КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ МОНИТОРИНГА РИСКА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

О. В. Яковлев, кандидат технических наук. Академия гражданской защиты МЧС России

Рассмотрена проблема мониторинга риска чрезвычайных ситуаций, вызванных системными конфликтами. В качестве первого шага на пути решения проблемы сделана попытка формирования концептуальной модели информационной технологии мониторинга риска чрезвычайных ситуаций. Мониторинг риска описывается в виде технологического процесса, основная направленность которого уменьшение неопределённости в оценке риска.

Ключевые слова: риск, системный конфликт, мониторинг риска, информационная технология

EMERGENCY SITUATIONS RISK MONITORING. CONCEPTUAL MODEL OF INEORMATION TEHNOLOGY

O. V. Yakovlev. Civil Defence Akademy, EMERCOM of Russia

Present article is devoted to a problem of monitoring of emergency situations generated by system conflicts. As a first step on the problem decision attempt of emergency situations risk monitoring conceptual model formation is made. Risk monitoring is described in terms of technology process of risk assessment indetermination reduction.

Key words: risk, systems, risk monitoring, information technology

Под концептуальной моделью будем понимать модель, отражающую с определенной полнотой объект исследования в том или ином содержательном аспекте, записанную на естественном языке с использованием обычной логики рассуждений [1].

В коллективной монографии ведущих ученых института системного анализа РАН указывается, что «…одним из главных ресурсов, которым располагает наша цивилизация в управлении новыми видами рисков, являются новые информационные технологии, их важнейшая часть – математические модели, использующие формализованное описание, отражающее наш опыт, знание законов природы». В качестве вывода делается следующее утверждение: «…проведение исследований в данном направлении позволит научиться работать на опережение угроз и опасностей» [2].

В [3] отмечается, что, несмотря на все усилия исследователей и разработчиков систем, не удается создать объекты гарантированной безопасности. При этом еще раз подтверждается одно из положений системного анализа о том, что в сложных системах в большей мере проявляются системные свойства, которых может не быть у отдельных элементов системы.

Данное обстоятельство приводит к тому, что в сложных системах, несмотря на высокую надежность отдельных элементов, не всегда удается избежать отказов, сбоев в работе, аварийных и чрезвычайных ситуаций. Как отмечено в [4], «наиболее серьезные угрозы и опасности находятся на системном уровне».

Примером тому могут служить крупные аварии и катастрофы в системах с высоким уровнем заложенной при проектировании надежности. Анализ развития таких аварий имеет ряд общих черт, а именно: развитие аварийной ситуации начинается с накопления ряда мелких отклонений в функционировании объекта, каждое из которых в отдельности не представляет угрозы безопасности. По мере накопления таких отклонений возникает ситуация, когда персонал сталкивается с определенными трудностями в эксплуатации объекта, что приводит к ошибкам персонала. Неправильные управляющие воздействия в

значительной мере усугубляют ситуацию и, в совокупности с отклонениями протекания технологического процесса от нормы, приводят к возникновению чрезвычайной ситуации на объекте [2].

Для того, чтобы учесть системные свойства опасностей, присущих новым технологиям, целесообразно, на наш взгляд, при анализе риска учитывать также и его системные свойства.

Системные свойства риска особенно наглядно проявляются при моделировании процессов функционирования сложных технологических систем.

Вновь создаваемые системы, реализующие новые технологии, вступают во взаимодействие с окружающей средой и с другими системами. Причем, взаимодействие таких систем носит далеко не всегда бесконфликтный характер. Скорее наоборот, возникновение новых систем, в которых реализуются сложные новые технологии, почти всегда сопровождается конфликтными ситуациями.

Согласно [5], конфликт является основным способом взаимодействия сложных систем. Понятие конфликта используется во многих областях знаний: в социологии, военном деле, политологии, психологии и др. Использование понятия конфликта при моделировании процессов взаимодействия сложных систем позволяет выявить критически опасные стороны и факторы таких систем и избежать развития неблагоприятных ситуаций при реализации таких систем. Наиболее ярко свойство конфликтности проявляется в химико-технологических, военных и топливно-энергетических системах.

Рассмотрим проявления конфликта систем с позиций теории управления, составляющей важную часть кибернетики.

С позиций теории управления, как наиболее разработанного раздела кибернетики, любая система рассматривается как совокупность управляющей и управляемой системы, между которыми образованы информационные и энерго-вещественные связи, реализующие управляющие воздействия и информационные обратные связи.

