбора методов и процессов оценки безопасности ЧМИ критических систем. Приводятся результаты экспертного ранжирования высокоуровневых принципов проектирования безопасных ЧМИ. Обоснован выбор профиля методов для комплексной оценки безопасности ЧМИ на всех этапах жизненного цикла. В результате анализа принципов проектирования безопасных ЧМИ выполнено их ранжирование.

Ключевые слова: *информационно-управляющие системы, человеко-машинный интерфейс, человеческий фактор, безопасность, риск, юзабилити, качество, Safety Case.*

Введение

Модернизация атомных электростанций (АЭС) требует разработки новых информационно-управляющих систем (ИУС). Функциональные возможности ИУС, надежность и эффективность деятельности человека в большой степени зависят от человеко-машинных интерфейсов (ЧМИ) [1].

Актуальными в области ЧМИ в настоящее время являются исследования человеческого фактора с целью уменьшения вероятности ошибок; анализ надежности действий оператора, связанных с риском и учетом оценки возможных последствий; разработка методик для оценки безопасности [2].

При оценке безопасности критических систем получил распространение подход, основанный на методологии Safety Case [3]. Он предполагает комплексную оценку безопасности системы и ее программного обеспечения (ПО). Как показывает анализ публикаций, вопросы оценки безопасности ЧМИ в рамках Safety Case не рассматривались.

Цель работы - адаптация методологии Safety Case для разработки методики комплексной оценки безопасности ЧМИ критических систем.

1. Формализация объекта оценки

Современные ИУС АЭС представляют собой сложные комплексы распределенной обработки информации, в которых ЧМИ, как правило, реализован на базе рабочих станций. Основная цель таких ЧМИ – предоставлять персоналу информацию о состоянии систем энергоблока, а также предоставлять интерфейс для управления исполнительными механизмами. Информация представляется на мониторах блочного щита управления (БЩУ) и рабочих станциях персонала.

На рис. 1 представлена модель человеко-машинной системы, интерфейс которой состоит из двух частей: аппаратной (HW) и программной (SW). Аппаратная часть ЧМИ кроме мониторов может включать стандартную клавиатуру с трекболом и функциональную клавиатуру.

Основным компонентом отображения информации ИУС являются видеокадры (ВК), которые организованы в виде нескольких систем с многоуровневой иерархической структурой и возможностью перемещения как между уровнями иерархии, внутри уровней, так и между системами.

Кроме того, видеокадры могут вызываться через меню или с функциональной клавиатуры. ВК представляют оператору технологическую информацию в реальном масштабе времени в виде мнемосхем (анимированных фрагментов технологических схем или рисунков технологического оборудования), диаграмм, гистограмм, таблиц, графиков и т.п. Детальная структура системы отображения уточняется на стадии проектирования. Модель программной компоненты ЧМИ можно представить множеством уровней (рис. 1):

$$HMI = \{STR, PER, ST, COMP, VD\},$$

где STR – стратегия; PER – возможности; ST – структура; COMP – компоновка; VD – визуальный дизайн.

