УДК 628.012.011.56:628.512:621.311.25:621.039

# ЭВОЛЮЦИЯ АСУТП АЭС ДЛЯ ВВЭР, ПРОБЛЕМЫ, НЕРЕШЕННЫЕ ВОПРОСЫ, НОВЫЕ УГРОЗЫ И ВОЗМОЖНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ

**И.Р. Коган**
*ОАО «Атомэнергопроект»*
Россия, 105005, Москва, Бакунинская ул., 7, стр. 1
E-mail: kogan@aep.ru

**А.Г. Полетыкин**
*Институт проблем управления им. В.А. Трапезникова РАН*
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: poletik@inbox.ru

**В.Г. Промыслов**
*Институт проблем управления им. В.А. Трапезникова РАН*
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: poletik@inbox.ru

**Е.Ф. Жарко**
*Институт проблем управления им. В.А. Трапезникова РАН*
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: zharko@ipu.ru

**Ключевые слова: АСУТП, АЭС**

**Аннотация:** Работа посвящена российским АСУТП АЭС. Прослеживается эволюция от первого поколения (релейная техника), через второе (унифицированные технические средства), до современных систем третьего поколения (микропроцессоры): рассматриваются функции, задачи, структурны решения. Приводятся описание и характеристика состояния российского приборостроения в этой области, его конкурентоспособности и перспективах. Проводится попытка анализа существующих проблем, нерешенных вопросов, новых угроз (кибервойны) и способов их решения для перспективного (четвертого) поколения.

## 1. Введение

Согласно [1] атомная энергетика и информационные технологии относятся к приоритетными направлениями развития науки и техники в РФ. АСУТП АЭС сочетают эти два направления и являются одним из высокотехнологичных отечественных продуктов, используемых с успехом в России и на мировом рынке. Это, в частности, подтверждается пуском АЭС «Бушер» в Иране и АЭС «Куданкулам» в Индии, которые построены по проектам РФ и оснащены отечественным оборудованием и АСУТП. Значительная

часть решений по АСУТП эксплуатируются и на отечественных АЭС, начиная с блока №3 Калининской АЭС.

Отечественные АСУТП АЭС для водо-водяных энергетических реакторов (ВВЭР), которые мы будем рассматривать в работе, прошли несколько этапов в своем развитии. Первый этап – это построение систем на основе жесткой логики, релейной техники, индивидуальных приборов контроля и управления и информационно вычислительных систем. Эти АСУТП были реализованы на малогабаритных реле и бесконтактных элементах и поставлены на Нововоронежскую АЭС (блок № 5) и другие АЭС и выполняли весь набор функций и задач, обеспечивающих надежную и безопасную работу АЭС по существующим тогда нормам. Это было достигнуто усилиями многих организаций, среди которых следует отметить Институт Атомэнергопроект, ЦНИИКА,ОКБ ГП, РНЦ КИ и СНИИП. Используемые средства имели относительно малый срок службы и низкую надежность. На данный момент времени завершена модернизация этих систем автоматизации этих АЭС с использованием современных средств автоматизации.

Второе поколение АСУТП АЭС было создано в эпоху массового строительства АЭС с ВВЭР, когда понадобились унифицированные решения. Отличия состоят в расширении перечня функций и задач, применением модульной унифицированной элементной базы на базе бесконтактных элементов и появлением компьютерных систем и дисплейных средств контроля. Типичные представители АСУТП этого поколения установлены на АЭС с реакторной установкой ВВЭР-320 (Запорожская и последующие АЭС). Переход на бесконтактные элементы способствовал повышению надежности, но внес и такие негативные моменты как задержки в прохождении команд и тендеции формирования ложных команд при отказах в элементной базе. Ключевую роль в этой работе играли следующие организации: Институт Атомэнергопроект, ЦНИИКА,ОКБ ГП, РНЦ КИ, СНИИП и НПО «Элва».

Третье поколение появилось в РФ в период массовой компьтеризации систем управления, когда иностранные заказчики потребовали, чтобы АСУТП были микропроцессорными и соответствовали требованиям МАГАТЭ в части функциональности, надежности и безопасности. Этот момент совпал с развалом промышленности в РФ, включая производство элементной базы и выпуск продукции Минприбором. Эта задача была успешно решена и такие АСУТП появились в России (Калининская АЭС, Нововоронежская АЭС) и за рубежом ( Иран, Индия). Ключевую роль в этой работе играли следующие организации: Институт Атомэнергопроект ,ОКБ ГП, РНЦ КИ, ИПУ РАН, СНИИП, ВНИИА и НИИИС.

