УДК 621.3.019.3

А.В. ФЕДУХИН[*], Ар.А. МУХА[*]

ОБЕСПЕЧЕНИЕ ЖИВУЧЕСТИ СИСТЕМ ПРОТИВОАВАРИЙНОЙ АВТОМАТИКИ НА ГИДРОЭЛЕКТРОСТАНЦИЯХ

[*]Институт проблем математических машин и систем НАН Украины, г. Киев, Украина

Анотація. *Стаття присвячена подальшим дослідженням безпеки систем протиаварійної автоматики ГЕС. Проведено аналіз стану проблеми забезпечення безпеки і живучості критичних інфраструктур типу ГЕС, розроблені рекомендації щодо підвищення живучості комп'ютеризованих систем протиаварійної автоматики на сучасних ГЕС.*
Ключові слова: *критична інфраструктура, живучість, кластерна структура.*

Аннотация. *Статья посвящена дальнейшим исследованиям безопасности и живучести систем противоаварийной автоматики ГЭС. Проведен анализ состояния проблемы обеспечения безопасности и живучести критических инфраструктур типа ГЭС, разработаны рекомендации по повышению живучести компьютеризированных систем противоаварийной автоматики на современных ГЭС.*
Ключевые слова: *критическая инфраструктура, живучесть, кластерная структура.*

Abstract. *The article is devoted to further studies of the safety and survivability of emergency control systems of hydroelectric power plants. The analysis of the problem state of ensuring the safety and survivability of critical infrastructures such as hydroelectric power stations has been carried out and recommendations for improving the survivability of computerized systems of emergency control at modern hydroelectric power stations have been developed.*
Keywords: *critical infrastructure, survivability, cluster structure.*

1. Введение

Плотины и плотинные гидроэлектростанции (ГЭС) в частности, несмотря на свою красоту и экономическую полезность, являются объектами повышенной опасности для людей. Это связано не только с безопасностью обслуживающего персонала станции в случае аварии, но и с безопасностью людей, проживающих вблизи от этих объектов. В связи с этим данные объекты относятся к так называемым критическим инфраструктурам (КИ).

Помимо случившихся в последнее время техногенных аварий на ГЭС и других КИ, серия террористических актов, прокатившихся по миру в конце XX начале XXI столетия, показала, что человечество вступило в новый этап, когда для решения важных политических задач в вооруженном противостоянии могут использоваться достаточно малочисленные боевые группы или даже отдельные «смертники».

В настоящее время в качестве цели, поражение которой может нанести огромный ущерб государству и ее гражданам, правильнее рассматривать не только военные, но и объекты гражданского сектора критического применения, в том числе и ГЭС, выведение из строя которых, в том числе и за счет «каскадного эффекта», может привести к ущербу, сопоставимому с ударами, наносимыми вооруженными силами противника [1].

В качестве основных источников угроз для КИ рассматриваются следующие:

• терроризм и другие действия криминального характера (нападения, в том числе вооруженные, подрывы, поджоги, использование в террористических целях авто- и авиатранспорта, опасных веществ);

ISSN 1028-9763. Математичні машини і системи, 2018, № 2

• человеческий фактор и техногенные аварии (технические поломки, аварии, утечки опасных материалов, взрывы, пожары, влияние прочих физических воздействий);

• природные явления и стихийные бедствия (штормы, ураганы, наводнения, землетрясения, цунами и т.п.).

Отличительной особенностью современной эпохи является то, что наибольшую угрозу для КИ представляют действия диверсионных групп террористических международных организаций. Беспрецедентные возможности в сфере телекоммуникационных технологий и компьютерных систем (КС), стремительное развитие международной системы торгово-транспортных отношений способствуют возрастанию как масштабов, так и эффективности подобной деятельности, позволяя быстро преодолевать значительные расстояния и проникать через охраняемые границы.

Угрозы могут также возникать и в связи с созданием новых технологий, разработкой более совершенных методов и способов нанесения поражения объектам инфраструктуры за счет исследования и переоценки сильных и слабых сторон в организации их безопасности.

Разработанные и реализуемые мероприятия по защите современных КИ, таких как объекты энергетики, не в полной мере соответствуют уровню угроз и требуют настоятельного совершенствования. В связи с этим, в последние годы наблюдается значительное повышение интереса к такой характеристике систем, как живучесть, не только в практическом, но и в теоретическом плане. Это можно объяснить следующими обстоятельствами [2].

Во-первых, возрастание масштабов и стоимости КС приводит к значительному росту ущерба от длительного отключения даже части КС, увеличению доли технологически связанных нарушений работоспособности, а, следовательно, масштабов «поражения» системы.

Во-вторых, в больших КС возрастают сложность и трудоемкость восстановительных операций. Поэтому стремление к уменьшению размеров «поражения» КС одновременно является стремлением к созданию более благоприятных условий для восстановления требуемого уровня функционирования.

В-третьих, вследствие развитых связей между различными КС и подсистемами по различным каналам (по информационным каналам, по материальным и энергетическим потокам) значительную роль могут играть вторичные последствия нарушений работоспособности элементов КС. Ущерб от вторичных последствий может оказаться неизмеримо выше, чем от первичных последствий, вплоть до полного прекращения функционирования или гибели самой КИ. Поэтому возникает проблема устранения или ограничения вторичных последствий.

Наконец, существует проблема быстрого и оптимального включения сохранившихся в КС ресурсов в интересах выполнения жизненно важных функций после сильного на нее воздействия. Ясно, что решение этой проблемы требует от КС новых качеств, которыми она может и не располагать, если спроектирована для работы только в нормальных условиях эксплуатации.

Цель исследования – анализ состояния проблемы обеспечения безопасности и живучести КИ типа ГЭС на примере станций на реках РФ, разработка рекомендаций по повышению живучести компьютеризированных систем противоаварийной автоматики (СПА) на современных ГЭС.

2. Состояние проблемы обеспечения живучести ГЭС

При отсутствии в открытой печати и Интернете достаточной информации о состоянии безопасности и живучести на украинских ГЭС анализ проблемы будем проводить на примере

ГЭС РФ, что является достаточно репрезентативным, так как отечественные станции и станции РФ строились во времена бывшего СССР по единым нормативным документам.

Анализ безопасности и живучести ГЭС на примере аварии на Саяно-Шушенской ГЭС РФ [3] показал, что инфраструктура и системы ГЭС на момент аварии не удовлетворяли требованиям гарантоспособности, предъявляемым к объектам КИ.

Разберемся, что изменилось в подходах к проектированию и эксплуатации систем современных ГЭС, принят ли системный подход к обеспечению безопасности ГЭС, называемый гарантоспособностью, в практику обеспечения жизнедеятельности данных объектов критического применения. Рассмотрим основные нормативные материалы РФ, касающиеся обеспечения безопасности ГЭС.

Анализ начнем с основного терминологического стандарта СО 34.21.307-2005 [4], разработанного ОАО «Всероссийский научно-исследовательский институт гидротехники им. Б.Е. Веденеева».

К большому сожалению, в терминологии как не было, так и нет терминов «критическая инфраструктура» и «гарантоспособность». Приводится ряд разрозненных терминов в области безопасности гидротехнических сооружений (ГТС), которые не обеспечивают системного подхода к решению проблемы безопасности. В документе приведены общеизвестные термины: техногенная безопасность, система обеспечения безопасности, обеспечение безопасности, программа обеспечения безопасности, анализ безопасности, отказоустойчивость, живучесть и т.п.

Примечание 1. В соответствии с классификацией уровней безопасности предшественником аварии на СШГЭС явилась эксплуатация ГТС в условиях развивающихся процессов снижения прочности и устойчивости элементов гидроагрегата (ГА-2), соответствующих критическому уровню безопасности.

За прошедшие 15 лет в стандарте не появилось ни одного термина в области развития системного подхода, называемого методологией обеспечения гарантоспособности критических инфраструктур. Известно [5], что включает в себя понятие гарантоспособность.

Базовой платформой гарантоспособности систем является отказоустойчивость, а атрибутами понятия гарантоспособность – безотказность, готовность, живучесть, обслуживаемость, достоверность, информационная безопасность (целостность, конфиденциальность) и функциональная безопасность.

Вопросы отказоустойчивости, безопасности и живучести, являющиеся основополагающими в создании гарантоспособных систем, остаются на сегодняшний день очень актуальными. Только системный подход к решению данной проблемы на всех этапах жизненного цикла систем (от формирования концепции до утилизации) позволит создавать системы с высоким уровнем гарантоспособности.

Другим важным нормативным документом в области безопасности ГЭС является стандарт РД 153-34.2-35.520-99 [6]. В этом стандарте сформулированы технические требования к программно-техническим комплексам (ПТК) для АСУ ТП ГЭС. Приведем несколько основополагающих требований к ПТК.

ПТК является основой для построения АСУ ТП любой электростанции. ПТК представляет собой совокупность средств вычислительной техники, программного обеспечения и средств создания и заполнения машинной информационной базы при вводе системы в действие, достаточных для выполнения одной или более задач АСУ ТП. Средства ПТК должны обеспечивать уровень надежности, соответствующий требованиям технического задания на конкретную АСУ ТП.

Требования к техническим средствам

В документе указано, что электрические защиты, входящие в состав ПТК, могут быть выполнены либо на традиционных средствах релейной техники, либо на специализирован-

ных средствах микропроцессорной техники. Все цифровые устройства ПТК должны выполнять функции самодиагностики. Диагностика должна выявлять возникновение отказа с точностью до типового элемента замены. В составе ПТК должны быть предусмотрены стандартные средства резервирования для обеспечения высокой живучести и надежного функционирования системы при возможных отказах оборудования, ошибках персонала и возникновении непредвиденных ситуаций. Должна обеспечиваться возможность замены отказавших устройств ПТК в «горячем» режиме (без отключения питания).

