УДК 004: 621.039

ТЕНДЕНЦИИ РАЗВИТИЯ АСУ ТП НА НОВОВОРОНЕЖСКОЙ АЭС

Д.В. Терехов*, Е.В. Сидоренко, А.Д. Данилов*****

**** Филиал АО «Концерн Росэнергоатом», «Нововоронежская атомная станция»***
396071, Воронежская обл., г. Нововоронеж, промышленная зона Южная, 1.
***** Нововоронежское представительство ООО Корпорация «Электросевкавмонтаж»***
350911, Краснодарский край, г. Краснодар, ул. Трамвайная, 5
****** Воронежский государственный технический университет***
3940029, г. Воронеж, Московский проспект, 14

Рассмотрена эволюция АСУ ТП на атомных электрических станциях от традиционных средств автоматики с жесткой логикой на основе архаичных средств (стрелочных приборов, самописцев, световых индикаторов, ключей индивидуального управления оборудованием и т.п.) до современных автоматизированных информационно-управляющих систем на основе программно-технических комплексов высокого уровня. Приведена характеристика особенностей, влияющих на проектные решения по АСУ ТП, таких как непрерывность процессов, многообразие оборудования и оснастки, сложность и разнородность программных и технических средств, централизация информации и т.д. Показано, что современные АСУ ТП для объектов ядерной энергетики должны содержать в себе систему верхнего блочного уровня. Рассмотрена общая архитектура такой системы и представлен ее состав на примере АСУ ТП НВ АЭС-2. Проведен детальный анализ проблем функционирования данной системы, заключающихся в неэффективной работе коммуникационной шины из-за лавинообразных информационных процессов при передаче широковещательных сообщений, что парализует работу сети и всей АСУ ТП. Предложены первоочередные мероприятия, направленные на повышение устойчивости АСУ ТП: автоматическое восстановление работоспособности за заданное время, исключение ложной работы регуляторов и блокировок, визуализация информации по параметрам на панелях безопасности и экране общего пользования. Проведен анализ вопросов кибербезопасности работы информационных подсистем АСУ ТП АЭС и предложено решение для повышения уровня путем дублирования и резервирования каналов передачи данных.

Ключевые слова: автоматизированная система управления технологическим процессом, программно-технический комплекс, система верхнего блочного уровня, широковещательный шторм, кибербезопасность.

ВВЕДЕНИЕ

Атомные электрические станции (АЭС) как сложные производственные объекты ядерной энергетики и задачи управления отдельными технологическими процессами и всем производственным комплексом от входа сырья в реактор и до выхода электрической энергии являются одними из основных вопросов обеспечения бесперебойной и надежной эксплуатации объекта. Строительство и эксплуатация АЭС сопровождались созда-

нием и серийным освоением выпуска автоматизированных комплексов аппаратуры контроля, управления и защиты, обеспечения ядерной и радиационной безопасности.

Разработка новых отечественных реакторов велась параллельно с разработкой новых автоматизированных систем управления технологическими процессами (АСУ ТП).

Первые АСУ ТП строились на основе традиционных средств автоматики с жесткой логикой, а программируемые контроллеры практически не применялись. Кроме этого средства контроля и управления блочного пульта АЭС создавались на основе архаичных средств – стрелочные приборы, самописцы, световые индикаторы, ключи индивидуального управления оборудованием и т.п. В результате отечественные АСУ ТП АЭС занимали огромные помещения, требовали большого количества эксплуатационного и ремонтного персонала.

Основные задачи, решаемые первыми АСУ ТП, в принципе, актуальны и сейчас. К ним относят

– получение информации с помощью контрольно-измерительной аппаратуры о состоянии параметров объекта контроля и управления и представление ее в удобном для последующей обработки виде; ряд параметров, например, расход или уровень теплоносителя, регистрируется в прямом виде, другие с помощью различных преобразователей формируются косвенным путем;

– отслеживание изменения параметров объекта, обеспечение стабильности регулируемого технологического процесса и поддержание его в установленных границах в соответствии с заданным законом регулирования;

– технологическая защита и блокировка с целью обеспечения нормального функционирования оборудования при изменении режима работы или возникновении локальных нарушений в работе оборудования путем включения резервных вспомогательных механизмов либо обеспечением заданной последовательности переключений в процессе управления (с целью упрощения управления и предотвращения ошибок).