Во второй части работы будут описаны задачи АСУТП АЭС третьего поколения, технические решения, включая подходы ИПУ РАН к созданию систем верхнего блочного уровня (СВБУ) [2-3], особенности применения программируемой автоматики, методы верификации и валидации, средства автоматизации проектирования и интеграции АСУТП на заводах изготовителях.

В третьей части будет критически проанализирован опыт внедрения и эксплуатации АСУТП АЭС третьего поколения, не решенные проблемы.

Четвертая часть будет посвящена новым проблемам, связанные с началом эпохи кибервойн, которые угрожают всей цифровой инфраструктуре общества, к которой относятся и АСУТП АЭС [4].

В заключительной пятой части работы будут очерчены контуры АСУТП АЭС четвертого поколения: функции, надежность, безопасность, защищенность, эффективность и конкурентоспособность.

# 2. АСУТП АЭС третьего поколения

Разработка АСУТП базировалась на накопленном опыте эксплуатации АСУТП в РФ, системных проработках ИПУ РАН по перспективному проекту АСУТП [], а также постановке на производство в ВНИИА современной техники автоматизации по лицензии фирмы Siemens (Германия).

Требования Заказчиков о необходимости создания современной цифровой АСУТП и развал промышленности в РФ не позволявший обеспечить производство технических средств даже второго поколения привели к необходимости создания новой системы и средств для ее реализации.

Конкурентоспособность и привлекательность АСУТП для потенциального Заказчика тогда (90-годы) и сейчас определяется следующими признаками:

- выполнением НД, наличием сертификатов соответствия;
- наличием референции;
- уровнем автоматизации;
- удобством в эксплуатации (ЧМИ, глубокой самодиагностикой, сервисными средствами, отсутствием необходимости проведения профилактики на работающем блоке);
- ценой.

По этим направлениям и были развернуты работы по созданию новой АСУТП АЭС 3-го поколения. Разработка базировалась на следующих основных подходах:

- система создается в полном соответствии с требованиями ГОСТ 34 серии и, в первую очередь с соблюдением всех этапов и стадий (ТЗ на АСУТП, Техпроект и т.д.);
- система реализуется, как правило, на программируемой современной технике, а также с использованием средств «жесткой логики», реализуемой на ПЛИС , для отдельных задач, связанных безопасностью АЭС;
- система АСУТП энергоблока должна строиться как комплекс состоящий из ряда подсистем/ПТК интегрированных в единую систему с помощью системы верхнего блочного уровня(СВБУ) , которая интегрирует все подсистемы нижнего уровня, решает общеблочные задачи, а также обеспечивает обмен сигналами между ПТК нижнего уровня в предусмотренном проектом объеме;
- основной вид управления оборудованием для обеспечения безопасности АЭС и персонала, а также защиты дорогостоящего оборудования- автоматический;
- основной вид дистанционного управления оборудованием нормальной эксплуатации- с мониторов рабочих станций, куда также выведена сигнализация положения оборудования, аварийная и предупредительная сигнализация по параметрам и неисправностям оборудования;
- для проверки работоспособности средств и проектных решений, а также обоснования ЧМИ предусмотрен полигон АСУТП, оснащенный математической моделью объекта.

Технический проект АСУТП третьего поколения был разработан впервые для АЭС «Бушер» (Иран) конце 1990-х годов.

Работа велась в ОАО «Атомэнергопроект» с привлечением других организаций.

Основные решения проекта состоят в следующем:

- централизация контроля и управления на БПУ (в блочной части) и ЦПУ (в части общестанционных систем);
- применение программируемой техники;
- создание единого ЧМИ для контроля и управления блоком в нормальном режиме и при нарушениях нормальной эксплуатации;

- приближение средств автоматизации к объекту;
- оптимальный уровень автоматизации, разгрузка операторов от выполнения редких операций, не влияющих на ТП выработки электроэнергии;
- унификация средств автоматизации и рациональное распределение задач между ними;
- устранение замечаний EUR к проекту АЭС-92 (отсутствие единого мониторного контроля и управления, а также недостаточность обоснований по защите от отказов по общей причине).