Выходные каналы устройств вывода дискретных сигналов должны быть гальванически разделены один от другого. Должен быть предусмотрен контроль исправности выходных каналов. При обнаружении повреждения выходной сигнал должен блокироваться. Системы передачи данных должны быть отказоустойчивыми по отношению к техническим средствам и защищены от отказов или разрушения аппаратуры передачи данных (кабелей, разветвителей, связевых процессоров и т.п.), например, резервированием и реконфигурированием.

Требования к электропитанию

Электропитание всех устройств ПТК должно производиться от собственных источников питания, получающих энергию от трехфазной сети переменного тока 380/220 В. Как правило, электропитание устройств ПТК осуществляется от двух независимых источников питания. Питание устройств ПТК, реализующих функции технологических защит, должно осуществляться с наивысшей надежностью: либо от аккумуляторной батареи, либо от источника переменного тока с резервированием от аккумуляторной батареи.

Технические средства, реализующие функции технологических защит, должны сохранять работоспособность при изменении частоты сети в пределах от 47 до 52 Гц. Должна предусматриваться звуковая и световая сигнализация об исчезновении напряжения или его понижении ниже заданного уровня на любом фидере питания ПТК, а также о переключении питания с одного фидера на другой. Основным принципом организации электропитания должно быть распределение питающего напряжения таким образом, чтобы неисправность отдельного элемента сети электропитания не приводила к полному отказу ПТК.

Требования к программному обеспечению

Программное обеспечение (ПО) ПТК должно отвечать следующим принципам:

- надежность (соответствие заданному алгоритму, отсутствие ложных действий, защита от разрушения и несанкционированного доступа как к программам, так и к данным);
- живучесть (выполнение возложенных функций в полном или частичном объеме при сбоях и отказах, восстановление после сбоя);
- устойчивость (сбой в работе отдельных приложений не должен приводить к отказу системного ПО и системы в целом).

Требования к безопасности

Требования к безопасности являются приоритетными по отношению к другим требованиям. ПТК должен быть построен таким образом, чтобы ошибочные действия оперативного персонала или отказы технических средств не приводили к ситуациям, опасным для жизни и здоровья людей.

Требования к надежности

Требования к надежности являются приоритетными по отношению к другим требованиям. ПТК должен создаваться как восстанавливаемая и ремонтопригодная структура, рассчитанная на длительное функционирование. Требования к показателям надежности устанавливаются отдельно для каждой функции (с учетом самодиагностики и восстановления)

только для внезапных и независимых отказов. Срок службы ПТК должен быть не менее 10 лет. Должна предусматриваться возможность продления этого срока путем замены отслуживших элементов на новые.

Должны быть использованы следующие основные способы повышения надежности:

• повышение аппаратной надежности элементов ПТК;

• наличие аппаратной, информационной, функциональной и алгоритмической избыточности, обеспечивающей работоспособность систем при единичных отказах без остановки оборудования;

• диагностика технических средств и программного обеспечения;

• защита от выдачи ложных команд и недостоверной информации;

• рациональное распределение функций управления между техническими средствами и персоналом;

• использование рационального человеко-машинного интерфейса, позволяющего быстро и однозначно идентифицировать и управлять ситуацией;

• передача и обработка информации в цифровой форме, использование специальных кодов для защиты информации в процессе обмена;

• контроль информации на входе, использование избыточности в наиболее ответственных случаях; хранение наиболее важной информации и программного обеспечения в энергонезависимом запоминающем устройстве;

• защита данных и программного обеспечения от несанкционированного доступа;

• облегченный режим работы элементов ПТК;

• гальваническая развязка каналов, модулей, шин и т.п.;

• организация нормальной эксплуатации ПТК и обеспечение запасными частями;

• повышение уровня квалификации обслуживающего персонала.

В качестве показателя надежности принимается среднее время наработки на отказ (табл. 1) (среднее время восстановления принимается равным 1 ч).

Таблица 1. Требования по надежности к основным функциям ПТК

Наименование функции	Среднее время наработки на отказ, млн ч (для отказа типа несрабатывание функции)	Среднее время наработки на отказ, млн ч (для отказа типа ложное срабатывание функции)
Технологические защиты (на одну защиту)	0,2	1,0
Управление исполнительными механизмами (на один механизм)	0,2	1,0
Автоматическое управление (на один канал)	0,1	1,0
Автоматическое регулирование вспомогательными механизмами (на один контур)	0,05	0,1
Аварийная и предупредительная сигнализация (на один сигнал)	1,0	1,0
Измерения, индикация (на один канал)	0,1	0,1
Регистрация (на один канал)	0,1	0,1
Расчет оперативных показателей (на один канал)	0,1	0,1

Примечание 2. Анализируя требования к средней наработке на отказ, приведенные в табл. 1, не поддаются осмыслению соотношения между ними для основных ответственных функций ПТК для случаев несрабатывания и ложного срабатывания. Требования по надежности оказываются выше для случаев ложного срабатывания ответственных систем (технологических защит, управления и автоматического регулирования исполнительными

и вспомогательными механизмами, автоматического управления, чем для случаев их несрабатывания. Данная ситуация противоречит основным требованиям к безопасности, предъявляемым к системам критического применения – несрабатывание перечисленных выше систем должно классифицироваться как опасный отказ и к выполнению этих функций должны предъявляться более высокие требования по надежности. Требования по надежности к аварийной и предупредительной сигнализации установлены равными требованиям для ложного срабатывания функций технологических защит и управления исполнительными механизмами.

Требования к живучести

Живучесть системы должна обеспечиваться по основным функциям, в частности, при:

- повреждении всех кабелей, идущих в одном канале, туннеле;
- полной потере электроснабжения переменным током от системы собственных нужд (на время не более 1 часа);
- повреждении любого из одиночных элементов аппаратуры ПТК.

Требования к достоверности

Для определения достоверности ряда аналоговых сигналов может проводиться проверка соответствия сигнала его значению, рассчитанному с использованием других параметров. При несовпадении результатов сигнал объявляется недостоверным и запоминается его последнее представительное значение, зафиксированное системой. Контроль достоверности дискретной информации обеспечивается в основном сравнением альтернативных сигналов. В отдельных случаях достоверность сигнала определяется специальными алгоритмами сравнения параметров.

Требования к условиям эксплуатации

Технические средства, размещаемые непосредственно на технологическом оборудовании, должны устанавливаться в местах, исключающих прямое попадание влаги, агрессивных сред и механических воздействий либо иметь специальную защиту от перечисленных воздействий. Конструктивное исполнение технических средств, устанавливаемых открыто в машинном зале, должно обеспечивать защиту от несанкционированного вмешательства в их работу посторонних лиц.

В результате анализа требований, предъявляемых к ПТК, можно сделать следующие замечания: весь комплекс требований выглядит как рекомендуемый и не реальный для безоговорочного воплощения его в действительность. Свидетельством тому являлось состояние ПТК на момент аварии на СШГЭС, ни о каком резервировании выполнения функций контроля и защиты на станции не могло быть и речи, тем более об обеспечении важнейших требований по живучести. Реально можно было бы распространить эти требования по надежности и отказоустойчивости на СПА, но в структуре ПТК такой комплекс программно-технических средств даже не выделен, хотя понятно, что именно он обеспечивает безопасность ГЭС в целом.

3. Анализ состояния инфраструктур новых ГЭС

Следует рассмотреть, что нового в области безопасности и живучести инфраструктур внедрено при строительстве новых ГЭС.

Богучанская ГЭС (БоГЭС)

БоГЭС – гидроэлектростанция на реке Ангара, у города Кодинска Красноярского края, входит в Ангарский каскад ГЭС, являясь его четвёртой, нижней ступенью. Ввод БоГЭС на

полную мощность состоялся в июле 2015 года после наполнения водохранилища до проектной отметки 208 метров (рис. 1) [7].

Примечание 3. Фоновая сейсмичность территории, согласно карте ОСР-97С, составляет 7 баллов по шкале MSK-64 (повторяемость 1 раз в 5000 лет), согласно результатам сейсмо – районирования – 6 баллов.

В станционной части плотины размещены водоприемники с затворами и сороудерживающими решетками, а также напорные водоводы диаметром 10 м для подачи воды к турбинам ГЭС. Для пропуска излишних расходов воды в период строительства и эксплуатации БоГЭС имеются два водосброса, расположенных в пределах бетонной плотины. Водосбросы регулируются плоскими затворами, управление которыми осуществляется с помощью козловых кранов или плоскими колесными затворами.

Здание гидроэлектростанции имеет классическую приплотинную конструкцию, расположено за станционной частью плотины на уровне нижнего бьефа. Машинный зал состоит из 9 агрегатных секций, конструктивно не разделенных между собой, что не способствует обеспечению высокого уровня живучести станции.

Рис. 1. Общий вид машинного зала БоГЭС

Все 350 сотрудников эксплуатационных служб и производственных подразделений БоГЭС располагаются в одном служебно-производственном корпусе (СПК) [8]. СПК БоГЭС расположен на левом берегу Ангары вдоль русла реки, правое крыло корпуса примыкает к торцу монтажной площадки машинного зала. В СПК находятся Центральный пульт управления новой Ангарской ГЭС и различные технологические помещения. Также в здании расположены рабочие места для сотрудников и руководства станции.

В помещении Центрального пульта управления (ЦПУ) организовано дежурство начальника смены станции. На установленном в ЦПУ щите управления с помощью светодиодной индикации представлена мнемосхема состояния электрических сетей и оборудования гидроагрегатов БоГЭС. В режиме реального времени отображаются готовность к пуску, генераторные режимы, сигналы автоматики при возникновении нештатных ситуаций, сведения о ремонте, оперативном резерве, состоянии работы выключателей, блочных и автотрансформаторов, а также многие другие параметры.

