Разработка комплекта нормативных документов, обеспечивающих создание, внедрение и эксплуатацию АСУ ТП нового поколения на базе программных и программируемых средств

Авторы:

А.Н. Анохин – *ПНИЛ «ЭРГОЛАБ», ИАТЭ НИЯУ «МИФИ», Обнинск*

О.Л. Боженков – ОАО «ВНИИАЭС», Москва

И.Д. Ракитин, В.П. Сивоконь, С.А. Шумов – ОАО «СНИИП», Москва

Обнинск, 2009

Преимущества компьютеризированных систем контроля и управления по сравнению с традиционными:

- Улучшается диагностика состояния оборудования АЭС;
- Возможность для персонала получать информацию, которую он не имел при использовании обычных систем;
- Более точная и надежная информация;
- Возможность для проектантов представлять информацию в виде, который наилучшим образом соответствует задачам персонала и его информационным потребностям;
- Повышение эффективности в выработке энергии и снижение стоимости эксплуатации.

Иерархическая взаимосвязь между документами МАГАТЭ и МЭК

- Высший уровень: документы МАГАТЭ по безопасности;
- Первый уровень: стандарт МЭК 61513 «Общие требования к системам, важным для безопасности АЭС»;
- Второй уровень: детализация требований по общим вопросам (имеются ссылки в документе первого уровня);
- Третий уровень: требования к конкретному оборудованию, техническим методам или конкретной деятельности.

Документы МАГАТЭ:

- **Основы безопасности:** содержат основные цели, концепции и принципы обеспечения безопасности и защиты в освоении и применении ядерной энергии для мирных целей;
- **Требования безопасности:** устанавливают требования, которые необходимо выполнять для обеспечения безопасности. Эти требования определяются целями и принципами, изложенными в Основах безопасности ;
- **Руководства по безопасности:** рекомендуют меры, условия или процедуры выполнения требований безопасности.

Документы МАГАТЭ (продолжение):

Документ NS-R-1 «Проектирование атомных электростанций. Требования безопасности».

- Роль человеческого фактора;
- Человеко-машинный интерфейс (ЧМИ);
- Организация пультов управления;
- Помещение пульта управления;
- Применение компьютеризованных систем в важных для безопасности системах;
- Автоматический контроль;
- Функции системы защиты;
- Применение компьютеризованных систем защиты;
- Разделение систем защиты и систем контроля и управления.

Документы МАГАТЭ (продолжение):

NS-G-1.2. «Оценка безопасности и независимая проверка для атомных станций. Руководство по безопасности»

- Рекомендации по оценке безопасности в процессе проектирования, а также рекомендации по независимой проверке оценки безопасности АЭС в целом;
- Предлагаемый отечественный РД: «Оценка безопасности и независимая проверка (верификация) для систем контроля и управления, важных для безопасности атомных станций».

Документы МАГАТЭ (продолжение):

NS-G-1.3. «Системы контроля и управления, важные для безопасности АЭС»

- Данное Руководство заменяет предыдущие руководства по безопасности №№ 50-SG-D3 и 50-SG-D8.
- Руководство содержит руководящие материалы по проектированию СКУ, важных для безопасности АЭС, включая все элементы таких систем - от датчиков до исполнительного оборудования, а также интерфейсы оператора (ЧМИ) и вспомогательное оборудование.
- Может быть основой для разработки отечественного РД «Системы контроля и управления, важные для безопасности на АЭС: проектирование»

Документы МАГАТЭ (продолжение):

NS-G-1.1. «Программное обеспечение для компьютерных систем, важных для безопасности АЭС»

- Целью данного документа является регулирование процессов получения (сбора) доказательной информации и подготовки документации, используемой для обоснования безопасности, применительно к ПО компьютерных систем, важных для безопасности АЭС, на всех фазах жизненного цикла таких систем.
- Может быть основой для разработки отечественного РД «Программное обеспечение для компьютерных систем, важных для безопасности на АЭС», хорошо согласованного с российскими ОПБ и ПБЯ.

Документы МЭК

Стандарт МЭК 61513 «Общие требования к системам контроля и управления, важным для безопасности АЭС»

Сходства и различия со стандартом МЭК 61508 «Функциональная безопасность»:

61508	61513
Анализ источников опасности и риска контролируемого объекта.	Определена исходная информация, которая требуется разработчикам СКУ от основного проекта и от документа по анализу безопасности.
Вероятностный подход к оценке значимости СКУ для безопасности.	Качественный (детерминистский) подход к такой оценке.
Установление уровней полноты безопасности по МЭК61508 почти полностью соответствует категоризации функций в МЭК61513.	