В проектах АЭС 2006 и ВВЭР ТОИ ведется эволюционное развитие отдельных направлений с целью дальнейшего усовершенствования АСУТП третьего поколения.

Для интеграции АСУТП потребовалась интегрирующая система, соединяющая все цифровые ПТК в единое целое. Такой системой стала система верхнего блочного уровня (СВБУ), предложенная одним из авторов данной статьи И.Р. Коганом (Институт Атомэнергопроект и М.А. Зуенковым (ИПУ РАН).

СВБУ создана для обеспечения централизации контроля и управления технологическим процессом для достижения следующих целей:

- экономически эффективного производства продукции;
- соблюдения эксплуатационных пределов;
- соблюдения пределов и условий безопасной эксплуатации оборудования;
- улучшения характеристик технологических процессов и работы технологического оборудования;
- уменьшения трудоемкости эксплуатации оборудования, улучшения ремонтопригодности технических средств, снижения численности обслуживаемого персонала, улучшения потребительских характеристик элементов АСУТП;
- улучшения условий труда персонала, сокращения его числа и уменьшения последствий от ошибочных действий оператора.

На основе теоретических исследований существующих методов управления, а также в результате анализа мирового опыта были сформулированы следующие основные задачи СВБУ:

- регистрация текущего состояния и технологических событий, аварийных и переходных процессов;
- представление обобщенной информации по готовности технических систем безопасности;
- ведение протокола текущих событий;
- представление информации о режимах работы оборудования и автоматики;
- представление справочной информации;
- сбор данных о командах персонала;
- отображение мнемосхем и видеограмм на графических дисплеях;
- отображение информации для управления на видеодисплеях;
- аварийная и предупредительная сигнализация на видеодисплеях;
- регистрация приема, выдачи и обработки управляющих воздействий, введенных с СВБУ, в архиве СВБУ с присвоением им меток времени;
- регистрация приема, выдачи и обработки управляющих воздействий, введенных при помощи ключей индивидуального управления, в архиве СВБУ;
- представление информации по расчетным задачам и задачам анализа оперативного состояния и диагностики;
- архивация ресурса работы оборудования и диагностики его работы;
- регистрация и архивация состояния, ремонтов и замен технологического оборудования;

- регистрация записей операторов и их архивация;
- распечатка данных за смену и периодических отчетов;
- управление локальными регуляторами с рабочих станций;
- контроль и управление режимом технологической защиты (технологической блокировки) с рабочих станций;
- управление программами логического управления с рабочих станций;
- сбор и обработка информации о состоянии средств и систем АСУТП;
- диагностика технических и программных средств АСУТП;
- ведение единого времени и присвоение метки времени при сборе данных;
- информационная поддержка управления штатным функционированием системы;
- операторское управление функционированием СВБУ;
- автоматическое управление в части автоматического реконфигурирования резервируемых элементов СВБУ, и рестарта системы после отказа по общей причине (обесточивания);
- управление контрольными и диагностическими задачами.

СВБУ представляет собой распределенный программно-технический комплекс, основными элементами которого являются автоматизированные рабочие места, дублированные серверы, локальная вычислительная сеть и шлюзовые устройства.

Взаимодействие СВБУ со смежными программно-техническими комплексами АСУТП осуществляется через шлюзы, подключенные к ЛВС СВБУ, в которых на программном уровне обеспечивается информационная совместимость с СВБУ.

Особенностью взаимодействия элементов СВБУ является применение технологии «клиент-сервер», в результате чего алгоритм функционирования каждой подсистемы разбивается на совокупность алгоритмов функционирования шлюзов, серверов и рабочих станций, решающих соответствующие им задачи внутри себя и обменивающихся между собой сетевыми сообщениями.

СВБУ создавалась для разных АЭС разными организациями. Технические средства были созданы ФГУП НИИИС на основе импортных комплектующих. Программное обеспечение для российских АЭС создавалось на основе зарубежной программной платформы ВНИИАЭС, для экспортных контрактов – на основе отечественной разработки ИПУ РАН (Система «Оператор»).