После возведения СПК все производственные и эксплуатационные подразделения ГЭС сконцентрированы в одном офисном здании, что позволяет сосредоточить эксплуата-

ционный персонал в непосредственной близости от рабочих мест, обеспечить оперативность принимаемых управленческих решений, но при этом значительно снижается уровень живучести станции.

Рассматривая общий вид машинного зала (рис. 1), не трудно видеть, что он представляет собой типовую конструкцию, мало отличающуюся от конструкции машинных залов других ГЭС. Значительным ухудшением безопасности нового решения, на наш взгляд, является расположение шкафов автоматики и контрольно-измерительных приборов (КИП) на одном уровне с гидроагрегатами.

Примечание 4. На Саяно-Шушенской ГЭС (рис. 3) шкафы были приподняты над уровнем гидроагрегатов на несколько метров, что давало некоторый резерв времени для срабатывания СПА в случае затопления машинного зала.

Расчеты специалистов Красноярского научного центра Сибирского отделения РАН показывают [9], что принятые в проекте БоГЭС величины суммарной пропускной способности плотины и объема ежегодного сброса воды водохранилища не рассчитаны на пропуск максимальных объемов половодий. Результатом этого может стать перелив воды через гребень каменно-набросной плотины, что может привести к катастрофическому разрушению плотины.

Примечание 5. Специалисты Сибирского федерального университета выполнили предварительную оценку последствий аварии, связанной с разрушением плотины БоГЭС и образованием волны прорыва. Учитывая, что в зоне затопления находится 48 населенных пунктов, возможное число пострадавших может достичь 230 тысяч человек.

Нижне-Бурейская ГЭС (НБГЭС)

Другая новейшая ГЭС в Амурской области [10] – Нижне-Бурейская ГЭС.

Рис. 2. Общий вид инфраструктуры НБГЭС

Это самая маленькая из каскада плотина высотой 48м оборудована пятью поверхностными водосбросами (рис. 2), перекрываемыми сегментными затворами, управление которыми производится с помощью гидроприводов. Также имеются плоские ремонтные и аварийно-ремонтные затворы, управление которыми производится с помощью козлового крана.

Примечание 6. В процессе работы над статьей на НБГЭС произошла авария [11]. 24 августа 2017 г. при штатном регулировании водосброса в пролете № 1 водосливной плотины произошло повреждение затвора, регулирующего сброс воды (всего на плотине пять таких затворов [12]), следствием чего возникло подтопление пристанционной площадки. Вода прямым потоком через водосброс начала поступать в нижний бьеф. В результате в нижнем бьефе произошел подъем воды, который угрожал подтоплению машинного зала станции. Причиной аварии стало разрушение пальца опоры сегмента затвора №1 с последующим разрушением привода и обрушением затвора в нижний бьеф. Пострадавших нет, оборудование машинного зала ГЭС повреждений не получило. Обслуживающим персоналом только лишь по истечении 40 мин. были введены в штатный режим работы те механизмы, которые задействованы в пропуске воды.

Не трудно видеть, что на новой НБГЭС, построенной уже после аварии на СШГЭС, по прежнему ликвидацию аварийной ситуации на сливном затворе станции осуществляют вручную люди, а не система противоаварийной автоматики.

На сегодняшний день настоятельно требуется пересмотр применяемых конструкций ремонтно-аварийных и сливных затворов ГЭС как недостаточно надежных и внедрение современных дисковых затворов высокого уровня гарантии (ВУГ) с двумя способами управления: гидравлическим и гравитационным [13]. Арматура таких затворов приводится в действие с помощью гравитационного противовеса (закрывающего груза) и гидравлического сервопривода. Сервопривод открывает диск затвора и действует в качестве мощного гидравлического демпфера во время закрытия. Такая резервированная система надежна в случаях любых критических ситуаций даже при полном отключении электропитания.

Саяно-Шушенская ГЭС

Следует посмотреть, что изменилось в машинном зале СШГЭС в результате ее восстановления после аварии 17 августа 2009 года.

Как и до аварии, основное электротехническое оборудование ГЭС размещается в здании ГЭС:

• в машинном зале – гидроагрегаты, вспомогательное оборудование, устройства автоматического управления и контроля;

• на центральном посту управления – пульт оператора-диспетчера или автооператор ГЭС.

Рис. 3. Общий вид машинного зала СШГЭС до аварии

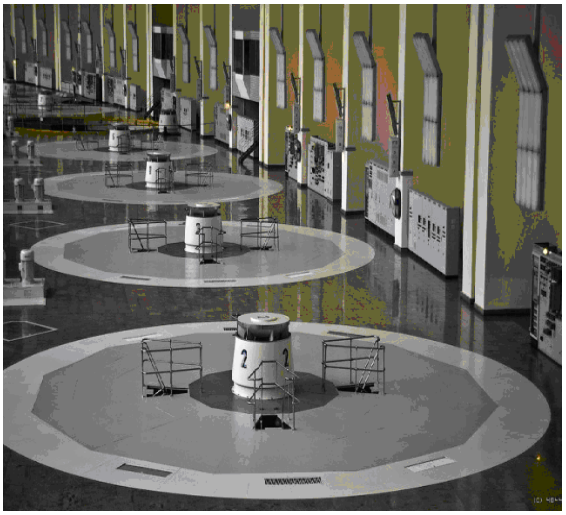

Рис. 4. Машинный зал СШГЭС после аварии и восстановления

Пол машинного зала [14] находится ниже станционной площадки всего на 6 м. Площадка ограждена со стороны реки подпорной стенкой, на станционной площадке размещены два здания служебно-технологических корпусов, то есть в инфраструктуре СШГЭС, с точки зрения обеспечения живучести, изменений не произведено.

Стены и крыша машинного зала станции также остались прежними и, на наш взгляд, слабыми – крыша на базе пространственной перекрёстно-стержневой конструкции, состоящей из унифицированных металлических элементов.

Значительным ухудшением безопасности нового решения (рис. 4), как нам кажется, является расположение шкафов автоматики и КИП на одном уровне с гидроагрегатами. Очевидно, такой вариант размещения оборудования принят в качестве стандарта при дальнейшем проектировании современных ГЭС. На Саяно-Шушенской ГЭС до аварии (рис. 3) они были приподняты на несколько метров и ограждены перилами безопасности, что давало некоторый резерв времени в случае затопления машинного зала для успешного срабатывания СПА.

4. Основная проблематика в области инжиниринга новых ГЭС

В работе [15] рассматривается состояние проблемы безопасности и живучести на примере каскада ГЭС на крупных сибирских реках РФ.

С целью обеспечения безопасности и защищенности ГЭС Сибири от тяжелых аварий необходима постановка специальных исследований причинно-следственного комплекса аварии для создания научно обоснованных нормативных документов в области расчетного анализа критериев риска, живучести и безопасности. С этой целью необходимо:

• разработать критерии безопасности плотин гидротехнических сооружений и оценить фактические коэффициенты запаса;

• провести расчетно-экспериментальный анализ параметров ресурса, живучести, безопасности и рисков в условиях тяжелой катастрофы ГЭС;

• разработать методологию оценки и повышения защищенности станций как критически важных объектов от тяжелых катастроф по критериям рисков;

• разработать методику уточненной расчетной оценки динамики, гидродинамики и аэродинамики возникновения и развития тяжелой катастрофы на гидроагрегатах.

• провести модельные расчеты аварийных ситуаций и сценариев их развития для всех существующих ГЭС;

• разработать модели и методы оценки социальных, экологических и экономических последствий аварий ГЭС;

• спроектировать и внедрить встроенные системы мониторинга и диагностики технического состояния технологического оборудования и плотины на всех существующих ГЭС с созданием единого пункта контроля;

• разработать методику построения специальной системы управления и автоматизированной защиты ГА и ГЭС в условиях перехода от штатной к аварийной и катастрофической ситуациям.

Оценки сейсмической опасности зоны Саяно-Шушенской, Красноярской и Богучанской ГЭС и их водохранилищ указывают на возможность возникновения сейсмических событий, способных вызвать серьезные последствия для безопасной эксплуатации ГЭС.

Принципиальное значение для безопасной эксплуатации имеет создание системы технического и геодинамического мониторинга гидротехнических сооружений и водохранилищ. В законе «О безопасности гидротехнических сооружений» необходимо предусмотреть разработку декларации безопасности каскада ГЭС в дополнение к декларации безопасности отдельных ГТС, входящих в состав каскада.

На государственном уровне отсутствует единая система контроля состояния каскадов ГЭС и водохранилищ. Для организации региональной системы технического и геоди-

намического мониторинга каскадов ГЭС целесообразно создание Инженерно-технологического центра мониторинга с решением следующих задач:

• создание банка данных геодинамической, технической, технологической информации о состоянии ГТС и их элементов;

• долго-среднесрочный и оперативный прогноз безопасности каскадов ГЭС в целом, контроль за состоянием проблемных природных территорий в зонах ГЭС и водохранилищ, контроль технического состояния ГТС с целью обеспечения информацией органов, ответственных за безопасность гидросооружений;

• математическое моделирование на основе данных мониторинга катастрофических процессов в природной среде и аварийных ситуаций в гидротехнических системах для прогнозных оценок последствий возможных тяжелых катастроф с целью их предотвращения.

Успешное строительство гидросооружений и их надежная эксплуатация определяются тем, как в процессе проектирования удалось осуществить совместимость сооружения с окружающей средой, насколько экономичны и надежны сооружения [16].

На основе анализа опыта проектирования, строительства и эксплуатации ГТС можно выделить пять основных видов проблем: технические, экономические, технико-экономические, экологические и социальные.

Технические проблемы содержат три группы:

• функциональная надежность;

• конструктивная надежность;

• живучесть.