С созданием сложных технологических систем данная классическая структура управления уже не отражает многие реальные системные взаимодействия. Неучет таких системных взаимодействий не позволяет обеспечить требуемый уровень безопасности новых технологий в процессе их реализации.

Классический подход к моделированию сложных технологических систем с выделением системы из внешней среды приводит к чрезмерному упрощению модели системы и, как следствие, не позволяет смоделировать те опасные процессы и ситуации, развитие которых может привести к возникновению ЧС. Даже выделяя систему из внешней среды, как это рекомендуется при проведении исследований систем управления, мы тем самым исключаем из рассмотрения многие факторы, учет которых в системном конфликте с внешней средой мог бы нам позволить оценить возможность возникновения ЧС.

Иными словами, такой подход не рассматривает возможности возникновения ЧС как «штатного» режима функционирования сложной системы. ЧС рассматривается как исключительный (в прямом и переносном смысле этого слова) вариант развития событий в процессе эксплуатации системы.

Соответственно, и в модели, описывающей процесс эксплуатации системы, реализующей сложную технологию, возможность возникновения ЧС также не принимается во внимание.

Для того, чтобы ввести в процесс управления возможность возникновения ЧС, необходимо рассматривать не только сам процесс управления, но и процесс взаимодействия с другими системами. Причем, рассматривать не только «дружественное» взаимодействие, но и возможности возникновения межсистемных конфликтов. Ведь создание практически любой новой сложной технологической системы вызывает ответную реакцию не только внешней среды, но и других взаимодействующих систем.

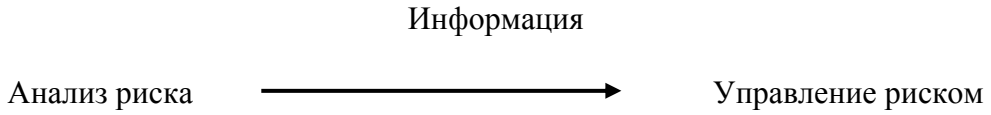
Наличие системных конфликтов является неизбежной реальностью нашей жизни. Разрешение таких конфликтов происходит в различных формах. Одной из форм разрешения конфликтов при взаимодействии систем являются чрезвычайные ситуации.

В чрезвычайных ситуациях расширяется круг взаимодействующих систем и возникают новые формы взаимодействия с образованием дополнительных энерго-вещественных и информационных связей. Включение в круг взаимодействующих систем одной только системы предупреждения и ликвидации ЧС уже значительно усложняет общую картину взаимодействия.

Тем не менее, моделирование чрезвычайных ситуаций на основе системных конфликтов до сих пор не привлекает должного внимания специалистов. Объяснение такому положению достаточно простое. Разработчик системы редко бывает заинтересован в выявлении всех возможных критических ситуаций, способных возникнуть в процессе будущей эксплуатации системы. В лучшем случае разработчик представит ограниченный перечень критических ситуаций, разрешение которых предусмотрено проектом, и не будет акцентировать внимание на возможных системных конфликтах, перелагая их и их возможные последствия на заказчика системы.

В этой связи смена парадигмы управления системой при моделировании процессов в сложных технологических системах на парадигму взаимодействия систем, в том числе и конфликтного, расширяет возможности по анализу рисков и их управлению [6].

Схематическая связь процессов анализа риска и управления риском достаточно проста и может быть представлена на основе приведенной в [7] методологической схемы анализа и управления риском следующим образом:



Относительно структуры и содержания приведенной в методологической схеме анализа и управления риском указывается, что «дискуссии по вопросу о том, какие этапы следует выделять как самостоятельные и как их обозначать, что включает анализ риска, управление риском, не закончены и по сей день, и это естественно, так как анализ и управление риском – новые научные направления, еще не завершившие стадию своего становления» [8].

В основе анализа и управления риском, как видно, лежат информационные процессы.

Отметим, что информационные аспекты многих научных направлений, бывшие ранее в качестве обеспечивающих, в новом веке начинают выходить на первый план. Так, академик В. М. Глушков в своих трудах [9] развил новые подходы к пониманию процессов управления с позиций бурно развивающихся информационных технологий. В новой трактовке предложено процессы управления рассматривать с точки зрения информационного взаимодействия сложных систем.

Мониторинг риска будем рассматривать также в качестве информационного процесса. Основная направленность данного информационного процесса – уменьшение неопределенности в оценке риска. При таком подходе мониторинг риска можно считать обеспечивающим процессом в более широком процессе анализа риска. Подобный подход применен в [10] при анализе гидрометеорологической безопасности.