ЭВОЛЮЦИЯ ТЕХНИЧЕСКИХ СРЕДСТВ АВТОМАТИЗАЦИИ

Надежность АСУ ТП в целом в проектах вплоть до 1990-х гг. обеспечивалась за счет независимости ее элементов, локализации отдельных алгоритмов, регуляторов, индивидуальных замеров на отдельных различных технических средствах; таким образом, отказ одного элемента системы не приводил к отказу другого. Уровень диагностики аппаратуры 1960 – 1990-х гг. был достаточно низок либо вообще отсутствовал. Достижение «уставок» срабатывания защит и блокировок по технологическим параметрам инициировалось от приборов КИП, имеющих кинематику, и при достижении параметром величины определенного проектом значения замыкался соответствующий микропереключатель. Схемы защит и блокировок, реализованные на релейных схемах, отдавали одними своими «сухими» контактами инициативный сигнал в исполнительную часть, другими, дублирующими, контактами в схему сигнализации и в архив информационной вычислительной системы.

Как правило, все схемы блокировок были реализованы по принципу «1 из 1», т.е. один датчик работает с индивидуальным вторичным прибором, который и инициирует через промежуточное реле воздействие в исполнительную схему – отключение или включение механизма (механизмов), закрытие или открытие задвижки (задвижек), запуск последовательного функционально-группового управления с выдачей соответствующей сигнализации на БЩУ. Схемы защит для повышения надежности и исключения ложных срабатываний строились по мажоритарному принципу «2 из 3».

Первые системы сбора и представления информации базировались на аппаратуре М7000, М-60, ИФ-500, СВРК-01 и т.п. Системы собирали и представляли информацию на верхний уровень в информационную вычислительную систему в дружественном интерфейсе на сформированных бланках; с заданной дискретизацией выполняли архивирование (для пятого блока СМ-2М дискреты каждые 2 с, аналоги каждые 4 с); были пре-

дусмотрены инициативные сигналы, которые ложились в архив по мере возникновения. Управление оборудованием АЭС при помощи традиционных ИВС не предусматривалось. Представление информации от различных информационных систем (ИВС, СВРК, системы диагностики технологического оборудования) реализовывалось на индивидуальных мониторах. Представляемые слайды невозможно было объединить на одном формате, что создавало определенные неудобства [1].

Дальнейшее развитие АСУ ТП в атомной энергетике получило в 2000-х гг. в связи со строительством блоков в Иране, Китае и возобновлением сооружения блоков в России. Новые требования к современной АСУ ТП диктовались мировым уровнем развития компьютерной техники с высокой производительностью и человеко-машинным интерфейсом, т.е. конфигурации блочного пункта управления (БПУ). Конфигурация АСУ ТП базируется на функционально-ориентированных программно-технических управляющих комплексах. В частности, это управляющие системы безопасности, системы нормальной эксплуатации, важные для безопасности, в составе СКУ РО, СКУ ТО, СКУ СВО, ЭЧСР и т.д. и системы контроля и диагностики технологического оборудования. От функциональных ПТК информация централизованно собирается, регистрируется и отображается на системе верхнего блочного уровня (СВБУ), предоставляющего оператору возможность воздействия на исполнительные механизмы с монитора без использования традиционных ключей или кнопок [2 – 8]. Техническая реализация предопределена мировым подходом к организации корпоративных сетей. Таким образом, применяются процессоры, коммутаторы и серверное оборудование известных мировых брендов (HewlettPackard, Siemens, ShneiderElectric и т.п.), соответственно используется и программное обеспечение, поддерживаемое данной аппаратной базой (Novell, Microsoft). Управление элементами систем выполняется уже не по проводным связям, а по локальной сети с использованием общепринятых в мире сетевых топологий и протоколов.

Наравне с развитием компьютерной техники меняются технологии по изготовлению чувствительных элементов первичных измерительных преобразователей. Используемые ранее грубые мембраны заменяются на современные чувствительные кристаллы. Новые технические средства, используемые в АСУ ТП, открыли возможности повышения точности измерений дискретизации архивирования, т.е. замены аналоговой обработки данных оцифрованными параметрами [9]. Данное решение повышает помехозащищенность передаваемых дистанционно данных и позволяет работать уже с гораздо большими массивами, что несомненно находит отражение в реализации новых систем управления, печенью которых завладевает микропроцессор [10, 11] . Микропроцессорная система контролирует все, в том числе и себя, и соседний микропроцессор, обмениваясь при этом пакетами необходимой информации; вся диагностическая информация ложится в архив и становится инициативной, т.е. приоритетной. Контролируется малейшее отклонение технологического параметра и с ювелирной точностью укладывается в архив. При этом высокая чувствительность приводит к большим потребностям архивного пространства.