Решение проблем функциональной надежности позволяет наделить их качествами, обеспечивающими выполнение ими своего назначения:

• геометрическим соответствием назначению (геометрические параметры);

• водонепроницаемостью;

• долговечностью.

Проблемы конструктивной надежности охватывают задачи обеспечения физической долговечности конкретного сооружения в условиях воздействии определенной окружающей (природной и техногенной) среды. При строительстве и эксплуатации гидротехнические сооружения должны обладать следующими качествами конструктивной надежности:

• общей и местной устойчивостью при воздействии статических и динамических нагрузок и температуры;

• общей и местной прочностью при действии статических и динамических нагрузок и температуры;

• стойкостью к трещинообразованию;

• жесткостью – устойчивостью к деформациям;

• выносливостью – усталостной прочностью при действии длительных динамических нагрузок;

• общей и местной фильтрационной прочностью сооружений и их оснований;

• морозостойкостью;

• коррозионной стойкостью к воздействию воздушной и водной сред с учетом возможных антропогенных воздействий;

• износостойкостью – стойкостью к воздействию наносов (мусора, льда и т.п.), воздействию колес автотранспорта и т.п.;

• кавитационной стойкостью;

• температурной устойчивостью к воздействию высоких и низких температур, что особенно значимо для гидросооружений, построенных в районах с суровым континентальным климатом;

• биостойкостью к воздействию живых организмов и продуктов их жизнедеятельности.

Проблемы живучести в [15] не раскрыты вообще. Дано лишь тривиальное определение живучести как свойства сооружения выполнять свои функции при действии сверхнормативных нагрузок и воздействий.

Технико-экономические проблемы объединяют семь групп: технологичность, стандартизация и унификация, транспортабельность, совместимость, ремонтопригодность, контролепригодность и противоаварийность.

Противоаварийные проблемы содержат круг вопросов, связанных с обеспечением безопасности людей и территорий при строительстве и эксплуатации гидросооружений при возможных авариях с прорывом напорного фронта. Рассмотрение сценариев возможных аварий на проектируемом сооружении и их учет позволяют предупредить или существенно снизить последствия возможных аварий.

К сожалению, рассмотренные проблемы касаются только плотин и плотинных сооружений ГЭС. Создается впечатление, что сами ГА, их системы управления и контроля, ПТК и входящая в него СПА беспроблемны и полностью удовлетворяют требованиям безопасности и живучести, предъявляемым к объектам КИ.

5. Основные положения в области живучести КС

В настоящее время свойство живучести распространяют не только на военные технические системы (ВТС), но и на КС общего назначения. Следует ознакомиться с этим понятием более подробно. Существует множество подходов к трактовке понятия живучести КС критических инфраструктур (КИ).

Живучесть – свойство системы сохранять и восстанавливать способность к выполнению основных функций в заданном объеме и в течение заданной наработки при изменении структуры системы и/или алгоритмов и условий ее функционирования вследствие непредусмотренных регламентом нормальной работы неблагоприятных воздействий (НВ) [2]. В то же время существует и другое более естественное и понятное определение живучести.

Живучесть – свойство сложной системы адаптироваться в изменяющихся условиях функционирования противостоять неблагоприятным воздействиям и достигать цели функционирования за счет изменения поведения и структуры [17, 18].

КС, как любым сложным системам, присущи определенная избыточность, адаптивность, отказоустойчивость и живучесть. Свойство живучести позволяет системе сохраняться целостной в условиях НВ (случайных или целенаправленных), влекущих разрушение структуры, нарушение целостности, снижение безопасности и качества функционирования.

Повышение живучести отдельных компонент (подсистем) КС позволяет парировать широкий класс средств и способов неблагоприятного воздействия, минимизировать возможности целенаправленного изменения, уничтожения, копирования и блокирования информационных потоков и данных; значительно снизить риск дезорганизации работы КС и сетей путем воздействия на их системы защиты.

Свойства безопасности и живучести закладывается в КС во время проектирования, что позволяет сохранять полную или ограниченную работоспособность КС вследствие изменения условий эксплуатации, структуры и алгоритмов при наличии отказавших составных частей и не допускать перехода их неисправностей в критические (опасные) отказы [3].

Безопасность и живучесть КС может обеспечиваться посредством улучшения свойств ее подсистем, компонентов и элементов, мониторингом и управлением рисками в период нормальной эксплуатации, восстановлением работоспособного состояния после

аварии или сбоя, использованием избыточности – резервирования и диверсности (разнообразия). В соответствии с [19], данный подход является наиболее важным и иногда единственным способом обеспечения безопасности и живучести критических систем и инфраструктур в целом. Увеличение живучести, снижение уязвимостей может быть достигнуто за счет функциональной информационной диверсификации наиболее важных узлов и связей между ними.

Эффект взаимозависимости между подсистемами КС очевиден, когда благодаря геометрической близости и единству информационного пространства, изменение состояния одной подсистемы КС вызывает изменения в состоянии безопасности и живучести всех зависимых подсистем КС.

С одной стороны, взаимозависимость обеспечивает живучесть КС, обусловливая ее работоспособность и быстрое восстановление после воздействия неблагоприятных факторов, с другой стороны, дефициты безопасности одной подсистемы могут влиять на другие зависимые подсистемы КС. В этом контексте уровень живучести КС в целом обусловлен уровнем уязвимости самой незащищенной подсистемы в КС.

В работе [19] сформулирован принцип инфраструктурного резервирования и диверсности для обеспечения безопасности и живучести КС, состоящий в использовании избыточности на инфраструктурном уровне. Под инфраструктурным резервированием понимается избыточность, реализованная на инфраструктурном уровне (зданий, помещений, цехов, участков, служб, подсистем и т.п.), для повышения безопасности и живучести КС. Данный вид резервирования приводит к увеличению способности к выполнению основных функций в условиях работы, отличных от нормальной эксплуатации, а значит и живучести.

Под инфраструктурной диверсностью понимается разнообразие между подсистемами КС и связями между ними. Инфраструктурная диверсность позволяет снизить риски комплексных аварий, поскольку снижается множество общих уязвимостей системы в целом.

В [20] сформулированы основные принципы и способы обеспечения живучести систем. Спроецируем эти принципы на объект наших исследований – КС КИ.

Принцип 1 – элементы КС должны иметь малую структурную значимость и высокую устойчивость. Анализируя матрицу состояний способности, можно заметить, что существуют подмножества элементов, утрата работоспособности которых приводит к потере состояния работоспособности всей КС. Такие подмножества называют «минимальным сечением» структуры. Наибольшую «опасность» представляют сечения, состоящие из малого числа элементов. Очевидно, что элементы «минимальных сечений» должны быть резервированными. Поиск таких элементов структурно возможен с помощью показателя значимости. Рассчитав показатели значимости для каждого элемента КС, легко ранжировать эти элементы по данному признаку. Защита или резервирование элементов, расположенных первыми в ранжированной строке, дает больший эффект.

Принцип 2 – структура КС должна обеспечивать, по возможности, большее или достаточное (в задачах оптимизации) число состояний работоспособности. Очевидно, что чем большим числом состояний работоспособности обладает КС, тем выше вероятность реализации хотя бы одного из них. Увеличение числа вариантов построения КС, обеспечивающих ее эффективное функционирование, а также числа конъюнкций в ДСНФ функции состояний однозначно способствует увеличению показателей живучести при прочих равных условиях.

Принцип 3 – состояния работоспособности КС должны обеспечиваться как можно меньшим числом элементов. Сокращение числа элементов, обеспечивающих состояние работоспособности, снижает уязвимость КС. Реализация данного принципа приводит к построению КС на основе модулей, каждый из которых способен обеспечить состояние работоспособности всей КС.

Принцип 4 – различные состояния работоспособности КС должны обеспечиваться различными элементами. Следствием реализации этого принципа является увеличение числа элементов, которые составляют «минимальное сечение» структуры КС. Естественно, чем больше элементов составляют «минимальное сечение», тем ниже вероятность их одновременного поражения, тем выше показатель живучести КС.

6. Количественные характеристики живучести систем

Метрики живучести как одного из важных атрибутов гарантоспособности вытекают из соответствующих основных свойств отказоустойчивости систем [2].

Ниже приводятся основные количественные характеристики живучести систем.

Коэффициент живучести G – отношение числа состояний, соответствующих работоспособной системе, ко всей совокупности состояний:

$$G = \frac{M}{C_l^i}, \tag{1}$$

где M – количество работоспособных состояний системы для обобщенного отказа i-той кратности;

C_l^i – общее количество состояний системы;

i – кратность отказа;

l – количество функциональных единиц живучести системы.

C_l^i – число сочетаний из l по i определяется по формуле $C_l^i = \frac{l!}{(l-i)!i!}$.

Коэффициент деградации D – отношение числа состояний, соответствующих неработоспособной системе, к общему количеству состояний системы:

$$D = \frac{N}{C_l^i}, \tag{2}$$

где N – число состояний, соответствующих неработающей системе;

C_l^i – общее количество состояний системы;

i – кратность отказа;

l – количество функциональных единиц живучести системы.

Выживаемость системы $R(n)$ – вероятность сохранения работоспособности при n-кратном неблагоприятном воздействии (НВ):

$$R(n) = 1 - Q(n) = P\left(F = \frac{1}{A_n}\right), \tag{3}$$

где F – функция работоспособности системы, принимающая значение 1, если система работоспособна, и 0, если система неработоспособна;

A_n – событие, происходящее при n-кратном появлении НВ.

Запас живучести (d-живучесть) d – критическое число дефектов, уменьшенное на единицу:

$$d = C - 1, \tag{4}$$

где С – критическое число дефектов, которое определяет потерю работоспособности системы.

Запас живучести (m-живучесть) m – максимальное число дефектов, которое еще может выдержать система без потери работоспособности:

$$m = \max(i)\{m_i\}, \quad (5)$$

где m_i – число дефектов i-ой кратности, которое еще может выдержать система без потери работоспособности.

