ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ РИСКАМИ ДЛЯ КРИТИЧЕСКИ И СТРАТЕГИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ РФ

Дтн, проф. Костогрызов А.И., главный научный сотрудник Института проблем информатики РАН

Краткая аннотация: *в результате сравнительного анализа существующих подходов к обеспечению безопасности в системах различного функционального назначения определены цели, задачи, вероятностные модели и методы управления техногенными рисками для критически и стратегически важных объектов (КСВО) РФ. В работе представлен подход к управлению рисками, в т.ч. «прецедентный принцип» определения допустимых рисков, методы и аналитические инструментарии обоснования эффективных упреждающих мер противодействия рискам. Их применение целенаправленно ведет к непревышению допустимого риска и снижению возможного ущерба КСВО для определенного множества угроз.*

Ключевые слова: *анализ, безопасность, качество, риск, системная инженерия, управление, функционирование*

Ежегодно в промышленном секторе России происходят тысячи чрезвычайных ситуаций техногенного характера, приводящих к гибели людей и громадному материальному ущербу КСВО. Примерами КСВО

в полной мере можно считать предприятия оборонно-промышленного, нефтегазового и энергетического комплексов, угледобывающей и металлургической промышленности, транспортные системы, системы переработки полезных ископаемых, системы долговременного хранения продукции и др. На многих предприятиях при кажущейся видимости системного контроля ситуаций ощущается отсутствие объективных методов прогноза рисков и обоснования эффективных упреждающих мер противодействия рискам, несовершенство нормативной базы, дефицит действенных технологий и средств системного контроля, мониторинга, раннего обнаружения и парирования развития свойственных КСВО техногенных аварий и катастроф. Проявлениями недопустимо высоких рисков такого рода эксцессов стали аварии на электроподстанции Чагино, Каширской ГРЭС, Саяно-Шушенской ГЭС и др., что свидетельствует об остроте и практической важности научного решения проблемы эффективного управления техногенными рисками.

Необходимо отметить, что первые требования, аналогичные требованиям к оценке рисков заложены на уровне научно-технических основ системной инженерии, исследований и стандартов обеспечения надежности [1-5 и др.]. Среди отечественных нормативных документов необходимо отметить ГОСТ Р 27.001-96, ГОСТ 27.002-89, РД 50-699-90, ГОСТ 27.003-90, ГОСТ Р 27.101-96, ГОСТ 15.206-84, ГОСТ 27.301-96, ГОСТ 27.310-95, ГОСТ Р 27.302-96, ГОСТ 27.410-87, ГОСТ Р 27.402-96, ГОСТ Р 27.403б РД 50.656-88, РД 50-423-83, РД 50-490-84, МР 252-87, РД в 50-503-84 РД 50-476-84, РД 50-690-90 и др. Управление надежностью осуществляется по ГОСТ Р 51901-2002.

Важное значение для определения требований по оценке и снижению рисков имел Федеральный закон РФ от 21.12.1994 №68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» и последующие за ним национальные стандарты серии ГОСТ Р 22 по безопасности в чрезвычайных ситуациях, а также Федеральный закон РФ от 21.07.1997 N 116-ФЗ "О промышленной безопасности опасных производственных объектов" с соответствующими нормативными документами. Необходимость противодействия актам незаконного вмешательства (в т.ч. террористическим актам или покушениям на их совершение, угрожающим безопасному функционированию объектов топливно-энергетического комплекса) вылились в требования противодействия рискам на уровне Федерального закона РФ от 21.07.2011г. N 256-ФЗ «О безопасности объектов топливно-энергетического комплекса».

Проведенный анализ показал [6], что существующие методы количественного анализа рисков в приложении к техногенным ситуациям (т.е. являющимся следствием развития техники, результатом применения различных технологий производства), характеризуемым множеством случайностей, для различных приложений являются несовместимыми. Вероятностная интерпретация расчетных рисков зачастую принципиально различается. Несмотря на логическую идентичность воздействия угроз и реализации процессов контроля, мониторинга и восстановления нарушаемой целостности, существующие подходы к прогнозированию рисков не позволяют в общем случае обосновывать требования к системным процессам при ограничениях на допустимые риски и ресурсы.

В настоящей работе под риском понимается мера опасности с учетом тяжести последствий (оценка с помощью вероятностной меры).