СИСТЕМА ВЕРХНЕГО БЛОЧНОГО УРОВНЯ

На сегодня объект управления (энергоблок АЭС) характеризуется следующими особенностями, влияющими на проектные решения по АСУ ТП [2]:

– непрерывность технологического процесса;

– многообразие применяемого технологического оборудования – большое количество запорной и регулирующей арматуры, механизмов и агрегатов, разнообразие измеряемых параметров (табл. 1) [5];

– наличие как быстропротекающих, так и инерционных ядерно-физических и тепловых процессов, контролируемых традиционными средствами контроля, а также при помощи специализированных вычислительных программ;

– сложная структура АСУ ТП, содержащая большое количество систем, на основе

разнородных программных и технических средств;

– использование в АСУ ТП преимущественно современных цифровых средств автоматики, обладающих развитыми средствами самодиагностики;

– централизация информации о состоянии технологического объекта управления (ТОУ) и формирование команды дистанционного управления средствами вычислительной техники;

– система верхнего блочного уровня (СВБУ) должна получать информацию о состоянии ТОУ и элементов ПТК АСУ ТП от всех систем АСУ ТП.

СВБУ должна передавать команды управления системам АСУ ТП

– автоматической противопожарной защиты (САППЗ);

– контроля и управления оборудованием нормальной эксплуатации (НЭ) реакторного отделения (СКУ РО);

– контроля и управления оборудованием специальной водоочистки (СКУ СВО);

– контроля и управления вентиляционным оборудованием (СКУ В);

– контроля и управления турбинного отделения (СКУ ТО);

– контроля и управления вспомогательным оборудованием турбогенератора (СКУ ТГ);

– радиационного контроля (СРК).

Таблица 1

Количество технологического оборудования для автоматизации НВАЭС-2

Технологическое оборудование энергоблока, количество				
Точки контроля	Электроприводная запорная арматура	Насосы, вентиляторы, электронагреватели	Регулирующая арматура	ФГУ
6600	3500	620	230	112
Технологическое оборудование общестанционных объектов (ОСО), количество				
Точки контроля	Электроприводная запорная арматура	Насосы, вентиляторы, электронагреватели	Регулирующая арматура	
4160	2630	1370	315	

В ПО «Портал», используемом на СВБУ первого блока НВОАЭС-2, для оптимизации использования архивного пространства применен так называемый телеграммный принцип обработки сигналов. Идея принципа заключается в том, что регистрация параметра выполняется, только если он меняется на установленную величину. Таким образом, в статике процесса за счет работы регуляторов технологические параметры стабильны, и это позволяет при нормальной эксплуатации эффективно экономить дисковое пространство, что обеспечивает долгосрочный архив [12]. Однако при отклонении от нормальных режимов эксплуатации, работе блокировок и защит, развитии аварийных ситуаций параметры технологического процесса меняются очень быстро, происходит активная работа электроприводной арматуры и механизмов – растет информационная нагрузка на СВБУ, что может спровоцировать отказ системы [3].

Блочный пункт управления тоже претерпел кардинальные изменения. Минимизируется количество ключей управления, отсутствуют мнемосхемы. Визуализация требуемой информации производится на экранах мониторов в различных интерпретациях. Основной инструмент оператора – манипулятор «мышь» и большое количество мониторов с многооконным интерфейсом. Проектант, фактически, предоставляет право оператору самому выбирать необходимую картинку и тем самым определять конфигурацию БПУ в зависимости от текущих задач эксплуатации и ведения технологического процесса, предоставляя ему максимум информации, т.е. формировать правильную эргономику своего рабочего места.

На НВ АЭС-2 создана современная управляющая технологическим процессом систе-

ма нормальной эксплуатации, построенная на базе программно-технических комплексов. Общая архитектура АСУ ТП НВ АЭС-2 и состав систем АСУ ТП приведены на рис. 1, 2. Система обладает глубокой внутренней самодиагностикой и охвачена Ethernet-сетью (единой коммуникационной шиной), по которой обменивается данными внутри себя, с соседними ПТК, отдает информацию на верхний уровень и представляет БПУ.