Примечание 7. Дефект – это единица измерения ущерба, нанесенного системе неблагоприятным воздействием. Это может быть один элемент, удаленный из системы в результате НВ, потерянная для потребителей мощность системы энергетики в результате НВ и т.д. Критическим называют минимальное число дефектов, появление которых приводит к общей потере работоспособности системы.

Не трудно видеть, что чем больше число состояний, соответствующих работоспособной системе, тем меньше число состояний, соответствующих неработоспособной системе и чем больше число дефектов, которое может выдержать система без потери работоспособности, тем выше ее живучесть.

7. Кластерная структура как способ повышения живучести

Кардинальное решение в направлении повышения живучести достигается путем реализации принципа инфраструктурного резервирования и диверсности [19] посредством инфраструктурной декомпозиции КС на автономные кластеры, представляющие собой функционально обособленные подсистемы.

В первую очередь, вопросы обеспечения живучести наиболее остро ставились в отношении технических систем (ТС) морского применения. Показательным примером тому является кластерная структура рабочих отсеков атомной глубоководной станции АС-12 проекта 10831 [21], приведенная на рис. 5.

В этой ТС кластеры представляют собой герметично закрываемые рабочие отсеки повышенной прочности, устойчивые к высокому давлению на больших глубинах в случае затопления или взрыву в каждом из них.

Рис. 5. Инфраструктурное резервирование рабочих кластеров атомной глубоководной станции повышенной живучести АС-12

Во всех внештатных ситуациях глубоководная станция сохраняет функционирование и обеспечивает жизнедеятельность экипажа или его эвакуацию.

Аналогичные требования целесообразно распространить и на СПА как системы критического применения, ответственные за безопасность всей КИ ГЭС. Рассмотрим их реализацию более подробно.

8. Организация кластерной структуры СПА

Воспользуемся идеей повышения живучести глубоководной станции АС-12 путем кластеризации системы применительно к СПА.

С целью повышения отказоустойчивости и живучести СПА для ее реализации предлагается использование нового класса самопроверяемых двухканальных структур с реконфигурацией, получивших название самопроверяемых двухканальных квазимостиковых структур (СДКМС) [22], в которых каждый вычислительный канал состоит из n при-

близительно равнонадежных функциональных субблоков (ФСБ), которые с помощью схем реконфигурации (СР) образуют n дублированных узлов.

Исследованиями доказано, что квазимостиковая структура характеризуется более высоким уровнем отказоустойчивости и, как следствие, живучести, так как имеет значительно большее количество работоспособных состояний, чем простая дублированная структура. Квазимостиковая структура также способна к автоматической реконфигурации в одноканальную структуру без дополнительного вмешательства и изменения функции восстанавливающего органа (ВО).

Исследованиями также установлено [23], что средняя наработка до отказа СДКМС интенсивно возрастает с уменьшением времени восстановления и имеет отчетливую тенденцию к увеличению с ростом количества узлов более 4 при фиксированном времени восстановления.

Вероятность безотказной работы СДКМС также возрастает с уменьшением времени восстановления и возрастает при увеличении количества узлов, а коэффициент вариации наработки до отказа СДКМС снижается с уменьшением времени восстановления и ростом количества узлов.

При увеличении количества равнонадежных узлов тенденция уменьшения коэффициента вариации наработки до отказа является дополнительным фактором, влияющим на рост вероятности безотказной работы восстанавливаемой СДКМС. Кроме того, с ростом количества узлов уменьшается сложность ФСБ, из которых состоит узел, что упрощает программную и/или техническую реализацию самопроверяемой схемы внутреннего контроля (ССВК), задачей которой является обнаружение неисправностей заданного класса в вычислительном канале и собственных неисправностей. Увеличение количества узлов повышает точность контроля и диагностики неисправностей структуры и, как следствие, приводит к уменьшению времени восстановления и возрастанию показателей надежности восстанавливаемой СДКМС в целом.

На рис. 6 в качестве примера изображена квазимостиковая структура типа СДКМС отказоустойчивого ядра СПА, декомпонированная на 7 кластеров.

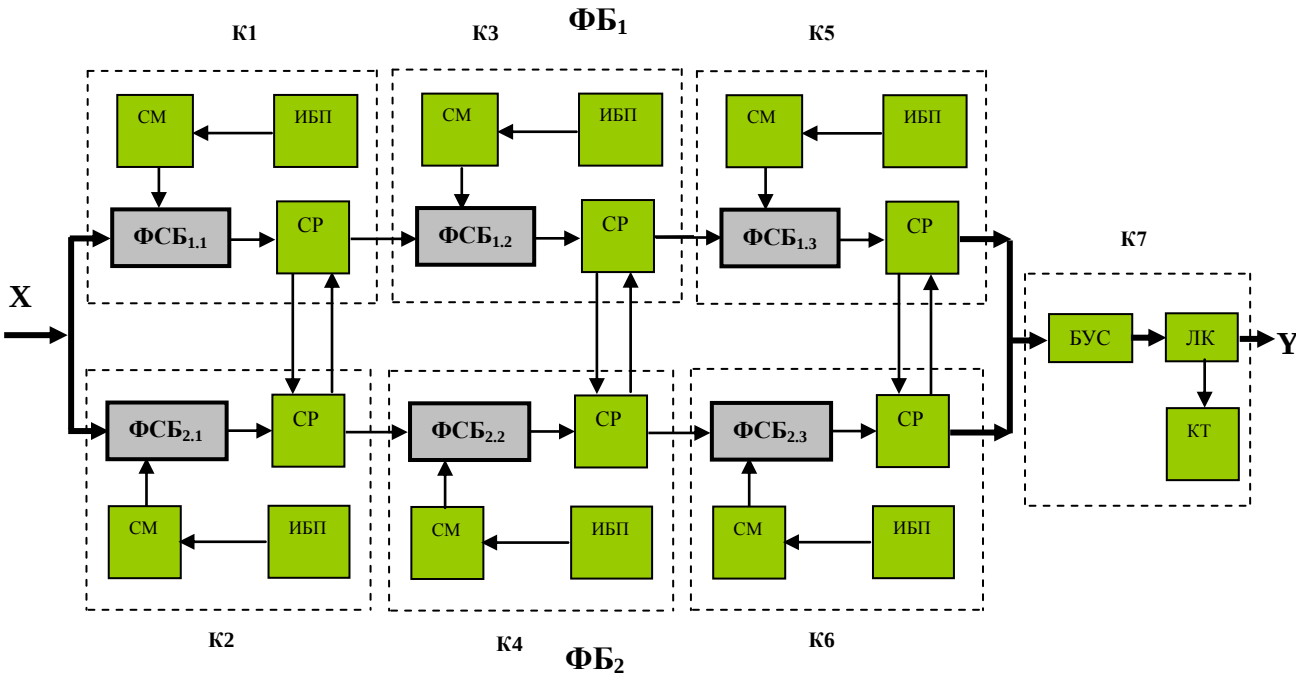

Рис. 6. Структурная схема СПА повышенной живучести на СДКМС

Техническая реализация квазимостиковых структур типа СДКМС наиболее эффективна как на базе современных программируемых логических интегральных схем (ПЛИС), представленных в виде наборов интегральных микросхем (ПЛИС-систем), или на базе единого кристалла ПЛИС [24], так и традиционно на базе микропроцессоров (МП) и микроконтроллеров (МК).

9. Методология проектирования СПА на новой элементной базе ПЛИС

В настоящее время создана новая методология проектирования системы на кристалле ПЛИС (System-on-Chip, SoC). Система на кристалле – это сверхбольшая интегральная схема (СБИС), содержащая на кристалле различные сложные функциональные блоки (СФБ), которые образуют законченное изделие для автономного применения в электронной аппаратуре [24].

СФБ, предназначенные для использования в разнообразных проектах, часто называют IP (Intellectual Property)-модулями. Эти клонированные модули должны быть повторяемыми и настраиваемыми под решаемые задачи в ряде проектов SoC. Повторное применение таких модулей (IP Core reuse) можно назвать вычислительными заготовками по причине их функциональной и технологической адаптируемости, что позволяет уменьшить трудозатраты и сроки проектирования архитектуры SoC несмотря на то, что недостающие функциональные блоки приходится проектировать самостоятельно.

В состав СФБ, как правило, входит микропроцессорное ядро с периферийными устройствами в различном сочетании. СФБ, используемые при проектировании SoC, имеют две основные формы представления:

• в виде топологических фрагментов, которые могут быть непосредственно реализованы в физической структуре кристалла. Это аппаратно реализованные (hard) СФБ;

• в виде моделей на языке описания аппаратуры (Verilog, VHDL), которые средствами САПР могут быть преобразованы в топологические фрагменты для реализации на кристалле, то есть синтезируемые (soft) СФБ.

Имеется большой выбор библиотек специализированных СФБ для различных прикладных областей и технологий изготовления микросхем, в частности, библиотек СФБ для ПЛИС, представленных в виде синтезируемых блоков на языках высокого уровня, списков цепей в элементном базисе производителей ПЛИС и готовых макросов с топологической реализацией.

В работе [25] показано эффективное применение ПЛИС в технологических компьютерных системах (ТКС), позволяющих помогать лицам, которые принимают решение при контроле сложных процессов, выявлении и предупреждении опасностей и т.д., то есть помощь в решении проблемных ситуаций до того, как они станут необратимыми.

Комплексное применение таких систем позволяет создавать типовые конфигурации систем для решения задач в разных областях их применения, включая и СПА повышенной отказоустойчивости, живучести и производительности.

В [26] рассмотрено применение ПЛИС-технологии повышения отказоустойчивости информационно-управляющих систем (ИУС) как ключевого элемента концепции построения «системы на кристалле» (System on Chip-SOC).