В АСУТП третьего поколения программное обеспечение играет ключевую роль. Поэтому для достижения заявленных целей пришлось создать технологическую базу обеспечения безопасности, верификации и аттестации программного обеспечения. Из-за того, что первые АСУТП строились для иностранного заказчика, за основу были взяты международные стандарты. В современных системах, важных для безопасности АЭС, программное обеспечение применяется повсеместно, начиная от контроллеров и заканчивая общестанционными системами, предназначенными для организации управления многоблочных АЭС в целом. Обеспечение качества программного обеспечения – непрерывный процесс в течение всего жизненного цикла ПО [9]. Определение качества программного обеспечения помогает оценить программные изделия; оценить принципы организации программного обеспечения; улучшить процессы создания программного обеспечения.

Требуемое качество программного обеспечения трудно достичь. Процесс получения требуемого качества программного обеспечения затрагивает процесс разработки, методы и управление процессом. Качество программного обеспечения достигается благодаря применению методологии разработки и использованию методов верификации и валидации в течение жизненного цикла разработки ПО для систем важных для безо-

пасности АЭС. На рис. 1 представлено место верификации и валидации программного обеспечения в контексте обеспечения качества и иерархии стандартов.

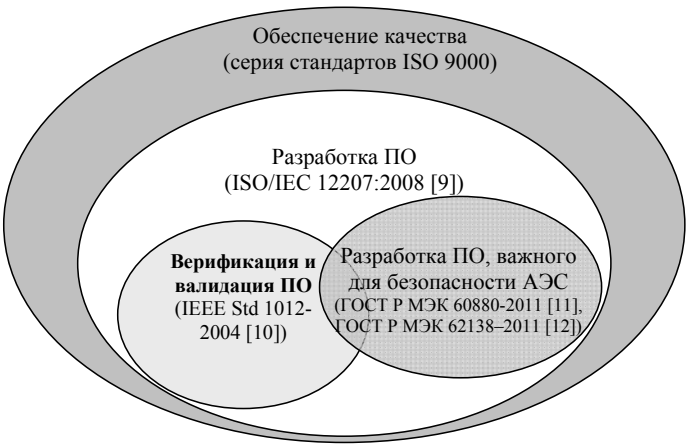


**Рис. 1.** Место верификации и валидации программного обеспеченияв обеспечении качества ПО систем, важных для безопасности АЭС.

Институт проблем управления им. В.А. Трапезникова РАН (ИПУ РАН) проводил работы по верификации программного обеспечения систем важных для безопасности, относящихся к классам безопасности 2-4 согласно классификации по НП-001-97 [6]. В частности, по требованиям для класса 3 (системы, важные для безопасности) были верифицированы операционная система Lics, ПО СВБУ, по классам 2 и 3 компоненты УКТС и перегрузочных машин ЗАО «Диаконт».

Хотя классификация систем по безопасности, применяемая в разных странах различна (рис. 2), методики верификации основаны на одних и тех же стандартах (рис. 1). Это, в частности, было подтверждено тем, что надзорные органы Индии остались удовлетворенными качеством тех материалов, которые были им предоставлены в части подтверждения качества ПО. Можно утверждать, что технология создания ПО для АЭС в России не уступает мировому уровню и само ПО имеет экспортный потенциал в любые страны мира.

**Таблица 1.** Сравнение классов безопасности систем АЭС.

<table>
<tr><th>Стандарт или нормативный документ</th><th colspan="5">Классы безопасности<br>(степень важности увеличивается слева направо)</th></tr>
<tr><td>ПНАЭГ-01-011 [6]</td><td colspan="2">Класс 4</td><td colspan="2">Класс 3</td><td>Класс 2</td><td>Класс 1</td></tr>
<tr><td rowspan="2">IAEA<br>NS-R-1 [7]</td><td colspan="2" rowspan="2">Системы, не важные для безопасности</td><td colspan="2">Системы, важные для безопасности</td><td colspan="2">Нет</td></tr>
<tr><td colspan="2">Системы, связанные с безопасностью</td><td>Системы безопасности</td></tr>
<tr><td>ГОСТ Р МЭК 61226-2011 [3]</td><td>Неклассифицированные</td><td>Класс С</td><td>Класс В</td><td>Класс А</td><td>Нет</td></tr>
<tr><td>IEEE 603 [8]</td><td colspan="3">Не класс 1Е</td><td>Класс 1Е</td><td>Нет</td></tr>
</table>

В АСУТП третьего поколения ПО играет также главенствующую роль в процессах испытаний, интеграции, пуско-наладочных работах и сопровождении. В частности, вначале стихийно, а затем целенаправленно под руководством специалистов ОАО «Атомстройэкспорт», была создана безбумажная технология обмена исходными дан-

ными, необходимыми всем разработчикам подсистем АСУТП. Ее можно считать примером успешного создания CALS-технологии.