Документы МЭК (продолжение)
МЭК 61226 «Классификация функций контроля и управления, важных для безопасности»

- С внедрением компьютерных систем контроля и управления АЭС, важные для безопасности функции стали распределяться по нескольким системам.
- Цель – классификация важных для безопасности функций по категориям, в зависимости от их вклада в предупреждение и смягчение Постулированных Исходных Событий (ПИС), а также:
- Формулирование требований к проектированию систем и оборудования, выполняющих эти функции.

Документы МЭК (продолжение)
МЭК 61226: Категоризация функций

- **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.

- **К категории В** относят функции, которые играют дополнительную роль по отношению к функциям категории А в достижении или поддержании безопасности АЭС, в особенности функции, необходимые для эксплуатации после достижения контролируемого состояния с целью предотвращения развития проектных событий (ПС) до недопустимых последствий или для смягчения последствий ПС.

- **К категории С** относят функции, которые играют вспомогательную или косвенную роль в достижении или поддержании безопасности АЭС.

Сравнение классов (категорий) безопасности систем АЭС, приведенных в различных

Стандарт или нормативный документ	Классы безопасности (степень важности увеличивается слева направо)				
ПНАЭГ-01-011 (Российский)	Класс 4		Класс 3	Класс 2	Класс 1
МАГАТЭ NS-R-1	Системы, не важные для безопасности		Системы, важные для безопасности		Нет
			Системы, связанные с безопасностью	Системы безопасности	
МЭК 61226	Неклас-сифици-рованные	Класс С	Класс В	Класс А	Нет
IEEE 603	Не класс 1Е			Класс 1Е	Нет

ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

Российские нормативные документы:

- 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».

ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

Международные нормативные документы:

- 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».

Верификация и валидация ПО (V&V)

- Процесс V&V программного обеспечения определяет подтверждается ли в ходе разработки ПО и в результате его разработки, что разработанный продукт удовлетворяет требованиям его предназначения, а также потребностям пользователей
- Это определение может включать анализ, оценку, сравнение, проверку, и тестирование продуктов и процессов разработки ПО

Иллюстрация V&V

- **Верификация**

  Разрабатываем ли мы продукт **правильно**?

- **Валидация**

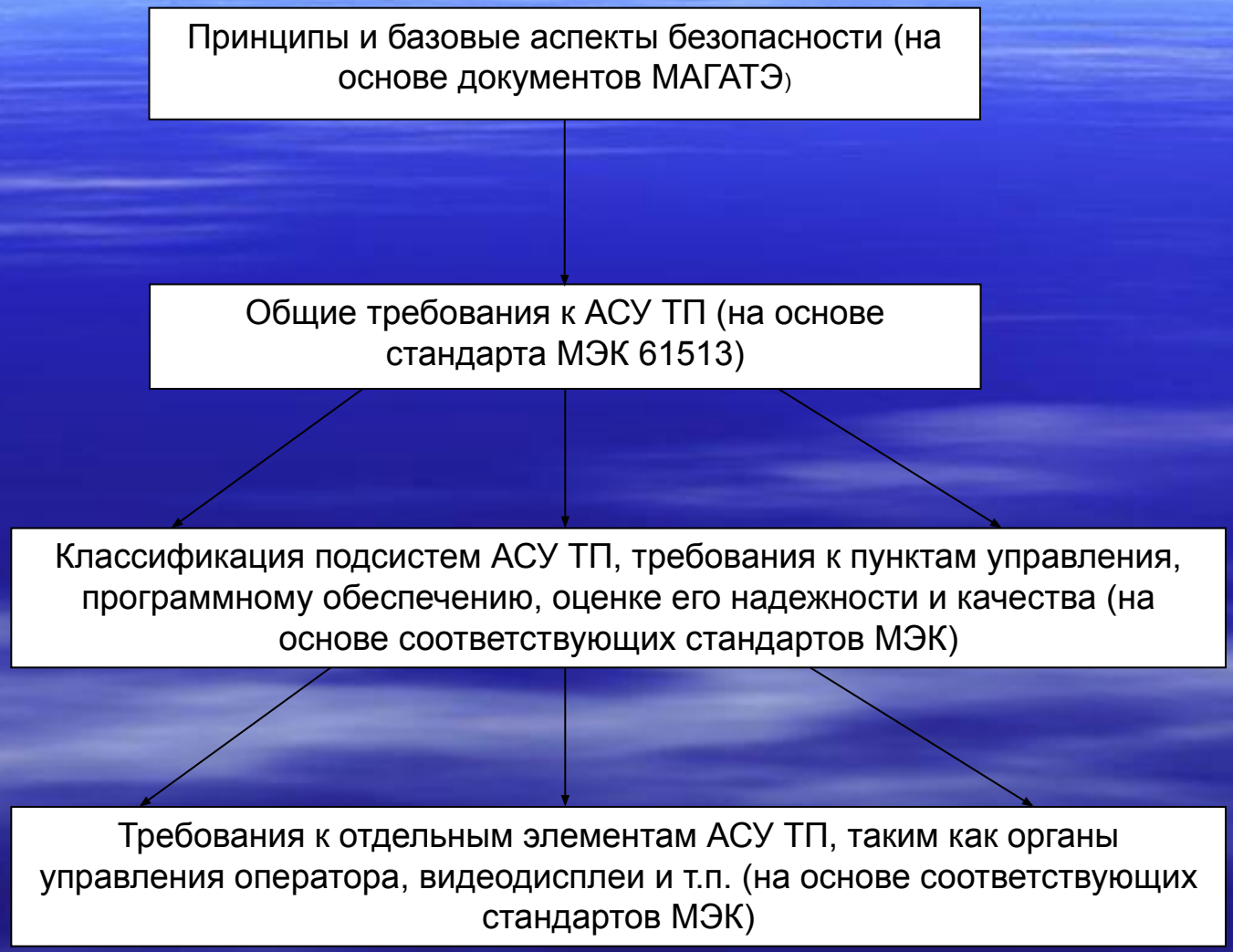
  Разработали ли мы **правильный** продукт?