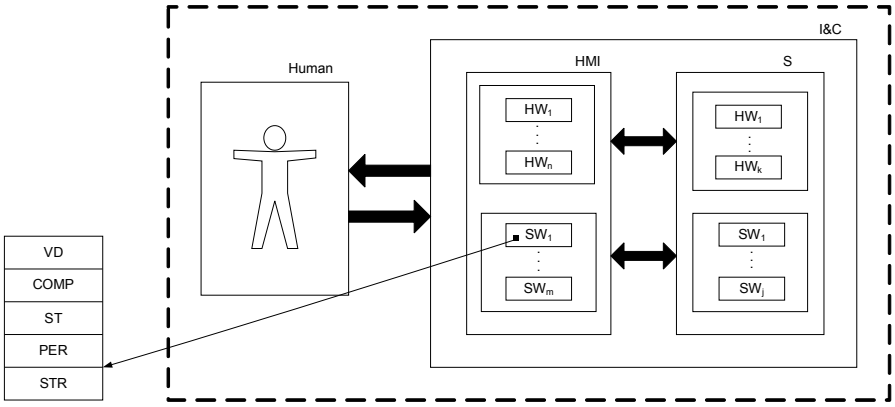

Рис. 1. Модель объекта оценки

Уровень STR определяет цель интерфейса и потребности пользователя; на уровне PER определяются функциональные спецификации и требования к информации; уровень ST предназначен для проектирования взаимодействия и информационной архитектуры; уровни COMP и VD задают информационный и визуальный дизайн интерфейса. Как отмечается в [1] основным условием достижения высокого качества ЧМИ является следование стандартам.

2. Анализ нормативной базы

Проблема оценки безопасности ЧМИ в рамках Safety Case является междисциплинарной.

Для ее научного обоснования и решения необходимы знания таких дисциплин, как проектирование систем, эргономика и удобство, инженерия человеческого фактора, программная инженерия, безопасность и управление риском.

В каждой из этих областей существует своя нормативная база, регламентирующая подходы, процессы, методы и средства проектирования и оценки, которые могут быть полезны для создания эффективной методики комплексной оценки безопасности ЧМИ.

На рис. 2 приведена возможная профилеобразующая база стандартов для выбора методов и процессов оценки безопасности ИУС АЭС.