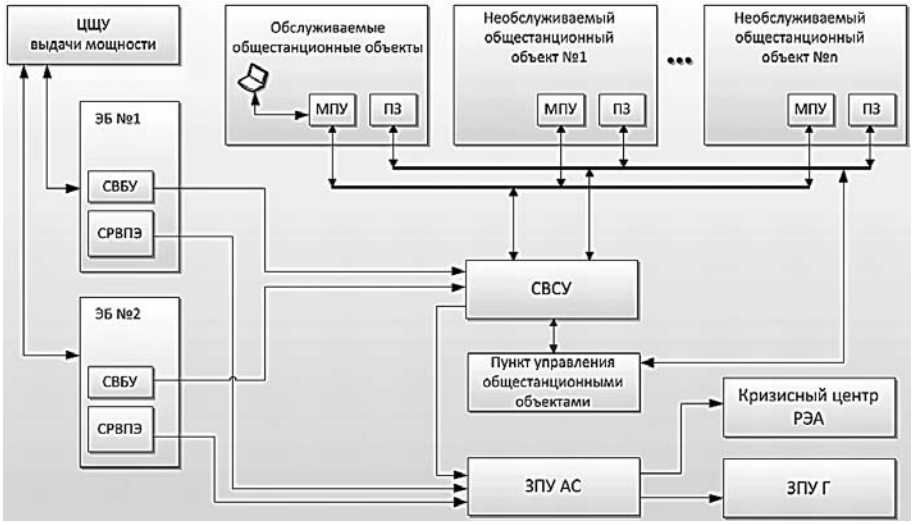

Рис.1. Общая архитектура АСУ ТП НВ АЭС-2

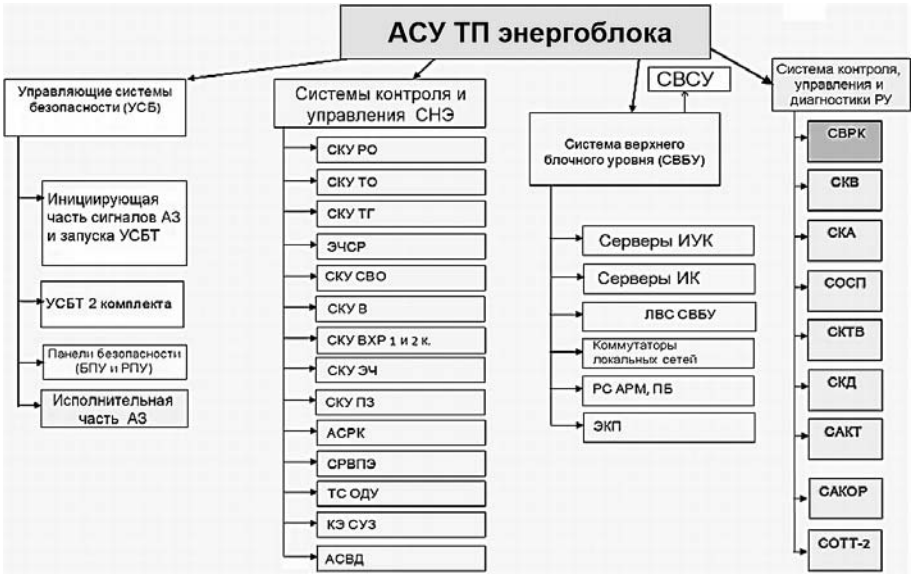

Рис. 2. Состав систем АСУ ТП

ПЕРЕДАЧА ШИРОКОВЕЩАТЕЛЬНЫХ СООБЩЕНИЙ

Проблемным компонентом в данной АСУ ТП является общая коммуникационная шина – основной связующий элемент в функционировании всей системы в целом. Опасен не столько разрыв данной цепи, сетевые топологии позволяют и дальше функционировать при таких единичных отказах или нарушениях кольца, сколько «забивание» шины большим количеством диагностических широковещательных сообщений. Широковещательные сообщения активно используются сетевыми сервисами для оповещения участников

информационного обмена о своем присутствии и состоянии. Считается нормальным, если широковещательные пакеты составляют не более 10% от общего числа пакетов в сети. В случае, если широковещательные сообщения не находят своего адресата или не успевают обрабатываться центральными процессорными модулями участников информационного обмена, возникает лавинообразный процесс их размножения (сообщений, предназначенных всем), что парализует работу сети, и, как результат, единая централизованная АСУ ТП перестает функционировать. Данное явление в сетевых топологиях носит название «широковещательный шторм» (от английского broadcaststorm) – лавина (всплеск) широковещательных пакетов [13 – 15].

При возникновении широковещательного шторма оператор не видит истинного состояния технологического процесса, не может воздействовать на механизмы, арматуру, регуляторы. Технологические алгоритмы, заложенные в ПТК, не получают достоверной исходной информации и формируют ложные управляющие команды. Динамическая устойчивость блока, базирующаяся на регуляторах и блокировках, теряется и в результате происходит срабатывание защит или систем безопасности, инициированных либо действиями оператора в соответствии с требованиями технологического регламента, либо достижением одним из параметров уставки по эксплуатационному пределу. Блок отключается от сети, реакторная установка переводится в подкритичное состояние.