В отличие АСУТП АЭМ третьего поколения впервые была включена функция регистрации важных параметров безопасности ("Черный ящик"). Формально система регистрации важных параметров безопасности (СРВПЭ) входит в СВБУ, но на многих АЭС (например, «Бушер», «Куданкулам») она была разработана с использованием тех же самых программных комплексов и с участием тех же коллективов.

# 3. Критический анализ современных АСУТП АЭС

## 3.1. Устойчивость к внешним воздействующим факторам

Накопленный опыт эксплуатации АЭС в мире показал, что не смотря на особое внимание к проектам АЭС недоучет внешних факторов приводит к трагическим последствиям. Одним из таковых являются события на АЭС «Фокусима» в Японии. АЭС Куданкулам в Индии и последующие проекты АЭС в РФ (НВАЭС2) оснащены пассивными системами безопасности (СПОТ) , позволяющими преодолевать запроектные ситуации связанные с полной потерей источников переменного тока, что имело место в Японии. СПОТ позволяет обеспечить отвод тепла от реактора в атмосферу без активных систем. Для контроля за ситуацией в нашей АСУ ТА предусмотрена система аварийного и поставарийного мониторинга ограниченной группы параметров, которая обеспечивается электропитанием на не менее чем 24 часа, что способствует преодолению такого рода ситуаций. Средства контроля при этом рассчитаны на работу в таких условиях. В следующих проектах эти режимы должны быть еще более глубоко проработаны.

## 3.2. Отказ по общей причине в АСУТП

Применение программируемой техники позволило сократить количество средств и реализовать самодиагностику. Но при этом внесло негативное явление, связанное с применением одного программного обеспечения во всех каналах систем безопасности. Отсутствие наглядности в программном обеспечении, методик его анализа и расчета надежности не позволяют убедительно обосновать отсутствие отказов во всех каналах систем безопасности по общей причине, обусловленной наличием программного обеспечения. В связи с этим в последних проектах АСУТП применены аварийные защиты состоящие из основного и диверсных комплектов, работающих на разных программных платформах. Это усложняет эксплуатацию АСУТП и повышает ее стоимость. Над этим необходимо работать на последующих проектах в направлении уменьшения количества диверсных защит например, за счет применения одной такой системы, а не в каждом канале безопасности.

## 3.3. Инфрмационная поддержка оперативного персонала

В проектах третьего поколения реализуется информационная поддержка персонала в объеме светозвуковой сигнализации, привлекающей внимание операторов к возникновению на блоке событий связанных с выходом параметров за пределы нормальной эксплуатации , срабатывания устройств защит и автоматики, включая защиты безопасности реакторной установки, а также системы поддержки по параметрам безопасности и расчета и анализа технико-экономических показателей работы энергоблока для контроля и управления им с точки зрения выработки электроэнергии с минимальными затратами при безусловном соблюдении пределов и условий безопасной эксплуатации.

Большое количество сообщений, выводимых операторам (до 60000) в разных режимах работы энергоблока не дает возможность быстрого реагирования на них. В проекте принято разделение этих сигналов по группам важности с подавлением части сигналов не актуальных для текущего момента. Кроме этого во многих случаях при одном событии возникает группа сигналов, связанных с ним и работой устройств автоматики. В международной практике применяется принцип «одно событие – один обобщенный сигнал по его преодолению». Этот подход не нашел решений в наших проектах.

## 3.4. Ошибки персонала

Повышение надежности технологического оборудования и средств АСУТП сократили их вклад в останов блока. При этом стало существенным влияние ошибок персонала на ложные остановы блока и большие временные затраты на проверки АСУТП при плановых периодических ремонтах, что не позволяет сократить его время.

Повышение уровня автоматизации способствует снижению ошибок оперативного персонала. При этом должна бать такая информированность персонала, что бы он при нештатных ситуациях, включая отказы средств автоматики, мог вмешаться и продолжить процесс.

Для сокращения трудозатрат на эксплуатацию необходимо продолжение работ по унификации средств на АЭС и программных платформ, а также создание единого человеко машинного интерфейса.

