ИЗВЛЕЧЕНИЕ СКРЫТЫХ ЗНАНИЙ ИЗ ТРЕБОВАНИЙ НОРМАТИВНЫХ ДОКУМЕНТОВ И РЕЗУЛЬТАТОВ МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ДЛЯ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ СЛОЖНЫХ СИСТЕМ

дтн, проф. Костогрызов А.И, дтн, проф. Григорьев Л.И.,
дтн, проф. Кершенбаум В.Я., дтн, проф. Степанов П.В.

Введение. О рисках в последнее время заговорили все и уверенно, предполагая, что назначение и сущность рисков всем понятны, а эффекты от управления рисками - очевидны. Однако, если внимательно углубиться в содержание нормативно-методических документов (см. краткий обзор ниже) и современных исследований в области рисков, то бросается в глаза научно-технологический разрыв между системным желанием предотвратить негативное развитие событий и неадекватным упрощением методов прогнозирования рисков для эффективной реализации этого желания. Речь идет об использовании существующих «упрощенных» подходов к прогнозированию рисков на ранних стадиях. Наряду с этим нельзя не отметить сосредоточение исследовательских усилий на технологиях прогнозирования, охватывающих главным образом отдельные периоды реализации угроз и появление возможных ущербов во времени (например, технология ТОКСИ+Risk). Конечно, такое состояние дел можно было бы объяснить определением риска (в общем случае риск оценивается произведением вероятности реализации угроз, приводящих к ущербу, на получаемый при этом ущерб). Но, представляется, что суть проблемы гораздо глубже. Реакция на риски, закрепленная на уровне стандартов (см, например, ГОСТ Р ИСО 31000 «Менеджмент риска. Принципы и руководство»), гласит: первое – попытаться избежать опасного развития события оперативной реакции на первые признаки угроз, а уж потом, если угрозы реализовались – искать пути спасения…. Так вот, складывается впечатление, что именно этим «первым» сегодня пренебрегают. А это – глубоко ошибочная недооценка возможностей адекватного прогнозирования рисков для обеспечения комплексной безопасности (т.е. «надо сосредотачиваться не на лечении запущенной болезни, а на ее предупреждении»)!

Вспомним исследования в области надежности сложных систем (когда понятие рисков лишь зарождалось) - можно констатировать, что в моделировании критичных процессов преимущественное внимание уделялось начальному периоду возникновения первых признаков угроз и их развития. Причем – на уровне функций распределения (ФР), играющих центральное место в теории вероятностей и позволяющих установить прогнозную функциональную зависимость вероятности отказа от времени. Исходя из этой зависимости решались обратные задачи с ответами на вопросы: «Как построить надежные системы из ненадежных элементов? Как сделать так, чтобы гарантированно не было критичных отказов?». Это – итоги воспитания и результаты исследований глубоко уважаемых в мире российских школ надежности (Колмогорова А.Н., Гнеденко Б.В., Дружинина Г.В., Махутова Н.А., Рябинина И.А. и др.).

Сегодня создание технологий эффективного управления рисками, базирующихся на современных методах упреждающего прогнозирования, существенно отстает от потребностей практики. И не только в сфере пожарной безопасности, но и в иных сферах безопасности от техногенных и природных угроз (в промышленности, энергетике, геологоразведке и добыче природных ископаемых, на транспорте и др.). Во многом это объясняется трудоемкостью и высокой стоимостью разработки и сопровождения технологий прогнозирования рисков. Но это лишь пол-правды, самое обидное – наблюдается неполное понимание того, какие скрытые знания и как могут быть извлечены из результатов вероятностного моделирования.

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 стандартом ГОСТ Р ИСО 31000 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.

Первые модели и методы прогнозирования рисков в интересах надежности и безопасности систем были разработаны десятки лет назад. И научные исследования в этом направлении продолжаются [1-13 и др.]. Однако, эта креативная деятельность нуждается в подтверждающих оценках, убеждающих в практичности и эффективности. А для этого необходимо разбираться в «анатомии» зависимостей рисков от периода прогноза и иных характеристик угроз и мер противодействия угрозам. Общение со специалистами показало, что это сегодня - остро актуально. Поэтому в статье даны ответы на «элементарные» и «комплексные» вопросы: «Полезно ли

оценивать риски частотой нарушений? Для чего задаются «допустимые риски»? Какие цели достижимы при существующем «упрощенном» прогнозировании риска? Какие скрытые знания можно извлечь при адекватном прогнозировании рисков? На сколько % реально отличаются результаты при грубом (но широко распространенном) и более детальном моделировании?» и др. Вопросы звучат банально, но складывается впечатление, что для извлечения прагматических эффектов ответы необходимо адекватно переосмыслить.

Полученные результаты направлены на дальнейшее решение проблемы обоснования эффективных упреждающих мер в обеспечение комплексной безопасности на основе вероятностного прогнозирования рисков.

1. Краткий обзор состояния проблемы. Современные тенденции таковы, что сегодня эффективные практические решения и, как следствие, высокий уровень безопасности систем различного функционального назначения во многом связаны с рациональным применением стандартов системной инженерии.

Примечание. Системная инженерия – это избирательное приложение научно-технических усилий на том, как рациональным образом построить и эффективно эксплуатировать сложные системы. В некоторых работах 30-40 летней давности можно встретить перевод выражения «system engineering» на русский язык как «системотехника».