Примечание. Согласно ст.2. Федерального закона "О техническом регулировании" риск – это «…вероятность причинения вреда… с учетом тяжести этого вреда". В приложении к опасным производствам риск аварии рассматривается как мера опасности, характеризующая возможность возникновения аварии и тяжесть ее последствий. Единым стандартом ISO/IEC16085 и IEEE 16085-2006 «ИТ. Системная и программная инженерия. Процессы жизненного цикла. Управление рисками» риск определен как вероятность наступления опасного события с его последствиями, а в стандарте ГОСТ РВ 51987-2002 «ИТ. КСАС. Требования и показатели качества функционирования информационных систем. Общие положения» - как возможная опасность неудачи предпринимаемых действий. Наконец, последним стандартом ISO 31000 «Менеджмент риска. Принципы и руководства» риск определяется как эффект неопределенности при достижении целей (при этом эффект может носить как отрицательный, так и положительный оттенок). Есть и другие определения. Это говорит о том, что научная дискуссия относительно определения риска не завершена.

Учитывая, что затраты на ликвидацию последствий аварий и катастроф на порядок превышают затраты на превентивные меры, цели настоящей работы состоят в формулировании основ современной стратегии эффективного управления рисками, реализующей «прецедентный принцип» определения допустимых рисков, обоснование и реализацию эффективных упреждающих мер противодействия рискам. При этом основными объектами методического приложения рассматриваются сложные системы КСВО с повторяемыми процессами функционирования, периодически контролируемым состоянием и возможностями требуемого восстановления нарушаемой целостности системных компонентов для выполнения функций согласно назначению.

Интегральными целями эффективного управления рисками являются предотвращение или ограничение угрозы жизни и здоровью персонала системы (в т.ч. предприятия) и проживающего вблизи населения, снижение экономических потерь и материального ущерба

при реализации угроз. К примеру, угрозы для информационных систем формируются с учетом факторов, воздействующих на информацию – см. ГОСТ Р 51275. А для промышленных предприятий реализация угроз заключается в негативном воздействии дестабилизирующих факторов (ДФ). Для каждой из систем КСВО должно быть сформировано свое множество угроз, в противодействие которым строятся системы управления рисками.

Исходя из интегральных целей частными целями управления рисками могут выступать: предупреждение реализации угроз (негативного воздействия ДФ); предотвращение появления аварийных ситуаций; локализация развития аварийных ситуаций в начальный период их возникновения; снижение или удержание в допустимых пределах рисков и/или снижение затрат и/или возможных ущербов в практике создания, эксплуатации, технического обслуживания, модернизации и развития системы и ее составных компонентов при задаваемых ограничениях.

Достижение целей в общем случае реализуется на основе решения комплекса основных задач системной инженерии по нормативно-правовому, организационно-методическому, опытно-конструкторскому, эксплуатационно-производственному и квалификационно-кадровому направлениям.

В общем случае для систем различного приложения реализация угроз, мер контроля, мониторинга и восстановления целостности составных подсистем оцениваемой системы может быть абстрактно представлена в виде, приведенном на рис. 1 (интерпретация: система находится в состоянии безопасности, когда

И 1-я , И 2-я …И последняя подсистемы находятся в состоянии безопасности, для подсистем с резервированием возможны выражения ИЛИ). Такая общность позволяет выбрать единые исходные данные и расчетные показатели для отдельных элементов и систем в целом.

Рис. 2 Иллюстрация угроз, мер контроля, мониторинга и восстановления целостности составных подсистем оцениваемой системы

При оценках защищенности систем от опасных воздействий основным показателем является риск (вероятность) опасного воздействия в течение заданного периода функционирования системы. Опираясь на существующие прецеденты, предлагается как интегральные показатели рисков нарушения целостности на практике использовать в качестве основного - риск (вероятность) нарушения целостности (качества и/или безопасности функционирования) в течение заданного периода времени для составных компонентов и системы в целом, а в качестве дополнительных: среднюю наработку на

нарушение целостности составных компонентов и системы в целом; среднее время восстановления системы с учетом рисков, а также возможные ущербы. При этом определение самого понятия приемлемого уровня целостности (т.е. уровня качества и/или безопасности) отдается на откуп заказчикам конкретной системы. Они должны формулироваться с учетом необходимости выполнения системой задаваемых функций в реальных (в т.ч. небезопасных) условиях функционирования.