В проектах третьего поколения заложен ряд систем направленных на поддержку экспдуатации в части сокращения трудозатрат на профилактические ремонты. К ним относятся системы диагностирования арматуры, позволяющая перейти от ревизии по графику к ревизии по оценке состояния арматуры, системы контроля вибрации подшипников механизмов и диагностики их работоспособности, система контроля остаточного ресурса реакторной установки, системы контроля течей и т.п.

## 3.5. Маневренность энергоблока

В настоящее время энергосистемы ужесточают вопросы необходимости участия энергоблоков не только в базовом режиме, но и в режиме участия в поддержании частоты в энергосистеме. Стоимость продаваемой электроэнергии ставится в зависимость от реализации этой задачи. На данном этапе предусмотрен очень не большой диапазон участия (от+2 до -8%). Что не достаточно как для РФ так и для инозаказчиков.

## 3.6. Сложность и/или простота

Современные АСУТП АЭС состоят из большого числа разнообразного оборудования, что безусловно усложняет эксплуатацию и ремонт. Но сейчас это обычный прием в технике, когда сложные системы строятся из «кубиков», которые совместимы по интерфейсам, но внутри разные.

Что касается изготовления, поставки, наладки, получается весьма неплохо. Например, для АЭС «Куданкулам» оборудование было изготовлено с высокой степенью готовности и интегрированности друг с другом. Это позволило совершить то, во что никто из российских специалистов изначально не верил: на АЭС все оборудование было смонтировано и налажено силами индийских специалистов с минимальным обучением и участием российских шеф-наладчиков. Это свойство российских технологий может показаться весьма привлекательным при строительстве АЭС в странах, ограничивающих привлечение иностранной рабочей силы.

### 3.7. Экраны коллективного пользования

На российских блочных пультах применяются экраны коллективного пользования, входящие в АСУТП АЭС – на зарубежных АЭС (например, «Бушер», «Куданкулам») , построенных по российским проектам, не применяются. И те и другие работают успешно. Возникает вопрос: а нужны ли они вообще? Необходимо проанализировать опыт эксплуатации и решить этот вопрос.

### 3.8. Интеллектуальные алгоритмы

Нужно констатировать, что ожидания о массовом внедрении функционально-группового управления и других «интеллектуальных» алгоритмов не оправдались, несмотря на то, что технические средства располагают всем необходимым. Это обстоятельство также требует проведения исследований, на основе которых необходимо решать, нужно ли усложнять технические возможности АСУТП, либо наоборот упрощать.

## 4. Кибербезопасность

### 4.1. Кибербезопасность АСУТП и ее место в безопасности АЭС

Система управления технологическими процессами АЭС включена в процесс взаимодействия в сложной неоднородной среде, где возможно присутствие конфликта интересов на всех уровнях от индивидуального до государственного, который приведет к тому, что отдельные лица или группы лиц будут заинтересованы в нанесении тем или иным способом вреда АЭС и одним из проводников данных действий является АСУТП АЭС.В случае конфликта на межгосударственномуровне злоумышленные действия могут быть классифицированы как военные [5,6]. Озабоченность вызывают не только внешние угрозы; серьезный риск для безопасности могут представлять хорошо информированные инсайдеры, имеющие злые намерения, или даже невинное, неумышленное действие.

Под термином «кибербезопасность» в статье понимается предотвращение незаконного или нежелательного проникновения, умышленного или неумышленного вмешательства в штатную и запланированную работу, или получения ненадлежащего доступа к конфиденциальной информации в АСУТП. Для обозначения других аспектов безопасности (ядерной, физической будет использован термин безопасность с поясняющим прилагательным). В узкоспециализированном контексте АЭС используется понятие ядерной безопасности - свойство АСУТП при нормальной эксплуатации и нарушениях нормальной эксплуатации, включая аварии, ограничивать радиационное воздействие на персонал, население и окружающую среду установленными пределами.

АСУТП взаимодействует непосредственно с оборудованием АЭС и привязано к процессу производства энергии, поэтому разглашение производственных тайн и сбои в передачи информации – не единственные последствия нарушения кибербезопасности для АСУТП АЭС. Более серьезными последствиями являются вероятность человеческих жертв или экономических потерь, вред окружающей среде, нарушения норм и правил ядерной безопасности в эксплуатации. Для АЭС последствия нарушений могут выходить за пределы АЭС и иметь влияние на состояние целого региона или государства.