V&V ПО в контексте обеспечения качества и иерархии стандартов.

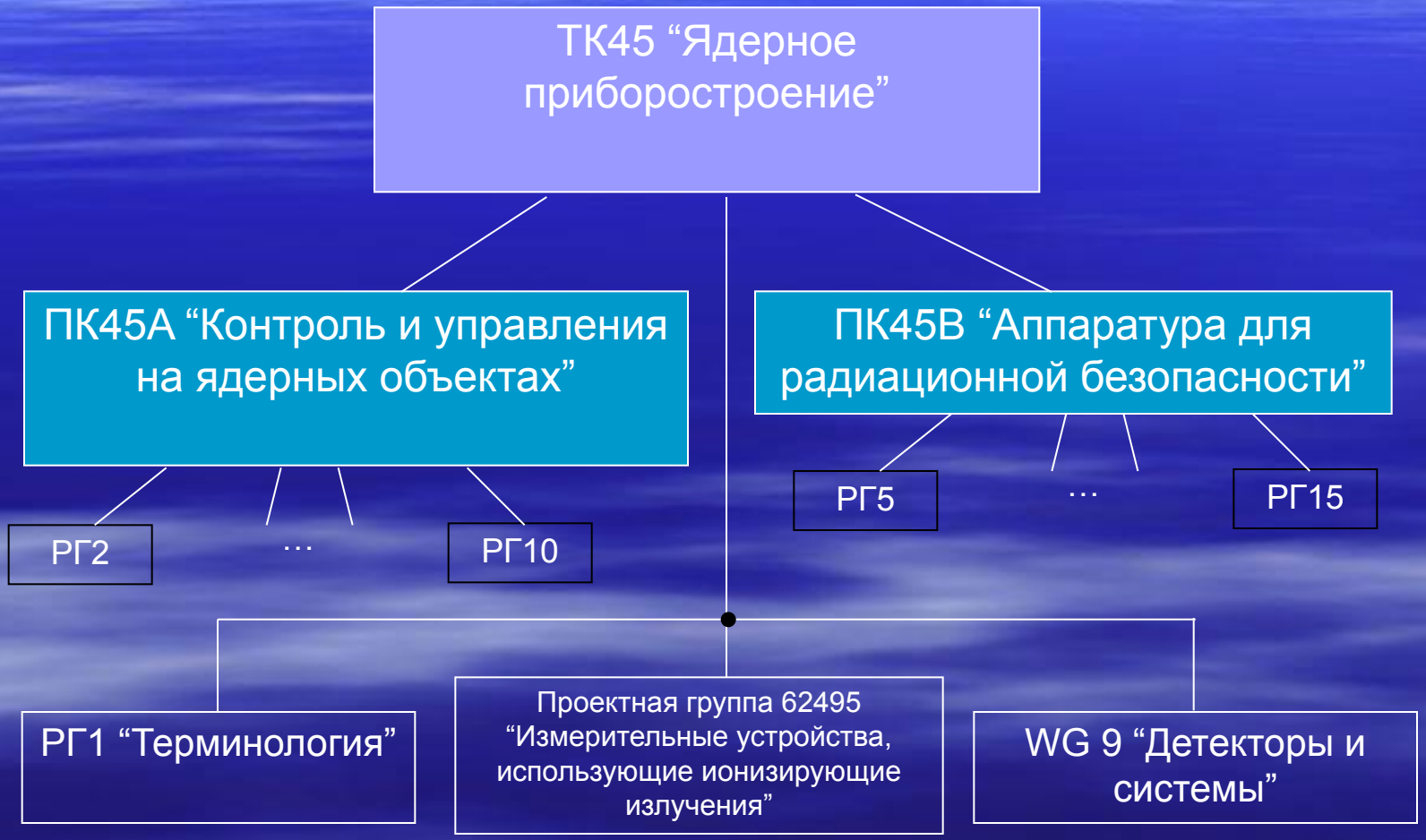
ПРОЕКТИРОВАНИЕ БЛОЧНЫХ ПУНКТОВ УПРАВЛЕНИЯ (БПУ), ФУНКЦИОНАЛЬНЫЙ АНАЛИЗ, ЧЕЛОВЕКО-МАШИННЫЙ ИНТЕРФЕЙС (ЧМИ)