Использование информации о риске при принятии решений по управлению риском вводит информационный процесс мониторинга риска в контур управления риском. Данное обстоятельство позволяет рассматривать информационный процесс мониторинга риска как составную часть информационного процесса принятия решения по управлению риском. Информационный процесс мониторинга риска протекает также и на этапе контроля эффективности принимаемых решений по управлению риском.

Таким образом, функционально мониторинг риска как информационный процесс тесно связан как с функциями анализа, так и с функциями управления риском, что соответствует общей методологии мониторинга, принятой в [11, 12].

Под информационно-технологическим процессом (ИТП) мониторинга риска чрезвычайных ситуаций будем подразумевать основной макропроцесс преобразования информации о риске ЧС в оценку риска. ИТП будем рассматривать как технологическую реализацию операций, выполняемых в соответствии с концептуальной моделью исчисления рисков, приведенной [6]. ИТП состоит из связанного набора действий, выполняемых в определенной последовательности с использованием различных методов обработки и инструментальных средств, охватывающих все этапы обработки информации, начиная с получения первичных данных и заканчивая передачей информации о риске ЧС, необходимой для решения задач анализа и управления риском.

Сущностью ИТП в автоматизированной информационно-управляющей системе управления риском ЧС является сбор, преобразование и представление информации в соответствии с целями и требованиями потребителей – органов управления предупреждением и ликвидацией ЧС.

Анализ задач мониторинга риска, приведенных в таблице, показывает, что все указанные задачи можно условно подразделить на три основные группы:

– задачи аналитического мониторинга;

– задачи ситуационного мониторинга;

– задачи операционного мониторинга.

Таблица. **Задачи мониторинга риска**

<table>
<tr><td colspan="3">Мониторинг риска</td></tr>
<tr><td>Аналитический мониторинг</td><td>Ситуационный мониторинг</td><td>Операционный мониторинг</td></tr>
<tr><td>Выделение информационных признаков риска
Исчисление риска
Оценка риска</td><td>Наблюдение (за источниками информации о риске)
Отслеживание (изменений в развитии риска)
Контроль (параметров, определяющих риск)</td><td rowspan="2">Контроль результатов управления риском</td></tr>
<tr><td colspan="2">Формирование базы знаний проблемной области риска</td></tr>
<tr><td colspan="3">Разработка информационной технологии мониторинга риска</td></tr>
</table>

Соответственно, для решения выделенных групп задач должны использоваться апробированные или специально разработанные:

– информационная технология аналитического мониторинга;

– информационная технология ситуационного мониторинга;

– информационная технология операционного мониторинга.

Рассмотрим в отдельности каждую из указанных технологий.

Информационная технология аналитического мониторинга рисков предназначается для решения задач выявления информативных признаков риска ЧС.

Информационная технология аналитического мониторинга рисков должна включать как автоматизированные, так и неавтоматизированные методы обработки информации.

Функционально информационная технология аналитического мониторинга может быть представлена в виде пошаговой процедуры выполнения различных операций (сбор, обработка, анализ, представление и другие) с применением различных программно-технических средств.

На первом шаге производится определение перечня возможных рисков ЧС.

Вторым шагом является выявление возможных источников информации для мониторинга рисков ЧС в соответствии с выделенным и структурированным на первом шаге множеством рисков.

На третьем шаге формируется сеть сбора информации от источников информации с учетом возможностей действующей автоматизированной информационно-управляющей системы российской системы предупреждения и ликвидации ЧС (АИУС РСЧС) и возможностей организации дополнительных информационных связей на основе комплексирования информационно-технических элементов в подсистему АИУС РСЧС.

Четвертый шаг – сбор информации от источников информации о рисках ЧС.

Пятый шаг – представление собранной информации в заданных формах отображения для последующей обработки и анализа.

На шестом шаге производится обработка данных и их анализ с применением технологий системного моделирования и интеллектуальных информационных систем. На данном этапе используются различные методы работы: моделирование процессов, развитие которых может приводить к возникновению ЧС; проведение экспертных оценок, обработка нечетких знаний, выявление прецедентов и другие.

На седьмом шаге по результатам обработки и анализа данных осуществляется выделение информативных признаков риска.

На восьмом шаге проводится оценка риска возникновения ЧС на основе выделенных информативных признаков в соответствии с принятой концепцией исчисления рисков.

На девятом шаге проводится анализ качества решения выполненной задачи по мониторингу рисков рассмотренного вида ЧС и выработка рекомендаций по управлению качеством мониторинга рисков.

На десятом шаге вносятся коррективы в технологию мониторинга рисков ЧС с учетом выработанных на девятом шаге рекомендаций.