Причинами появления широковещательного шторма, приводящего к сбою в работе сетевой коммуникационной шины, являются петли коммутации; неисправность сетевого оборудования; атаки на сеть.

Петля коммутации – это логическое кольцо для проходящего сигнала, аппаратно представляемая как раздача информации от коммутатора самому себе [13 – 15]. В этом случае сегмент сети начинает работать исключительно на передачу данных по этому кольцу и «забивает» весь полезный трафик. Как правило, петли коммутации возникают при неправильной конфигурации сети в процессе наладки сети или при ее диагностике с выполнением перекоммутаций. В сконфигурированной и работающей сети петля не возникнет – необходимо сделать соответствующие коммутации. Петлю можно создать ошибочным воздействием или по злому умыслу. Совершенно очевиден и способ борьбы с данным нарушением и он по большей части организационный. Все работы, которые связаны с переключениями на общей шине, должны быть строго взвешены и выполняться по тщательно спланированному алгоритму с пошаговым контролем выполняемых действий.

Неисправное сетевое оборудование также может генерировать поток широковещательных сообщений, а значит, необходимо контролировать состояние сетевого оборудования и при превышении нормированного значения широковещательных сообщений более 10% от общего трафика, создаваемого конкретным абонентом, его («шумящего» абонента) необходимо локализовать и отключить от сети.

Для установления рисков отказа общей шины на Нововоронежской АЭС был выполнен анализ устойчивости блока при потере шины и рассмотрены возможные меры по стабилизации ситуации. Исходя из указанных причин и способов борьбы с широковещательным штормом с учетом анализа устойчивости блока при отказе общей шины были разработаны первоочередные мероприятия, направленные на повышение устойчивости АСУ ТП. Основная концепция мероприятий заключается в следующем:

– обеспечение автоматического восстановления работоспособности шины за заданное время;

– работоспособность защит основного оборудования не должна зависеть от работоспособности общей шины, должна быть исключена ложная работа регуляторов и блокировок;

– должна быть обеспечена работоспособность основных регуляторов, влияющих на стабильную работу энергоблока в течение не менее 5 мин после постулируемого отказа общей шины;

– необходимая информация по параметрам, характеризующим работу энергоблока, в этом режиме должна быть представлена на панелях безопасности и экране коллективного пользования блочного пульта управления.

Кроме указанных технических мероприятий были разработаны организационные меры, направленные на ограничение доступа к общей шине, идентификации возникновения широковещательного шторма и действиям персонала по локализации и ликвидации шторма с минимальными потерями для блока.

При атаках на сеть можно различить как физическое воздействие (например, создание петли коммутации), так и воздействие вредоносным программным обеспечением, внедренным при создании ПО, обновлении или иным способом при получении доступа к сети АСУ ТП. Способы защиты от данных воздействий, нарушающих функционирование АСУ ТП, – это развитие технологий кибербезопасности [16], использование защищенного ПО и российской аппаратной части. Вопрос кибербезопасности для отрасли фактически находится в зародыше. На сегодня отсутствует нормативно-правовая база по этой тематике. Нет количественной и качественной оценки кибербезопасности. Это, по сути, защита сети и системы от человека (злоумышленника). Хакеру просто готовить кибератаки, поскольку вся необходимая исходная информация по аппаратной и программной части АСУ ТП лежит на общедоступных ресурсах в мировой сети. Благо, системы автоматизации не вызывают экономического интереса у злоумышленника, ему интереснее финансовые структуры, и потому большинство атак и угроз не направлены на АСУ ТП. Целенаправленные атаки на АСУ ТП в мире являются единичными случаями, успешных атак на российские системы АСУ ТП атомной энергетики не фиксировалось.

Однако очевидно, что уязвимость сети, в которой работает АСУ ТП, состояние ее кибербезопасности однозначно должна быть под контролем. Сегодня кибербезопасность на АЭС достигается за счет наличия мощной системы физических барьеров (ограничение доступа на объект, в конкретные помещения, все шкафы опечатаны и находятся на сигнализации). Тщательным подбором и работой с персоналом достигаются необходимые навыки и прививаются основные принципы культуры безопасности у работников как самой АЭС, так и подрядных организаций, работающих на АЭС. Административно-техническим персоналом станции обеспечивается необходимый контроль во время проведения работ [16].

