УДК 621.039.586

М. А. Ястребенецкий[1], Ю. В. Розен[1], Г. В. Громов[1], В. В. Инюшев[1], А. В. Носовский[1], М. Х. Гашев[2], Б. В. Столярчук[2]

[1]Государственный научно-технический центр по ядерной и радиационной безопасности, г. Киев, Украина
[2]Государственная инспекция ядерного регулирования Украины, г. Киев, Украина

Требования к информационным и управляющим системам АЭС Украины по результатам анализа аварии на АЭС Фукусима-1

Выводы из аварии на АЭС Фукусима-1 конкретизируются применительно к информационным и управляющим системам (ИУС), важным для безопасности. Рассмотрена их уязвимость к экстремальным внешним воздействиям. Представлены рекомендации по пересмотру действующих норм ядерной безопасности и по регулирован ию безопасности, относящиеся к ИУС и их компонентам.

Ключевые слова: авария, АЭС, Фукусима-1, функциональная безопасность, информационные и управляющие системы, компоненты ИУС, нормы и правила, стресс-тест.

М.О. Ястребенецький, Ю. В. Розен, Г. В. Громов, В. В. Інюшев, А. В. Носовський, М. Х. Гашев, Б. В. Столярчук

Вимоги до інформаційних і керуючих систем АЕС за результатами аналізу аварії на АЕС Фукусіма-1

Висновки з аварії на АЕС Фукусіма-1 конкретизуються стосовно інформаційних і керуючих систем (ІКС), важливих для безпеки. Виконано аналіз функціональної безпеки ІКС, які експлуатуються на АЕС України. Представлено рекомендації з перегляду чинних норм ядерної безпеки і з регулювання безпеки, що ставляться до ІКС і їх компонентів.

Ключові слова: аварія, АЕС, Фукусіма-1, функціональна безпека, інформаційні та керуючі системи, компоненти ІКС, норми і правила, стрес-тест.

В отличие от крупных ядерных аварий на Three Mile Island и Чернобыльской АЭС, авария на Фукусима-1 не имела непосредственной связи с работой информационных и управляющих систем: по сигналу о превышении пикового ускорения и в условиях потери внешнего электроснабжения АЭС все работавшие энергоблоки были остановлены системами аварийной защиты, запущены резервные дизель-генераторы и включены аварийные электронасосы системы отвода остаточных тепловыделений. Однако в результате последующего полного обесточивания, вызванного затоплением дизель-генераторов и разрядом аккумуляторных батарей, перестали функционировать активные элементы систем безопасности, и избежать перегревания и повреждения ядерного топлива оказалось невозможным [1]—[7]. Тем не менее, эта авария заставила ещё раз обратить внимание на необходимость дальнейшего повышения функциональной безопасности ИУС*, которые создаются и/или эксплуатируются на энергоблоках АЭС Украины.

Функциональная безопасность ИУС обеспечивается за счёт:

соответствия параметров и характеристик требованиям норм и правил по ядерной и радиационной безопасности на всех стадиях жизненного цикла системы и её компонентов;

соблюдения установленного порядка разработки, проектирования, изготовления, испытаний, приёмки и эксплуатации новых и модернизированных систем и компонентов, важных для безопасности.

На конференции по ядерной безопасности в Вене 20—24 июня 2011 г., Генеральный директор МАГАТЭ Юкия Амано сделал пять предложений, вытекающих анализа аварии на японской АЭС «Фукусима-1»: ужесточить нормы ядерной безопасности и обеспечить их повсеместное соблюдение; провести ревизию и осуществлять регулярный контроль за безопасностью действующих АЭС; повысить эффективность функционирования национальных регулирующих органов в области атомной энергетики; укрепить глобальную систему реагирования на чрезвычайные ситуации; повысить роль МАГАТЭ в информировании о ядерных событиях [7].

В соответствии с заявлением Совета Европейского союза от 24.03.2011, первоочередной задачей является целевая переоценка безопасности европейских АЭС на основе всесторонней и открытой оценки риска путём проведения стресс-тестов, предложенных Ассоциацией западноевропейских органов регулирования ядерной безопасности (WENRA) [4]. Должны быть детально проанализированы экстремальные естественные события и их комбинации, которые влияют на возможность выполнения функций безопасности и могут привести к тяжёлой аварии. Проведение стресс-тестов на АЭС Украины предусмотрено Планом действий [1]. Под стресс-тестами понимаются дополнительные проверки, основанные на материалах проекта, отчетах по анализу безопасности, выполненных ранее исследованиях, экспертных оценках и инженерных допущениях с учетом более жестких воздействий и возможного наложения негативных факторов [2].

* Под функциональной безопасностью ИУС понимают свойство, которое заключается в способности системы правильно выполнять все требуемые функции, важные для безопасности, и соответствовать заданным характеристикам во всех предусмотренных проектом режимах и условиях эксплуатации, нарушениях условий эксплуатации и проектных авариях [8].

Целью настоящей статьи является подготовка предложений по переоценке безопасности АЭС Украины в свете событий на японской АЭС Фукусима-1 применительно к проблемам функциональной безопасности ИУС и их компонентов. Приведенные в статье соображения не являются исчерпывающими и могут дополняться и корректироваться в связи с выходом новых норм, правил и стандартов, а также с учётом результатов целевой внеочередной проверки и реализации плана действий по дальнейшему повышению безопасности АЭС, предусмотренных постановлением коллегии Государственной инспекции ядерного регулирования Украины [1].

Анализ безопасности эксплуатируемых ИУС

Из рассмотренных в [2] направлений переоценки безопасности (уязвимости к экстремальным внешним воздействиям) непосредственно к ИУС и их компонентам относятся следующие.