Современная АСУТП АЭС реализуется как распределенная по функциям и средствам система с компонентами, взаимодействующими между собой и объектом посредст-

вом локальной вычислительной сети. Функционально, как часть одного процесса, АСУТП объединена с другими бизнес-системами АЭС, имеется тенденция к появлению возможности удалённого доступа к сервисам АСУТП (пока в основном к ограниченному набору сигналов для кризисных центров) с использованием общедоступных линий связи. Многообразие функций АСУТП, интегрированность с объектом управления, очевидно, приводит к многообразию угроз и потенциальной опасности при нарушении кибербезопасности АСУТП АЭС.

Тематика обеспечения кибербезопасности АСУТП не является абсолютно новой и обсуждается, как на международном, так и на российском уровне (стандарты, разрабатываемые IEC (International Electrotechnical Commission), в части кибербезопасности цифровых систем управления АЭС, стандарты серии ISO/IEC 27000 [9] в части общих принципов обеспечения безопасности цифровых систем управления; Руководящий документ МАГАТЭ [10] и др.). Основное внимание нами уделено аспектам кибербезопасности, которые будут иметь, на наш взгляд, наибольшее значение в будущем.

## 4.2. «Перспективные» киберугрозы и меры защиты

Вместе с развитием АСУТП будут развиваться и совершенствоваться угрозы кибербезопасности. Нами выделены следующие основные «перспективные» угрозы:

- фактором уязвимости для безопасности такого сложного объекта, как АСУТП АЭС, является её значительная сложность. АСУТП включает в себя большое количество объектов и субъектов, связанных отношениями кибербезопасности, что может привести к наличию внутренних противоречий или неполноте политик безопасности;
- АСУТП постепенно переходят на готовые коммерческие компоненты и протоколы передачи, и объединяются с бизнес-сетями. В результате АСУТП уязвимо перед теми же программными атаками, что и деловые и настольные устройства, что позволяет уменьшить требования к наличию специальных знаний по АСУТП у злоумышленников и расширить их потенциальный круг;
- наличие широкой кооперации, партнерства со сторонними организациями при создании и эксплуатации АСУТП привело к резкому увеличению численности организаций и групп, имеющих необходимые специальные знания и навыки для атаки на АСУТП;
- применение готовых коммерческих компонентов ведет к существенной функциональной и аппаратной избыточности системы, что дает в руки злоумышленника набор средств для атаки, наличие которых не учитывалось при проектировании АСУТП и оценки её влияния на безопасность;
- миниатюризация компонентов систем управления позволяет более легко нарушать физические барьеры безопасности и встраивать в АСУТП компоненты, имеющие вредоносное или двойное назначение, трудно обнаруживаемые при первичном осмотре.

В соответствии с сформулированными «перспективными» киберугрозами, создание кибербезопасной АСУТП может быть обеспечено применение следующих мер для их нейтрализации:

- обязательное создание формальной модели безопасности для АСУТП АЭС [11], охватывающий все этапы жизненного цикла. Модель должна использоваться для верификации политики безопасности АСУТП на предмет удовлетворения норм и правил ядерной безопасности АЭС. Модели безопасности позволяют, благодаря более компактному, формальному описанию, – выявить требования к безопасности и важные характеристики среды на уровне детальности, необходимом для рассмотрения вопросов безопасности с общим пониманием контекста

- проектирование АСУТП с реализацией уровней и зон безопасности, позволяющих ограничить и локализовать нарушения безопасности и не допустить полного вывода АСУТП из строя
- для критических с точки зрения кибербезопасности компонентов АСУТП необходимо применять полностью верифицированный программный код и технические средства;
- заложить в проекты и реализовать функции обеспечения целостности (неизменности) программ и статических данных, защиту потоков информации и динамических данных от искажений в процессе эксплуатации;
- использования принципа разнообразия не только для повышения надежности, но и кибербезопасности (удешевление и миниатюризация компонентов предоставляют возможность введения принципа разнообразия на всех уровнях системы).

Внедрение указанных мер не устранит угрозы кибербезопасности, но позволит при определенных усилиях снизить риски, связанные с ними, до уровня приемлемого для эксплуатанта АЭС, общества и государства. Отметим, что в виду постоянства угроз, их эволюционирующего характера, деятельность по аудиту кибербезопасности, внедрения мер по ее улучшению, должна проводиться на постоянной основе, в течении всего жизненного цикла АСУТП.