Ключевым моментом при построении и организации системы управления рисками (СУР) является определение допустимого риска. Для каждого объекта существует свой норматив допустимости (приемлемости). Приоритетным является выбор критерия допустимости риска, основанного на прецедентном принципе. А именно: принимаемые упреждающие меры снижения риска или удержания его в допустимых пределах считаются достаточными только тогда, когда за период эксплуатации объекта не произойдет дестабилизаций, которые могли бы быть предотвращены за счет использования упреждающих мер (в т.ч. с использованием технологий сбора и анализа информации, мониторинга и контроля ситуации и принятия адекватных последовательных мер противодействия рискам). Определение достигаемых при этом количественных значений частных и интегральных показателей рисков по единой методике, носящей универсальной характер, даст представление об уровне приемлемого риска не только для этих объектов, выбранных в качестве сравнительного эталона, но и для других объектов с аналогичными природно-климатическими и

техническими условиями эксплуатации. До тех пор, пока не будет сформирована, обработана и обобщена представительная база знаний об условиях функционирования различных производственных объектов с выявленными по единой методике общими закономерностями в разрастании опасностей, в возможностях применяемых систем сбора и обработки информации, технологиях мониторинга и контроля ситуации, а также в мерах противодействия рискам, для каждого критичного объекта допустимый уровень риска будет оставаться уникальным, он должен быть количественно обоснован непосредственно руководством предприятия.

Для реализации представленных выше идей предлагается использовать вероятностные модели для количественного прогнозирования рисков в зависимости от характеристик угроз и применяемых мер контроля, мониторинга и восстановления целостности [2-10 и др.].

Для крупных предприятий КСВО, существенно зависящих от непрерывного энергоснабжения объектов, актуальным является вопрос автоматизации систем инженерного обеспечения (СИО). Требуется спрогнозировать надежность системы электропитания при функционировании комплексного центра обработки информации (КЦОИ) как заданного фрагмента СИО в неавтоматизированном режиме и с использованием автоматизированной системы управления (АСУ) СИО. Логические компоненты системы электропитания КЦОИ приведены на рис. . Здесь выделены: подсистема 1 – городское электроснабжение, формализуемое как основная и резервная подсистемы; подсистема 2 – система электропитания КЦОИ, включая

главный распределительный щит (ГРЩ) во взаимодействии с двумя одинаковыми системами бесперебойного питания (СБП), система кондиционеров (СКВ) поддерживаемая двумя одинаковыми источниками бесперебойного питания (ИБП), сервер, поддерживаемый одним ИБП, диски для хранения информации, поддерживаемые двумя одинаковыми ИБП. Вся подсистема 2 поддерживается дополнительно системой гарантированного электроснабжения с помощью двух дизель-генераторных установок (ДГУ).

Рис. 3 Логические подсистемы фрагмента

Для решения используется модель «Прогноз комплексного качества» инструментария «ПВК оценки качества производственных процессов». Считается, что надежность системы электропитания обеспечивается, если И в 1-й подсистеме, И во 2-й подсистеме в течение прогнозируемого срока не будет нарушений электроснабжения.

Результаты комплексной оценки функционирования системы с использованием АСУ СИО отражены на рисунке 5. Их анализ показывает, что, при реализуемой в рамках АСУ СИО технологии контроля, мониторинга и восстановления целостности наработка системы электропитания на отказ составит 42219 часов, а вероятность надежного функционирования системы равна 0.828.

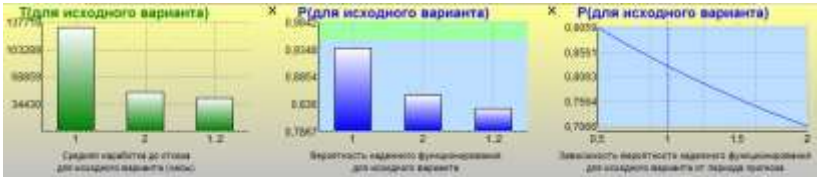

Рис. 5 Результаты оценки надежности системы электропитания при реализации АСУ

В свою очередь, если предположить, что те же самые средства работают под контролем в неавтоматизированном режиме (отсутствует мониторинг, реализуемый в АСУ), с прежними характеристиками, то показатели эффективности принимают значения, приведенные на рис. 6.