Стойкость к землетрясениям. Исходя из уроков аварии на АЭС Фукусима-1, к числу наиболее важных направлений следует отнести оценку риска от экстремальных механических воздействий, вызванных землетрясениями, которая предусматривает:

определение функций, которые должны быть выполнены при возникновении, во время прохождения и после окончания землетрясения;

установление состава ИУС и их эксплуатационно-автономных компонентов (изделий), участвующих в реализации этих функций;

назначение требуемой категории сейсмостойкости для каждого изделия;

определение требований к испытательным воздействиям, имитирующим при проверке сейсмостойкости реальные воздействия, которые могут быть вызваны землетрясениями в местах размещения изделий;

оценка соответствия изделий установленным требованиям к сейсмостойкости путём анализа нормативно-технической документации и/или экспериментальной проверки типовых (представительных) образцов;

выработка рекомендаций по обеспечению сейсмостойкости изделий или компенсирующих мероприятий, необходимых для обеспечения безопасности в условиях возможных (ожидаемых) сейсмических воздействий в местах их эксплуатации.

Оценка риска от землетрясений фактически составляет содержание *сейсмической квалификации* оборудования [9], которая должна охватывать компоненты систем безопасности и нормальной эксплуатации, в том числе те, которые инициируют работу и управляют обеспечивающими системами, например аварийными дизель-генераторами. Сейсмическая квалификация должна производиться в процессе валидации (предварительных и приёмочных испытаний изделий) и предусматривать оценку влияния экстремальных механических воздействий, вызванных землетрясениями, не только на сами изделия, но и на их крепление к строительным или промежуточным конструкциям, а также на внешние электрические и оптические кабели в местах их присоединения к изделию.

Требования к испытательным воздействиям устанавливают расчетом и/или моделированием спектров ответа строительных конструкций на сейсмические воздействия, возможные при землетрясениях, или на основании обобщенных значений спектров ответа в местах предполагаемой установки изделий, рекомендованных в [10]. Указания по определению сейсмостойкости эксплуатируемого оборудования приведены в [11].

Идентификация опасных событий. Не менее актуальной представляется оценка риска от ошибок ИУС и/или их компонентов, которые должны *обнаруживать* опасные внешние и внутренние события, способные привести к экстремальным воздействиям на оборудование АЭС, и *инициировать* срабатывание соответствующих исполнительных систем для минимизации риска от влияния таких воздействий. Отказ этих систем (компонентов) с большой вероятностью приведёт к возникновению аварийной ситуации, которая может перерасти в аварию.

События на АЭС Фукусима-1 показали, что землетрясения относятся к наиболее опасным внешним событиям. В настоящее время на энергоблоках Украины для идентификации землетрясений, интенсивность которых больше установленной, используются сейсмические датчики [8]. Каждый из них сам определяет превышение уровней ускорения, регламентированных для проектного и максимального расчётного землетрясений, и выдаёт команды (дискретные сигналы) в систему аварийной и предупредительной защиты, систему управления машиной перегрузки ядерного топлива и др. Применяемые сейсмодатчики соответствуют действующим нормам и правилам [12], однако следует провести их переоценку, чтобы подтвердить соответствие сейсмодатчиков новым, более жёстким требованиям к функциональной безопасности.

Специфичным для сейсмодатчиков является экспериментальная проверка корректности формирования выходных сигналов при различных формах спектров сейсмоускорений на входе (контроль точностных характеристик сейсмодатчиков). Требования к точностным характеристикам и методика проверки соответствия должны быть предметом специального исследования.

К числу опасных внутренних событий, также возникавших во время аварии на АЭС Фукусима-1, следует отнести *возгорания*. Согласно [1], должны быть подготовлены «предложения по повышению пожарной безопасности АЭС Украины и действенному механизму координации, нормирования и надзора». В помещениях энергоблока должны быть предусмотрены информационные системы обнаружения и оповещения о пожаре (системы пожарной сигнализации) и/или управляющие системы автоматического пожаротушения, которые должны удовлетворять тем же требованиям к функциональной безопасности, что и другие ИУС класса безопасности 2, а также противопожарным нормам [13]. Примером такой системы, созданной украинскими специалистами, является комплекс средств пожарной сигнализации и управления аппаратурой автоматического пожаротушения СПС1 [14]. Однако во многих случаях системы пожарной сигнализации, действующие на энергоблоках АЭС Украины, разрабатывались без учёта норм и правил по ядерной и радиационной безопасности и поэтому требуют переоценки.

Кроме того, следует выполнить переоценку соответствия противопожарным нормам [13] компонентов других информационных и управляющих систем, важных для безопасности, а также стойкость изделий класса безопасности 2 к воздействию огнетушащего вещества, заполняющего помещение при срабатывании системы автоматического пожаротушения.

Стойкость к экстремальной температуре. Согласно Плану действий [1], при проведении стресс-тестов должна оцениваться чувствительность к внешним воздействиям, в том числе к экстремально высоким и/или низким температурам.

Для компонентов ИУС требования стойкости к экстремальным значениям воздействующих факторов окружающей среды установлены в [12] в виде верхнего предельного значения температуры (которое может быть достигнуто при нарушении рабочих условий эксплуатации в помещении, где расположено изделие) и времени, равного ожидаемой максимальной продолжительности предельных условий эксплуатации. Верхние предельные значения температуры определяют на основании расчетов, а при их отсутствии — исходя из обобщенных предельных значений, приведенных в [12] для соответствующей группы условий эксплуатации с учётом возможных причин нарушения рабочих условий. Ожидаемая продолжительность существования предельных условий указана там же в зависимости от причины нарушения (малая или максимальная течь, нарушение теплоотвода из герметичного ограждения, разрывы линий от технологического оборудования к датчикам, отключение вентиляции, неисправность системы кондиционирования).