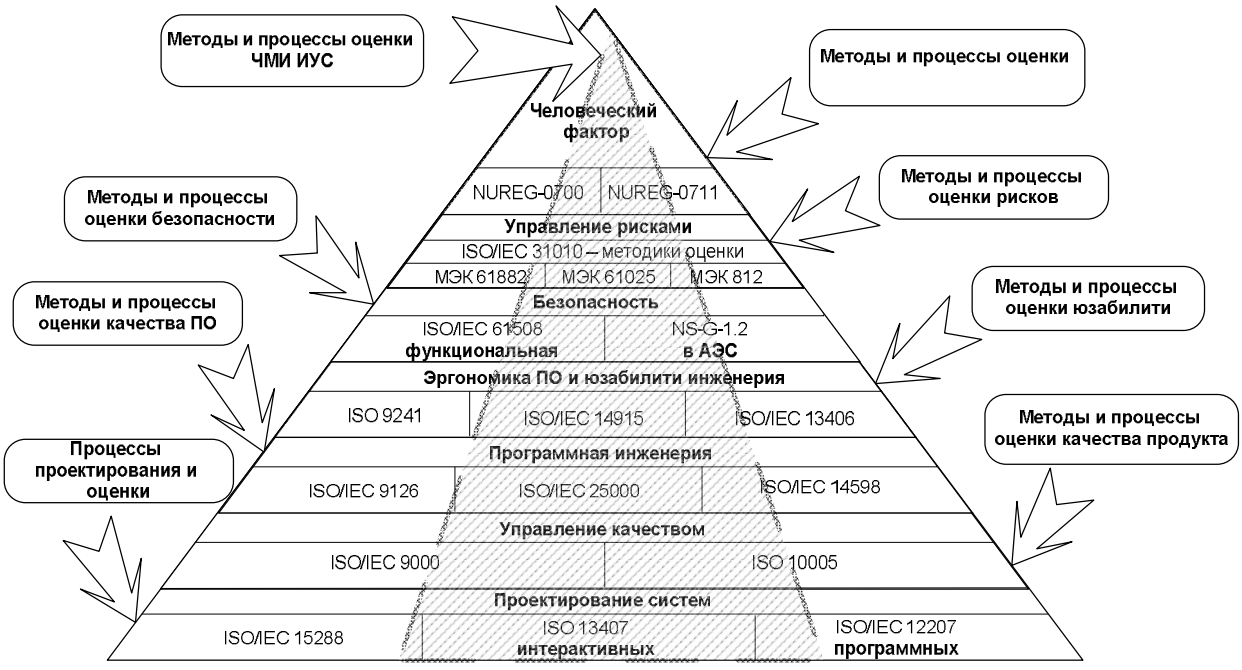

Рис. 2. Профилеобразующая база стандартов

3. Принципы проектирования

Основные принципы проектирования и требования к ЧМИ ИУС АЭС сформулированы в [4,5]. Эти же принципы могут быть использованы в качестве критериев при оценке безопасности ЧМИ ИУС. Ниже приведены результаты экспертного анализа и ранжирования этих принципов/критериев.

Безопасность персонала (БП) – принцип допускает двоякое толкование. В широком смысле БП является следствием выполнения системой основного ее назначения – обеспечения безопасности АЭС. В этом смысле, он является интегральной характеристикой, неприменимой в качестве элементарного принципа проектирования. В узком смысле – в качестве самостоятельного критерия – этот принцип можно отнести только к обеспечению безопасности обслуживания самой ИУС, что имеет достаточно малый вес по сравнению с обеспечением эффективности работы оператора.

Когнитивная совместимость (КС) и *физиологическая совместимость* (ФС) – эти принципы требуют учитывать при проектировании ЧМИ физиологические и психологические возможности оператора и уровня его подготовки. В качестве критериев, эти принципы позволяют оценить качество информации, а также удобство ее восприятия, анализа и понимания. Это очень важные критерии для учета человеческого фактора.

Согласованность (СГ) относится к числу приоритетных принципов/критериев. Только взаимная непротиворечивость поступающей к оператору по разным каналам информации может позволить ему уверенно принимать правильные решения. В случае противоречивых данных должна быть четко прописана иерархия приоритетов источников информации.

Понимание ситуации (ПС) является одним из наиболее важных, т.к. он характеризует способность ЧМИ выполнять его основную функцию – обеспечить понимание ситуации оператором путем предоставления ему достоверной информации о состоянии систем.

Целевая совместимость (ЦС) указывает на то, что система должна отвечать требованиям пользователей. Эта характеристика также относится к наиболее важным, т.к. система обязана соответствовать своему назначению.

Устойчивость и управление ошибками (УУО) – приоритет этого принципа зависит от класса системы. Для систем, важных для безопасности, как характеристика, которая может прямо влиять на безопасность АЭС, имеет высокий приоритет.

Структура элементов (СЭ) – этот принцип обеспечивает представление информации персоналу в соответствии с распределением ролей при управлении энергоблоком, при этом наиболее важная информация, относящаяся к безопасности, должна быть доступна всему оперативному персоналу. Этот принцип достаточно важен, но не является критическим.

К числу менее приоритетных принципов проектирования относятся: *когнитивная нагрузка* (КН), *пользовательская модель совместимости* (ПМС), *своевременность* (СВ), *логическая структура* (ЛС), *совместимость управления* (СУ), *гибкость* (ГБ), *обратная связь* (ОС), *простота конструкции* (ПК). Все перечисленные принципы должны приниматься во внимание при проектировании ЧМИ ИУС, однако, поскольку реальные ЧМИ являются компромиссным решением, удовлетворяющим перечисленным критериям не в полной мере, наибольшее внимание должно уделяться высокоприоритетным принципам.

На рис. 3. приведены результаты ранжирования принципов проектирования безопасных ЧМИ.

Рис. 3. Ранжирование принципов проектирования

4. Выбор методов

На сегодняшний день задача выбора методов для обеспечения оценки безопасности в рамках Safety Case осложняется большим количеством методик различной степени формализации, сложности, возможностью применения на этапах жизненного цикла и т.д. Поскольку в данной работе рассматривается только программная часть ЧМИ, можно существенно ограничить круг анализируемых подходов и методов. В рамках UCD-процесса проектирования интерактивных систем, ориентированного на пользователя разработано большое количество методов, имеющих отношение к юзабилити [6]. По нашему мнению эти методы наиболее эффективны на предпроектном этапе сбора информации, на этапе анализа контекста использования (анализ задач), а

также на этапе верификации и валидации готового изделия (юзабилити тестирование). Процессы и методы оценки безопасности ЧМИ, разработанные в рамках программной инженерии, ориентированы главным образом на метрическую оценку готового продукта.