Действующие на практике стандарты лишь отражают суть научно-технических достижений, фиксируя де-юре те требования и рекомендации, выполнение которых может способствовать повышению качества и безопасности систем. К настоящему времени в мире уже не один год действуют стандарты для систем любой области приложения – это набравший популярность ISO 9001 (требования к системе менеджмента качества), ISO/IEC 15288 (первый стандарт по системной инженерии, регламентирует процессы жизненного цикла систем), существенно повлиявшие на последующее развитие стандартизации, а также стандарты ISO серий 14000 (менеджмент экологической безопасности), 18000 (менеджмент охраны труда), 20000 (сервис-менеджмент), 27000 (менеджмент информационной безопасности), 31000 (менеджмент риска) и др. При этом под системой согласно ГОСТ Р ИСО/МЭК 15288-2005 и ГОСТ Р ИСО 9001-2008 понимается комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей.

Среди отечественных нормативных документов необходимо отметить ГОСТ Р 27.001-96 (системообразующий стандарт), ГОСТ 27.002-89 (термины и определения), РД 50-699-90 (общие правила классификации отказов и предельных состояний), ГОСТ 27.003-90 (состав и общие правила задания требований по надежности), ГОСТ Р 27.101-96 (системы обеспечения надежности), ГОСТ 15.206-84 (программы обеспечения надежности), ГОСТ 27.301-96 (основные положения по расчету надежности), ГОСТ 27.310-95 «Надежность в технике. Анализ видов, последствий и критичности отказов», РД 50.656-88 (расчеты безотказности восстанавливаемых изделий), РД 50-423-83, РД 50-490-84 (расчеты долговечности изделий), МР 252-87 (расчет ремонтопригодности), РД в 50-503-84 (расчет комплектов ЗИП), ГОСТ Р 27.302-96 (анализ возможных причин и последствий отказов), ГОСТ 27.410-87, РД 50-476-84 (основные положения испытаний на надежность), РД 50-690-90 (оценка показателей надежности по экспериментальным данным), ГОСТ Р 27.402-96 (планы испытаний для контроля наработки на отказ), ГОСТ Р 27.403 (планы испытаний для контроля вероятности безотказной работы), ГОСТ Р 27.404 (планы испытаний для коэффициента готовности), РД 50-519-84, РД 50-686-89 (методы подтверждения ремонтопригодности), РД 50-424-83 (методы форсированных испытаний), РД 50-706-91 (контроль надежности изделий по параметрам технологического процесса их изготовления). Управление надежностью осуществляется по ГОСТ Р 51901-2002 «Управление надежностью. Анализ риска технологических систем». 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 от 21.07.1997 N 116-ФЗ "О промышленной безопасности опасных производственных объектов" с соответствующими нормативными документами РД 08-120-96 «Методические рекомендации по проведению анализа риска опасных промышленных объектов», РД 03-418-2001 «Методические указания по проведению анализа риска опасных производственных объектов», РД 03-496-2002 «Методические указания по оценке ущерба от аварий на опасных производственных объектах», ПБ 08-624-03 «Правила безопасности в нефтяной и газовой промышленности» и др. 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» и др.

Результаты проведенного научно-технического анализа законов, отечественных и международных стандартов и иных нормативно-методических документов показали следующее.

1. В жизненном цикле остаточный системный риск будет иметь место всегда. На уровне законодательных и нормативно-методических документов для обеспечения безопасности объективно востребованы определение, анализ и контроль рисков и принятие управляющих воздействий для поддержания целостности в результате сравнения прогнозируемого и допустимого рисков.

Примечание. Под целостностью системы, процесса, объекта понимается такое их состояние, при котором обеспечивается достижение целей их функционирования. К примеру, нарушения целостности, возникающие в результате реализации различного рода угроз, могут привести к нарушению безопасности или качества функционирования, к снижению эффективности системы, к аварийным ситуациям и, как следствие, к реальным или возможным ущербам или упущенной выгоде.

Для приложений, в которых уже были многочисленные факты трагедий с гибелью людей - в сфере промышленной, пожарной, радиационной, ядерной безопасности - требования к допустимым рискам выражены количественно, как правило, на вероятностном уровне, и качественно на уровне необходимых требований к исходным материалам, используемым ресурсам, технологиям и начальным состояниям, условиям эксплуатации. Для иных приложений требования к допустимым рискам задаются преимущественно на качественном уровне в форме требований к выполнению конкретных условий.

2. Во всех случаях эффективное управление рисками для любого рода систем при штатных начальных состояниях возможно и целесообразно на основе:

а) использования исходных ресурсов и защитных технологий с более лучшими характеристиками с точки зрения безопасности, в т.ч. для восстановления целостности;

б) рационального применения адекватной системы ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления целостности;

в) рационального применения мер противодействия рискам (включая избегание рисковых ситуаций).

3. Существующие методы количественного анализа рисков в приложении к техногенным ситуациям, характеризуемым множеством случайностей, для различных приложений являются узкоспециализированными и несовместимыми. Вероятностная интерпретация расчетных рисков зачастую принципиально различается. Аналитические зависимости рисков от процессов возникновения, развития и нейтрализации возможных угроз для сложных структур не установлены. 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 в условиях ограничений на допустимые риски и ресурсы.

Именно потому, что существующие технологические решения и методы не позволяют решать задачи оптимизации в жизненном цикле сложных систем, эффект от их использования сегодня существенно ограничен. А это не позволяет утверждать о наличии полного научного решения проблемы обоснования эффективных упреждающих мер в обеспечение комплексной безопасности на основе прогнозирования рисков.

