

УДК 621.039.58

## МЕТОД ОПИСАНИЯ СЦЕНАРИЕВ КАСКАДНЫХ И МЕЖСИСТЕМНЫХ АВАРИЙ С УЧЕТОМ ВЕРОЯТНОСТНЫХ ФАКТОРОВ

Кандидат физ.-мат. наук *В.А. Пантелеев*

Институт проблем безопасного развития атомной энергетики РАН, Москва, Россия

Кандидат физ.-мат. наук *И.А. Кириллов*

ООО «Кинтех Лаб», Москва, Россия

*Каскадное распространение структурных разрушений и функциональных отказов является одним из наиболее опасных видов стихийных бедствий или техногенных аварий. Предложен подход к описанию сценариев каскадных и межсистемных аварий для их системной идентификации, классификации и использования при подготовке стратегий управления рисками и стойкостью критической инфраструктуры с стохастической природы зависимостей между активами, приводящими к каскадным авариям.*

**Ключевые слова:** авария, природная катастрофа, техногенная тяжелая авария, сценарий, каскад, «эффект домино», контрмеры, аварийное реагирование, вероятностный анализ безопасности.

## METHOD FOR DESCRIBING SCENARIOS OF CASCADE AND INTERSYSTEM ACCIDENTS WITH TAKING INTO ACCOUNT PROBABILISTIC FACTORS

Ph.D. (Phys.-Mat.) *V.A. Panteleev*

Nuclear Safety Institute of the Russian Academy of Science

Ph.D. (Phys.-Mat.) *I. Kirillov*

Kintech Lab Ltd., Moscow, Russia

*Cascade propagation of the structural or functional failures is one of the most dangerous types of natural disasters or technogenic severe accidents. A framework for systemic description of the cascade and intersystem accident scenarios for identification, classification and use during strategy development for risk and resilience management taking into account the stochastic nature of the dependencies between assets leading to cascade accidents.*

**Keywords:** accident, natural disaster, technogenic severe accident, scenario, cascade, “domino effect, likelihood, resilience, emergency response, probability safety analysis.

### Введение

Известно, что наиболее тяжелые по последствиям техногенные аварии, как правило, происходят по каскадным сценариям, когда опасное природное явление, авария и/или отказ одного элемента приводит к отказам и/или авариям других элементов системы [1-4].

Природные стихийные бедствия во многих случаях так же сопровождаются каскадным развитием техногенных аварий. Одним из ярких примеров такого каскадного развития событий явилось сильное землетрясение 2011 года в Японии, вызвавшее волну цуна-

ми, которая явилась основной причиной крупной аварии с выходом радиоактивных веществ в окружающую среду на АЭС «Фукусима-1» [5]. Подобные аварии в различных литературных источниках и различных отраслях называются каскадными авариями, авариями с эскалацией масштабов последствий или «эффектом домино».

Аварии данного типа характерны для различных отраслей человеческой деятельности, как в современном мире, так и в историческом прошлом [6]. Каскадная авария, как стихийное бедствие, так и тяжелая техногенная авария, это наиболее сложный вариант развития событий с точки зрения оценки безопасности систем, аварийного планирования и реагирования. Поэтому интерес к проблемам «эффекта домино», «каскада» и т. д. постоянно растет в научной литературе и нормативных документах.

В настоящее время при оценке безопасности опасных производственных объектов в мировой практике и России на нормативном уровне требуется проведение анализа каскадного развития аварий [7-11]. При этом необходимо отметить, что в перечисленных документах и методиках, в основном, декларируется необходимость рассматривать, в общем очевидные, взаимосвязи между блоками объекта связанные с воздействием поражающих факторов на аварийном блоке на соседние объекты, содержащие опасные вещества.