Опыт показывает, что время, необходимое для ликвидации нарушения и восстановления рабочих условий эксплуатации, не превышает установленной в [12] продолжительности существования предельных условий. Однако это справедливо только в тех случаях, когда такое нарушение вызвано одним независимым исходным событием. Если же нарушение является следствием другого события (например, землетрясения), для его устранения может понадобиться значительно большее время, в течение которого управляющие системы безопасности должны выполнять заданные функции в условиях предельной температуры. Рассматривается возможность *не ограничивать* время работы изделий класса безопасности 2 при экстремальных значениях воздействующих факторов окружающей среды.

Стойкость к комбинации внешних воздействий. Комбинации экстремальных естественных событий или *одновременное* действие экстремального естественного события и вызванных им нарушений рабочих условий эксплуатации оборудования могут влиять на возможность выполнения функций безопасности и стать причиной тяжёлой аварии. Однако для ИУС и их компонентов такое наложение негативных факторов не характерно (например, сейсмическое воздействие закончится значительно раньше, чем начнёт заметно изменяться температура в помещении из-за отказа системы кондиционирования и вентиляции, вызванного землетрясением). Это позволяет проверять стойкость изделия поочерёдно к каждому виду внешних воздействий при номинальных значениях остальных воздействующих факторов (стойкость к одновременному воздействию нескольких факторов не проверяют, за исключением экстремальных значений температуры и влажности).

Защищённость от террористических угроз. Согласно [1], требуется подготовить предложения относительно форм, методов и сроков оценки защищенности АЭС от террористических угроз и противоправных действий.

В отношении ИУС, важных для безопасности, должны быть предусмотрены требования по защите от несанкционированного доступа к составным частям эксплуатационно-автономных изделий, программному обеспечению, базам данных и архивам для предотвращения возможности умышленного или неумышленного вывода из работы, изменения режимов, условий или алгоритмов формирования выходных сигналов (команд), изменения программ и данных, порчи или хищения, которые могут создать угрозу для безопасности.

Кроме того, должны быть предусмотрены требования по защите программного обеспечения от нежелательного и небезопасного вмешательства в его работу и от несанкционированного изменения, которое могло бы осуществляться воздействием через внешние компьютерные сети и/или при использовании нерезидентных носителей данных. При этом должна быть исключена возможность доступа из сети Интернет к программному обеспечению, выполняющему функции категорий В и С, а программное обеспечение, выполняющее функции категории А, должно быть полностью изолировано от взаимодействия с внешними компьютерными сетями*.

Пересмотр норм и правил по ядерной безопасности

В числе краткосрочных мероприятий, предусмотренных в [1], указана необходимость анализа нормативно-правовой базы по ядерной и радиационной безопасности, разработки предложений по ее усовершенствованию и повышению требований по безопасности для действующих и новых энергоблоков АЭС.

Требования к функциональной безопасности ИУС и их компонентов регламентированы в нормах и правилах НП 306.5.02/3.035 [12], введенных в действие в 2000 г. Начиная с этого времени специалисты атомных станций, проектных организаций, предприятий-разработчиков и изготовителей технических средств, а также экспертных организаций и органа государственного регулирования ядерной безопасности Украины используют этот нормативный документ при разработке и оценке безопасности всех новых и модернизованных ИУС и их компонентов на энергоблоках Украины, а также на энергоблоках ряда зарубежных АЭС.

Однако уже после разработки НП 306.5.02/3.035 были приняты новые стандарты МАГАТЭ, МЭК и других международных организаций, в которых аккумулирован опыт мирового сообщества по обеспечению безопасности АЭС, включая функциональную безопасность информационных и управляющих систем. Эти стандарты существенно изменили требования к ИУС и их компонентам, в частности к электромагнитной совместимости, надежности, верификации и валидации программного обеспечения, квалификации оборудования и т. д. Кроме того, широкомасштабная модернизация ИУС, которая проводится на всех АЭС Украины в рамках программ повышения безопасности и продления срока эксплуатации действующих энергоблоков, способствовала накоплению собственного опыта нормирования, обеспечения и оценки функциональной безопасности систем и компонентов, реализованных с применением современных информационных технологий, новейших электронных компонентов, оптических сетей передачи данных, компьютерных средств диагностики, отображения, архивирования и т. п.

---

* Классификация функций по категориям в зависимости от их роли в обеспечении безопасности регламентирована в международном стандарте [15] и идентичном ему государственном стандарте Украины [16].

В связи с этим возникла необходимость пересмотра действующего нормативного документа с целью гармонизации с требованиями новых международных стандартов, а также с учётом опыта его применения. Предполагается, что по результатам пересмотра в состав создаваемой в Украине иерархической пирамиды законодательных и нормативных документов в области ядерной и радиационной безопасности будут включены:

нормативно-правовой акт Государственной инспекции ядерного регулирования Украины — нормы и правила [17], содержащие регулирующие требования к функциональной безопасности ИУС и их компонентов;

отраслевой стандарт Министерства энергетики и угольной промышленности Украины [18], содержащий общие технические требования к ИУС и их компонентам, необходимые и достаточные для выполнения регулирующих требований.

Оба документа имеют одинаковую структуру, при этом каждое из регулирующих требований [17] детализировано в [18] с такой степенью подробности, которая допускает возможность непосредственного использования при разработке, испытаниях и оценке конкретных систем и их компонентов.

Разработанные проекты нормативных документов имеют ряд существенных отличий от действующих норм и правил, которые и представлены ниже.

Классификация по безопасности гармонизирована с международными стандартами [15], [19] и идентичными им государственными стандартами Украины [16], [20]: за основу приняты *категории* выполняемых функций, по которым определяются *классы безопасности* ИУС и их компонентов [21], при этом число классов увеличено с двух до трех, как принято в европейских странах*. В то же время сохранена преемственность действующей в Украине классификации по безопасности, установленной в НП 306.2.141 [22], которая допускает возможность уточнения и детализации классификационных критериев и использования классификационных признаков, которые устанавливаются в нормах и правилах, относящихся к отдельным видам систем и элементов.