Информационная технология ситуационного мониторинга рисков предназначена для выявления, отслеживания и контроля информативных признаков риска ЧС в определенной ситуации риска.

Данная технология так же, как и информационная технология аналитического мониторинга может быть представлена в виде последовательности технологических операций по обработке различных видов информации, выполняемых в виде пошаговой процедуры. Учитывая схожесть смыслового описания *первых шести* технологических операций аналитического и ситуационного мониторинга рисков, приводим пошаговую процедуру ситуационного мониторинга, начиная с седьмого шага.

Седьмой шаг – производится запрос к базе знаний аналитического мониторинга рисков и выполняется моделирование процессов развития рисков ЧС на заданном временном интервале.

Восьмой шаг – оперативная оценка риска с использованием системы поддержки принятия решений по оценке риска.

Девятый шаг – выдача данных по оценке риска ЧС ОВ во внешнюю, по отношению к системе мониторинга рисков, систему принятия решений по управлению риском, и в подсистему операционного мониторинга.

Десятый шаг – анализ проведенных работ по мониторингу рисков и выработка рекомендаций по совершенствованию технологии ситуационного мониторинга.

Информационная технология операционного мониторинга рисков предназначена для решения задачи мониторинга риска в процессе и по результатам управления риском ЧС.

На наличие некоторой общности в задачах мониторинга рисков и управления рисками уже указывалось ранее.

В решении задач управления рисками ЧС операционный мониторинг следует рассматривать как одну из функциональных составляющих управления рисками. Технологически операционный мониторинг рисков является элементом системы поддержки принятия решений по управлению рисками.

Операционный мониторинг рисков решает две основные задачи:

– мониторинг риска в процессе управления риском определенного вида ЧС;

– анализ эффективности управления риском.

Решение указанных задач производится в рамках информационной технологи системы поддержки принятия решений по управлению риском ЧС.

Поскольку вопросы управления риском ЧС являются предметом отдельной самостоятельной области исследования, ограничимся рядом замечаний относительно интеграции технологии операционного мониторинга в интеллектуальную технологию поддержки принятия решений.

Считаем целесообразным проводить подобную интеграцию на основе сопряжения моделей и методов, применяемых в сопрягаемых технологиях. Для этой цели, на наш взгляд, наиболее предпочтительным являются концепции теоретико-множественного и категорийно-функторного подходов.

Применение указанных подходов предполагает дальнейшую реализацию сопряжения технологий с использованием программно-технических продуктов, разработанных на основе объектно-ориентированного подхода к программированию.

Литература

1. Калинин В. Н., Резников Б. А. Теория систем и управления: Структурно-математический подход. – Л., 1979.

2. Управление риском. Риск. Устойчивое развитие. Синергетика / В. А. Владимиров, Ю. Л. Воробьев, Г. Г. Малинецкий [и др.]. – М., 2000.

3. Ларичев О. И., Мечитов А. И. Методологические проблемы анализа риска и безопасности использования новых технологий // Системные исследования. Методологические проблемы: ежегодник / под ред. Д. М. Гвишиани, В. Н. Садовского. – М., 1988.

4. Малинецкий Г. Г. Сценарии, стратегические риски, информационные технологии. // Информационные технологии и вычислительные системы. – 2002. – № 4.

5. Дружинин В. В., Конторов А. С., Конторов М. А. Введение в теорию конфликтов. – М., 1989.

6. Яковлев О. В. Концептуальные основы мониторинга риска в условиях системных конфликтов // Проблемы анализа риска. – 2007. – № 3.

7. Быков А. А., Порфирьев Б. Н. Об анализе рисков, концепциях и классификации рисков // Проблемы анализа риска. – 2006. – № 4.

8. Акимов В. А. Оценка и прогноз стратегических рисков России: теория и практика // Стратегические риски чрезвычайных ситуаций: оценка и прогноз: материалы конф. – М., 2003.

9. Глушков В. М. Кибернетика, вычислительная техника, информатика: избр. тр.: в 3-х т. – Т.1: Математические вопросы кибернетики. – Киев, 1990.

10. Тертышников А. В., Яковлев О. В. Основы технологий мониторинга гидрометеорологической безопасности. – Химки, 2006.

11. Герасимов И. П. Научные основы мониторинга окружающей среды // Изв. АН СССР. – Сер. Геогр. – 1975. – № 3.

12. Яковлев О. В. Информационный мониторинг риска чрезвычайных ситуаций: от истоков возникновения до наших дней // Научные и образовательные проблемы гражданской защиты. – 2008. – № 1.