В то же время как показывает опыт, при развитии каскадных аварий затрагивают самые различные элементы инфраструктуры, относящиеся к различным подсистемам. Так при землетрясении и последующего цунами в Японии в 2011 г., воздействие цунами явилось пусковым механизмом для нарушений в работе телекоммуникационных сетей, разрушения объектов транспортной инфраструктуры (аэропорты, железнодорожный транспорт, автомобильные эстакады), разрушения гидротехнических сооружений, аварии на сетях водо- и электроснабжения и, в конце концов, авария на АЭС «Фукусима». Похожий спектр аварийных межсистемных последствий, развивающихся по каскадному механизму, был характерен для крупнейшей аварии на гидротехнических сооружениях произошедшей в Китае в 1975 г. (Дамба Банцяо (Banqiao dam)) [12] при которой: по официальным данным, учитывающим только погибших непосредственно во время затопления составило — более 25 000 жертв. С учетом погибших из-за голода и эпидемий, вызванных наводнением — более 170 000 жертв.

В связи с этим актуальным является разработка методов описания сценариев каскадных и межсистемных аварий. Метод описания должны быть пригодны к использованию для анализа сценариев межсистемных аварий, для оценки живучести элементов сетей (компьютерных, жизнеобеспечения, логистических, систем управления и т.д.) и их интерфейсов, и для риск-информированного анализа критически важных элементов, где могут зародиться или усиливаться внутрисетевые каскады отказов/разрушений или происходить межсетевая эскалация аварии, приводящая к глобальному коллапсу системы-систем.

На предшествующей стадии исследования были предложен концептуальный подход описания сценариев каскадных и межсистемных аварий для их системной идентификации, классификации и использования при подготовке стратегий управления рисками и стойкостью критической инфраструктуры в детерминистском приближении. Разработанная схема основана на представлении о катастрофе как распространении волны повреждений /отказов/ дисфункций в пространственно-временном континууме через доступные связи (зависимости и/или взаимозависимости) между активами. Предложен минимальный набор понятий для описания феноменологии каскадной аварии, определен перечень различных видов зависимостей и взаимозависимостей между активами, определены способы взаимодействия активов с точки зрения каскадного развития аварии. Показана применимость метода для древовидных типов каскадов - линейных и ветвящихся, а так же что отличные от физической взаимозависимости могут привести к неприемлемой эскалации аварии, когда синергия сурового климата с опасными техногенными отказами мо-

жет угрожать выживанию актива. Разработанный метод был разработан в детерминистском приближении [6].

Целью настоящей статьи является развитие метода с учетом вероятностных аспектов развития каскадных аварий.

### Термины и определения

Среди понятий, необходимых для описания сценариев каскадных аварий, следует выделить следующие:

**Система** - комбинация взаимодействующих элементов, организованных для достижения поставленных целей;

**Актив** – узел техногенной системы, элемент природной среды, процедура подсистемы управления, которые контролируются администрацией системы жизнеобеспечения (СЖО) в результате прошлых событий и от которых ожидается надежное функционирование для достижения целей СЖО, экономической выгоды и безопасности в будущем;

**Опасность** – возможность возникновения обстоятельств (сочетания событий и методов), при которых существование или отсутствие неконтролируемых физических (энергии, массы) или логических (информации, административных процедур) потоков или их сочетание могут таким образом повлиять на сложную систему, что приведет к ухудшению или невозможности её функционирования и развития;

**Зависимость активов** – состояние двух активов системы, в котором один из активов использует результаты или информация о функционирования другого.

### Материальные и нематериальные агенты каскадного развития аварий

Возможны различные виды связей - зависимости (dependency) и взаимозависимости (interdependency) - между активами внутри и между системами, которые должны быть учтены при анализе сценариев каскадной аварии. Обычно выделяют следующие типы взаимосвязей [13]: - физическая; - логическая; - кибернетическая; - географическая.

Такая классификация связей и взаимосвязей позволяет описать каскадное развитие аварий в детерминистской постановке [6]. Для описания каскадного развития аварий с учетом вероятностных факторов предложенный метод нуждается в развитии.

При каскадном развитии аварий целесообразно выделить связи материальных и нематериальных агентов развития аварии. К материальным агентам относятся:

- **Опасные воздействия** - физические воздействия одних активов на другие, которые при достижении определенных величин приводят к отказу активов подвергшихся взаимодействию. Примерами таких зависимостей могут быть опасные факторы промышленных аварий (тепловые потоки от пожаров, ударные волны от взрывов, разлетающиеся осколки оборудования, волны прорыва гидротехнических сооружений, цунами и т.д.)

