

УДК 621.3.019.3

К ВОПРОСУ О ЖИВУЧЕСТИ СИСТЕМ ПРОТИВОАВАРИЙНОЙ АВТОМАТИКИ НА ГИДРОЭЛЕКТРИЧЕСКИХ СТАНЦИЯХ

Муха А.А.

Институт проблем математических машин и систем
Национальной академии наук Украины

Статья посвящена вопросам живучести информационных систем противоаварийной безопасности. Сформулированы принципы инжиниринга сложных систем гидроэнергетического назначения и методы оценки надежности, безопасности и живучести с учетом требований по гарантоспособности, основанных на безопасных проектных решениях инфраструктуры, схем управления, контроля и защиты.

Ключевые слова: живучесть, гарантоспособность, безопасность компьютерных систем.

Введение. Плотины и плотинные гидроэлектростанции (ГЭС) в частности, не смотря 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).

Постановка проблемы. 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);
- 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 настоящего совершенствования. В связи с этим, в последние годы наблюдается значительное повышение интереса к такой характеристике, как *живучесть*, как в теоретическом, так и в практическом плане. Это можно объяснить, по-видимому, следующими обстоятельствами [2].

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

Во-вторых, в больших КС возрастает 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 распо-

лагать, если спроектирована для работы только в нормальных условиях эксплуатации.

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

Живучесть технических систем. В настоящее время свойство *живучесть* распространяют не только на военные технические системы, но и на КС общего назначения. **Анализ последних исследований и публикаций** [2; 3; 4] показывает, что 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 тоже время существует и другое определение более 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 [3; 4].

КС, как любым сложным системам, присуща 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 закладываются 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 [5].

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 [6], данный подход является наиболее важным и иногда единственным способом обеспечения безопасности и живучести критических систем и инфраструктур в целом.

Оценка и обеспечение безопасности и живучести КС является многокритериальной задачей. Увеличение живучести, снижение уязвимости может быть достигнуто за счет функциональной информационной диверсификации наиболее важных узлов и связей между ними.

Эффект взаимозависимости между подсистемами КС очевиден, когда благодаря близости или различного рода влияниям (физическим, географическим, информационным, логическим и пр.), изменение состояния одной подсистемы КС вызывает изменения в состоянии безопасности и живучести всех зависимых подсистем КС.

С одной стороны, взаимозависимость обеспечивает живучесть КС, обуславливая ее работоспособность и быстрое восстановление после воздействия неблагоприятных факторов, с другой, 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 [6] 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, для повышения безопасности и живучести КС. Данный вид резервирования приводит к увеличению робастности КС, как способности к выполнению основных функций в условиях работы, отличных от нормальной эксплуатации – *живучести*.

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

В [7] сформулированы основные принципы и способы обеспечения живучести КС.

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 состояния 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 составляет "минимальное сечение", тем ниже вероятность их одновременного поражения, тем выше показатель живучести КС.

Кластерная структура – как способ повышения живучести. Кардинальное решение в направлении повышения живучести достигается путем реализации **принципа инфраструктурного резервирования** и диверсности [6] 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 является кластерная структура рабочих отсеков атомной глубоководной станции АС-12 проекта 10831 [8], приведенная на рис. 1.

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



Рис. 1. Инфраструктурное резервирование рабочих кластеров атомной глубоководной станции повышенной живучести АС-12

Во всех этих ситуациях глубоководная станция сохраняет функционирование и обеспечивает сохранность экипажа или его эвакуацию.

Аналогичные требования целесообразно распространить и к СПА, как к системам критического применения, ответственным за безопасность всей КИ ГЭС. Рассмотрим их реализацию более подробно.

Организация инфраструктурного резервирования СПА. Выделив часть ранее не решенных проблем, при построении систем СПА, воспользуемся идеей повышения живучести глубоководной станции АС-12 путем кластеризации системы. Во-первых, с целью повышения отказоустойчивости и живучести СПА для ее реали-

зации предлагается использование нового класса **самопроверяемых двухканальных структур** с реконфигурацией, получивших название самопроверяемых двухканальных квазимостиковых структур (СДКМС) [9], в которых каждый вычислительный канал состоит из приблизительно равнонадежных функциональных субблоков (ФСБ), которые с помощью схем реконфигурации (СР) образуют 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 [10], 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. 2 в качестве примера изображена квазимостиковая структура типа СДКМС отказоустойчивого ядра СПА, декомпозированная на 7 кластеров.

Во-вторых, техническая реализация квазимостиковых структур типа СДКМС наиболее эффективна как на базе современных ПЛИС-систем (в виде наборов интегральных микросхем (ИМС) и больших интегральных микросхем (БИС) или на базе единого кристалла ПЛИС) [11], так и в виде разнообразных микропроцессоров (МП) и микроконтроллеров (МК).