Методы оценки рисков приведены в [7]. Оценку риска можно проводить с различной степенью глубины и детализации. Возможно применение одного или нескольких методов. При выборе методов должно быть представлено обоснование их пригодности. Методы должны иметь следующие характеристики:

− быть научно обоснованными;

− соответствовать исследуемой системе;

− давать понимание природы и характера риска, способов его контроля и обработки.

Выбор метода может осуществляться исходя из следующих факторов:

- цель оценки;
- стадия разработки системы;
- тип системы;
- объем ресурсов и возможностей;
- характер и степень неопределенности;
- сложность методов;
- возможность получения количественных выходных данных;
- применимость метода;
- наличие и доступность информации о системе;
- потребности лиц, принимающих решения.

В табл. 1 приведены результаты сравнительного анализа нескольких методов-кандидатов для Safety Case.

При выборе методов учитывались рекомендации и данные по применимости конкретного метода на этапах процесса оценки риска ЧМИ.

Многокритериальный анализ решений (MCDA). Целью данного анализа является оценка совокупности вариантов объектов путем применения ряда критериев. В случае ЧМИ совокупностью вариантов может быть множество прототипов.

Таблица 1

Сравнительный анализ методов оценки риска

Тип методики	**1**	**2**	**3**	**4**
Контрольные листы	L	L	L	+
Предварительный анализ опасности	L	H	M	–
Анализ сценария	M	H	M	–
Анализ «дерева» неисправностей	H	H	M	_
Анализ «дерева» событий	M	M	M	_
Анализ причин и последствий	H	M	H	_
Анализ видов и последствий отказов (FMEA и FMECA)	M	M	M	+
Исследование опасности и работоспособности (HAZOP)	M	H	H	+
Оценка надежности оператора (HRA)	M	M	M	+
Многокритериальный анализ решений (MCDA)	L	H	M	+
Столбцы таблицы: 1-ресурсы и возможности; 2- характер и степень неопределенности; 3-сложность; 4- возможность применения для ЧМИ Значимость факторов: L – низкая; M – средняя; H – высокая. “+” – применим; “-” – нет данных				

Результатом анализа является установление упорядочения по предпочтению имеющихся вариантов. В процессе анализа составляются матрицы вариантов и критериев, которые ранжированы и объединены для обеспечения оценки каждого варианта.

Постановка задачи многокритериального анализа решений для сравнения различных вариантов прототипов ЧМИ с точки зрения требований безопасности дана в [3].

Входными данными являются возможные варианты прототипов ЧМИ для анализа и критерии оценки.

Данный метод особенно полезен на ранних этапах проектирования в условиях неопределенности.

Исследование опасности и работоспособности (HAZOP). Это общий процесс идентификации риска, направленный на определение возможных отклонений от ожидаемого или требуемого функционирования [7].

Методика может применяться на различных этапах проектирования систем управления критичными для безопасности объектами, компьютерных систем (CHAZOP), включая и программное обеспечение.

В [8] предлагается HAZOP-подобная методика DOP для оценки ЧМИ автомобильных информационно-коммуникационных систем.

Методика HAZOP основана на применении управляющих слов. В зависимости от объекта анализа меняется состав и интерпретация управляющих слов. Возможность применения HAZOP для оценки риска ЧМИ обусловлена тем, что управляющие слова могут применяться к физическим параметрам и передаче информации. HAZOP позволяет в явном виде учитывать причины и последствия ошибок персонала.