- **Материальные потоки** - физические агенты воздействия связанные с потоками вещества или энергии изменение которых за определенные пределы приводит в сочетании с определенной длительностью приводит к развитию аварийного каскада. Примерами таких связей могут быть потоки сырья, электроэнергии, потоки в системах жизнеобеспечения, противоаварийные силы и средства и т.д. Здесь необходимо подчеркнуть, что ключевым параметром в этом виде связей является продолжительность прекращения потока (частичного или полного) приводящее к исчерпанию резервов зависимой системы. В случае если продолжительность отказа связи меньше времени исчерпания резервов зависимого актива то, как правило, каскадного развития аварии не происходит. Однако

при превышении времени исчерпания резервов происходит резкое изменение состояния зависимого актива и вероятно каскадное развитие аварии с качественным изменением состояния зависимого актива и каскадным развитием масштаба аварии.

К **нематериальным связям** относятся связи в системах управления в широком смысле этого слова, как при заблаговременном, так и оперативном принятии и передаче управляющих решений. Характерны следующие отклонения приводящие к каскадному развитию аварий:

- недоучет возможного масштаба реализации материальных агентов развития аварий за счет необоснованного исключения из рассмотрения ряда реалистичных сценариев на заблаговременном и оперативных стадиях управления (например - интенсивность и продолжительность осадков, высота волн цунами, магнитуда землетрясения, продолжительность перебоев в «материальных потоках», недоучет зависимости и взаимозависимости активов системы в целом и т.д.);

- получение недостоверной, неполучение, несвоевременное получение информации необходимой для принятия решений;

- принятие ошибочных решений;

- задержка в принятии решений;

- недоведение, искажение, задержка в получении управляющих решений до противоаварийных сил и средств;

Здесь необходимо отметить что в ряде реальных случаев возможна комбинация отклонений в системе управления приводящая к каскадному развитию аварий с многократным увеличением последствий. Так например при катастрофе с прорывом дамбы Баньцяо в 1975 году:

- при проектировании из соображений экономии было уменьшено количество водосбросов более чем в два раза;

- метеослужбы не смогли предсказать масштабы осадков и наводнений от супертайфуна Нина для подготовки населения, сил и средств к возможным последствиям;

- высшее руководство на стадии развития угрожающей ситуации на дамбе не разрешило начать водосброс в связи подтоплением территорий ниже дамбы;

- через некоторое время разрешение было дано, но оно не было своевременно получено из-за отказа связи;

- решение об открытии водосбросных сооружений было принято с задержкой после образования трещины на дамбе – к этому моменту водоспуски уже были забиты илом и не могли выполнять своих функций.

- организация эвакуации населения была затруднена неработоспособностью коммуникаций, что значительно увеличило масштаб прямых потерь от волны прорыва. В населенных пунктах, где приказы об эвакуации дошли своевременно потери были относительно низкие.

В качестве примера важности для эффективности контрмер своевременность их проведения можно привести оценки относительной эффективности контрмеры «укрытие на 48 ч» проведенные с использованием методологии ВАБ-3 в работе на примере модельной аварии с выбросом радиоактивных веществ в атмосферу [13] (см. рис. 1). Относительная эффективность резко уменьшается при задержке реализации контрмеры Ч+ от 0 до 4 ч (в 2 раза). В интервале Ч+ от 4 до 24 ч относительная эффективность уменьшается до 0,2. После задержки более чем на 24 ч эффективность укрытия медленно спадает. При укрытии на 48 ч на 8-е сут, относительная эффективность контрмеры достигает ~ 0,15 эффективности укрытия до подхода облака радиоактивных веществ.