Гармонизация с международной классификацией функций, систем и компонентов устраняет трудности при оценке безопасности информационно-управляющих систем и компонентов, поставляемых зарубежными фирмами на АЭС Украины, способствует экспорту продукции украинских производителей для зарубежных АЭС и облегчает прямое внедрение в Украине международных стандартов, аккумулирующих многолетний мировой опыт нормирования, оценки и обеспечения безопасности ИУС.

Охвачены все стадии жизненного цикла ИУС и их компонентов:

проектирование ИУС, разработка программно-технических комплексов, технических средств, программного обеспечения;

квалификация оборудования, верификация программного обеспечения, валидация и приемочный контроль продукции на предприятиях-изготовителях;

испытания при вводе в эксплуатацию, техническое обслуживание, проверки и восстановление ИУС и их компонентов;

внесение изменений и модернизация действующих систем.

Таким образом, наряду с требованиями к *продуктам* (системам и компонентам), проекты нормативных документов устанавливают также требования к *процессам* их создания, внедрения и эксплуатации, что является необходимым условием обеспечения функциональной безопасности.

Включены новые требования, отсутствовавшие в НП 306.5.02/3.035:

требования к защите от кибернетических угроз (cyber security), препятствующие нежелательному и небезопасному вмешательству в работу ИУС и/или несанкционированному изменению программного обеспечения и данных путём воздействия через внешние компьютерные сети или при использовании нерезидентных носителей данных;

требования к управлению конфигурацией, позволяющие в каждый момент времени достоверно идентифицировать все характеристики системы и/или ее компонентов, включая возможные изменения характеристик в течение жизненного цикла;

требования к системам и оборудованию блочного щита управления, которые должны обеспечивать оперативный персонал полной, точной, своевременной и легко обозримой информацией и предоставлять ему необходимые средства ручного управления;

требования к системам и оборудованию резервного щита управления, с помощью которых персонал может переводить и удерживать реактор в подкритическом состоянии, отводить остаточное тепло, контролировать основные параметры энергоблока и оценивать состояние систем безопасности в ситуациях, когда утрачена возможность выполнять эти функции из помещения блочного щита.

Расширены требования к электромагнитной совместимости. К видам помех, регламентированных в НП 306.5.02/3.035, в проектах нормативных документов [17], [18] добавлены электромагнитные воздействия, возможные в рабочих и предельных условиях эксплуатации, по отношению к которым должна обеспечиваться невосприимчивость ИУС и их компонентов: кондуктивные помехи, наведенные радиочастотными полями; помехи от затухающего колебательного магнитного поля; колебательные затухающие помехи; кондуктивные несимметричные помехи. Уточнены критерии соответствия продукции требованиям невосприимчивости к электромагнитным помехам, учитывающие электромагнитную обстановку в местах эксплуатации изделий, их назначение и класс безопасности. Методы испытаний помехоустойчивости [23], [24] и невосприимчивости к кратковременным изменениям напряжения и частоты питающего тока гармонизированы с новыми государственными стандартами Украины, идентичными стандартам МЭК. Кроме норм эмиссии излучаемых радиопомех, которые были регламентированы в [12], установлены также требования к допускаемому уровню помех от компонентов ИУС в сеть первичного электропитания.

Учтены особенности новой элементной базы, применяемой для реализации функций, важных для безопасности. В частности, установлены требования к разработке и имплементации электронных проектов программируемых логических интегральных схем (ПЛИС), конфигурируемых пользователем [8].

Разработанные ГНТЦ ЯРБ проекты нормативных документов [17] и [18] были разосланы на отзыв и доработаны с учетом замечаний и предложений эксплуатирующей

* Стандарт EN 61226, идентичный [15], принят Европейским комитетом по стандартизации в электротехнике (CENELEC) и в настоящее время внедрен в 31 европейской стране.

организации и её обособленных подразделений (АЭС), разработчиков и изготовителей программно-технических комплексов и организаций, проектирующих ИУС для АЭС Украины, специалистов ГНТЦ ЯРБ и Государственной инспекции ядерного регулирования Украины. Однако авария на АЭС Фукусима-1 заставила еще раз вернуться к этим документам, чтобы по результатам анализа произошедших событий внести в них необходимые *изменения и дополнения*.

Повышены требований по сейсмостойкости компонентов ИУС, выполненных в виде эксплуатационно-автономных изделий.

В действующих нормах и правилах [12] предусмотрено, что параметры сейсмических воздействий устанавливают на основании расчетов, учитывающих ожидаемую интенсивность землетрясения на площадке АЭС, данные сейсмического микрорайонирования, проектную высотную отметку и условия размещения изделий (на строительных или промежуточных конструкциях), или исходя из обобщенных параметров сейсмических воздействий, которые приведены в зависимости от уровня установки (проектной высотной отметки) и условий размещения изделий. Например, для максимального расчётного землетрясения (7 баллов для всех энергоблоков Украины) при размещении непосредственно на строительных конструкциях на уровне 10 м был регламентирован спектр сейсмического ускорения с наибольшим значением в горизонтальной плоскости 1,25 м/с^2 (на частоте 4 Гц). Для такого же землетрясении при размещении изделия на уровне 30 м максимальное ускорение составляет 2,5 м/с^2 и т. п.

Японское землетрясение может заставить учёных-сейсмологов пересмотреть параметры спектра сейсмических воздействий и, соответственно, проектные нормы. До сих пор считалось, что при 9-балльном землетрясении ускорение грунта может быть максимум 4 м/с^2, однако японская катастрофа показала около 27 м/с^2 [25]. Для 7 баллов это может соответствовать максимальному ускорению на уровне земли 6-7 м/с^2.