Анализ видов и последствий отказов (FMEA). Методика FMEA позволяет установить характер отказов, механизмы их возникновения и воздействия. FMEA может сопровождаться анализом критичности, при котором определяют значимость отказа каждого типа (FMECA). Анализ FMEA применяется как для систем, так и для их компонент, в том числе и программных - SFME(C)A.

Процесс HAZOP сходен с FMEA в том, что он позволяет определить виды отказов, их причины и последствия. Отличие состоит в том, что HAZOP проводится в обратном порядке от нежелательных результатов и отклонений до возможных причин и видов отказов, тогда как FMEA начинается с определения вида отказа. Возможный профиль методов для Safety Case и процесс комплексной оценки безопасности ЧМИ ИУС АЭС на всех этапах жизненного цикла показан на рис. 4.

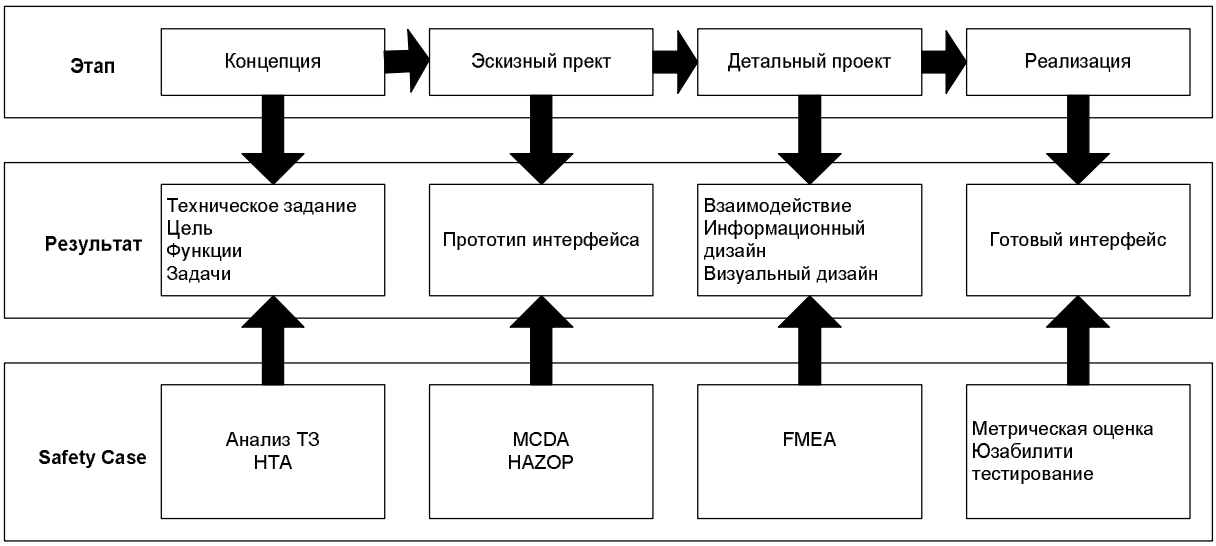

Рис. 4. Методика оценки безопасности ЧМИ ИУС

Выводы

В основу оценки безопасности компьютеризованных ЧМИ ИУС положена методология Safety Case, позволяющая повысить полноту и достоверность комплексной оценки на всех этапах жизненного цикла от концепции до готового продукта.

Обоснование и выбор методов выполнен с помощью полученной междисциплинарной профилеобразующей нормативной базы, что позволило объединить в рамках Safety Case методы программной инженерии, оценки рисков, инженерии человеческого фактора и юзабилити.

В результате анализа принципов проектирования безопасных ЧМИ выполнено их ранжирование.

Дальнейшие исследования будут направлены на детализацию методики и разработку инструментальных средств оценки безопасности ЧМИ.

Литература

1. Анохин, А.Н. Проектирование интерфейсов [Текст] / А.Н. Анохин, Н.А. Назаренко // Биотехносфера. – 2010. – № 2 (8). – С. 21 – 27.