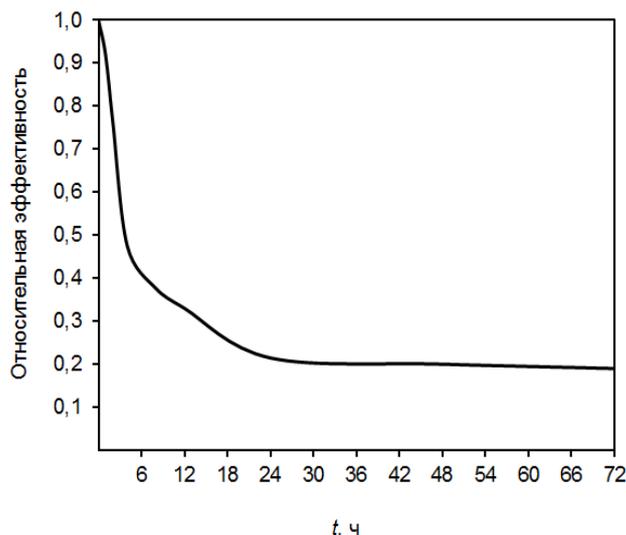


Рис. 1. Относительная эффективность контрмеры «укрытие на 48 ч» в зависимости от времени реализации по математическому ожиданию коллективной дозы

### Вероятностные метрики зависимостей и взаимозависимостей

Из предложенной выше классификации типов связей можно сделать следующие выводы:

- физические и географические воздействия относятся к материальным агентам и могут быть отнесены как к опасным воздействиям, так и материальным потокам;
- логические и кибернетические связи для каскадных аварий (кроме самих ИТ систем) относятся к нематериальным агентам развития каскада.

Для оценки вероятностных характеристик каскада предлагается каждому виду связей поставить в соответствие следующие вероятностные характеристики:

- для материальных агентов типа «Опасное воздействие»  $P_0$  – вероятность развития каскада за счет вовлечения зависимого актива из-за превышении интенсивности опасных воздействий;
- для материальных агентов типа «Материальные потоки»  $P_p$  – вероятность развития каскада за счет исчерпания внутренних резервов стойкости зависимого актива;
- для нематериальных агентов  $P_n$  – вероятность несрабатывания логической или кибернетической связи в связи с нарушением в ИТ системах, ошибками лиц принимающих решения, задержкой в принятии решений и т.д.

В начальном приближении величины  $P_0$ ,  $P_p$  и  $P_n$  могут быть представлены в точечном приближении как отдельные фиксированные значения. На последующих этапах указанные величины сами в свою очередь могут быть рассмотрены как случайные величины характеризующиеся функциями распределения.

### Схемы каскадных аварий в детерминистской и вероятностной постановке

Активы системы, с точки зрения развития каскадной аварии в детерминистской постановке могут взаимодействовать четырьмя различными способами, характеризующими результат взаимодействия и существенных для генерации сценариев каскадной аварии [6]:

- 1 - «развитие каскада» - взаимодействие актива-инициатора на  $i$ -й стадии развития каскада приводит к выходу из строя другого актива на  $i+1$ -й стадии развития аварии. Каскад развивается;

2 - «не срабатывание защиты» - взаимодействие актива-инициатора на  $i$ -й стадии развития каскада приводит к выходу из строя другого актива на  $i+1$ -й стадии развития аварии за счет неэффективности системы защиты. Каскад развивается;

3 - «срабатывание защиты» - взаимодействие актива-инициатора на  $i$ -й стадии развития каскада не приводит к выходу из строя другого актива за счет эффективного срабатывания системы защиты. Каскадная цепь прерывается;

4 - «нет взаимодействия» - взаимодействие между активами отсутствует. Развитие аварийной цепи не происходит.

На рис. 2. приведен пример ветвящегося межсистемного каскада в детерминистской постановке.