Требование обоснования безопасности в терминах рисков утверждены на уровне Федеральных законов (например, «Технический регламент о требованиях пожарной безопасности» и др.), Федеральных норм и правил (например, «Общие требования к обоснованию безопасности опасного производственного объекта», утв. пр. Ростехнадзором от 15.07.2013 № 306 и др.) и развивающих их методических материалов. Но борьба на первых порах больше идет за число. И для предприятия оказывается важным, чтобы это число было ниже допустимого риска, например 10^{-4}. И неважно, что значение допустимого риска никак аналитически не связано с возможными угрозами, сложностью производства, реализуемыми процессами контроля, мониторинга и восстановления нарушаемой целостности. К примеру, за рубежом задаваемый уровень допустимого риска обосновывается лишь исходя из социально-экономических соображений (если ради выгоды, получаемой от эксплуатации объекта, общество готово пойти на этот риск), сам риск не связывают аналитически с адекватными расчетными методами его прогноза. А дальше начинаются манипуляции вокруг этого числа, включая различные уловки для «подгонки» под требуемый уровень. В ряде логичных случаев это срабатывает. В иных несоответствия «всплывают» при эксплуатации в виде различных нарушений комплексной

безопасности. При этом «допустимый» риск вовсе не играет той главной роли, которую он призван играть в системном анализе – для решения обратных задач (обоснования требований к средствам и методам обеспечения комплексной безопасности при задаваемых условиях). Отсутствует принципиальная возможность эффективного управления рисками за счет численного решения оптимизационных задач в жизненном цикле объектов (систем). А это – не меньшая угроза для самого бизнеса – см. рис. 1. В итоге на многих предприятиях при кажущейся видимости системного контроля ситуаций «с болью в сердце и мыслями об упускаемой выгоде» переживается отсутствие объективных методов прогнозирования рисков.

Рис. 1 Отсутствует принципиальная возможность эффективного управления рисками за счет численного решения оптимизационных задач

2. Анализ показателей рисков и простейшие формы задания уровней допустимых рисков

Ущерб в той или иной степени научились оценивать (учтем, что разброс в оценках может достигать сотен процентов). Поэтому, оставляя оценку возможного ущерба за рамками настоящей работы, остановимся именно на исследованиях вероятностной составляющей риска. Для прогнозирования рисков в интересах упреждения опасного развития событий самое сложное – это построить и правильно интерпретировать зависимость риска от времени прогноза (т.е. ФР времени между соседними нарушениями системной целостности). Какой разброс в оценках возможен здесь? Чтобы ответить на этот и поставленные выше вопросы, необходимо разобраться в типовых показателях рисков и применяемых методах их прогнозирования, в определении и использовании понятия «допустимого риска», а затем сравнить различные варианты.

На практике вероятностные оценки нарушения целостности нередко осуществляют по показателям частоты нарушений или каких-либо неблагоприятных событий. Например, применительно к безопасности это могут быть частоты реализации разнородных угроз, способных при развитии привести к аварии. Т.е. частотой подменяются оценки вероятности нарушения целостности за заданный период. Правомерно ли это?

Из теории вероятностей известно, что для определенной ФР одной из ее характеристик является математическое ожидание (МОЖ) $T_{МОЖ}$. В свою очередь, для ФР времени на нарушение целостности обратное значение МОЖ времени между соседними нарушениями системной целостности представляет собой частоту $\boldsymbol{\lambda}$ нарушений, т.е. $\boldsymbol{\lambda} = 1/ T_{МОЖ}$. Если задавать наступление событий лишь частотой λ (без указания вида самой ФР), то на практике могут получаться существенные различия в оценках. Так, вероятность того, что событие произошло до момента $T_{МОЖ}$, может быть равно 0 при аппроксимации с помощью детерминированной ФР и 0.36 при экспоненциальной аппроксимации. Т.е. в результате ошибочного выбора ФР получается

громадная разница при одинаковом λ! С одной стороны это означает неоднозначность вероятностной оценки событий, ориентируясь лишь на частоту, а с другой – необходимость поиска (или создания) более адекватной ФР времени между соседними нарушениями системной целостности.

Инженеры чаще сегодня ориентируются на экспоненциальную ФР: $P(t, \lambda) = 1 - exp(-\lambda \cdot t)$. Если, например, для времени прогноза порядка года положить λ от 10^{-3}раз в год и меньше, то с точностью до $o(\lambda^2 \cdot t^2)$ по формуле Тэйлора $P(t, \lambda) \approx \lambda \cdot t$. И, если t=1 год, то абсолютное значение частоты, убрав размерность, практически совпадает с вероятностью. Именно малостью значений $\lambda \cdot t$ объясняется возможность оперирования частотой вместо вероятности нарушения. Если же значение $\lambda \cdot t$ возрастает, то оно способно превысить 1 и по определению в общем случае не может восприниматься как вероятность. В качестве показателя риска совершенно корректно ориентироваться на вероятность нарушения с учетом возможного ущерба.

Особое значение имеет понятие «допустимого риска» (по сути - это должен быть результат согласия всех вовлеченных в небезопасный бизнес сторон с тем условием, что он не губит бизнес, всеми однозначно интерпретируется, не исключая аварийных ситуаций, и научно обоснован). Зачастую «допустимый риск» трактуется как «пограничная полоса», т.е. предполагается, что если не пересекаешь эту полосу – нарушений не будет. Но ведь это не так! Остаточный риск все-равно сохраняется. В системном анализе и исследовании операций подобные ограничения рассматриваются как отправная точка для решения обратных задач поиска эффективных упреждающих мер обеспечения целостности системы. Комплексное применение выработанных таким образом мер способствует непревышению допустимого риска (например, допустимого риска аварии). Это – классический подход, который должен работать корректно. А как на самом деле?

Здесь вполне уместно обратиться к сложившейся форме количественного задания требований к уровням допустимых рисков. Простейшими формами задания требований являются:

«частота нарушений не должна превышать допустимого уровня $\lambda_{доп.}$»**;**

и/или «вероятность нарушения в течение времени $t_{зад.}$ не должна превышать допустимого уровня $P_{доп.}(t_{зад.})$ »;

и/или их комбинация.