2. Орєхова, А.О. Аналіз вимог до інтерфейсів інформаційно-управляючих систем АЕС [Текст] / А.О. Орєхова, В.С. Харченко // Вісник ХНТУ ім. Петра Василенка. Технічні науки. Випуск 102. "Проблеми енергозабезпечення та енергозбереження в АПК України". – Х.: ХНТУСГ, 2010. – С. 109 – 111.

3. Орехова, А.А. Оценка безопасности ЧМИ ИУС АЭС на основе нечеткого многокритериального анализа вариантов [Текст] / А.А. Орєхова, В.С. Харченко // Обчислювальній інтелект. Матеріали І-ї МНТК. – Черкаси: Маклаут, 2011. – С. 219-220.

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

5. Human-System Interface Design Review Guide-

lines, NUREG-0700 [Text] / U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research Washington, 2002. – 659 p.

6. Bevan, N. International Standards for HCI and Usability [Text] / N. Bevan // International Journal of Human-Computer Studies. – 2006. – 55 (4). – 11 p.

7. Risk management – Risk assessment techniques: [Text] / ISO/IEC 31010:2000.

8. Fowkes M. Recommended methodology for preliminary safety analysis of the HMI of an IVIS concept or design [Text] / M. Fowkes, D.D. Word, P. Jesty // HASTE Deliverable 4. – V.1.01, October 2005.

Поступила в редакцию 23.02.2012

Рецензент: д-р техн. наук, проф., проф. кафедры Б.М. Конорев, Харьковский национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина.

МЕТОДИКА КОМПЛЕКСНОЇ ОЦІНКИ БЕЗПЕКИ ЛЮДИНО-МАШИННОГО ІНТЕРФЕЙСУ ІКС КРИТИЧНОГО ЗАСТОСУВАННЯ

А.О. Орєхова, В.Р. Тілінський, В.С. Харченко

Запропоновано підхід для оцінки безпеки людино-машинних інтерфейсів інформаційно-керуючих систем АЕС, заснований на методології Safety Case . Розглядається модель об'єкта оцінки з урахуванням людського фактора. Запропоновано нормативна профілеутворююча база для вибору методів і процесів оцінки безпеки ЛМІ критичних систем. Наводяться результати експертного ранжирування високорівневих принципів проектування безпечних ЧМІ. Обгрунтовано вибір профілю методів для комплексної оцінки безпеки ЛМІ на всіх етапах життєвого циклу. В результаті аналізу принципів проектування безпечних ЛМІ виконано їх ранжирування.

Ключові слова: інформаційно-керуючі системи, людино-машинний інтерфейс, людський фактор, безпека, ризик, юзабіліті, якість, Safety Case.

INTEGRATED HMI SAFETY ASSESSMENT METHODOLOGY FOR SAFETY-CRITICAL I&C SYTEMS

N.A. Orekhova, V.R. Tilinskiy, V.S. Kharchenko

A safety assessment approach for human-machine interfaces of Nuclear Power Plant information and control systems (I&Cs) based on the Safety Case methodology is proposed. I&C assessment model is described taking into account human factor impact. Normative profile-generated base for choice of HMI safety assessment methods is developed. Ranking of major design principles of safe HMI is provided. Set of methods for comprehensive HMI safety assessment at life cycle stages is justified. As a result of analysis of principles of planning of safe I&Cs their ranging is executed.

Keywords: information and control systems, human-machine interface, human factors, safety, hazard, usability, quality, Safety Case.

Орехова Анастасия Александровна – аспирант кафедры «Компьютерные системы и сети», Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»», Харьков, Украина.

Тилинский Виталий Рудольфович – главный инженер по проектам информационных систем ООО «Вестрон»», Харьков, Украина.

Харченко Вячеслав Сергеевич – д-р техн. наук, проф., заслуженный изобретатель Украины, заведующий кафедрой «Компьютерные системы и сети», Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»», Харьков, Украина.