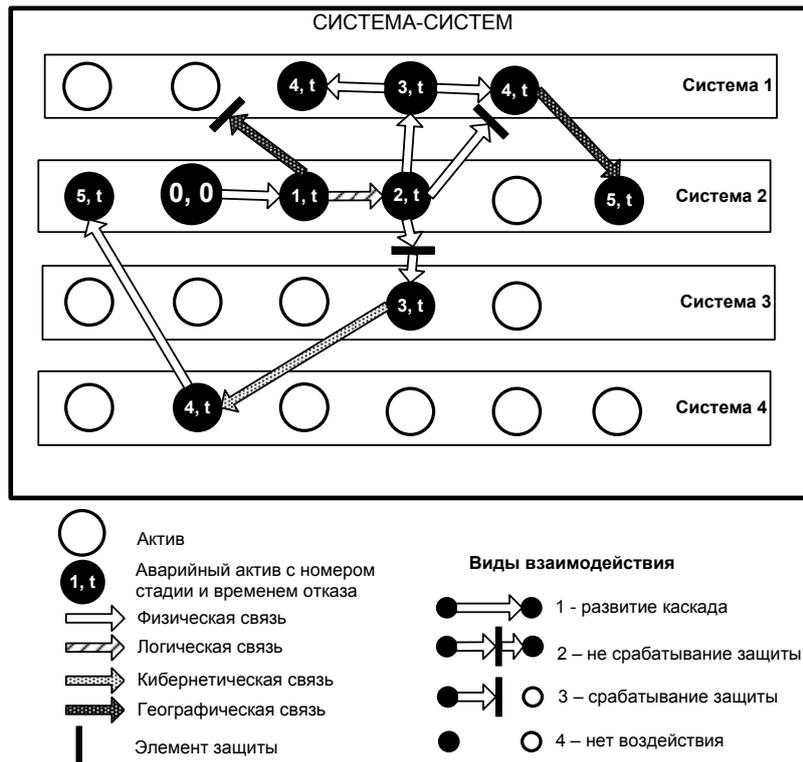


Рис. 2. Пример схемы ветвящегося межсистемного каскада в детерминистской постановке

В вероятностной постановке целесообразно рассматривать следующие виды взаимодействия при развитии каскадной аварии:

1 - «развитие каскада» за счет физической связи по механизму «Опасное воздействие» - взаимодействие актива-инициатора на  $i$ -й стадии развития каскада приводит к выходу из строя другого актива на  $i+1$ -й стадии развития аварии с вероятностью  $P_0$  каскад развивается;

2 - «развитие каскада» за счет географической связи по механизму «Опасное воздействие» - взаимодействие актива-инициатора на  $i$ -й стадии развития каскада приводит к выходу из строя другого актива на  $i+1$ -й стадии развития аварии с вероятностью  $P_0$  каскад развивается;

3 - «развитие каскада» за счет физической связи по механизму «Материальный поток» - взаимодействие актива-инициатора на  $i$ -й стадии развития каскада приводит к выходу из строя другого актива на  $i+1$ -й стадии развития аварии с вероятностью  $P_0$  каскад развивается;

4 – «развитие каскада» за счет географической связи по механизму «Материальный поток» – взаимодействие актива-инициатора на  $i$ -й стадии развития каскада приводит к выходу из строя другого актива на  $i+1$ -й стадии развития аварии с вероятностью  $P_o$  каскад развивается;

5 – «развитие каскада» за счет логической связи по механизму «Нематериальная связь» – взаимодействие актива-инициатора на  $i$ -й стадии развития каскада приводит к выходу из строя другого актива на  $i+1$ -й стадии развития аварии с вероятностью  $P_n$  каскад развивается;

6 – «развитие каскада» за счет кибернетической связи по механизму «Нематериальная связь» – взаимодействие актива-инициатора на  $i$ -й стадии развития каскада приводит к выходу из строя другого актива на  $i+1$ -й стадии развития аварии с вероятностью  $P_n$  каскад развивается;

7 – «нет взаимодействия» - взаимодействие между активами отсутствует. Развитие аварийной цепи не происходит.

На рис. 3. приведен пример ветвящегося межсистемного каскада в детерминистской постановке.