- Использование методов инженерной психологии при разработке и внедрении цифровых систем и интерфейсов слабо отражено в существующих российских нормативных документах.
- Наиболее полезными в качестве основы для разработки соответствующих российских стандартов и регулирующих документов, касающихся функционального анализа, человеко-машинного интерфейса и проектирования БПУ, являются документы, разработанные в МЭК, NRC и EPRI.

Иерархическая структура разрабатываемых российских руководящих документов:



Структура МЭК/ТК45 «Ядерное приборостроение»



Рабочие группы ПК45А:

- РГА2 – датчики и измерительная техника
- РГА3 – Применение цифровых процессоров для обеспечения безопасности на атомных станциях
- РГА5 – Измерения, связанные со специальными технологическими процессами и радиационным контролем
- РГА7 – Надежность электрического оборудования в системах безопасности реакторов
- РГА8 – Пункты управления (БПУ, ДПУ)
- РГА9 – Измерительные системы
- РГА10 – Усовершенствование и модернизация систем контроля и управления атомных станций

Рабочие группы ПК45В:

- РГВ5 – Измерения излучений в окружающей среде
- РГВ7 – Оборудование для контроля внешнего загрязнения тела, конечностей и одежды персонала
- РГВ8 – Носимые активные электронные мониторы эквивалентной дозы и мощности эквивалентной дозы
- РГВ9 – Стационарное оборудование для контроля уровней излучений и активности на ядерных объектах
- РГВ10 – Измерительная аппаратура для измерения радона и его дочерних продуктов
- РГВ14 – Пассивные интегрирующие дозиметрические системы для контроля внешнего облучения
- РГВ15 – Аппаратура для обнаружения несанкционированного перемещения объектов, использующая спектрометрию, индивидуальные электронные дозиметры и портативные измерители мощности дозы

Итоги заседаний МЭК/ТК45 в Иокогаме (10 – 18 сентября 2009г.)

Количество рассмотренных проектов стандартов:

- ТК45: 4 проекта;
- ПК45А: 14 проектов;
- ПК45В: 12 проектов.

Основные проекты ТК45 и ПК45А:

- 60050-395 «Международный электротехнический словарь: часть 395 – Ядерное приборостроение»
- 61513 «Общие требования к системам контроля и управления», изд.2;
- 61500 «Передача данных в системах, выполняющих функции категории А», изд.2;
- 62566 «Выбор и применение сложных электронных компонентов для систем, выполняющих функции категории А»
- 62645 «Требования к защищенности программного обеспечения».

Основные проекты ПК45В:

- 62463 «Рентгеновские установки для обнаружения незаконно перемещаемых предметов отдельными лицами»;
- 62484 «Основанные на спектрометрии портальные мониторы для обнаружения и идентификации незаконно перемещаемых радиоактивных материалов»;
- 62523 «Радиографическая система для проверки транспорта и перевозимого груза»;
- 62533 «Чувствительные портативные приборы для обнаружения радиоактивных веществ»

Спасибо за внимание!