Какие инженерные объяснения бытуют на практике? – Они таковы:

- если задается ограничение по вероятности $P_{доп.}(t_{зад.})$, это означает, что превышения «пограничной полосы» не должно происходить на интервале времени от 0 до $t_{зад.}$ Для экспоненциальной аппроксимации существует однозначная функциональная зависимость: $\lambda_{доп.} = -ln(1-P_{доп.}(t_{зад.}))$. Т.е. эта зависимость означает, что задаваемой максимально допустимой вероятности нарушения безопасности $P_{доп.}(t_{зад.})$ соответствует значение максимальной частоты нарушений;

- если задаться максимально допустимой частотой нарушений $\lambda_{доп.}$, то в случае применения экспоненциальной аппроксимации подразумевается связь вероятности нарушений за время *t:* $P(t, \lambda_{доп.}) = 1 - exp(-\lambda_{доп.} \cdot t)$ – т.е. та же условная «пограничная полоса», но уже в виде функции от t и без явной привязки к значению $t_{зад.}$. Этот уровень ограничения сверху по функции $P(t, \lambda_{доп.})$ логично также интерпретировать как «допустимый» для периода времени от 0 до *t.*

Несмотря на явную неполноту простейших форм задания требований к «допустимым рискам» (фактически – лишь задание в одной или нескольких точках) и отсутствие какой-бы то ни было связи с видом реальной ФР времени между соседними нарушениями системной целостности (зависящей на практике от многих параметров: структуры системы, разнородности угроз, разнотипности мер противодействия угрозам и пр.), эти формы прижились. В дальнейшем изложении работы будем ориентироваться именно на эти приведенные выше простейшие формы требований к «допустимым рискам». Они также позволяют извлечь очень полезные знания.

Действующие сегодня многие нормативы безопасности характеризуют частоту нарушений для отдельных средств и систем на уровне 10^{-3} – 10^{-7} раз в год. По сути это – одно нарушение за тысячи лет, т.е. «вживую» непроверяемо! На практике оценивается с помощью математического и/или физического моделирования. А по статистике лишь на предприятиях нефтегазового комплекса России – это тысячи аварийных ситуаций ежегодно, инцидентов же с предотвращением аварий происходит на порядки больше! Соответственно, возникает важный вопрос: а какую частоту нарушений использовать при оценках риска и где ее взять? – Если только частоту событий, завершившихся авариями, то получаемые оценки будут успокаивающе заниженными! Это – выходные, а не входные данные, и все это понимают. Представьте: если руководствоваться

этими частотами и учесть, что 50-70% аварий происходит по причине «человеческого фактора», это означает, что частота критичных ошибок со стороны человека составляет на опасных предприятиях 1 раз в тысячи лет! Но ведь практика свидетельствует, что это не так! Ошибки допускаются гораздо чаще (например, раз в месяц), но они контролируются и большинство из них своевременно исправляется. Как следствие этого противодействия угрозам достигается обеспечение безопасности. Ответ напрашивается очевидный - частота нарушений, используемая при оценках риска, сама должна рассчитываться по результатам вероятностного моделирования либо браться из «жизни» с учетом наблюдаемых первых признаков угроз, мелких и крупных отступлений от правил безопасности. Для адекватного моделирования важна не конечная частота нарушений целостности, а частота изначальных разнородных событий, ведущих к нарушениям, в т.ч. связанных с «человеческим фактором» (например, частота инцидентов, как приведших к авариям, так и нейтрализованных за счет мер контроля, технического обслуживания и своевременной реакции на начальные признаки развития угроз). Использование именно этой суммарной частоты, на порядки превышающей предоставляемую стандартной статистикой частоту произошедших нарушений, предоставляет возможность научного обоснования эффективных упреждающих мер для обеспечения комплексной безопасности.

3. Некоторые способы повышения адекватности прогнозирования рисков

Для практического применения рекомендуются методы, описанные в приводимой литературе (далеко не исчерпывающей список адекватных моделей), где субъективные весовые коэффициенты исключены. Последнее – важно, т.к. продолжают широко применяться методы, базирующиеся на экспертных оценках, в т.ч. с использованием различного рода субъективно назначаемых коэффициентов (что еще как-то воспринималось на заре исследований, но сегодня не имеет прямого отношения к современной науке).

Суть – в разработке и использовании математических моделей для расчетов показателей рисков, базирующихся на классически построенном вероятностном пространстве (Ω, B, P), где Ω – конечное пространство элементарных событий; B – класс всех подмножеств множества Ω, удовлетворяющий свойствам сигма-алгебры; P – вероятностная мера на пространстве элементарных событий. При этом, поскольку пространство $\Omega=\{\omega_k\}$ – конечное, в моделях установлено отображение $\omega_k \rightarrow p_k = P(\omega_k)$ такое, что $p_k \geq 0$ и $\sum_k p_k = 1$.

При оценках защищенности систем от опасных воздействий в качестве основного показателя планируется использовать риск нарушения целостности в течение заданного периода времени для составных компонентов и системы в целом. А в качестве дополнительных показателей будут использованы: средняя наработка на нарушение целостности составных компонентов и системы в целом, среднее время восстановления системы с учетом рисков, математическое ожидание возможных ущербов.

При этом само понятие приемлемого уровня целостности должно быть определено в терминах штатного состояния системы. Они должны формулироваться с учетом необходимости выполнения системой задаваемых функций в реальных (в т.ч. небезопасных) условиях функционирования.

Для сложных структур предлагается нетрадиционный метод комбинации моделей, позволяющий в автоматическом режиме генерировать новые модели, за счет чего окажется возможным расчет формализованных показателей рисков. При этом появляется возможность рассмотрения разнородных угроз возможного возникновения и развития чрезвычайных ситуаций природного и техногенного характера с учетом предпринимаемых технологических мер контроля, мониторинга и восстановления целостности (как системы в целом, так и составных подсистем).

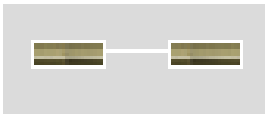
Основные идеи комбинации и, как следствие, автоматической генерации новых моделей для комплексных исследований заключаются в следующем.