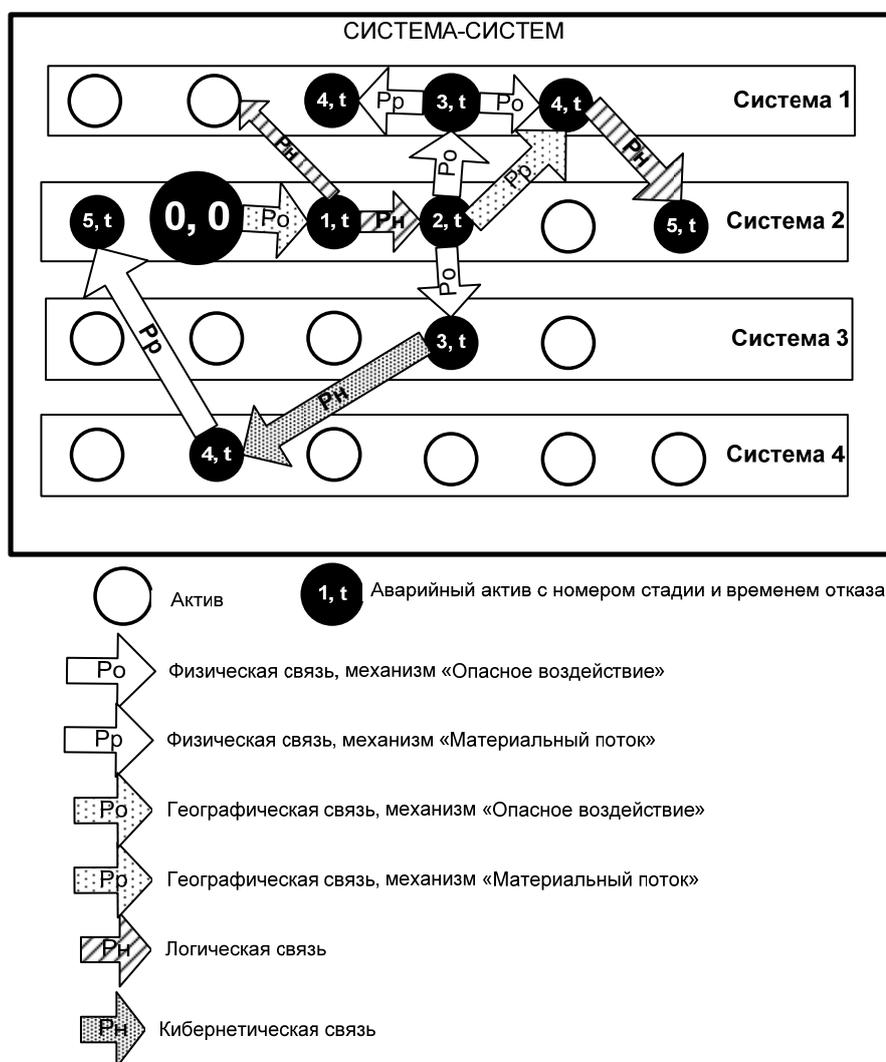


Рис. 3. Пример схемы ветвящегося межсистемного каскада в вероятностной постановке

Таким образом, предложенный концептуальный подход к описанию и классификации каскадных и межсистемных аварий, учитывает наиболее существенные факторы развития каскадов, включая вероятности развития аварийный каскадов. Метод может быть использован для классификации сценариев системных и межсистемных аварий, для оценки живучести сетей, отдельных элементов сетей и их интерфейсов, и для риск-информированного анализа критически важных элементов, где могут зародиться или усиливаться внутрисетевые каскады отказов/разрушений или происходить межсетевая эскалация аварии, приводящая к глобальному коллапсу системы-систем. Количественные оценки вероятности реализации каскадных связей между отдельными активами и вероятностные характеристики развития системных каскадов целом могут быть получены с использованием известных методов [14, 15].

### Благодарность

Авторы благодарны Российскому Фонду Фундаментальных Исследований за финансовую поддержку проекта 17-07-01475 «Стойкость региона к каскадному распространению системных аварий по взаимозависимым сетям жизнеобеспечения», в рамках которого выполнена данная работа.

