УДК 614.8:519.816

АНАЛИЗ ТЕХНОГЕННЫХ РИСКОВ СЛАБО ФОРМАЛИЗОВАННЫХ СИСТЕМ

Аноп М. Ф – асп., тел.: (423)232-02-02, e-mail: manop@iacp.dvo.ru; *Катуева Я. В*. – с.н.с., канд. тех. наук, тел.: (423)232-02-02, e-mail: gloria@iacp.dvo.ru (ИАПУ ДВО РАН)

Рассмотрены некоторые подходы к решению задачи оценки техногенных рисков сложных слабо формализованных систем. Проведена классификация систем относительно полноты информации и степени формализации исследуемого объекта. Рассмотрены методы и подходы к оценке рисков на основе уязвимости системы.

Some approaches to the solution of the assessment problem of technogenic risks for weakly formalized systems are considered. Classification of the systems concerning information completeness and the formalization degree of the object is made. The methods and approaches to risk assessment based on the system vulnerability are considered.

Ключевые слова: техногенный риск, сложная техническая система, уязвимость.

Введение

В последнее десятилетие наблюдается возрастание требований общества к решению задачи обеспечения безопасного функционирования техногенных систем, уровень сложности которых постоянно увеличивается. Технические высокорисковые системы различного назначения и критически важные объекты инфраструктуры присутствуют в десятках видов опасных производств и объектов гражданского и оборонного назначения. Ежегодное возникновение и развитие тысяч промышленных аварийных и катастрофических ситуаций техногенного, природного и антропогенного происхождения приводят к гибели и травматизму работников предприятий, населения окружающей территории, разрушению промышленной инфраструктуры и среды обитания.

Основным принципом в решении проблем безопасности на смену лозунгу «реагировать и управлять» становится принцип «предвидеть и предупреждать». Анализ, оценка и прогнозирование рисков необходимы не только при разработке автоматизированных управляющих или контролирующих систем,

а также для интеллектуальных систем, способных обеспечить эффективную экспертную поддержку принятия решений в сложных технических и информационно-технологических ситуациях. К их числу, в первую очередь, относятся так называемые слабо формализованные информационно сложные задачи, связанные с анализом, контролем и диагностированием сложных объектов, явлений и процессов. Моделирование сложных слабо формализованных систем часто связано с необходимостью учета нечетко заданных параметров или неточной технологической информации, возникающие вследствие разного рода причин: недостаточной изученности объектов, из-за участия в управлении системой человека, наличия качественных характеристик, неопределенности и т.д.

В данной работе предлагаются анализ известных методов решения проблемы оценки техногенных рисков, возникающих в процессе эксплуатации сложных слабо формализованных систем.

Слабо формализованные системы

Будем понимать под системой (от др.-греч. σύστημα — целое, составленное из частей; соединение) — множество элементов, находящихся в отношениях и связях друг с другом, которое образует определённую целостность, единство [1].

Сложная система — система, состоящая из множества взаимодействующих составляющих (подсистем), вследствие чего сложная система приобретает новые свойства, которые отсутствуют на подсистемном уровне и не могут быть сведены к свойствам подсистемного уровня [2].

Одним из этапов построения математической модели реальной системы является процесс формализации, который в общих чертах сводится к следующему. На основе содержательного описания определяется исходное множество характеристик системы. Для выделения существенных характеристик необходим анализ каждой из них. Слабо формализуемая система характеризуется наличием ряда объектов, процессов или функций, которые невозможно описать конечным числом математических выражений, описывающих состояние этой системы [3]. Многие системы управления подобными системами оперируют с нечеткими или неполными сведениями о собственных объектах, внешних сущностях, или в этих системах есть какие-либо неопределенные показатели, которые играют важную роль в функционировании, а также обладают слабо выраженной обратной связью – сложностью функциональной взаимозависимости между входными и выходными объектами (потоками).

Примерами могут служить системы управления, связанные с деятельностью крупных организаций в изменяющейся внешней среде, где неопределенными являются управляющие воздействия и характеристики процессов этой среды. Наиболее слабо формализованными системами являются распределенные народнохозяйственные иерархические системы, объединенные по территориально-административному признаку, принадлежащие при этом различным субъектам хозяйствования (корпорациям). Особую сложность при

формальном описании подобных систем представляет конфликт интересов собственников, порождающий неполноту, тенденциозность и фрагментарность информации, обусловленную большим количеством подсистем и объектов системы.