Необходимость существенного ужесточения испытательных воздействий, имитирующих землетрясения при проверке сейсмостойкости оборудования, обсуждается в течение последних лет и уже начинает практически реализовываться в разработках новых компонентов ИУС для отечественных и зарубежных АЭС. В проекте нормативного документа [18] предложено определять испытательные воздействия с учётом возможной реакции на колебания земной поверхности («спектра ответа») строительных или промежуточных конструкций в том месте, в котором будет размещаться (или размещается) изделие. При этом следует принимать во внимание синтезированную акселерограмму земной поверхности для максимального расчётного и/или проектного землетрясения, коэффициент демпфирования строительных конструкций, уровень установки и условия размещения (способ монтажа) изделия, учитывать его механическое старение и иметь необходимый запас жёсткости, компенсирующий возможные погрешности испытаний.

В случае отсутствия расчётных данных требуемые спектры испытательных воздействий могут быть определены на основании обобщенных значений, приведенных в [18], которые существенно превышают указанные в НП 306.5.02/3.035. Например, при размещении изделия непосредственно на строительных конструкциях на уровне 10 м наибольшее значение ускорения в горизонтальной плоскости для максимального расчётного землетрясения составляет 7,6 м/с^2 (в диапазоне частот от 2 до 10 Гц), а на высоте 30 м — 18,4 м/с^2.

Уточнение классификации. Первоначально, следуя рекомендациям [15] и [16], предполагалось функции обнаружения опасных событий и/или смягчения их последствий относить к самой низкой категории (С), что позволяло использовать для их реализации компоненты класса безопасности 3. Исходя из последствий аварии на АЭС Фукусима-1, предложено считать, что эти функции относятся к наиболее высокой категории (А), поскольку их отказы могут привести к аварийной ситуации или аварии. Это означает, что для обнаружения таких опасных событий, как землетрясение или пожар, должны использоваться технические средства не ниже второго класса безопасности. Применительно к компонентам ИУС такими функциями являются:

идентификация опасных ускорений земной поверхности, которые регламентированы как исходные события для соответствующих эксплуатационных режимов (перегрузка ядерного топлива, работа на мощности и т. п.);

выдача команд, инициирующих действия защитных, локализующих и/или обеспечивающих систем безопасности, которые предусмотрены для соответствующего исходного события, и управление работой этих систем непосредственно во время землетрясения и/или после него.

Предложено также изменить критерии, по которым устанавливается категория сейсмостойкости, приняв за основу не класс безопасности системы и/или изделия, как в [12], а *выполняемые функции*. К категории сейсмостойкости I в этом случае должны относиться изделия, участвующие в реализации тех функций, которые должны быть инициированы и/или выполнены:

во время землетрясения (обнаружение опасного сейсмического воздействия, аварийная остановка реактора, блокировка движущихся механизмов и т. п.);

непосредственно после землетрясения (поддержание реактора в подкритическом состоянии, аварийный отвод тепла, предотвращение выхода радиоактивных веществ за установленные границы, послеаварийный мониторинг параметров активной зоны реактора, состояния барьеров безопасности и радиационной обстановки).

Изделия категории сейсмостойкости I должны выполнять указанные функции во время и/или после сейсмических воздействий, вызванных максимальным расчетным землетрясением на площадке АЭС. Изделия, которые не вошли в категорию I, должны относиться к категории сейсмостойкости II, если нарушение их работы, вызванное землетрясением, может привести к перерыву в выработке электроэнергии. Они должны выполнять все предусмотренные проектом функции после сейсмических воздействий, вызванных проектным землетрясением (6 баллов для всех энергоблоков Украины).

Категорию сейсмостойкости III предложено устанавливать для изделий, которые по указанным выше критериям не могут быть отнесены к категориям I и II, требования сейсмостойкости для них не регламентируются.

Установление требований к хранению данных. Для систем и компонентов, которые сохраняют данные о причинах возникновения и путях протекания аварий и/или участвуют в выполнении функций, необходимых для ликвидации их последствий, в проектах нормативных документов [17] и [18] предложено регламентировать требования стойкости внешним и внутренним воздействиям (падению тяжелых предметов из-за разрушения конструкций,

ионизирующему излучению, заливанию водой и растворами и т. п.), которые могут возникать при проектных и запроектных авариях.

Здесь уместно сослаться на прецедент, связанный с сохранением данных о работе четвёртого энергоблока Чернобыльской АЭС непосредственно накануне аварии. На энергоблоках с реакторами РБМК-1000 для хранения информации о контролируемых параметрах и состоянии основного оборудования во всех режимах работы, включая аварийные, использовалась информационно-вычислительная система СКАЛА, разработанная Всесоюзным научно-исследовательским институтом электромеханики на базе полупроводниковой управляющей вычислительной машины ВНИИЭМ-3М. Данные накапливались на магнитофонах, помещенных в закрытый металлический шкаф, находившийся в специальной комнате. После аварии помещение было разрушено и залито водой с очень высоким уровнем радиации. Магнитофонные ленты были сняты через 2 ч после аварии (ключи от шкафов найти не удалось, их пришлось взламывать). Несмотря на тяжелейшие условия запроектной аварии вся информация была сохранена и смогла быть использована для анализа её причин.

В проекте [17] соответствующие требования сформулированы так: «При внешних и внутренних воздействиях, возможных в условиях запроектных аварий, информационные системы контроля за радиационной обстановкой и система послеаварийного мониторинга должны выполнять те функции, которые могут быть востребованы при ликвидации последствий этих аварий, и сохранять данные о причине возникновения и пути протекания аварии».

Требования к аварийной готовности и реагированию. В числе долгосрочных мероприятий реагирования на события, произошедшие на АЭС Фукусима-1, предусмотрено усовершенствование систем аварийной готовности [1], составной частью которых могут стать системы контроля за радиационной обстановкой и послеаварийного мониторинга. Предложено дополнить [17] и [18] требованиями к таким системам.