### Литература

1. Pietersen C.M. "Analysis of the LPG disaster in Mexico City". Loss Prevention Bulletin №64, IChemE, Rugby, Aug 1985.
2. Liquefied Naturalgas: An Overview of the LNG Industry for Fire Marshals and Emergency Responders. National Association of State Fire Marshals. - 2005, 23 p.
3. 9 самых масштабных аварий электросетей. <http://energосmi.ru/archives/16287>.
4. V. Panteleev. Quantitative Risk Assessment of Aircraft Impact on a High-Rise Building and Collapse in Resilience of Cities to Terrorist and other Threats/ Learning from 9/11 and further Research Issues, Proceedings of the NATO Advanced Research Workshop on Urban Structures Resilience under Multi-Hazard Threats: Lessons of 9/11 and Research Issues for Future Work, Moscow, Russia, 16-18 July, 2007, Series: NATO Science for Peace and Security Series, Subseries: NATO Science for Peace and Security Series C: Environmental Security, Pasman, Hans; Kirillov, Igor A. (Eds.). - 2008, XIII, 545 p.
5. Системный анализ причин и последствий аварии на АЭС «Фукусима-1» / Арутюнян Р. В., Большов Л. А., Боровой А. А., Велихов Е.П.; Ин-т проблем безопасного развития атомной энергетики РАН. — М. - 2018. — 408 с.: ил. — ISBN 978-5-9907220-5-7 (в пер.).
6. Пантелеев В.А., Кириллов И.А., Берберова М.А., Клименко С.В. Метод описания сценариев каскадных и межсистемных аварий, Ситуационные центры и информационно-аналитические системы класса 4I для задач мониторинга и безопасности (SCVRT2017), Труды Международной научной конференции., стр. 239 - 244, Москва-Протвино, 28-30 ноября 2017. Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances. (Seveso II Directive))
7. Руководство по безопасности "Методика оценки риска аварий на опасных производственных объектах нефтегазоперерабатывающей, нефте- и газохимической промышленности" (утв. приказом Федеральной службы по экологическому, технологическому и атомному надзору от 29 июня 2016 г. № 272
8. Руководство по безопасности «Методические основы по проведению анализа опасностей и оценке риска аварий на опасных производственных объектах, Утверждено приказом Федераль-

ной службы по экологическому, технологическому и атомному надзору от 11 апреля 2016 г. № 144, ОПВБ – 2013.

9. СТО Газпром 2-2.3-569-2011. Методическое руководство по расчету и анализу рисков при эксплуатации объектов производства, хранения и морской транспортировке сжиженного и сжатого природного газа. - 2011, 111 с.

10. СТО Газпром 2-1.1-356-2009. Методические указания по повышению устойчивости технологического оборудования производственных объектов предприятий ОАО «Газпром» к воздействию пожаров и взрывов и предотвращению каскадных эффектов. - 2009, 90 с.

11. Chapter 3 The World's Most Catastrophic Dam Failures: The August 1975 Collapse of the Banqiao and Shimantan Dams, by Yi Si in “The river dragon had come: The Three Gorges Dam and the Fate of China's Yangtze River and Its People». Dai Qing. edited by John G. Thibodeau and Philip B. Williams; with a foreword by Audrey Ronning, 1998. <https://journal.probeinternational.org/the-river-dragon-has-come/>.

12. Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kell. Critical Infrastructure Interdependencies // IEEE Control Systems Magazine, December 2001, p. 11—25.

13. Арутюнян Р.В., Пантелеев В.А., Сегаль М.Д. и др. Вероятностный анализ безопасности третьего уровня ВАБ-3 как этап повышения безопасности АЭС. — Атомная энергия. - 2017, т. 123, вып. 6, с. 344—349.

14. Lannoy, A. et al. 2004. Lifetime Management of Structures. Høvik: Det Norske Veritas C.

15. Johansen, I. Tien, Probabilistic multi-scale modeling of interdependencies between critical infrastructure systems for resilience, Sustainable and Resilient Infrastructure. - 2017, DOI: 10.1080/23789689.2017.1345253

#### Сведения об авторах:

**Пантелеев Владимир Александрович** — старший научный сотрудник ИБРАЭ РАН, Москва, Россия, (495) 955 22 14, e-mail: bob\_rsi@mail.ru;

**Кириллов Игорь Александрович** — научный сотрудник, ООО «КинТех Лаб», Москва, Россия, (499) 704 25 81, e-mail: kirillov@kintechlab.com.