1-я идея. Поскольку модели математические, то путем смыслового переобозначения исходных данных и, соответственно, расчетных показателей возможно использование одних и тех же моделей для оценки разных показателей. Идея упомянута лишь для понимания логики в генерации моделей.

2-я идея. Для комплексной оценки в приложении к системам сколь угодно сложной параллельно-последовательной структуры существующая модель может быть развита традиционными методами теории вероятностей. Сложность оценивается количеством составных

элементов. Для этого надо знать наработку на нарушение целостности каждого из элементов. С учетом идеи 1 далее достаточно логического переопределения понятия наработки (например, для анализа надежности это – наработка на отказ, а для безопасности – наработка на нарушение целостности). В качестве логических элементов могут выступать отдельные составные элементы системы, объекта или отдельные объекты или совокупности объектов.

Для простейшей структуры из двух независимых элементов, соединенных последовательно, что означает логическое соединение «И» (рис. 2), или параллельно, что означает логическое соединение «ИЛИ» (рис. 3) в условиях независимости выражения для ФР – классические. Тогда логическая интерпретация элементарного события «нарушение безопасности» для представления системы в виде последовательного соединения следующая: чтобы система, состоящая из подсистем, была в течение времени прогноза в состоянии безопасности, необходимо, чтобы все подсистемы («И» 1-я, «И» 2-я,…, «И» последняя) находились все это время в состоянии безопасности. Логическое выражение «ИЛИ» используется, если есть резервирование.



Функция распределения (ФР) времени наработки $B(t) = 1 - [1 - B_1(t)][1 - B_2(t)]$

Рисунок 2 - Система из последовательно соединенных элементов

ФР времени наработки $B(t) = B_1(t)B_2(t)$

Рисунок 3 - Система из параллельно соединенных элементов

Исходные ФР рассчитываются по адекватным моделям или при упрощенном варианте – аппроксимируются экспоненциальным распределением. Применяя приведенные рекуррентные соотношения (рис. 2-3), можно получать соответствующие оценки для сколь угодно сложной логической структуры с параллельно-последовательным соединением элементов. Для новой структуры - это уже новые вероятностные модели, генерируемые по формулам на рис. 2-3. Именно эти соотношения реализованы в программных инструментариях, поддерживающих прогнозирование рисков и обоснование эффективных упреждающих мер в обеспечение комплексной безопасности.

3-я идея. На выходе моделирования системы – вероятность нарушения целостности в течение заданного прогнозного периода времени – см. рис. 4, 5. В рамках предлагаемых технологий ожидается численный просчет этой вероятности для всех точек заданного периода прогноза ($T_{зад.}$) от нуля до бесконечности для каждого элемента. В итоге будут получены траектории ФР времени сохранения целостности по каждому из элементов в зависимости от реализуемых мер контроля, мониторинга и восстановления целостности. В свою очередь, известный вид этой ФР, построенной по точкам с использованием программных комплексов, позволит традиционными методами математической статистики определить среднее время сохранения целостности каждого из элементов системы. А это – необходимые исходные данные для применения генерируемых моделей и, соответственно, оценки показателей функционирования некой системы параллельно-последовательной структуры любой степени сложности. Именно в этом – главное отличие предлагаемых нами авторских решений.

Рис. 4 Суть прогнозирования в терминах функции распределения времени до нарушения безопасности

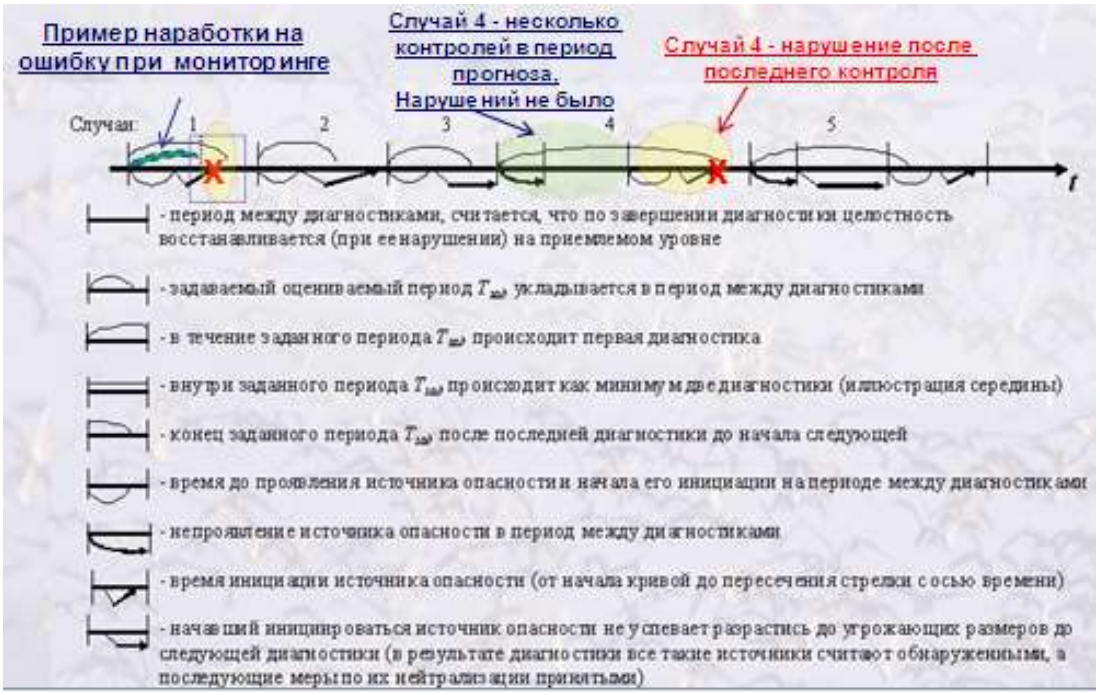


Рис. 5 Случаи 1, 4 – нарушение безопасности, 2, 3, 5 – отсутствие нарушений в период прогноза Тзад.