Информационная система контроля за радиационной обстановкой должна осуществлять автоматизированный контроль за сбросами и выбросами радиоактивных веществ в окружающую среду в помещениях и на территории АЭС, в санитарно-защитной зоне и зоне наблюдения во всех эксплуатационных режимах, во время и после аварий, включая запроектные, а также при снятии с эксплуатации.

Информационная система послеаварийного мониторинга должна осуществлять поддержку персонала АЭС и экспертов по безопасности во время управления авариями, ликвидации их последствий и возвращения реакторной установки в контролируемое состояние, а также в процессе последующего анализа причин возникновения и путей протекания проектных и запроектных аварий. Система послеаварийного мониторинга должна обеспечивать получение, архивирование, хранение, отображение и регистрацию данных:

о характере и времени возникновения исходных событий, нарушений эксплуатационных пределов и условий, аварийных ситуаций и аварий;

о командах защитных действий, выданных системами безопасности, и действиях персонала, направленных на обеспечение безопасности;

о состоянии конструкций, систем и элементов, важных для безопасности, значениях технологических параметров и радиационной обстановке в процессе устранения нарушений или при возникновении аварийной ситуации, развитии аварии и в послеаварийный период.

Средства отображения информации, входящие в состав системы послеаварийного мониторинга, должны быть расположены в помещениях БЩУ и, в обоснованных случаях, РЩУ, а также в кризисных центрах.

Системы должны сохранять способность к выполнению предусмотренных функций при внешних и внутренних воздействиях, возможных в условиях нормальной эксплуатации, во время ожидаемых нарушений нормальной эксплуатации, в аварийных ситуациях и после любой проектной аварии. При внешних и внутренних воздействиях, возможных в условиях запроектных аварий, информационные системы контроля радиационной обстановки и система послеаварийного мониторинга должны выполнять те функции, которые могут быть востребованы при ликвидации последствий этих аварий, и сохранять данные о причине возникновения и пути протекания аварии. Архивные данные должны быть защищены от непреднамеренного или преднамеренного изменения в течение установленного срока.

Создание на каждой АЭС систем контроля за радиационной обстановкой и послеаварийного мониторинга, удовлетворяющих указанным требованиям, станет важным фактором усовершенствования всей системы аварийной готовности.

Совершенствование регулирования функциональной безопасности ИУС

Дальнейшее повышение функциональной безопасности ИУС остаётся среди приоритетных направлений деятельности органа государственного регулирования ядерной безопасности. К числу проблемных вопросов следует отнести продление срока эксплуатации информационных и управляющих систем и их компонентов, тиражирование пилотных модификаций и качество документов, обосновывающих безопасность.

Продление срока эксплуатации компонентов ИУС должно быть предметом постоянного внимания, поскольку большое число технических средств, важных для безопасности, эксплуатируется на энергоблоках АЭС Украины более 20 лет, а некоторые — ещё со времени пуска. Хотя в технической документации большинства компонентов регламентирована значительно меньшая долговечность (6–10, редко 15 лет), АЭС своими техническими решениями неоднократно продлевали срок эксплуатации этих изделий, несмотря на то что во многих случаях они не только морально, но и физически устарели. Не удивительно, что многие нарушения в работе АЭС были вызваны отказами компонентов ИУС, срок эксплуатации которых продлевался без достаточных оснований.

Действующие нормы и правила [26] устанавливают требования к порядку и содержанию работ, которые проводят с целью получения объективных данных о способности компонентов ИУС, важных для безопасности, выполнять свои функции с требуемой надежностью по истечении регламентированного для них срока эксплуатации. Выполнение таких работ, включающих обследование технического состояния и анализ эксплуатационной надежности, является необходимым условием для принятия решения о продлении регламентированного срока эксплуатации компонента.

Рассматривая вопрос о возможности продолжения эксплуатации энергоблоков после установленного срока, следует оценить обоснованность принятых АЭС технических решений по продлению срока эксплуатации компонентов ИУС на основании анализа результатов выполненных обследований их технического состояния и эксплуатационной надежности.

Необходимо пересмотреть документ [26], в котором кроме ранее предусмотренных работ нужно регламентировать также проверку соответствия изделий требованиям действующих норм, правил и стандартов по ядерной и радиационной безопасности и оценку влияния обнаруженных отклонений на безопасность энергоблока, включая оформление соответствующего отчёта.

Кроме того, целесообразно вернуться к практике, когда технические решения АЭС о продлении срока эксплуатации вместе с обосновывающими документами представлялись на согласование органу государственного регулирования ядерной безопасности (по крайней мере для компонентов управляющих систем безопасности и систем нормальной эксплуатации, участвующих в выполнении функций категории А, а также для изделий тех видов, отказы которых приводили к нарушениям в работе АЭС).

Особенности тиражирования «пилотных» модификаций. Практика использования норм и правил [27] показывает, что внедрение (тиражирование) «пилотных» модификаций ИУС и программно-технических комплексов (ПТК) нередко сопровождается:

изменением состава основных и/или дополнительных функций, требований к функционированию и основных характеристик;

изменением элементной базы, покупных комплектующих изделий и/или программного обеспечения, выбором других поставщиков продукции;

изменением интерфейса «человек — машина», которое обусловлено опытом эксплуатации «пилотной» модификации и/или требованиями заказчика;

изменением видов и количества входных-выходных сигналов и/или интерфейсов вследствие особенностей смежных систем и оборудования, с которыми должна взаимодействовать модифицированная ИУС (ПТК).

В то же время требуемый в [27] сравнительный анализ зачастую проводится поверхностно и не позволяет выявить возможные (необходимые) отличия при тиражировании «пилотной» модификации на данном энергоблоке. Обосновывающие документы не направляются для проведения экспертизы ядерной и радиационной безопасности, несмотря на наличие в них существенных отличий от документов «пилотной» модификации.