Доступ к локальной сети АСУ ТП ограничен от внешнего мира и от корпоративной сети с помощью шлюзов и так называемых «диодов», ограничено применение внешних накопителей, из которых возможно поступление вредоносных программ, широко используется система ограничения доступа с помощью паролей. Программный продукт перед использованием обязательно проходит валидацию и верификацию.

Вопрос кибербезопасности программно-технических комплексов и АСУ ТП в целом требует постоянного внимания. Надо признать, что программные продукты для компьютеров современной архитектуры всегда могут иметь ошибки и быть уязвимыми для кибератак. Таким образом, сейчас ведется активная работа по оценке угроз систем АСУ ТП от кибератак; на базе ВНИИАЭС организован центр компетенций по кибербезопасности.

Управляющие системы безопасности в структуре АСУ ТП блока занимают отдельную нишу. К структуре построения управляющих систем безопасности предъявляются повышенные требования по качеству изготовления, приемке, монтажу, надежности ее функционирования, проведения соответствующих технических обслуживаний и ремонта, периодичности опробования, подтверждения проектных характеристик и ресурса [17, 18]. Для достижения указанных критериев система должна быть достаточно простой как конструктивно, так и по выполняемым функциям (реализованным в ней алгоритмам), иметь необходимый уровень диагностики и архивирования событий, инициирующих ее работу. Правила и нормы в атомной энергетике предусматривают применение в УСБТ основных принципов надежности – независимости, резервирования и разнообразия [17, 18]. Проект первого блока НВАЭС-2 предусматривает две одинаковые независимые

управляющие системы безопасности. Принцип разнообразия был реализован путем наращивания каждого из комплектов дополнительной диверсной системой защиты, построенной на жесткой логике от альтернативного изготовителя. Такое построение позволяет выполнять поставленные задачи каждым комплектом УСБТ вне зависимости от состояния сети, общей шины, программного продукта и таким образом уйти от возможного отказа по общей причине.

ЗАКЛЮЧЕНИЕ

1. Автоматизируемые функции АСУ ТП на первом блоке НВ АЭС-2 реализуются на основе информационной модели, отражающей способы управления объектом с участием СВБУ. Структура АСУ ТП и ее программно-аппаратная часть апробированы и успешно эксплуатируются на действующих и модернизируемых блоках российского образца и могут быть рекомендованы как концептуальная основа для применения в новых проектах. Однако результаты эксплуатации показывают необходимость совершенствования полученного продукта. В частности, альтернативные «Порталу» российские проекты используют собственное ядро программного продукта [11] и, пользуясь современными объемными высокоскоростными элементами памяти, применяют аналогичные СМ-2М подходы к архивированию событий. Нагрузка при таком подходе на сеть, центральный процессор и периферию постоянна и не зависит от течения технологического процесса.

2. Необходимо активно развивать системы поддержки принятия решений для оператора на основе баз данных и баз знаний, содержащих максимально возможный набор продукционных моделей, обеспечивающих его необходимыми решениями в зависимости от того или иного состояния блока, течения технологического процесса или внештатной ситуации.

3. Необходимо совершенствование методов обеспечения кибербезопасности для программно-технических комплексов АСУ ТП и, в первую очередь, для российских разработок и продуктов.

4. Требуется повысить эффективность работы коммуникационной шины, обеспечив бесперебойный обмен широковещательными сообщениями, устранив возможность появления широковещательного шторма по указанным выше причинам.

5. На базе имеющейся аппаратной и программной российской продукции создать типовой проект АСУ ТП, привязанный к российскому блоку, и использовать его как законченную конкретную конфигурацию. В проекте такой АСУ ТП должен быть заложен полный жизненный цикл, привязанный к блоку АЭС, включая монтаж, ввод в эксплуатацию, сопровождение при эксплуатации, ремонт, модернизацию, вывод из эксплуатации и утилизацию.

Литература

1. *Менгазетдинов Н.Э., Бывайков М.Е., Зуенков М.А.* Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУ ТП для АЭС «Бушер» на основе отечественных информационных технологий. – М.: ИПУ РАН, 2013. – 95 с.

2. Нововоронежская АЭС-2. Проект «АЭС-2006». Электронный ресурс http://www.rosenergoatom.ru/upload/iblock/f01/f01b5ca309dbda1917c112d6897c0959.pdf (дата доступа 05.09.2017).

3. *Крушельницкий В.Н., Топчиян Р.М.* Предварительный отчет по обоснованию безопасности. Общее описание атомной станции. Нововоронежская АЭС-2 Энергоблок № 1. – М.: ФГУП «Атомэнергопроект», 2007.