В основе моделирования лежат информационные процессы, поскольку само создание модели базируется на информации о реальном объекте. В процессе реализации модели получается информация о данном объекте, одновременно в процессе эксперимента с моделью вводится управляющая информация, существенное место занимает обработка полученных результатов, т.е. информация лежит в основе всего процесса моделирования.

Особый класс информационно сложных задач представляют собой задачи, связанные с качественным анализом и обработкой экспериментальных данных, характеризующих течение процессов различной природы и, в частности, задачи анализа и идентификации слабо формализованных временных процессов – процессов, законы поведения которых неизвестны или недостаточно изучены. Характерными примерами таких задач являются задачи, связанные с визуальным анализом изменения контролируемых параметров в системах технической диагностики, задачи визуального анализа процессов в системах, задачи идентификации и распознавания сложных процессов в системах автоматического распознавания и др.

Таким образом, слабо формализованные техногенные системы можно разделить по следующим уровням знаний об объектах систем и протекающих в них процессах:

1. Объединенная территориально-распределенная система (ОТРС) – совокупность объектов техносферы, расположенных на определенной территории. В этом случае дефицит информации может быть не только о показателях ее функционирования и взаимосвязях между составляющими ее компонентами-подсистемами, но недостаточной может быть информация о структурном составе системы в целом.

2. Подсистема, входящая в состав ОТРС, полностью принадлежащая одному субъекту хозяйствования (субъекту, заинтересованному в безрисковом функционировании системы) – корпоративная система. Как правило, структура и состав такой системы известны и формализованы, однако при математическом моделировании могут возникать проблемы, связанные с взаимодействием с другими системами, недостаточно формализованными и изученными процессами взаимовлияния систем и объектов, их составляющих.

3. Сложные технические системы (СТС) – критически важные или потенциально опасные объекты в составе корпоративных систем, в которых протекают слабо формализованные временные и иные процессы. Примером подобного класса объектов могут быть опасные производственные объекты: ректификационные колонны, био-реакторы и т.д.

Методы оценки техногенных рисков при дефиците информации о возможных состояниях системы и факторах, влияющих на качество ее функционирования

Техногенный риск – комплексный показатель надежности элементов техносферы. Он выражает вероятность аварии или катастрофы при эксплуатации машин, механизмов, реализации технологических процессов, строительстве и эксплуатации зданий и сооружений.

При анализе безопасности в техногенной сфере в первую очередь рассматриваются опасные производственные (промышленные) объекты и критически важные объекты, как объекты, которые могут нанести огромный ущерб населению, окружающей среде и экономике страны в целом. Такого рода объекты относятся к категории сложных систем как с точки зрения сложности их структуры, так и с точки зрения сложной динамики взаимодействия входящих в них элементов. В связи с этим, построение точных математических моделей этих систем и сценариев развития отказов при огромном количестве вариантов инициирующих воздействий и сложных, труднопрогнозируемых взаимодействиях большого количества элементов в процессе эскалации аварий, - не представляется возможным.

Тяжелые аварии в сложных технических системах, как правило, бывают сопряжены с длинными последовательностями отказов (сценариями развития аварий) их элементов. Многие из них являются редкими, непрогнозируемыми или необычными. Это обстоятельство, является принципиально важным при оценке уязвимости подобных систем, поскольку усилия проектировщиков бывают сосредоточены на том, чтобы при построении системы исключить прогнозируемые и часто встречающиеся опасные сценарии и взаимодействия.

При решении задач оценки рисков для обеспечения безопасности в техногенной сфере первостепенное значение имеет анализ и оценка влияния опасных процессов и инициирующих факторов, их взаимодействий на развитие техногенных катастроф. Полученные результаты проведенного анализа обычно представляются в виде сценариев возникновения и развития аварий и катастроф и вероятности возникновения инициирующего события.

Для проектируемых и эксплуатируемых технических систем должно осуществляться определение рисков R возможных техногенных отказов, повреждений, аварий и катастроф.

Система оценки риска состоит из трех составных частей:

1. правовая составляющая;
2. детерминистская составляющая;
3. вероятностная составляющая.

Правовая и детерминистская составляющие представляют собой качественную сторону понятия риск, вероятностная составляющая – количественную сторону понятия риск.