С целью сохранения функциональной безопасности при внедрении «пилотных» модификаций на других энергоблоках и повышения эффективности контроля рекомендуется при переработке норм и правил [27] отразить в них следующие положения, относящиеся к ИУС и ПТК:

«пилотной» модификацией следует считать первое применение ИУС или ПТК на энергоблоке с реактором определённого типа (ВВЭР-440, ВВЭР-1000) и реакторной установкой определённого проекта (В-213, В-302, В-338, В-320);

внедрением (тиражированием) «пилотной» модификации является повторение ИУС (ПТК), ранее внедрённой в эксплуатацию на энергоблоке с реактором *такого же типа* и реакторной установкой *того же проекта*, при условии идентичности выполняемых функций, основных параметров и характеристик, видов и количества входных и выходных сигналов и интерфейсов, элементной базы, покупных комплектующих изделий и программного обеспечения. Повторение ИУС (ПТК), ранее внедрённой на другом энергоблоке, не может считаться тиражированием «пилотной» модификации, если при этом требуется существенное изменение документации;

тиражирование «пилотной» модификации на других энергоблоках той же АЭС допускается при наличии технического решения, согласованного с Государственной инспекцией по ядерной безопасности на этой АЭС, тиражирование на других АЭС — только при наличии отраслевого технического решения эксплуатирующей организации, согласованного с Государственной инспекцией ядерного регулирования Украины (ГИЯРУ);

технические решения о тиражировании «пилотной» модификации должны направляться в ГИЯРУ для проведения государственной экспертизы и составления плана оценки безопасности;

результаты *каждой* модификации должны отображаться в отчете по анализу безопасности, который должен представляться в ГИЯРУ.

Качество обосновывающих документов. К документам, обосновывающим функциональную безопасность ИУС и их компонентов, относятся технические задания на разработку, отчеты по анализу безопасности, планы и отчеты по верификации и валидации, программы и методики испытаний и др.

Общие требования к документам, обосновывающим безопасность, содержатся в нормах и правилах [27] и отраслевом ГНД 306.7.02/2.041 [28], требования к отдельным документам — в [29], [30], [31], [32] и др. Многие из них устарели, противоречат друг другу и не соответствуют современным международным стандартам и действующим в Украине нормам и правилам. Отдельные документы ([30], [31]) в настоящее время перерабатываются.

Целесообразно предусмотреть разработку (взамен ГНД 306.7.02/2.041) норм и правил или отраслевого стандарта с общими требованиями к содержанию документов, обосновывающих функциональную безопасность ИУС и их компонентов, взаимно увязанными, согласованными с положениями [17], [18], [22], [27] и гармонизированными с требованиями действующих, новых и пересматриваемых международных стандартов [33], [34], [35], [36].

Выводы

Хотя авария на АЭС Фукусима-1 не имела непосредственной связи с работой информационных и управляющих систем, тем не менее она заставила ещё раз обратить внимание на необходимость дальнейшего повышения функциональной безопасности ИУС, которые создаются, модернизируются и эксплуатируются на энергоблоках АЭС Украины.

На основании анализа действующих норм, правил и стандартов по ядерной и радиационной безопасности, относящихся к ИУС и их компонентам, разработаны рекомендации по внесению в эти документы изменений и дополнений, направленных на повышение сейсмостойкости, надёжности идентификации опасных событий, стойкости к экстремальной температуре, защищённости от террористических угроз и др.

Кроме того, рассмотрены и обоснованы отличительные особенности проектов новых нормативных документов,

которые разрабатываются Государственной инспекцией ядерного регулирования Украины и Министерством энергетики и угольной промышленности Украины взамен НП 306.5.02/3.035–2000, в том числе касающиеся гармонизации с требованиями международных стандартов, охвата всех стадий жизненного цикла ИУС и их компонентов, установления требований к хранению данных, контролю за радиационной обстановкой и послеаварийному мониторингу.

Сформулированы проблемные вопросы, связанные с продлением срока эксплуатации, тиражированием пилотных модификаций, качеством документов, обосновывающих безопасность ИУС и их компонентов, и намечены возможные пути решения указанных проблем.