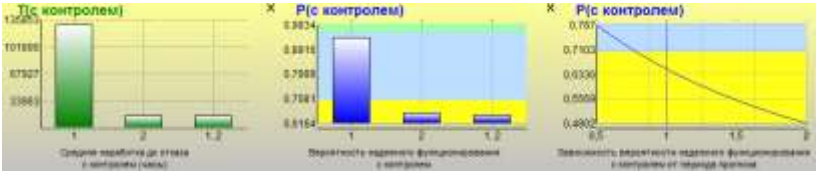

Рис. 6 Результаты оценки надежности системы электропитания, свойственные для неавтоматизированного режима (без внедрения АСУ)

Анализ показывает, что, в неавтоматизированном режиме наработка системы электропитания на отказ составит 16196 часов (это в 2.44 раза меньше, чем при внедрении АСУ), а вероятность надежного функционирования системы в течение года равна 0.649 (в 1.26 раза меньше, чем при внедрении АСУ).

В свою очередь, результаты анализа рисков показывают, что с внедрением АСУ СИО интегральный риск нарушения целостности системы электропитания в течение 0.5 – 2-х лет, изменяемый в диапазоне 0.0053 до 0.1145, в 4-8 раз ниже по сравнению с

неавтоматизированным режимом, когда риск колеблется от 0.0423 до 0.4564.

Таким образом, полученные результаты моделирования характеризуют эффективность внедрения АСУ СИО на рассмотренном фрагменте: наработка на отказ возрастает в 2.4 раза, а риски уменьшаются в 4-8 раз за счет рационального применения системного контроля, мониторинга и восстановления целостности системы.

Заключение

Реализация предложенных вероятностных моделей и методов управления техногенными рисками для критически и стратегически важных объектов РФ развивает существующие подходы к обеспечению безопасности и позволяет на современной научно-методической основе строить стратегию управления рисками, определять допустимые риски по «прецедентному принципу», сравнивать и в упреждающем режиме обосновывать рациональные меры контроля, мониторинга и восстановление нарушаемой целостности. Это позволяет поддерживать решения руководства предприятий в выработке эффективных упреждающих мер противодействия рискам и целенаправленных действий по предотвращению или ограничению угрозы жизни и здоровью персонала предприятий и проживающего вблизи населения, к снижению экономических потерь и материального ущерба предприятий при реализации различного рода угроз.

Литература

1. Гуд Г.Х., Макол Р.З**.** Системотехника: Введение в проектирование больших систем. – М.: Советское радио, 1962. – 383 с.
2. Моисеев Н.Н. Математические задачи системного анализа. – М.:

Наука, 1981. – 488 с.– 239 с.
3. Дружинин В. В., Конторов Д. С. Системотехника -М.:Радио и связь, 1985.- 200с.
4. Дружинин Г.В. Надежность автоматизированных производственных систем. — 4-е изд., перераб. и доп.—М.: Энергоатомиздат, 1986.-480 с.
5. Байхельт Ф., Франкен П. Надежность и техническое обслуживание. Математический подход. М.: Радио и связь, 1988. -392с.
6. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: ВПК, 2008. – 404с.
7. Григорьев Л.И., Кершенбаум В.Я., Костогрызов А.И. Системные основы управления конкурентоспособностью в нефтегазовом комплексе – М.:НИНГ, 2010, 374с.
8. Andrey Kostogryzov, Andrey Nistratov, George Nistratov SOME APPLICABLE METHODS TO ANALYZE AND OPTIMIZE SYSTEM PROCESSES IN QUALITY MANAGEMENT // InTech, 2012, ISBN979-953-307-778-8, 2012, pp. 127-196. http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management
9. Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov G. Prediction and optimization of system quality and risks on the base of modelling processes. American Journal of Operation Researches, Special Issue, Volume 1, 2013, pp. 217-244. http://www.scirp.org/journal/ajor/
10. Andrey Kostogryzov, Andrey Nistratov, George Nistratov The Innovative Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields. International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 3, September 2013, pp. 146-155. http://www.ijeit.com/archive.php