Для указанного множества подсистем, обеспечивающих функционирование анализируемого объекта, оценивается интегральный показатель - риск нарушения целостности как системы в целом, так и составных подсистем - с учетом предпринимаемых технологических мер контроля, мониторинга и восстановления целостности. И далее, исходя из этого показателя для различных значений заданного периода прогноза, рассчитывается средняя наработка системы до нарушения целостности (по идеям 1-3).

Определение достигаемых количественных значений частных и интегральных показателей рисков по единой методике, носящей универсальной характер, даст представление об уровне допустимого риска не только для 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 критичных 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 объекта допустимый уровень риска будет оставаться уникальным, он должен быть количественно обоснован непосредственно руководством предприятия.

Эффективное упреждающее управление процессами возникновения, развития, контроля и нейтрализации возможных угроз осуществляется в рамках формальных постановок оптимизационных задач путем целенаправленного использования моделей и выбранных критериев рациональности при ограничениях на ресурсы и варианты реализации процессов. Фокусирование внимания именно на процессах позволяет использовать для их описания лишь характеристики времени (среднее время или частота наступления событий), безразмерные или стоимостные характеристики, свойственные для объектов и систем различных приложений. Степень достижения ожидаемых результатов оценивается вероятностными показателями (например, «риск нарушения комплексной безопасности в течение заданного срока»), рассчитываемыми с использованием предлагаемых математических моделей.

Иллюстрируемые на рис. 6 постановки служат классическими ориентирами на пути целенаправленного решения задач эффективного управления рисками в жизненном цикле систем (они не исчерпывают всего множества возможных практических вариантов постановок). Решение поставленных задач заключается в вероятностном моделировании процессов возникновения, развития, контроля и нейтрализации возможных угроз.

Рисунок 6 – Пример постановки задач управления рисками в жизненном цикле систем

Смысл применения оптимизационных постановок задач в следующем – за счет упреждающего выбора рациональных значений управляемых параметров анализируемых сценариев угроз и реализуемых мер упреждения и реакции:

избежать излишних затрат при допустимых рисках и заданных критичных ограничениях на этапах концепции и ТЗ, разработки, оборудования и технического обслуживания объектов, систем и отдельных подсистем;

минимизировать риски в процессе эксплуатации объектов, систем и отдельных подсистем при заданных критичных ограничениях.

За рубежом аналитические методы прогноза риска строятся традиционными методами теории вероятностей. В некоторой мере построение этих методов аналогично предлагаемым. Разница в том, что планируемые к использованию авторские модели были созданы раньше (обеспечивая приоритет в отличие от альтернативных моделей) и с учетом большего количества системных процессов контроля и мониторинга и доведены до уровня автоматической генерации моделей в процессе построения сложных структур и проведения расчетов, чему практических аналогов нет. Западными учеными для некоторых систем простой структуры (несколько единиц элементов) аналитические зависимости выводятся вручную, занимая в печатном виде десятки страниц - например, в работах проф. Коловровского К. (см. K.Kolowrocki and J.Soszynska-Budny, *Reliability and Safety of Complex Technical Systems and Processes*, DOI:10.1007/978-0-85729-694-8, Springer-Verlag London Limited 2011 – 405p.), проф. Френкеля И. и др.(Frenkel I., Lisnianski A., Karagrigoriou A., Kleyner A. APPLIED RELIABILITY ENGINEERING AND RISK ANALYSIS: PROBABILISTIC MODELS AND STATISTICAL INFERENCE (QUALITY AND RELIABILITY ENGINEERING SERIES). Wiley, 2013. ISBN-10: 1118539427, ISBN-13: 978-1118539422). Соответственно, для новых структур при таком подходе требуются новые предварительные выводы формул, а это – неоправданные трудозатраты с потенциальной возможностью математических ошибок и ошибок программиста. Такой традиционный подход сдерживает широкое применение подобных результатов для перспективных систем сложной структуры, состоящей из десятков, сотен и более элементов. Тем самым предлагаемые модели имеют повышенную конкурентоспособность на международном научно-техническом рынке.

4. Какие скрытые знания могут быть извлечены из более адекватной ФР?

На рис. 7 проиллюстрированы ограничения к допустимым рискам, экспоненциальная и некая более адекватная ФР времени между соседними нарушениями системной целостности с одинаковой частотой нарушений λ.

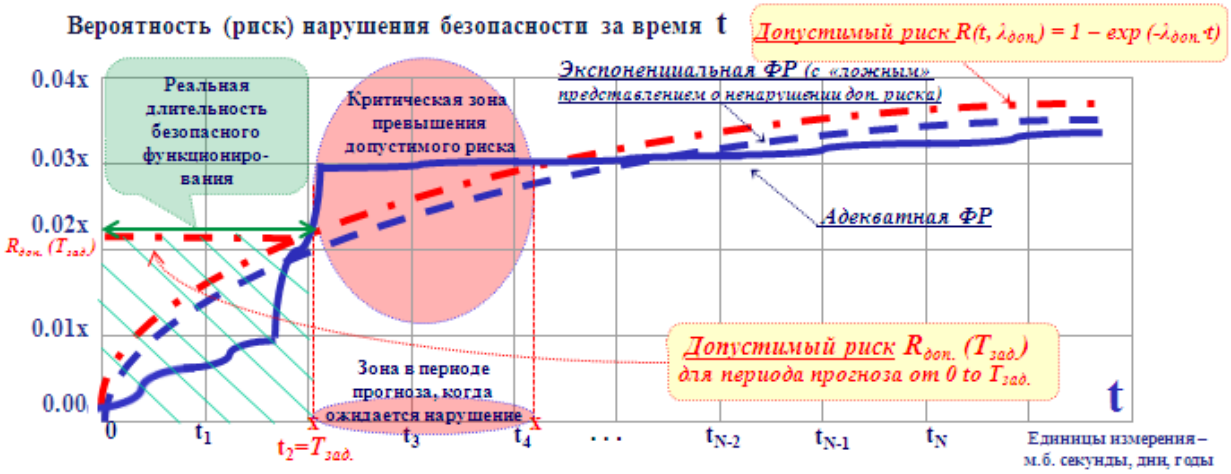


Рис. 7 Фрагменты ФР, демонстрирующие возможные варианты зависимостей ограничений на допустимый риск, экспоненциальную и более адекватную аппроксимацию ФР