Детерминистский подход к обеспечению безопасности предполагает формулировку и нормативное закрепление априори (до создания объекта)

системы обязательных требований при проектировании, создании, эксплуатации, выводе из эксплуатации объектов определенного класса. Подтверждение безопасности объекта, а следовательно и уменьшение риска, является выполнение на всех этапах жизненного цикла соответствующей системы требований. Формирование и развитие системы детерминистского подхода для конкретной области строится на основании опыта сооружения и эксплуатации, близких по аналогии объектов, инженерной интуиции, накопленного опыта анализа процессов и т.п. Эта составляющая системы оценки риска регламентируется системой правил, норм, стандартов и подобных документов различного уровня – от общегосударственного, до уровня отдельных предприятий. Например, в области использования атомной энергии она составляет тысячи документов объемом в десятки тысяч страниц. Именно по выполнению требований этих документов на всех этапах жизненного цикла объекта делается заключение о безопасности этого объекта и, следовательно, представляет ли это предприятие недопустимый риск для населения и окружающей среды. Заключение это качественное, т.е. отражает точку зрения экспертов или органов исполнительной власти.

К вероятностной составляющей системы оценки риска относится, в первую очередь, вероятность чрезвычайного события и последствия (ущерб) от этого происшествия или аварии [4].

Анализ уязвимостей как ядро оценки риска при недостаточной информации

Общий контекст анализа риска и защищенности для объектов техногенной сферы предполагает последовательный анализ:

- угроз, которым подвергается объект;
- уязвимостей объекта по отношению к выявленным угрозам;
- оценку ущербов от аварий, реализующихся в тех случаях, когда объект оказался уязвимым к действующим на него угрозам.

Анализ уязвимости является ядром оценки риска. Он призван дать ответ на вопрос, как будут развиваться события после того, как рассматриваемая система будет подвергнута инициирующему воздействию, и насколько вероятно, что эта система окажется поврежденной.

Изменения, происходящие в технической системе, призванной обеспечить получение определенного результата (или реализацию заданного технологического процесса), могут быть представлены в виде траектории в пространстве состояния системы Ω, определяющей переход от начального состояния системы *SC (start condition)* в ее конечное состояние *FC (final condition)*. В случаях, когда удается обеспечить подобный переход, говорят, что в системе реализован заданный сценарий S_0.

Примерами состояний системы являются: соответствие системы определенным требованиям, структурная целостность системы, неповрежденность ее элементов, выполнение системой заданных функций, обеспечение задан-

ной производительности и качества (продукций или услуг) и т.д. Требования качества определяют размерность и конфигурацию пространства состояний системы Ω.

Если в системе происходит инициирующее событие *IE (initialization event)*, она может отклониться от сценария S_0 и перейти к реализации нового сценария S_{IE}, заканчивающегося конечным состоянием FS_{IE}, отличным от заданного конечного состояния FC_0. Таким образом, инициирующее событие является автоморфным отображением пространства состояний.

Вследствие высокого уровня неопределенности, касающейся типа и интенсивности инициирующих событий, а также способности системы «сопротивляться» инициирующим воздействиям, мера уязвимости должна быть вероятностной, то есть определяться вероятностью отказа (O): $V = f(P[O])$.

В связи с тем, что свойства, характеризующие уязвимость системы, начинают проявляться только после того, как в ней произошло некоторое нештатное инициирующее событие H (или система подвергнута некоторому нештатному воздействию), мера уязвимости должна определяться условной вероятностью отказа системы, при условии, что система подвергнута инициирующему воздействию $V = f(P[O \mid H])$.

Очевидно, что на практике невозможно бывает обеспечить абсолютно точное достижение системой заданного конечного состояния *FS*. Реальные системы всегда будут подвергаться некоторым, иногда слабым, инициирующим воздействиям, которые будут несколько отклонять траекторию системы от заданного сценария S_0. Кроме того, отклонение от начального сценария обуславливается и естественной вариативностью параметров системы.

Поэтому при оценке уязвимости речь должна идти об условной вероятности выхода конечного состояния из заданной области D пространства состояний системы Ω.

Таким образом, под уязвимостью системы понимается условная вероятность выхода конечного состояния системы *FC* за границы заданной области D пространства состояний системы Ω, в случае, если произойдет инициирующее событие H [5]:

$$V = P[(\left\| FC_{IE} - FC_0 \right\| > \varepsilon_0) \mid H] \qquad (1)$$

В случае, когда в системе возможны различные аварийные состояния, анализ уязвимости предполагает анализ дерева сценариев и построение матрицы условных вероятностей достижения различных конечных состояний в случае различных инициирующих событий.

Очевидно, что анализ уязвимости должен проводиться в связке с другими этапами анализа риска, поскольку он должен следовать за анализом угроз и предшествовать калькуляции ущербов, реализуемых в случае достижения системой различных поврежденных конечных состояний.