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

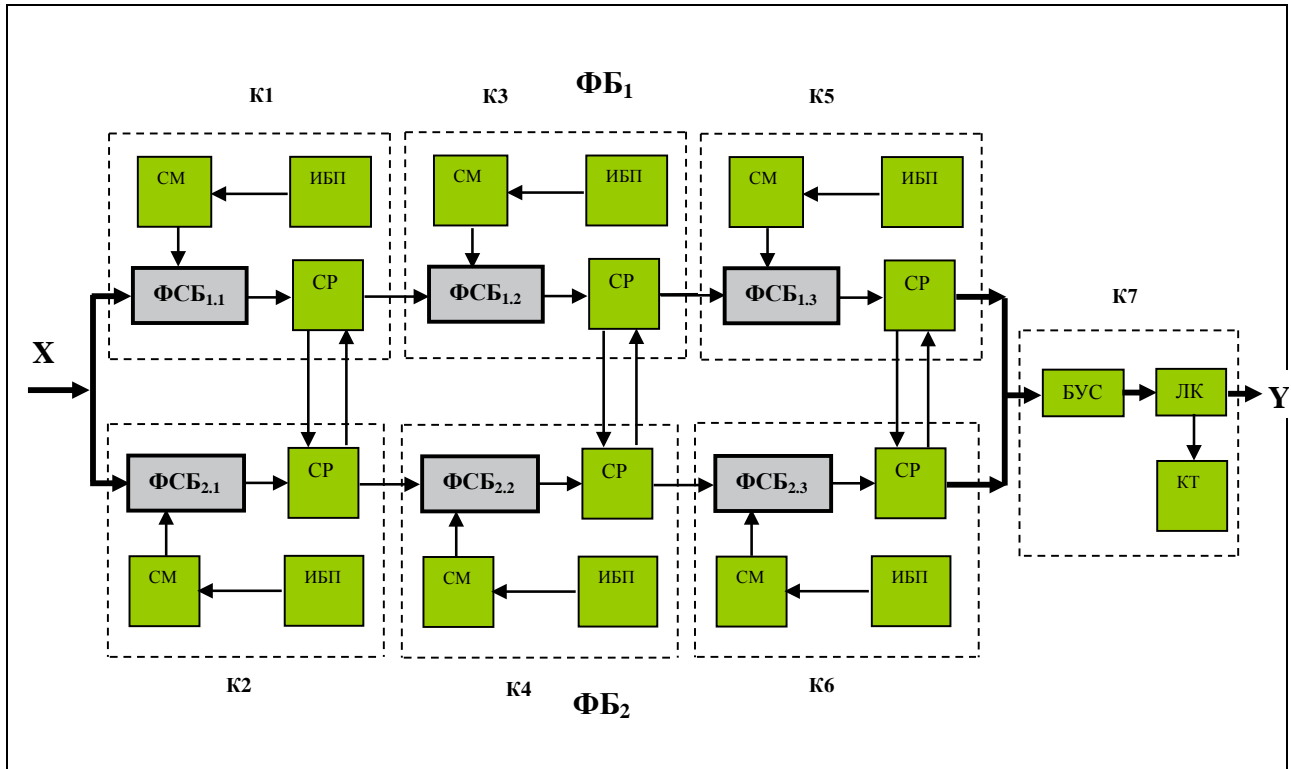


Рис. 2. Инфраструктурная схема СПА повышенной живучести на СДКМС



Рис. 3. h_1 -надежные реле ВУТ для построения кластера К7



Рис. 4. Общий вид статов для размещения h_1 -надежных электромагнитных реле с ВУТ в кластере К7

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 и техники.

На рис. 2 изображена кластерная структура реализации СДКМС. Каждый типовой кластер К1-К6 содержат 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) [12], предназначенных для электропитания всей АСУ ТП ГЭС, включая центральный пульт управления и контроля (ЦПУК) и механизмы управления аварийными заслонками (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 ВУТ (рис. 3), опломбированных и установленных на специальные статовы (рис. 4).

Каждый кластер СПА конструктивно представляет собой цельнометаллический или железобетонный отсек с прочным герметизированным входом (снабженным автоматическим или ручным запирающим), 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. 5, 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.

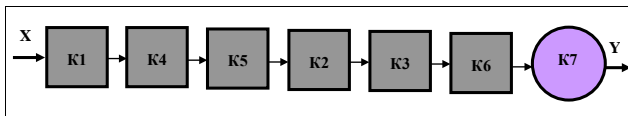


Рис. 5. Специальный порядок расположения кластеров в структуре СПА повышенной живучести

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

Анализ потенциальных уязвимостей кластерной структуры СПА. В отличие от кластеров К1-К6 (рис. 2), выполненных на элементах с симметричными отказами (ПЛИС, микропроцессорах, микросхемах, полупроводниковых приборах и т.п.), кластер К7 выполнен на h1-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 резком повышении уровня нижнего бьефа (в результате сильного паводка или аварии на верхней или нижней плотинах каскада ГЭС), в результате техногенной аварии в машинном зале ГЭС. 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 в организации теракта. 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. 5). Перечень работоспособных состояний СПА при повреждениях кластеров приведен в табл. 1.