## 5. АСУТП АЭС четвертого поколения, прогноз

Анализ зарубежных источников показывает, что компьютерные средства ввода и отображения информации полностью вытесняют традиционные приборы и ключи управления из компоновки блочных пультов. Примером может служить проект фирмы Mitsubishi [12], (рисунок пульта можно посмотреть в электронной монографии [3]), предлагаемый на американском рынке (рис. 23 в [3]): нет мозаичных панелей, индивидуальных ключей управлениями и приборов, нет деления на зоны безопасности и нормальной эксплуатации, остаются только пульты СВБУ, через которые можно выполнять все работы не вставая с места, и несколько широкоформатных дисплев. Это вполне оправдано, и, мы считаем, будет реализовано в АСУТП АЭС четвертого поколения.

Киберугрозы повлияют на АСУТП АЭС очень серьезным образом. Это скажется на программно технических средствах, всех этапах разработки и на конечном результате. Главное связано с тем, что киберугрозы будут рассматриваться наравне с угрозами землятресений, падения самолетов и другими угрозами безопасности, отраженными сейчас в нормативных документах. В обосновании безопасности АЭС придется оценивать риски, связанные с кибератаками. К чему это приведет, пока не ясно, но можно констатировать одно: современные программно технические средства АСУТП не годятся. АСУТП АЭС четвертого поколения будет основано на новых или обновленных технических средствах, надежно защищенных от кибератак. Сейчас таких нет (и быть не может так, как нет требований), поэтому возможно для наиболее важных узлов пройдется отказаться от микропроцессорной техники.

## 6. Заключение

Созданные АСУТП для АЭС в РФ и за рубежом успешно работают и положительно оцениваются Заказчиками.

Накопленный опыт позволил выявить ряд проблем требующих совершенства.

К их числу относятся: необходимость унификации и сокращения номенклатуры средств и программного обеспечения, повышения самодиагностики АСУТП и ее защищенности обеспечение участия в маневренных режимах для поддержания частоты в энергосистеме, обеспечение кибербезопасности.

# Список литературы


1. Указ Президента РФ от 7 июля 2011 г. № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации».
2. Бывайков М.Е., Жарко Е.Ф., Менгазетдинов Н.Э. и др. Опыт проектирования и внедрения системы верхнего блочного уровня АСУТП АЭС // Автоматика и телемеханика. 2006. № 5. С. 65-68.
3. Менгазетдинов Н.Э., Полетыкин А.Г., Промыслов В.Г., Зуенкова И.Н., Бывайков М.Е., Прокофьев В.Н., Коган И.Р., Коршунов А.С., Фельдман М.Е., Кольцов В.А. Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУТП для АЭС «Бушер» на основе отечественных информационных технологий. М.: ИПУ РАН, 2013. 95 с. http://www.ipu.ru/sites/default/files/page_file/busher.pdf
4. Менгазетдинов Н.Э., Полетыкин А.Г., Промыслов В.Г. Новые кибернетические угрозы и методы обеспечения кибербезопасности в цифровых системах // Энергетик 2012. № 7. С. 34-41.
5. Clarke Richard A. Cyber War. HarperCollins, 2010.
6. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. 1996.
7. Полетыкин А.Г., Промыслов В.Г., Менгазетдинов Н.Э. Концепция обеспечения защиты от несанкционированного доступа АСУТП АЭС «Бушер-1» // Автоматизация в промышленности. 2005. № 5. С. 3-5.
8. ISO/IEC 12207:2008. Systems and software engineering – Software life cycle processes.
9. IEC 62645 “Nuclear power plants – Instrumentation and control systems – Requirements for security programs for computer-based systems”. (Стандарт в процессе разработки).
10. Computer security at nuclear facilities reference manual International Atomic Energy Agency Vienna, 2011. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf
11. Промыслов В.Г., Полетыкин А.Г. Формальная иерархическая модель безопасности верхнего уровня АСУТП АЭС // Ядерные измерительно-информационные технологии. 2012. Т. 4 (44).
12. Hanada X. Satoshi, Ito Koji, Mashio Kenji. The Human Factors Engineering Process and Human System Interface Design of the US-APWR // Proceedings of ICAPP '2011. Nice, France, May 2-5, 2011. P. 101-108.