УДК 685.1

Е.В. Брежнев

Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков

РИСК-АНАЛИЗ МНОЖЕСТВЕННЫХ ОТКАЗОВ В ИНФРАСТРУКТУРАХ

В статье показано, что проблема обеспечения безопасности критической инфраструктуры должна быть решена комплексно для всех ее уровней с использованием единого подхода. Проведена классификация множественных отказов в критических инфраструктурах. Приведены основные причины множественных отказов и факторы связности, обуславливающие уязвимость систем к одной причине. Предложены основные принципы риск-анализа множественных отказов.

Ключевые слова: *безопасность, множественные отказы, причина, связывающие факторы.*

Введение

Постановка проблемы и анализ литературы. Критическая инфраструктура (КИ) представляет собой совокупность взаимовлияющих социотехнических систем, функционирующих для обеспечения жизненно важных потребностей общества [1]. Энергосистема (S_0) является одной из приоритетных систем, определяющих развитие всей инфраструктуры в целом. Она включает взаимосвязанные технико-технологические подсистемы, процессы и персонал. Энергосистема характеризуется общностью режимов в непрерывном процессе производства, преобразования, передачи и распределения электрической и тепловой энергии при общем управлении этими режимами. К основным подсистемам S_0 относятся подсистема генерации, передачи и распределения, управления и прочие обеспечивающие подсистемы.

Атомные электростанции (АЭС) являются подсистемой S_0 с наибольшей тяжестью последствий аварий. Множественные отказы являются одними из основных риск-факторов, снижающих уровень безопасности АЭС. Анализ атомных аварий, произошедших за два последних десятилетия, показывает, что их причинами являются как множественные отказы оборудования и систем АЭС, так и аварии в других подсистемах S_0.

Множественные отказы обуславливают риски для систем нормальной эксплуатации АЭС и систем безопасности (СБ). Статистика отказов в СБ АЭС показывает, что на 3000 отказов различного оборудования приходится 450 (15 %) множественных отказов. Примером множественных отказов в СБ является авария на Чернобыльской АЭС, степень тяжести которой отнесена по международной шкале (International Nuclear Event Scale) к седьмому уровню. В процессе подготовки и проведения испытаний с нагрузкой собственных нужд блока, персонал отключил ряд технических средств защиты. В результате реактор был приведен в неустойчивое состояние, что привело к неуправляемому росту мощности реактора и взрыву, с последующим выбросом радиоактивных отходов.

Авария в марте 2011 года на АЭС Фукусияма-1 (оператор – японская компания TEPCO), подтвердила актуальность проблемы управления рисками множественных отказов для инфраструктурного уровня в целом, когда аварии одной инфраструктуры обуславливают аварии другой инфраструктуры. Авария энергосистемы, связанная с землетрясением и цунами, привела к потере внешнего энергоснабжения АЭС, что обусловило сбои в работе систем охлаждения реактора, расплавлению топлива, взрывам и загрязнению окружающей среды радиоактивными отходами. Авария энергосистемы нанесла колоссальный экономический ущерб всем инфраструктурам Японии, исчисляемый сотнями миллиардов долларов. Авария подтвердила, что уровень инфраструктурной безопасности определяется безопасностью ее систем, подсистем на всех инфраструктурных уровнях. Безопасность АЭС определяется не только функциональной безопасностью самой станции, ее систем (подсистем), но и уровнем безопасности всех связанных с АЭС подсистем энергосистемы.

Множественные отказы систем АЭС снижают эффективность одного из ее базовых принципов безопасности – принципа единичного отказа. На практике этот принцип реализуется путем резервирования, предполагая применение двух или более аналогичных систем или независимых каналов одной системы. Однако множественные отказы приводят к одновременным отказам нескольких систем, резервирующих друг друга.

Существует множество методов оценки риска, обусловленного множественными отказами. Для уровня подсистем используется группа параметрических методов и оценивается вероятность наступления отказов систем и оборудования АЭС [2, 3].

Другая часть методов [4] оценивает риски возникновения множественных отказов на инфраструктурном уровне, например, каскадных аварий энергосети.

Таким образом, множественные отказы возникают на всех инфраструктурных уровнях и характеризуются высокой тяжестью последствий. Существует множество различных методов, оценивающих риски множественных отказов на разных уровнях инфраструктуры. Проблема снижения риска множественных отказов является комплексной и должна решаться для всех уровней инфраструктуры. Для этого необходимо разработать общую методологию, как единую платформу для проведения риск-анализа. Одним из первоначальных этапов может являться уточнение таксономии множественных отказов, анализ причин и подходов к оценке рисков, разработка общих принципов анализа множественных отказов в инфраструктурах.