Уязвимость системы характеризуется совокупностью сценариев случайных событий (отказов в системе) и причинно-следственных связей между

этими событиями, происходящими вслед за инициирующим событием вплоть до достижения системой конечных состояний. Принципы построения сценарных деревьев, описывающих сценарии развития аварий, подробно изучается в рамках теории структурирования сценариев [6]. Среди ее подходов центральное место занимают методы, базирующиеся на построении графовых моделей типа дерево событий или диаграмм влияния, описывающих вероятностные причинно-следственные связи между событиями в процессе эскалации аварии. Таким образом, анализ уязвимости предполагает детальное изучение дерева сценариев рассматриваемой системы.

Технические объекты, как правило, бывают, объединены в сетевые системы. Сложный характер взаимодействия различных элементов подобного рода систем в пространстве и времени выражается в частности, в появлении критических состояний СТС, для которых характерны каскадные разрушения, приводящие к наиболее тяжелым поврежденным состояниям и полному разрушению рассматриваемых систем.

При построении сетевых структурных моделей отбрасываются многие детали, что позволяет сосредоточиться на главных особенностях системы, определяющих характер развития аварии (в частности, вероятности достижения различных степеней повреждения). Кроме того, сети представляют собой чрезвычайно гибкую абстракцию, которая может широко применяться при изучении таких инфраструктурных систем как системы газо- и электроснабжения, транспортные инфраструктуры, телекоммуникационные системы и.т.д. Для подобных систем может быть построена иерархия математических моделей различной сложности, позволяющих описать различные аспекты уязвимости инфраструктуры систем по отношению к возможным инициирующим воздействиям. Существует ряд математических моделей, основанных на теории ветвящихся процессов, которые позволяют описать развитие каскадных процессов в сетевых системах, находящихся в критических состояниях [7, 8].

Заключение

Подход к проблеме обеспечения безопасности на основе анализа риска, как некоторой количественной оценки, особенно важен на региональном уровне, в первую очередь для регионов, где сосредоточен значительный потенциал опасных производств и объектов в сочетании со сложной социально-политической обстановкой и недостаточным финансированием.

Оценка уязвимости системы является ключевым этапом анализа риска. Она следует за оценкой угроз, которым подвергается техническая система, и формирует основу для последующей оценки ущербов. Для каждой рассматриваемой системы, прежде всего, необходимо определить множество возможных состояний системы. Оценка техногенного риска проводится на основе уязвимости, которая определяется как условная вероятность отказа в случае осуществления инициирующего события. В случае, если в системе могут реализовываться различные инициирующие события и множественные сце-

нарии отказов, уязвимость системы должна характеризоваться сценарным графом, описывающим вероятностные причинно-следственные связи между событиями в процессе развития аварии.

Библиографические ссылки

1. *Большой* Российский энциклопедический словарь.— М.: БРЭ.— 2003. - с. 1437.

2. *Лоскутов А. Ю., Михайлов А. С.* Основы теории сложных систем. М.-Ижевск: НИЦ "Регулярная и стохастическая динамика".- 2007. - 620 с.

3. *Шульгин А. О., Демурчев Н. Г.* Моделирование процессов управления в слабоформализованных системах. // Первая ежегодная научная конференция студентов и аспирантов базовых кафедр Южного научного центра РАН. Материалы молодежной конференции (Ростов-на-Дону, 15-21 апреля 2005 г.). Ростов-на-Дону: изд-во ЮНЦ РАН. - 2005. – С.219-221.

4. *Ковалевич О. М.* Система оценки риска и закон о техническом регулировании // Известия Академии Промышленной Экологии. - 2006. - N 4. - С. . 46-55.

5. *Махутов Н. А., Петров В. П., Резников Д. О.* Обеспечение защищенности критически важных объектов на основе снижения их уязвимости // Проблемы безопасности и чрезвычайнх ситуаций. – М.: ВИНИТИ. – 2009. - №2.- С. 50-69.

6. *Kaplan S., Visnepolschi S., Zlotin B., Zusman A*. New tools for failure & risk analysis. Anticipatory Failure Determination (AFD) and The Theory of Scenario Structuring / Ideation International Inc.- 1999, 2005. – USA: ISBN 1-928747-0-51.

7. *Carreras B, Lynch V, Dobson I, Newman D.* Dynamical and probabilistic approaches to the study of blackout vulnerability to the power transition grid. // 37th Hawaii International Conference on System Sciences, Hawaii.- 2004.

8. *Dobson I, Carreras B., Newman D., Lynch V.* Complex Systems Analysis of Series of Blackouts: Cascading Failure, Criticality, and Self-organization Bulk Power System Dynamics and Control –VI. – 2004. - Cortina d'Ampezzo, Italy