Таблица 1

Таблица работоспособных состояний СПА при повреждениях кластеров

№ з/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. 5) позволяет сохранять работоспособное состояние СПА даже при выходе из строя в результате взрыва 3-х кластеров одновременно.

Частично работоспособное состояние СПА (защитное) [29] по причине повреждения кластера К7, исключающее при этом опасный отказ системы, обеспечивается построением этого кластера на ***h₁-надежных*** элементах гравитационной автоматики – электромагнитных реле с ВУГ в герметичных противоударных защитных кожухах.

Для исключения возможности затопления кластера его входная дверь выполнена в виде автоматической заслонки с ВУГ и гравитационным способом аварийного запирания.

Выводы. Подытожив результаты исследований, возможно сформулировать основную парадигму в направлении повышения безопасности и живучести ГЭС – 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 программно-технических комплексов (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 контрольно-измерительных приборов (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 типовых элементов замены (ТЭЗ) без остановки функционирования всей СПА;

- построение выходных блоков управления исполнительными объектами в СПА на принципах 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.

Список литературы:

1. Баранник А. Организация обеспечения безопасности критической инфраструктуры в США // Зарубежное военное обозрение. – № 8. – 2009. – С. 3–10.
2. Черкесов Г.Н. Методы и модели оценки живучести сложных систем. – М.: Знание, 1987. – 32 с.
3. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. – К.: Наук. думка, 1990. – 184 с.
4. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Живучесть и надежность сложных систем. Методическое пособие. – Международный научно-учебный центр информационных технологий и систем ЮНЕСКО / МПИ, 2001. – 163 с.
5. Федухин А.В., Сеспедес Гарсия Н.В. Атрибуты и метрики гарантоспособных компьютерных систем // Математичні машини і системи. – 2013. – № 2. – С. 195–201.
6. Брежнев Е.В., Харченко В.С. Методология обеспечения безопасности критических инфраструктур в условиях неопределенности: концепция и принципы // Радіоелектронні і комп'ютерні системи. – 2015. – № 1(71). – С. 25–32.
7. Зыбин С.В., Лихицкая И.В. Принципы и способы обеспечения живучести компьютерных систем // Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – № 2(42). – С. 67–71.
8. Атомная глубоководная станция ЛоШарик [Электронный ресурс]. – Режим доступа: <http://masterok.livejournal.com/2715754.html>.
9. 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.
10. Федухин А.В., Пасько В.П., Муха Ар.А. К вопросу моделирования надежности восстанавливаемой квази-мостиковой структуры с учетом тренда параметров надежности составных частей // Математичні машини і системи. – 2016. – № 1. – С. 158–167.
11. Палагин А.В., Яковлев Ю.С. Особенности проектирования компьютерных систем на кристалле ПЛИС // Математичні машини і системи. – 2017. – № 2. – С. 3–14.
12. Системы бесперебойного питания [Электронный ресурс]. – Режим доступа: <http://kolkata.all.biz/ru/kompaktnye-vzlety-g424543#.WN59UbjGzCM>.
13. Федухин А.В. Гравитационная автоматика в системах защиты объектов критических инфраструктур // Математичні машини і системи. – 2017. – № 1 – С. 106–121.

Муха А.А.

Інститут математичних машин та систем
Національної академії наук України

ДО ЗАПИТАННЯ ПРО ЖИВУЧІСТЬ СИСТЕМ ПРОТИАВАРІЙНОЇ АВТОМАТИКИ НА ГІДРОЕЛЕКТРИЧНИХ СТАНЦІЯХ

Анотація

Стаття присвячена питанням відмовостійкості інформаційних систем протиаварійної безпеки. Сформульовано принципи інжинірингу складних систем гідроенергетичного призначення і методи оцінки надійності, безпеки і живучості з урахуванням вимог по гарантоздатності, заснованих на безпечних проектних рішеннях інфраструктури, схем управління, контролю і захисту.

Ключові слова: живучість, гарантоздатність, безпека комп'ютерних систем.

Mukha A.A.

Institute of Mathematical Machines and Systems Problems
of the Ukraine National Academy of Science

TO THE QUESTION OF THE SURVIABILITY ANTI-SAVE AUTOMATION SYSTEMS ON THE HYDRO-ELECTRIC STATIONS

Summary

The article is devoted to questions of survivability of information systems of emergency safety. The principles of engineering of complex hydropower systems and methods for assessing reliability, safety and survivability are formulated, taking into account the requirements for reliability, based on safe design infrastructure solutions, control, monitoring and protection schemes.

Keywords: survivability, dependability, security computer systems.