Цель статьи – разработка принципов общего подхода к риск-анализу множественных отказов критической инфраструктуры, классификация множественных зависимых отказов и факторов, обуславливающих их возникновение.

Основной материал

При проведении анализа множественных отказов необходимо рассматривать инфраструктуру как комплексную адаптивную систему, характеризующуюся эмерджентным поведением.

В основу риск-анализа множественных отказов в инфраструктурах могут быть положены следующие принципы:

– принцип системности. Принцип предполагает рассмотрение инфраструктуры как единой системы;

– принцип иерархии. Инфраструктура является иерархичной системой. Множественные отказы возникают на всех уровнях инфраструктуры. Анализ множественных отказов на одном уровне должен учитывать результаты анализа другого (нижнего уровня). Риск-анализ может проводиться как сверху вниз, исследуя возможности возникновения множественных отказов на инфраструктурном уровне и их последствия для всех нижних уровней, так и наоборот;

– принцип неопределенности. Анализ множественных отказов должен учитывать неопределенность, связанную с недостаточностью статистической базы отказов и с неточностью и неполнотой знаний о поведении критической инфраструктуры. Неопределенность обусловлена неполнотой знаний о природе рисков, которые могут привести к возникновению инфраструктурных аварий и катастроф.

В соответствии с принципом иерархии инфраструктура представляется в виде нескольких уровней. Анализ множественных отказов должен проводиться для каждого уровня инфраструктуры. Результаты анализа используются для разработки стратегий управления отказами инфраструктуры в целом (infrastructure fault management). При анализе безопасности инфраструктуры необходимо учитывать, что множественные отказы систем одного уровня приводят к появлению отказов систем всех взаимосвязанных уровней.

Число уровней инфраструктуры определяется степенью необходимой детализации и решаемой задачей. Так, например, к основным уровням инфраструктуры можно отнести:

– уровень инфраструктур (первый уровень). Этот уровень включает различные инфраструктуры: энергосистему (S_1), телекоммуникации (S_2), системы водоснабжения (S_3) и другие;

– уровень инфраструктурных систем (второй уровень). Так, например, для энергосистемы подсистемами являются генерирующие станции (АЭС, ГРЭС, ТЭЦ), подсистемы распределения и передачи и другие;

– уровень инфраструктурных подсистем (третий уровень). На этом уровне выделяются, например, для АЭС системы нормальной эксплуатации, системы безопасности, управления и т.д.

Общий вид критической инфраструктуры может иметь вид, представленный на рис. 1.

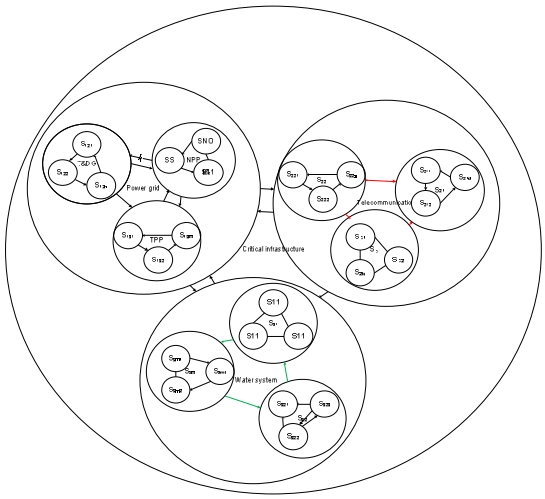

Рис. 1. Иерархическое представление инфраструктуры

Формально любая инфраструктура представляет собой взаимосвязанное множество узлов (nodes). Узлы каждого уровня иерархии взаимосвязаны между собой множеством связей. Каждый узел в свою очередь является сложной системой, включающей множество узлов следующего уровня и связей между ними.

Удобной моделью представления инфраструктуры является граф вида:

$$G = (X, V), \quad (1)$$

где X – множество узлов;

V – множество связей между узлами.

В свою очередь, каждый i-й узел j-го уровня иерархии инфраструктуры также может быть представлен в виде графа вида:

$$G_{ij} = \{(X_{ijs})_{IJS}, (V_{kij})_{KIJ}\}, \quad (2)$$

где $(X_{ijs})_{IJS}$ – s-я подсистема i-й системы (узла) j-го уровня иерархии, $i = \overline{1,I}$, $j = \overline{1,J}$, $s = \overline{1,S}$;

$(V_{kij})_{KIJ}$ – k-е ребро i-й системы j-го уровня иерархии $k = \overline{1,K}$.