4. *Швыряев Ю.В., Морозов В.Б., Токмачев Г.В. и др.* Обоснование безопасности проекта АЭС-2006 для условий площадки Нововоронежской АЭС-2 методами вероятностного анализа безопасности.// Тяжелое машиностроение. – 2009.– № 11.– С. 2-6.

5. *Антипов С.И., Сивоконь В.П., Бутко А.Б., Черняев А.Н.* О создании конкурентоспособной АСУ ТП для АЭС нового поколения. // Автоматизация в промышленности. – 2015. – Т. 11. – С. 36-40.

6. IAEA Publications. Доступно на сайте http://www-pub.iaea.org/MTCD/publications/ (дата доступа 05.09.2017).

7. European Utility Requirements (EUR). Электронный ресурс http://www.europeanutilityrequirements.org/Welcome.aspx (дата доступа 05.09.2017).

8. *Токмачев Г.В.* Подход к применению ВАБ при проектировании АЭС с реакторами ВВЭР нового поколения. // Известия вузов. Ядерная энергетика. – 2007. – № 3. – С 44-53.

9. *Данилов А.Д., Головнев В.Н.* Цифровые системы управления. – Воронеж: ВГЛТА, 2007. – 235 с.

10. *Данилов А.Д.* Микропроцессорные элементы и устройства локальной автоматики. – Воронеж: ВГЛТА, 2005. – 267 с.

11. *Данилов А.Д.* Технические средства автоматизации. – Воронеж: ВГЛТА, 2007. – 340 с.

12. Информационно-вычислительная система «Портал». Общее описание системы. Инв. № 590 85 090.23512.014-Ф.ПД.М. – М.: ОАО «ВНИИАЭС», 2011.

13. *Куроуз Д., Росс К.* Компьютерные сети. Настольная книга системного администратора. – М.: Изд-во «Э», 2016. – 912 с.

14. *Сергеев А.Н.* Основы локальных компьютерных сетей. – СПб: Лань, 2016. – 186 с.

15. *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы. 5-е изд. – СПб: Питер, 2016. –996 с.

16. *Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А.* Кибервойны – реальная угроза национальной безопасности. – М.: КРАСАНД, 2011. – 192 с.

17. НП-001-15. Федеральные нормы и правила в области использования атомной энергии. «Общие положения обеспечения безопасности атомных станций». – М.: ФБУ НТЦ ЯРБ, 2016. – 56 с.

18. НП-026-16. Федеральные нормы и правила в области использования атомной энергии. «Требования к управляющим системам, важным для безопасности атомных станций». – М.: Роспотребнадзор, 2016. – 30 с.

Поступила в редакцию 14.09.2017 г.

Авторы

Терехов Дмитрий Владимирович, начальник цеха тепловой автоматики и измерений
E-mail: TerehovDV@nvnpp1.rosenergoatom.ru

Сидоренко Евгений Васильевич, главный инженер
E-mail: sidorenko.eskm@mail.ru

Данилов Александр Дмитриевич, профессор, доктор техн. наук
E-mail: danilov-ad@yandex.ru

UDC 004: 621.039

DEVELOPMENT TRENDS OF MODERN AUTOMATED PROCESS CONTROL SYSTEMS AT NOVOVORONEZH NPP

Terekhov D.V.*, Sidorenko E.V.**, Danilov A.D.***

* Branch of JSC «Concern Rosenergoatom» «Novovoronezh Nuclear Power Plant»
1 Promyshlennaya zona Yuzhnaya, Novovoronezh, Voronezh Reg.,
396071 Russia
** JSC «Korporaciya AK «EHSKM», Novovoronezh office
5 Tramvajnaya, Krasnodar, Krasnodar Kray, 350911 Russia
*** Voronezh State Technical University,
14 Moskovsky prospect, Voronezh, 394029 Russia,

ABSTRACT

The evolution of automated process control systems at nuclear power plants from traditional automation means with hard-wire logic based on archaic means – arrow instruments, recorders, light indicators, keys for individual equipment control etc., up-

to-date automated information and control systems based on high-level software and hardware. Characteristics of the features that affect the design decisions for the process control system, such as the continuity of processes, the variety of equipment and accessories, the complexity and heterogeneity of software and hardware, the centralization of information, and so on. It is shown that modern automated process control systems for nuclear power facilities should contain a upper level system. The general architecture of such a system is considered and its composition is presented on the example of the automated process control system for NVNPP-2 A detailed analysis of the problems of the functioning of this system, consisting in ineffective operation of the communication busbars due to avalanche-type information processes in the transmission of broadcast messages, which paralyzes the network and automated process control system in a whole. Priority measures aimed to improve stability of the automated process control system are proposed: automatic recovery of operability within a specified time, elimination of false operation of controllers and interlocks, visualization of information by parameters from safety panels and common display. The analysis of the issues of cybersecurity of the information subsystems of the automated process control system of nuclear power plants was carried out and a solution was proposed to increase the level here by duplicating and reserving data transmission channels.