Список литературы

1. Постанова Колегії Держатомрегулювання № 2 від 19.05.2011 «Щодо плану дій з виконання цільової позачергової перевірки та подальшого підвищення безпеки АЕС України з урахуванням подій на Фукусіма-1 («stress-test»)».
2. *Гашев, М. Х.* Вопросы целевой переоценки безопасности действующих энергоблоков АЭС Украины в свете событий на АЭС Фукусима-1 в Японии / М. Х. Гашев, Г. В. Громов, А. М. Дыбач и др. // Ядерна та радіаційна безпека. — 2011. — № 3(51). — С. 3–8.
3. *Архангельський, К. Л.* Аналіз недоліків проекту АЕС «Fukushima Dai-Ichi» за наслідками важкої аварії в світлі подальшого посилення безпеки АЕС України / К. Л. Архангельський, С. Р. Михасюк // Ядерна та радіаційна безпека. — 2011. — № 3(51). — С. 9–14.
4. «Stress Tests» Specifications Proposal by the WENRA Task Force / 12 April 2011: http://www.wenra.org/dynamaster/file_archive/110421/0ea2c97b35d658d73d1013f765e0c87d/StressTestsSpecifications2011-04–21.pdf.
5. Nuclear Energy Agency. CNRA Forum on the Fukushima Accident: Insights and Approaches / OECD Conference Centre, 8 June 2011: http://www.oecd-nea.org/nsd/workshops/fukushima-forum.
6. Заявление Конференции МАГАТЭ по ядерной безопасности на уровне министров. Вена, 20 июня 2011 года / Информац. циркуляр IAEA INFCIRC/821: http://www.iaea.org/Publications/Documents/Infcircs/2011/Russian/infcirc821_rus.pdf
7. Новости ИТАР-ТАСС, 20 июня 2011. Гендиректор МАГАТЭ призвал принять меры по восстановлению доверия к атомной энергетике. http://www.atomic-energy.ru/news/2011/06/20/23605.
8. *Ястребенецкий, М. А.* Безопасность атомных станций: Системы управления и защиты ядерных реакторов / М. А. Ястребенецкий, Ю. В. Розен, С. В. Виноградская и др.; Под ред. М. А. Ястребенецкого. — К.: Основа-Принт, 2011. — 768 с.
9. *IEC 60980:1989.* Recommended Practice for Seismic Qualification of Electrical Equipment for Nuclear Power Generating Stations.
10. *ГОСТ 30546.1-98.* Общие требования к машинам, приборам и другим техническим изделиям и методы расчета их сложных конструкций в части сейсмостойкости.
11. *ГОСТ 30546.3-98.* Методы определения сейсмостойкости машин, приборов и других технических изделий, установленных на месте эксплуатации, при их аттестации и сертификации на сейсмическую безопасность.
12. *НП 306.5.02/3.035-2000.* Требования по ядерной и радиационной безопасности к информационным и управляющим системам, важным для безопасности атомных станций.
13. *НАПБ 03.005-2002 / ВБН В.1.1—034-03.307-2003.* Противопожарные нормы проектирования атомных электростанций с водо-водяными энергетическими реакторами.
14. *Бахмач, Е. С.* Обеспечение и оценка безопасности систем пожарной сигнализации и автоматического пожаротушения в помещениях АЭС / Е. С. Бахмач, М. И. Маршевский, Ю. В. Розен и др. // Ядерна та радіаційна безпека. — 2008. — № 1. — С.35—53.
15. *IEC 61226.* Nuclear power plants — Instrumentation and control systems important to safety — Classification. — 2005.
16. *ДСТУ IEC 61226:2007.* Атомні електростанції. Інформаційні та керуючі системи, важливі для безпеки. Класифікація контрольно-вимірювальних та керівних функцій (IEC 61226:2005, IDT).
17. Нормы и правила по ядерной и радиационной безопасности. Требования по ядерной и радиационной безопасности к информационным и управляющим системам, важным для безопасности атомных станций. — (Проект, редакция 2:2011).
18. Нормативний документ Міненерговугілля України. Інформаційні та керуючі системи, важливі для безпеки атомних станцій. Загальні технічні вимоги. — (Проект, редакция 2:2011).
19. *IEC 61513.* Nuclear power plants — instrumentation and control for systems important to safety — general requirements for systems. — 2001.
20. *ДСТУ IEC 61513:2009.* Атомні електростанції. Інформаційні та керуючі системи, важливі для безпеки. Загальні вимоги до систем (IEC 61513:2001, IDT).
21. *Ястребенецкий, М. А.* О классификации по безопасности информационных и управляющих систем и их компонентов / М. А. Ястребенецкий, Ю. В. Розен // Ядерная и радиационная безопасность. — 2004. — № 4. — С. 13–33.
22. *НП 306.2.141–2008.* Общие положения безопасности атомных станций.
23. *Розен, Ю. В.* Электромагнитная совместимость компонентов информационных и управляющих систем (1): правила нормирования и оценки помехоустойчивости / / Ядерная и радиационная безопасность. — 2007. — № 2. — С. 9–26.
24. *Розен, Ю. В.* Электромагнитная совместимость компонентов информационных и управляющих систем (2): Устойчивость к электромагнитным помехам / Ю. В. Розен // Ядерна та радіаційна безпека. — 2008. — № 4. — С. 58–76.
25. Сильные землетрясения могут быть во всей Украине // Газета «Сегодня», 23 марта 2011: http://www.segodnya.ua/news/14234522.html.
26. *НП 306.5.02/2.068-2003.* Требования к порядку и содержанию работ для продления срока эксплуатации информационных и управляющих систем, важных для безопасности атомных электростанций.
27. *НП 306.2.106-2005.* Вимоги до проведення модифікацій ядерних установок та порядку оцінки їх безпеки.
28. *ГНД 306.7.02/2.041–2000.* Методика оценки соответствия информационных и управляющих систем, важных для безопасности атомных станций, требованиям по ядерной и радиационной безопасности.
29. *ГНД 306.6.01/1.075-2003.* Інструкція про порядок розгляду та узгодження технічних умов на продукцію.
30. *КНД 306.302–96.* Безопасность АЭС. Требования к содержанию отчета по анализу безопасности АС с реакторами типа ВВЭР на стадии выдачи разрешения на ввод в эксплуатацию.
31. *НП 306.5.02/3.017–99.* Вимоги до програми забезпечення якості на всіх етапах життєвого циклу ядерних установок.
32. *ИН-Д.0.03.521–11.* Порядок оформления, согласования и утверждения технического задания на разработку и изготовление единичной/мелкосерийной продукции для АЭС.
33. Design of Instrumentation and Control Systems for Nuclear Power Plants. DS-431. Draft Safety Guide. Supersedes NS-G-1.1 and NS-G-1.3. — 03.08.2011.
34. *IEC 62566.* Nuclear Power Plants — Instrumentation and Control important to Safety — Development of HDL-programmed integrated circuits for systems performing category A functions. Draft 2011.
35. *IEC 61513.* Ed.2. Nuclear Power Plants. Instrumentation and Control Systems important to Safety — General requirements to Systems. Draft 2011.
36. *IEC 62465.* Nuclear Power Plants — Instrumentation and Control important to Safety — Requirements for security programmes for computer-based systems. Draft 2011.

Надійшла до редакції 25.08.2011.