Каждая вершина инфраструктуры может находиться в одном из множества состояний, например, *работоспособном, неработоспособном и частично работоспособном.* Поведение инфраструктуры описывается динамикой изменений этих состояний. Состояния систем одного уровня обуславливают изменение состояний систем другого уровня иерархии.

На инфраструктурном уровне возникают *множественные аварии*. Под множественными авариями будем понимать одновременное наступление аварий (или аварийных режимов работы) двух и более инфраструктур.

При множественных инфраструктурных авариях часть инфраструктур переходит в неработоспособное состояние. При этом часть подсистем второго и третьего уровней иерархии может находиться в работоспособном состоянии. При переходе в неработоспособное состояние происходит изменение связей между системами. Они могут нарушаться, изменяться, вызывая тем самым изменения состояния зависимых систем.

Предлагается рассматривать следующие виды множественных аварий: каскадные аварии, аварии по общей причине и усугубляющие аварии. Причинами множественных аварий являются сбои, отказы в работе систем второго и третьего уровней иерархии, действия человека, воздействия внешней среды и т.д. Для снижения последствий отказов для инфраструктурного уровня применяется множество стратегий. Если эти стратегии не эффективны, то множественные отказы систем “нижних” уровней приводят к сбоям и отказам, авариям в инфраструктурах.

Под *каскадными авариями* понимается последовательность нескольких аварий в инфраструктурах, когда авария инфраструктуры S_1 приводит к аварии инфраструктуры S_2. Данный вид аварий характерен для энергосистем. Характеризуется большими экономическими убытками, географическим размахом. Аварии, сбои в работе энергосистемы приводят к авариям и сбоям в работе АЭС. Примером подобной каскадной аварии является blackout 2003 [4].

Последствиями аварии в энергосистемы явилась остановка 17 реакторов в США и Канаде.

На рис. 2 приведен пример инфраструктурной каскадной аварии.

Так, например, авария в одной из подсистем S_1 энергосистемы приводит к потере внешнего энергоснабжения АЭС (S_2), что в свою очередь приводит к отказам систем S_{21}, S_{22}. Отказы S_{21}, S_{22} приводят к аварии на АЭС.

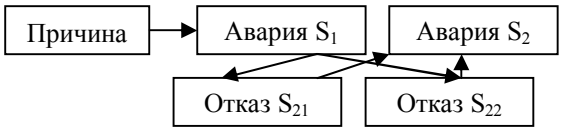

Рис. 2. Инфраструктурная каскадная авария

Под аварией по общей причине понимается одновременное возникновение аварий в двух или более инфраструктурах по одной причине. Примером такой инфраструктурной аварии являются недавние события в Японии.

К основным причинам аварий по общей причине относят:

– неадекватность дизайна, проектирования и производства подсистем S_0, например, ошибки в проектировании АЭС;

– ошибки оператора, сознательные действия человека (террористические и кибер атаки);

– влияние окружающей среды (ураганы, наводнения, землетрясения, цунами и пр.)

На рис. 3 приведен пример инфраструктурной аварии по общей причине.

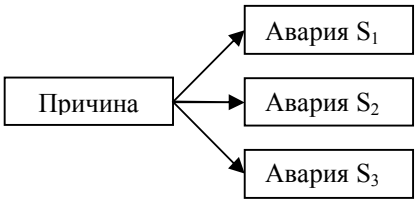

Рис. 3. Инфраструктурная авария по общей причине

Существует ряд подходов, который эффективно используется для обеспечения безопасности систем второго и третьего уровней инфраструктуры. К ним относят разделение, резервирование, диверсность.

Часть этих подходов применяется на инфраструктурном уровне. Например, в энергосистемах мощности резервируются для поддержания баланса между энергопотреблением и производством. Выбор места для размещения, например, АЭС может рассматриваться как пример физического разделения инфраструктур.

Диверсность не применяется на инфраструктурном уровне. Однако, очевидно, при использовании такого подхода в Японии можно было бы избежать подобных последствий от потери внешнего энергоснабжения АЭС. Так, в случае с Фукусиямой-1 диверсность внешнего энергоснабжения могла быть представлена в виде использования альтернативных экологически чистых источников энергии (ветряки, солнечная энергия и т.д.).