Ориентируясь на аппроксимацию экспоненциальной ФР, можно легко констатировать выполнение или невыполнение задаваемых требований к уровню допустимых рисков. Ниже «пограничной полосы» - требование выполнено, выше – не выполнено! И это – все извлекаемые знания… Из «плюсов» - лишь удобство сравнения. И все!

Ориентируясь на более адекватную ФР (например – из раздела 3), если при ее создании для каждого критичного составного элемента задавались характеристики угроз и предпринимаемые меры противодействия угрозам, возможно извлечение следующих знаний (см. рис.7):

- рассчитать реальную зависимость вероятности нарушения целостности системы и составных подсистем от характеристик разнородных угроз и предпринимаемых мер противодействия угрозам;

- оценить точность прогнозирования по сравнению с экспоненциальной аппроксимацией ФР;

- определить период эффективного функционирования, в течение которого нарушений не ожидается (по критерию непревышения допустимых рисков) – для определения упреждающих противодействий угрозам за время, не превосходящее данного периода;

- выделить зоны прогнозных периодов времени, когда возможны нарушения требований допустимого риска – для определения упреждающих противодействий угрозам или обоснованное уточнение риска для этих зон (в т.ч. избегание рисков или смягчение требований из-за неизбежного резкого возрастания рисков в пределах, признанных приемлемыми);

- сравнить периоды эффективного функционирования, в течение которого нарушений не ожидается (по критерию непревышения допустимых рисков) с соответствующими периодами при экспоненциальной аппроксимации ФР.

Кроме того, построив более адекватную ФР, возможно обычными расчетными методами извлечь дополнительные знания (см, например, [8-14]):

- рассчитать среднюю наработку на нарушение и, как обратную к ней величину - частоту нарушений целостности системы и составных подсистем в условиях задаваемых разнородных угроз и предпринимаемых мер противодействия угрозам;

- сравнить среднюю наработку на нарушение целостности или частоту нарушений целостности системы (и подсистем) со средней наработкой или частотой нарушений целостности при экспоненциальной аппроксимации ФР.

Кроме этого, зафиксировав уровни «допустимых рисков» для системы и составных подсистем, а также считая неизменными все параметры, за исключением одного, возможно решение различные оптимизационных задач, связанных с обоснованием эффективных упреждающих мер обеспечения целостности системы в условиях разнородных угроз. Классическими задачами являются максимизация эффекта (выгоды, уровня качества или безопасности и др.) или минимум рисков при ограничениях или минимизация затрат при ограничениях на допустимые риски и иных ограничениях.

5. Примеры моделирования и сравнительные оценки точности прогнозирования рисков

Возможности моделирования и сравнительные оценки точности прогнозирования рисков проведем на следующих примерах (для расчетов использовались модели, описанные в разделе 3 и поддерживаемые инструментально-моделирующими комплексами «Моделирование процессов», свидетельство Роспатента №2006610219, «Программно-вычислительным комплексом оценки качества производственных процессов», свидетельство Роспатента №2010614145).

Пример 1 [4]. Рассмотрим возможности современных систем противоаварийной защиты (ПАЗ) некой АСУ технологическими процессами (АСУ ТП) на объектах нефтегазового комплекса. Выполнение функций противоаварийной защиты, в т.ч. пожарной безопасности, осуществляется, как правило, на следующих принципах обеспечения многоуровневой противоаварийной защиты (самый высокий уровень обозначает остановку газопромысла в целом), учета взаимного влияния отдельных установок, использования результатов диагностики приборов и технологического оборудования. ПАЗ выделена в АСУ ТП функционально. Для обеспечения готовности к срабатыванию ПАЗ и отказоустойчивости АСУ ТП осуществляется:

резервирование процессорных модулей всех систем автоматического управления технологических цехов и оборудования;

резервирование модулей ввода для входных сигналов, по которым запускается ПАЗ;

передача данных от средств пожарогазобезопасности на отключение технологического оборудования по физическим линиям связи с дублированием;

создание системы экстренного останова;

многократное дублирование датчиков с постоянной диагностикой;

применение интеллектуальных приборов с функцией самодиагностики;

резервирование источников питания и др.

При обнаружении аварийной ситуации в автоматическом режиме, с целью исключения ложного срабатывания, запуск ПАЗ осуществляется после того, как измеряемый параметр превысил критическое значение в течение 0,5 секунд. После запуска противоаварийной защиты алгоритм действий выполняется независимо от текущих значений измеряемых и контролируемых параметров, приведших к запуску ПАЗ. Дистанционное управление с пульта оператора для цеха (агрегата) на время действия ПАЗ блокируется. Управление с пульта оператора возвращается

после завершения действия ПАЗ (истечения соответствующей временной задержки) по нажатию деблокирующей кнопки на мнемосхеме оператором.