Среди основных преимуществ «системы на кристалле», спроектированной на базе ПЛИС, следует выделить глубокую оптимизацию внутренней структуры и отсутствие чрезмерной избыточности, характерной для систем, построенных на основе универсальных компонентов.

Применение ПЛИС позволяет снизить риски десяти из шестнадцати видов общих рисков, которые возникают как в случае применения ПЛИС, так и в случае применения микропроцессоров. В то же время рассмотрение специфических рисков, возникающих в случае применения ПЛИС, позволило сделать вывод, что риски данной группы незначи-

тельны и могут быть снижены с использованием стандартных или специальных апробированных решений.

ПЛИС достигают показателя надежности в 10 FIT (failure in time), что соответствует 10 отказам за 10^9 часов работы. Наряду с высокой надежностью ПЛИС имеют преимущества в гибкости разработки системы на кристалле, такие преимущества могут быть использованы для:

• расширения структуры обеспечения отказоустойчивости и обеспечения широкого охвата ошибок вычислительного процесса на базе кристалла;

• обеспечения последовательности восстановления типа «остановка – фиксация – перезапуск»;

• отключения не всего вычислителя, а его частей, являющихся причиной ошибок.

Таким образом, одним из дальнейших и эффективных путей решения проблем построения отказоустойчивых систем является использование ПЛИС-технологий. Большая гранулярность и высокая гибкость данной технологии позволяют достигать максимально необходимой элементарности действий, что дает возможность проектировщику эффективно проводить структурирование и распределять ресурсы вычислительного процесса. При этом появляется дополнительная возможность реализации аппаратно-управляемого восстановления, частичной блокировки и маскировки отказавших функциональных блоков, дистанционного перепрограммирования и т.д. Основным доказательством эффективности применения ПЛИС-технологий при построении отказоустойчивых систем являются примеры их успешной эксплуатации в различных областях науки, техники и производства.

10. Проектное решение кластерной структуры СПА

На рис. 6 изображена кластерная структура реализации СДКМС. Каждый типовой кластер К1-К6 содержит соответствующий ФСБ СПА со своей ССВК, схему реконфигурации СР, системный монитор (СМ) и источник бесперебойного питания (ИБП) системного монитора.

Общее резервное электроснабжение кластеров осуществляется от систем бесперебойного питания (СБП) [27], предназначенных для электропитания всей АСУ ТП ГЭС, включая центральный пульт управления и контроля (ЦПУК) и механизмы управления аварийными затворами (АЗ) гидроагрегатов (ГА).

Режимный кластер К7, выполняющий наиболее ответственные операции по непосредственному управлению исполнительными объектами, имеет ограниченный доступ обслуживающего персонала ГЭС. Он содержит блок безопасных устройств сопряжения (БУС), логический коммутатор (ЛК) и контрольное табло (КТ), предназначенное для оперативного контроля за состоянием СПА в целом. ЛК выполнен на h_1-надежных электромагнитных реле с ВУГ (рис. 7), опломбированных и установленных на специальные стативы (рис. 8).

Каждый кластер СПА конструктивно представляет собой цельнометаллический или железобетонный отсек с прочным герметизированным входом (снабженным автоматическим или ручным запиранием), устойчивый к затоплению водой или внешнему воздействию бризантного взрывчатого вещества (БВВ).

Схематично специальная кластерная структура СПА, построенная на базе СДКМС из трех узлов, приведена на рис. 9. При этом очень важным в ней является порядок расположения кластеров, влияющий на количество работоспособных состояний СПА в результате НВ. Такая инфраструктурная диверсность позволяет снизить риски множественных аварий, поскольку снижается множество общих уязвимостей системы в целом.

Рис. 7. h_1 -надежные реле ВУГ для построения кластера К7

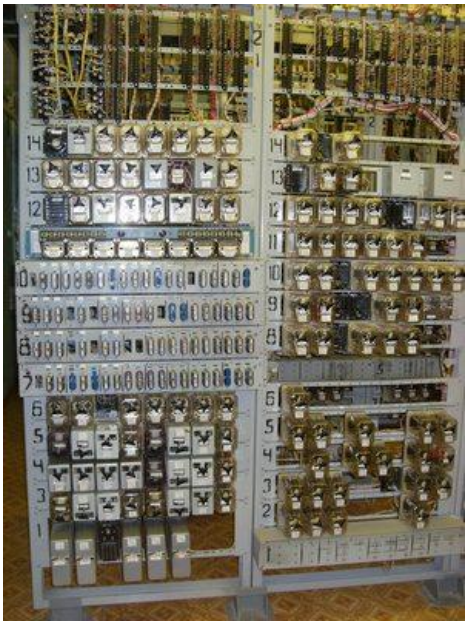

Рис. 8. Общий вид стативов для размещения h_1 -надежных электромагнитных реле с ВУГ в кластере К7

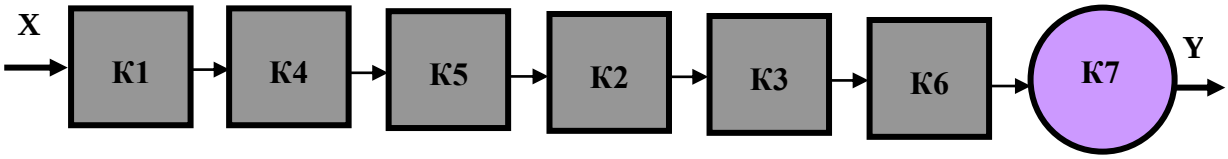

Рис. 9. Специальный порядок расположения кластеров в структуре СПА повышенной живучести

Каждый типовой кластер СПА, как правило, представляет собой функционально обособленную подсистему, технически выполненную в виде набора типовых элементов замены (ТЭЗ), обеспечивающих высокую ремонтопригодность СПА в целом.

Внутри кластерного отсека расположено рабочее место оператора системного монитора (СМ), который предназначен для контроля работоспособности, технической диагностики, технического обслуживания и ремонта оборудования кластера СПА ГЭС. СМ выполнен в виде стационарного одноплатного компьютера в защищенном исполнении или индивидуального мобильного планшета, используемого сотрудниками ГЭС для своей повседневной работы (с целью обеспечения требований по безопасности индивидуальные планшеты операторов СМ лишены возможности подключения к сети Интернет). Безотказное функционирование стационарного СМ дополнительно обеспечивается резервным электропитанием от ИБП.

11. Анализ потенциальных уязвимостей кластерной структуры СПА

В отличие от кластеров К1-К6 (рис. 6), выполненных на элементах с симметричными отказами (ПЛИС, микропроцессорах, микросхемах, полупроводниковых приборах и т.п.), кластер К7 выполнен на h_1 -надежных элементах гравитационной автоматики (реле с ВУГ) с исключением опасных отказов и не требует дополнительного резервирования.

При проектировании кластеров рассматривались следующие виды НВ:

• затопление кластера (во время аварии при неплотно закрытой входной двери);

• взрыв внутри кластера;

• взрыв внутри кластера и частичное повреждение одного соседнего кластера (в первую очередь против входа);

• взрыв внутри кластера и частичное повреждение двух соседних кластеров (перед и после взорванного).

Затопление кластера может произойти при разрушении плотины в результате землетрясения, при непредвиденном резком повышении уровня нижнего бьефа (в результате сильного паводка или аварии на верхней или нижней плотине каскада ГЭС), в результате техногенной аварии в машинном зале. В этих случаях затопление кластера может произойти только по причине неплотно закрытой оператором СМ входной двери, если это закрытие осуществляется им вручную.

Взрыв в кластере может произойти по причине умышленного террористического акта, совершенного либо оператором СМ, либо иным лицом при участии оператора. При взрыве внутри кластеров К1-К6 кластер полностью выходит из строя, а при сильном взрыве внутри кластера могут быть дополнительно повреждены один или два соседних кластера.

При воздействии всех перечисленных НВ СПА должна сохранять полную или частичную работоспособность с сохранением функциональной безопасности ГЭС, что обеспечивается отказоустойчивой структурой ядра СПА и специальным порядком расположения кластеров в помещении ГЭС (рис. 8). Перечень работоспособных состояний СПА при повреждениях кластеров приведен в табл. 2.

Таблица 2. Таблица работоспособных состояний СПА при повреждениях кластеров

№ п/п	Вид повреждения кластеров (частичное повреждение – ЧП)	Состояние СПА (работоспособное – Р, неработоспособное – НР, частично работоспособное – ЧР)
1	Затопление К1	Р
2	Затопление К2	Р
3	Затопление К3	Р
4	Затопление К4	Р
5	Затопление К5	Р
6	Затопление К6	Р
7	Затопление К7	ЧР (защитное)
8	Взрыв К1, ЧП К4	Р
9	Взрыв К4, ЧП К5	Р
10	Взрыв К5, ЧП К2	Р
11	Взрыв К2, ЧП К3	Р
12	Взрыв К3, ЧП К6	Р
13	Взрыв К6 ЧП К7	Р
14	Взрыв К7	ЧР (защитное)
15	Взрыв К4, ЧП К1 и К5	Р
16	Взрыв К5, ЧП К4 и К2	Р
17	Взрыв К2, ЧП К5 и К3	Р
18	Взрыв К3, ЧП К2 и К6	Р
19	Взрыв К6 ЧП К3 и К7	Р
20	Взрыв К7 ЧП К6	ЧР (защитное)

Анализ результатов, приведенных в табл. 1, показывает высокий уровень живучести СПА, построенной по кластерной структуре на базе СДКМС. Специальное расположение кластеров (рис. 9) позволяет сохранять работоспособное состояние СПА даже при выходе из строя в результате взрыва 3-х кластеров одновременно.