Аварии (отказы) по общей причине возникают по причине общей уязвимости группы инфраструктур (подсистем) к одной причине. Эта уязвимость

обуславливается действием фактором связности. Эти факторы влияют на инфраструктуру на протяжении всего ее жизненного цикла.

К основным факторам связности можно отнести:

– факторы единого дизайна (разработки). На этапе разработки формируется множество общих особенностей, которые характеризуют инфраструктуру на всех ее уровнях;

– факторы общего качества (производства). Производитель использует единые производственные процедуры, материалы, в том числе и для контроля качества производимой продукции;

– факторы единой системы обслуживания. Единый график обслуживания, тестирования и калибровки, единые процедуры тестирования, единый персонал обуславливают общую уязвимость и приводят к появлению множественных отказов;

– факторы общих условий эксплуатации. Идентичные (функционально и физически) компоненты управляются одной и той же эксплуатационной процедурой. В этой связи ошибки в процедуре могут привести к одновременному отказу подсистем;

– факторы общей эксплуатационной процедуры. Группа компонентов может находиться под влиянием идентичных стресс-факторов окружающей среды, таких как наводнение, пожар, землетрясение, повышенная влажность, температурные флуктуации.

Полностью действия этих факторов избежать нельзя, поскольку они являются неотъемлемой частью эволюционного развития сложных систем.

Поэтому единственным подходом может стать недопущение их чрезмерного влияния на инфраструктуру.

Риск множественных аварий (отказов) всегда присутствует, поэтому необходимо разработать стратегию их парирования и обеспечить инфраструктуру необходимым объемом ресурсов, которые будут использованы для реализации одной из возможных стратегий.

Выводы

Множественные отказы возникают на всех уровнях критической инфраструктуры. Последствия множественных отказов одного уровня могут распространяться на другие уровни иерархии. Множественные отказы нижних уровней иерархии могут обуславливать сбои в работе систем нормальной эксплуатации и систем безопасности, приводя к авариям на инфраструктурном уровне. Риск-анализ множественных отказов необходимо проводить для всех уровней инфраструктуры. Результаты анализа нижних уровней должны учитываться при анализе верхних уровней. Для анализа должна быть использована единая методология, с использованием унифицированных подходов.

Диверсность должна рассматриваться как средство повышения устойчивости к отказам по общей причине не только для уровня подсистем и элементов, но и всей инфраструктуры в целом. Для предотвращения аварий на АЭС, связанных с потерей внешнего энергоснабжения, может быть использована диверсность внешних источников.

Список литературы

1. Rinaldi J. Peerenboom Identifying, Understanding, and Analyzing Critical Infrastructure Dependencies / Rinaldi, J. Peerenboom // IEEE Control Systems Magazine. – Dec. 2001. – Vol. 21. – P. 11-25.

2. Procedure Guidelines in Modeling Common Cause Failures in Probabilistic risk assessment (NUREG/CR-5485) / A. Mosleh et. al., 1998. – 123 p.

3. Probabilistic Risk Assessment Procedure Guide for NASA / M. Stamatelatos et. al. – 2002. – 56 p.

4. U.S. – Canada power system outage task force. Final report on the august 14, 2003 blackout in the US and Canada: Causes and recommendation. Электронный ресурс. – Режим доступа к ресурсу: www. nerc.com.

Поступила в редколлегию 10.05.2011

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

РИЗИК АНАЛІЗ МНОЖИННИХ ВІДМОВ В ІНФРАСТРУКТУРАХ

Є.В. Брежнєв

В статті показано, що проблема забезпечення безпеки критичної інфраструктури повинна бути вирішена комплексно для усіх її рівнів, з використанням єдиного підходу. Проведено класифікацію множинних відмов в критичних інфраструктурах. Приведено основні причини множинних відмов та фактори зв'язності, які обумовлюють вразливість систем до одної причини. Запропоновані принципи ризик-аналізу множинних відмов в інфраструктурах.

Ключові слова: *безпека, множинні відмови, причина, зв'язуючи фактори.*

THE RISK ANALYSIS OF MULTIPLE FAILURES IN INFRASTRUCTURES

E.V. Bregznev

The problem of critical infrastructure safety assurance should be treated as the complex problem taking into account the safety of all its levels, based on the integrated approach. The multiple failures classification in critical infrastructure is suggested in the paper. The root causes of multiple failures and coupling factors which stipulate the infrastructure vulnerability to common cause are considered. The principles of infrastructure multiple failures' risk analysis are suggested.

Keywords: *safety, multiple failures, root cause, coupling factors.*