Key words: Automated Process Control System, software and hardware complex, broadcast storm, cybersecurity

REFERENCES

1. Mengazetdinov N.E., Byvaikov M.E., Zuenkov M.A. A set of works to establish the first control system of the upper level unit of the automated process control system for Bushehr NPP based on national information technologies. Moscow. IPU RAN Publ., 2013. 95 p. (in Russian).

2. Novovoronezh NPP-2. Design «AES-2». Available at http://www.rosenergoatom.ru/upload/iblock/f01/f01b5ca309dbda1917c112d6897c0959.pdf (accessed Sep 05 2017) (in Russian).

3. Krushelnitsky V.N.; Topchiyan R.M. Preliminary safety analysist report. General description of the nuclear power plant. Novovoronezh NPP-2 Power Unit No. 1. Moscow. FGUP «Atomenergoproekt» Publ., 2007 (in Rusian).

4. Shviryayev Yu.V., Morozov V.B., Tokmachev G.V. The rationale for the safety of the NPP-2006 design for NVNPP-2 site conditions by the methods of probabilistic safety analysis. *Tyazhyoloe Mashinostroenie*. 2009, no. 11, pp. 2-6 (in Russian).

5. Antipov S.I., Sivokon V.P., Butko A.B., Chernyaev A.N. Establishing of a competitive automated process control system for NPP of a new generation. *Avtomatizatsiya v promyshlennosti*. 2015, v. 11, pp. 36-40 (in Russian).

6. IAEA Publications. Available at http://www-pub.iaea.org/MTCD/publications/ (accessed Sep 05 2017).

7. European Utility Requirements (EUR). Available at http://www.europeanutilityrequirements.org/Welcome.aspx (accessed Sep 05 2017).

8. Tokmachev G.V. Approach to the use of PSA in the design of nuclear power plants with VVER type reactors of a new generation. *Izvestiya vuzov. Yadernaya energetika*. 2007, no. 3, pp. 44-53 (in Russian).

9. Danilov A.D., Golovnev V.N. *Digital Control Systems*. Voronezh. VGLTA Publ., 2007, 235 p. (in Russian).

10. Danilov A.D. *Microprocessor elements and local automation devices*. Voronezh. VGLTA Publ., 2005, 267 p. (in Russian).

11. Danilov A.D. *Automation hardware*. Voronezh. VGLTA Publ., 2007, 340 p. (in Russian).

12. Information and Computing System «Portal». General description of the system. Inv. No. 590 85 090.23512.014-F.PD.M. Moscow. JSC «VNIIAES» Publ., 2011.

13. Kurouz D., Ross K. *Computer networks. System Administrator's Desk Book*. Moscow. Izdatel'stvo «E» Publ., 2016, 912 p. (in Russian).

14. Sergeev A.N. *Fundamentals of local computer networks*. St. Petersburg, Lan' Publ., 2016, 186 p. (in Russian).

15. Olifer V., Olifer N. *Computer networks. Principles, technologies, protocols*. St. Petersburg. Piter Publ., 2016, 996 p. (in Russian).

16. Parshin S.A., Gorbachev Yu.E., Kozhanov Yu.A.. *Cyberwar is a real threat to national security*. Moscow. KRASAND Publ., 2011, 192 p. (in Russian).

17. NP 001-15. General Safety Assurance Provisions for Nuclear Power Plants. Moscow. FBU NTC YaRB Publ., 2016, 56 p. (in Russian).

18. NP 026-16. Requirements for Control Systems Significant for Nuclear Power Plants' Safety. Moscow. Rospotrbnadzor Publ., 2016, 30 p. (in Russian).

Authors

Terekhov Dmitry Vladimirovich, Head of the Instrumentation and Control Department
E-mail: TerehovDV@nvnpp1.rosenergoatom.ru

Sidorenko Evgeny Vasilevich, Chief Engineer
E-mail: sidorenko.eskm@mail.ru

Danilov Alexander Dmitrievich, Professor, Dr. Sci. (Engineering)
E-mail danilov-ad@yandex.ru