Частично работоспособное состояние СПА (защитное) [3] по причине повреждения кластера К7, исключающее при этом опасный отказ системы, обеспечивается построением этого кластера на h_1-надежных элементах гравитационной автоматики – электромагнитных реле с ВУГ в герметичных противоударных защитных корпусах. Для исключения возможности затопления кластера его входная дверь выполнена в виде автоматической заслонки с ВУГ и гравитационным способом аварийного запирания.

12. Заключение

В одной из последних публикаций [28] касательно аварии на СШГЭС утверждается, что станция не была спроектирована на подобное развитие сценария аварии, в мировой истории гидроэнергетики таких аварий не было, поэтому ни одна из существующих ГЭС не проектировалась на такое развитие событий. Авария аналогичного типа не была предусмотрена логикой работы автоматики, кроме того, она развивалась очень быстро. В результате существовавшие на тот момент системы автоматического управления и регулирования гидроагрегатами не смогли вовремя сработать и в короткое время были уничтожены потоком воды. Полное обесточивание станции привело к тому, что аварийные затворы оказались дистанционно неуправляемыми и не смогли предотвратить катастрофическое развитие аварии.

В результате восстановительных работ многое сделано в направлении повышения безопасности и живучести СШГЭС, а также накоплен соответствующий опыт в строительстве новых ГЭС в будущем, а именно:

1. В правила, определяющие требования к обеспечению надежности и безопасности объектов гидроэнергетики, внесено больше 100 дополнений и изменений.

2. Выполнена дополнительная установка дизельных генераторов на гребне плотины. В случае обесточивания они включаются автоматически и тем самым создают дополнительный источник питания, который позволяет управлять этими затворами.

3. На гребне плотины организовано круглосуточное дежурство и в случае необходимости сотрудник ГЭС сможет без промедления сбросить затворы в ручном режиме.

4. Всё оборудование системы связи вынесено на незатопляемые отметки.

5. Запрещено размещение людей на условно затопляемых отметках. На работы люди допускаются в пропускном режиме только по производственной необходимости.

6. Внедрена система поиска персонала. Каждый работающий на станции человек будет допускаться в машинный зал только по специальным пропускам с электронным чипом, наподобие бейджа. Этот пропуск отслеживается системой поиска персонала, где бы ни был сотрудник: на какой отметке, в теле плотины или в машинном зале, его легко можно будет отыскать.

7. Для повышения надежности и безопасности сооружений станции используется береговой водосброс. Он предназначен для пропуска экстремальных паводков и паводков редкой повторяемости.

8. Все оборудование системы связи [29] вынесено на незатопляемые отметки. Решено отказаться от использования медных кабелей в системах связи и перейти на оптоволокно. Как показала практика, оптические каналы практически неуязвимы для воды.

9. Внедрена система технологического телевидения, которая позволяет минимизировать нахождение людей на затопляемых отметках. Система позволяет наблюдать не только за несанкционированным доступом в помещения, но и осуществлять визуальный контроль за работой оборудования и сооружений, в том числе и при возникновении внештатных ситуаций.

10. Гидроагрегаты оснащаются большим количеством датчиков, контролирующих их состояние. При выходе контролируемых параметров за предельные величины агрегат

автоматически останавливается, а доступ воды к нему перекрывается специальными затворами.

11. Проводится периодический контроль состояния шпилек.

12. Ограничено участие станций в процессе регулирования параметров общей энергосистемы, вследствие чего агрегаты работают в наиболее оптимальном режиме, без значительных вибраций.

13. Предприняты меры, исключающие полное обесточивание станции. Установлены дополнительные дизельные электрогенераторы, автоматически запускаемые при исчезновении основного питания. При необходимости вырабатываемая ими энергия может использоваться для автоматического закрытия затворов на гребне плотины, что приведет к прекращению подачи воды к турбинам.

Следует сформулировать основную парадигму в направлении повышения безопасности и живучести ГЭС – это разработка принципов инжиниринга сложных систем гидроэнергетического назначения и методов оценки надежности, безопасности и живучести с учетом требований по гарантоспособности, основанных на безопасных проектных решениях инфраструктуры, схем управления, контроля и защиты, а именно:

• построение инфраструктуры и систем ГЭС с учетом требований по гарантоспособности к системам критического применения;

• внедрение мероприятий по сокращению времени принятия решений в аварийных ситуациях и минимизации ущерба в результате аварии;

• организация системы планово-предупредительной профилактики всех компонентов ПТК АСУ ТП;

• проектирование рабочих помещений и машинного зала ГЭС по кластерному принципу с разделением отсеков автоматическими гравитационными заслонками, перекрывающими их в случае аварии;

• расположение центрального пульта управления и контроля, средств автоматики и КИП, а также СПА в отдельных кластерах выше уровня возможного затопления служебных помещений станции при аварии;

• построение ядра СПА на основе СДКМС с использованием блочной компоновки оборудования, способной к горячей замене отказавших ТЭЗ без остановки функционирования всей СПА;

• построение выходных блоков управления исполнительными объектами в СПА по принципам гравитационной автоматики;

• организация основного и резервного электроснабжения ГЭС с учетом категории безопасности потребителя с использованием современных отказоустойчивых СБП;

• расположение систем аварийного электроснабжения СПА в отдельных кластерах выше уровня возможного затопления служебных помещений станции.

Как обстоят дела с безопасностью ГЭС в Украине. В настоящее время в нашей стране функционируют 10 крупных гидроэлектростанций мощностью более 10 МВт: Днепровская, Днестровская-1, Кременчугская, Каневская, Киевская, Среднеднепровская, Каховская, Днестровская-2, Теребля-Рика, Александровская; 4 гидроаккумулирующие станции и почти 50 ГЭС малой мощности до 10 МВт. Все станции объединены в энергетическую компанию «Укргидроэнерго», которая в свою очередь входит в Национальную энергетическую компанию и Минтопэнерго Украины [30].

На украинских ГЭС, в отличие от российских, значительно меньше напор воды, однако аварии, подобные той, что произошла на Саяно-Шушенской ГЭС, не исключены. ГЭС по уровню опасности сопоставимы с АЭС как по тяжести последствий аварий, так и по скорости их развития, ведь более 40% гидромеханического оборудования на украинских станциях нуждаются в обновлении. Какие-то рекомендации по повышению безопас-

ности и живучести на украинских ГЭС на сегодняшний день дать трудно, так как информации об их техническом состоянии в открытой печати практически не имеется.

Ведомственный надзор на ГЭС, осуществляемый организациями Минтопэнерго, недостаточен, он не относится к государственному регулированию и является внутренним делом Минтопэнерго. Мощности и функции Госгортехнадзора, также являющегося государственной независимой организацией (в свете уроков аварии на Саяно-Шушенской ГЭС), недостаточны. Целесообразно было бы ввести должности государственных инспекторов Госгортехнадзора на ГЭС. На каждой ГЭС рекомендуется разработать и реализовать программу действий, направленных на становление и развитие культуры безопасности. Такая программа может включать несколько уровней:

• техническую политику руководства по обеспечению безопасности;

• ответственность и обязанность руководства по обеспечению безопасности;

• ответственность и обязанности каждого работника по обеспечению безопасности.

Кроме того, на каждой ГЭС рекомендуется, хоть и с большим опозданием, разработать Программу обеспечения гарантоспособности [31], по результатам выполнения которой можно будет оценить количественную характеристику реально достигнутого уровня гарантоспособности станции и сравнить его с уровнем гарантоспособности лучших аналогичных ГЭС.

Проведем параллель между ГЭС и АЭС [30]. Можно констатировать, что принципы обеспечения безопасности ГЭС во многом должны быть аналогичны применяемым на АЭС. И вообще, принципы обеспечения безопасности техногенно опасных (или, как часто говорят, критических) объектов имеют много общего. Причем в наибольшей степени это относится к системам управления именно критическими объектами.

В ядерной энергетике экспертизы проводит Госкомитет ядерного регулирования и его организация технической поддержки – Государственный научно-технический центр по ядерной и радиационной безопасности. В ядерной энергетике имеются международные стандарты по АЭС, как и по иным объектам, представляющим угрозу для безопасности. Они делят системы и элементы АЭС на классы (категории) безопасности в зависимости от влияния на безопасность. Чем выше класс безопасности, тем более высокие требования к качеству изготовления, надежности, эксплуатации элементов и систем. Во исполнение этих требований на АЭС разработаны многотомные классификаторы всего оборудования. На ГЭС такой классификации пока что нет.

Одним из основных требований к АЭС является использование апробированной мировой инженерно-технической практики. Например, применительно к ГЭС ошибки при задании требований к системам управления и контроля, особенно к их быстродействию, очевидны. Так, авария на Саяно-Шушенской ГЭС развивалась в течение 1,5 – 2 с, а требования к системам управления по остановке ГА на этой ГЭС определены 10 с. Подобное несоответствие могло бы быть устранено, если бы имелась соответствующая модель поведения ГА в таких аварийных ситуациях. Целесообразно направить усилия научных коллективов – институтов Национальной академии наук, вузов страны, конструкторских бюро, поставщиков оборудования и др. на разработку моделей аварийных ситуаций на ГЭС, что позволит разработать методы их избегания.

В ядерной энергетике в настоящее время создано и функционирует Международное агентство по атомной энергии (сокр. МАГАТЭ, англ. International Atomic Energy Agency, сокр. IAEA) - международная организация по развитию сотрудничества в области мирного использования атомной энергии. Аналогичной международной организации в области гидроэнергетики не существует. Возможно, следует задуматься о целесообразности ее создания.

«Укргидроэнерго» на своем совещании 9 сентября 2009 г. по проблемам состояния гидротехнических сооружений и оборудования рассмотрело ряд дополнительных мер по

обеспечению безопасности ГЭС, а 11 сентября состоялось совещание по этим же вопросам в СНБО. Министерство по вопросам чрезвычайных ситуаций и делам защиты населения от последствий Чернобыльской катастрофы также усиливает меры по безопасности гидротехнических сооружений.

Большая работа в области безопасности КИ проводится Национальным институтом стратегических исследований (НИСИ). В работе [32] представлен ряд аналитических материалов по вопросам защиты КИ в Украине, освещены актуальные вопросы создания нормативных, организационных и методологических основ безопасности в этом направлении. В 2015 г., по аналогии с зарубежными изданиями, опубликована так называемая Зеленая книга по вопросам защиты КИ в Украине, подготовленная как отечественными, так и зарубежными экспертами в указанной сфере. Кроме того, при НИСИ создана Межведомственная экспертная рабочая группа (МЭРГ) по вопросам противодействия угрозам распространения оружия и материалов массового уничтожения, а также связанных с ними террористических угроз и защиты критически важной для обеспечения жизнедеятельности государства инфраструктуры. В [33] проанализированы современные методологические подходы к оценке критичности объектов инфраструктуры. Показано, что ввиду неопределенности, в частности, неточности и неполноты информации, необходимой для корректной оценки угроз и рисков КИ, многомерности и несопоставимости возможных последствий, необходимости учета многочисленных взаимосвязей и взаимозависимостей объектов КИ, универсальность оценки критичности может быть обеспечена применением методов нечеткой логики и экспертных оценок, предложена 3^x-уровневая иерархическая модель критериев определения КИ и представлены предложения по дальнейшим шагам развития в Украине Государственной системы защиты КИ.

По мнению специалистов НИСИ, сложная обстановка в области безопасности в Украине, характеризующаяся в том числе ростом вероятности террористических угроз, увеличением количества природных и техногенных катастроф, требует отнесения защиты КИ в область приоритетных направлений противодействия угрозам национальной безопасности. При этом особую опасность для функционирования КИ могут представлять собой угрозы, в ходе реализации которых кризисная ситуация на одном из элементов КИ, вследствие различных взаимосвязей, может вызвать кризисную ситуацию на аналогичных объектах или на объектах КИ другого назначения, например, каскадах ГЭС.

Именно поэтому при создании Государственной системы защиты КИ следует исходить из возможности системы обеспечить устойчивость КИ к угрозам всех видов, включая угрозы природного и техногенного характера, угрозы, вызванные противоправными действиями и любыми комбинациями из перечисленного. Задача по созданию такой системы Государственного управления безопасностью нашла свое отражение в решении Совета национальной безопасности и обороны Украины от 29 декабря 2016 г. «О совершенствовании мер обеспечения защиты объектов критической инфраструктуры», введенном в действие Указом Президента Украины № 8/2017 от 16 января 2017 г.

Необходимо усилить международное сотрудничество Украины в сфере защиты КИ в свете резолюции Совета безопасности ООН по защите критической инфраструктуры от террористических атак № 2341 от 13 февраля 2017 г. В связи с чем Кабинету Министров Украины рекомендовано:

• ускорить разработку и принятие Концепции создания Государственной системы защиты КИ в Украине как основы для разработки соответствующих нормативно-правовых актов и программ защиты КИ;

• скоординировать деятельность органов государственной власти, местного самоуправления, субъектов хозяйствования, учреждений и организаций, а также населения по решению практических задач, связанных с обеспечением защиты и устойчивости КИ;

• создать рабочую группу по разработке первоочередных нормативно-правовых актов по созданию Государственной системы защиты КИ, в частности, относительно разработки и принятия Закона Украины «О критической инфраструктуре и ее защите».

СПИСОК ИСТОЧНИКОВ

1. Баранник А. Организация обеспечения безопасности критической инфраструктуры в США / А. Баранник // Зарубежное военное обозрение. – 2009. – № 8. – С. 3 – 10.
2. Черкесов Г.Н. Методы и модели оценки живучести сложных систем / Черкесов Г.Н. – М.: Знание, 1987. – 32 с.
3. Федухин А.В. Гравитационная автоматика в системах защиты объектов критических инфраструктур / А.В. Федухин // Математичні машини і системи. – 2017. – № 1. – С. 106 – 121.
4. СО 34.21.307-2005 Безопасность гидротехнических сооружений. Основные понятия. Термины и определения.
5. Федухин А.В. Атрибуты и метрики гарантоспособных компьютерных систем / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2013. – № 2. – С. 195 – 201.
6. РД 153-34.2-35.520-99 Общие технические требования к программно-техническим комплексам для АСУ ТП гидроэлектростанций.
7. Богучанская ГЭС [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Богучанская_ГЭС.
8. Эксплуатационные службы Богучанской ГЭС приступили к работе в новом служебно-производственном корпусе станции [Электронный ресурс]. – Режим доступа: http://www.dagestan.rushydro.ru/press/news/81838.html.
9. Колотов А. Безопасность Богучанской ГЭС: вопросы остаются [Электронный ресурс]. – Режим доступа: http://www.plotina.net/boges-kolotov/.
10. Нижне-Бурейская гидроэлектростáнция [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Нижне-Бурейская_ГЭС.
11. Авария на Нижне-Бурейской ГЭС [Электронный ресурс]. – Режим доступа: https://lenta.ru/news/2017/08/25/accident/.
12. После аварии на Нижне-Бурейской ГЭС проверят все затворы [Электронный ресурс]. – Режим доступа: http://www.amur.info/news/2017/08/25/129215.
13. Федухин А.В. Гравитационная автоматика в системах защиты объектов критических инфраструктур / А.В. Федухин // Математичні машини і системи. – 2017. – № 1 – С. 106 – 121.
14. Саяно-Шушенская ГЭС [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Саяно-Шушенская_ГЭС.
15. Москвичев В.В. Проблемы развития энергетики и безопасность гидротехнических сооружений Красноярского края [Электронный ресурс] / В.В. Москвичев, В.Ф. Шабанов. – Режим доступа: http://www.plotina.net/experts/moskvichev/.
16. Гармонизация - системная методология проектирования гидросооружений [Электронный ресурс]. – Режим доступа: http://studbooks.net/1795385/geografiya/garmonizatsiya-sistemnaya_metodologiya_proektirovaniya_gidrosooruzheniy.
17. Додонов А.Г. Введение в теорию живучести вычислительных систем / Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. – К.: Наукова думка, 1990. – 184 с.
18. Додонов А.Г. Живучесть и надежность сложных систем. Методическое пособие / Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. – Киев: Международный научно-учебный центр информационных технологий и систем ЮНЕСКО/МПИ, 2001. – 163 с.
19. Брежнев Е.В. Методология обеспечения безопасности критических инфраструктур в условиях неопределенности: концепция и принципы / Е.В. Брежнев, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2015. – № 1 (71). – С. 25 – 32.
20. Зыбин С.В. Принципы и способы обеспечения живучести компьютерных систем / С.В. Зыбин, И.В. Лихицкая // Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – № 2 (42). – С. 67 – 71.
21. Атомная глубоководная станция ЛоШарик [Электронный ресурс]. – Режим доступа: http://masterok.livejournal.com/2715754.html.

22. Федухин А.В. К вопросу об аппаратной реализации избыточных структур: резервированная двухканальная система с реконфигурацией / А.В. Федухин., Ар.А. Муха // Математичні машини і системи. – 2010. – № 4. – С. 156 – 159.
23. Федухин А.В. К вопросу моделирования надежности восстанавливаемой квазимостиковой структуры с учетом тренда параметров надежности составных частей / А.В. Федухин, В.П. Пасько, Ар.А.Муха // Математичні машини і системи. – 2016. – № 1. – С. 158 – 167.
24. Палагин А.В. Особенности проектирования компьютерных систем на кристалле ПЛИС / А.В. Палагин, Ю.С. Яковлев // Математичні машини і системи. – 2017. – № 2. – С. 3 – 14.
25. Яковлев Ю.С. Средства сбора и предварительной обработки данных с использованием ПЛИС для технологических компьютерных систем и сетей / Ю.С. Яковлев, А.А. Тимашов // Математичні машини і системи. – 2017. – № 1. – С. 25 – 38.
26. Федухин А.В. ПЛИС-системы как способ повышения отказоустойчивости информационно-управляющих комплексов / А.В. Федухин, Ар.А. Муха, А.А. Муха // Математичні машини і системи. – 2010. – № 1. – С. 198 – 204.
27. Системы бесперебойного питания [Электронный ресурс]. – Режим доступа: http://kolkata.all.biz/ru/kompaktnye-vzlety-g424543#.WN59UbjGzCM.
28. Уроки аварии. Саяно-Шушенская ГЭС почти восстановлена [Электронный ресурс]. – Режим доступа: http://www.aif.ru/society/uroki_avarii_sayano-shushenskaya_ges_pochti_vosstanovlena.
29. Саяно-Шушенская ГЭС. 3 года спустя [Электронный ресурс]. – Режим доступа: https://neftegaz.ru/news/view/103804-Sayano-Shushenskaya-GES.-3-goda-spustya.
30. Артюх С. Авария на Саяно-Шушенской ГЭС. Уроки для Украины / С. Артюх, М. Ястребенецкий // Газета 2000. Электроэнергетика. – 04.12.2009.
31. Федухин А.В. Пакет прикладных программ GARANTmod в инжиниринге гарантоспособных систем / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2013. – № 3. – С. 178 – 185
32. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. мат-лів міжнар. експерт. нарад / Упоряд. Д.С. Бірюков, С.І. Кондратов; під заг. ред. О.М. Суходолі. – К.: НІСД, 2015. – 176 с.
33. Бобро Д.Г. Удосконалення методології ранжування об’єктів критичної інфраструктури та їх віднесення до критичної інфраструктури [Електронний ресурс] / Д.Г. Бобро. – Режим доступа: http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf.

Стаття надійшла до редакції 22.02.2018