В результате анализа ситуаций, являющихся источником подключения элементов противоаварийной защиты, сформированы следующие исходные данные для моделирования ПАЗ: (j=1,3) частота возникновения источника опасности = 1 раз в час, среднее время активизации источника опасности = 10 секунд, время между диагностиками целостности = 0.5с, длительность диагностики с выполнением действий противоаварийной защиты = 10с, наработка на ошибку = 2000 часов (соизмеримо с наработкой аппаратуры на отказ, периодом между техническим обслуживанием и профилактическими настройками).

Сравнение с возможностями ручной реакции на опасные воздействия по результатам контроля рассмотрим на примере процессов, связанных с хранением, подачей, отпуском и дренажными сбросами выветренного конденсата и дизельного топлива. В результате анализа ситуаций, являющихся источником ручной реакции на опасные воздействия по результатам контроля процессов сформированы следующие исходные данные для моделирования: (j=2,4) частота возникновения источника опасности = 1 раз в неделю (изменения показателей, свидетельствующие об ухудшении производственного процесса), время активизации источника опасности = 8 часов (соизмеримо с длительностью смены), время между диагностиками целостности = 8 часов (1 раз за смену), длительность диагностики с восстановлением целостности = 8 часов (включает непосредственно контроль и принятие, при необходимости, мер восстановления качества производства), наработка на ошибку = 1 месяц.

Исходные данные для моделирования с использованием подсистемы «Защищенность от опасных воздействий» инструментария «ПВК оценки качества производственных процессов» приведены на рис. 2 сверху. Требуется спрогнозировать степень защищенности предприятия в течение года (j=1,2) и 5 лет (j=3,4) и сравнить эффективность автоматической противоаварийной защиты (j=1,3) и ручной реакции на опасные воздействия по результатам контроля типовых процессов (j=2,4).

Результаты моделирования. Результаты оценки вероятности безопасного функционирования АСУ ТП показали следующее (см. рис. 8).

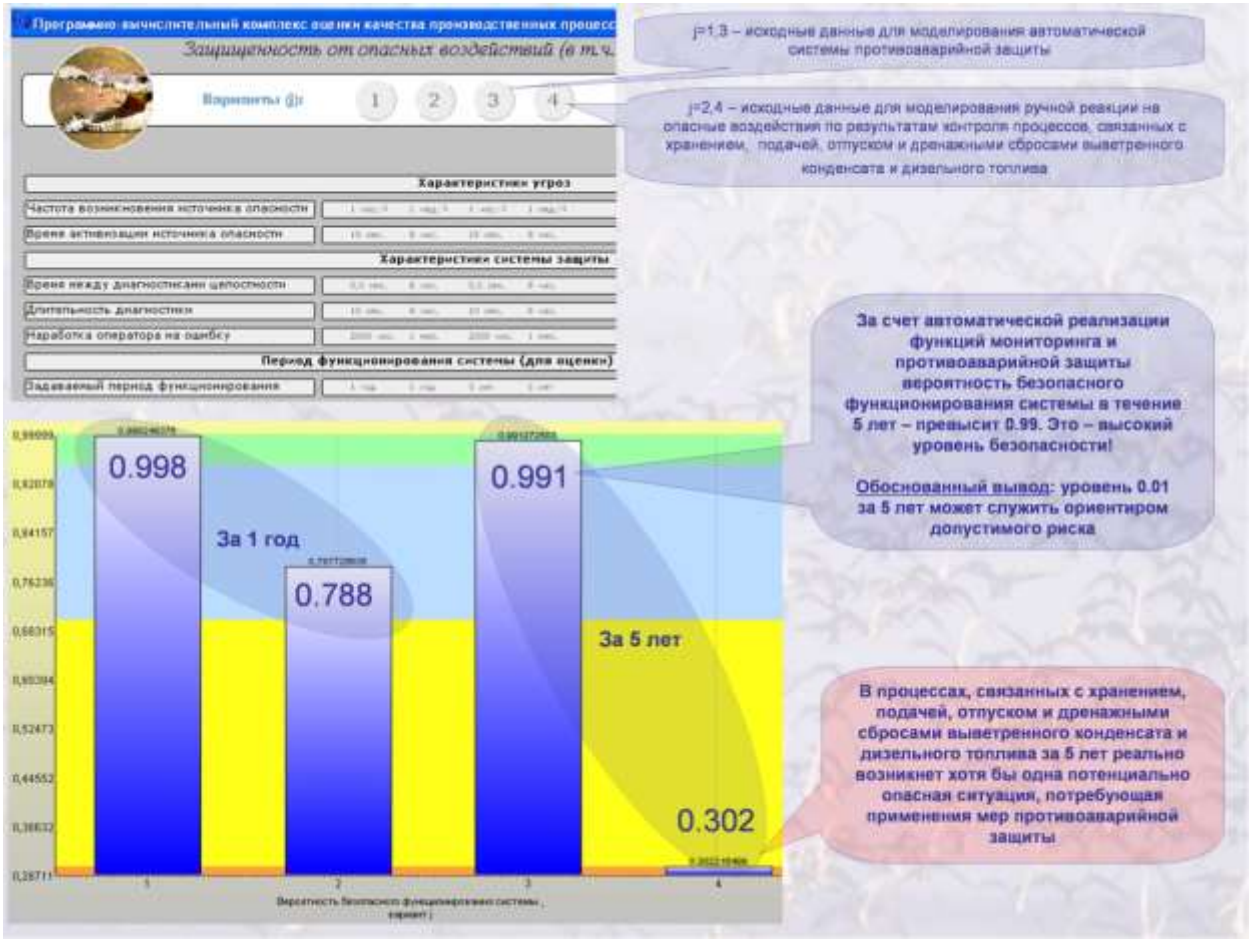


Рис. 2 Результаты сравнения ручной реакции на опасные воздействия и автоматической противоаварийной защиты (риск = дополнению до 1 изображенной вероятности безопасного функционирования АСУ ТП)

За счет автоматической реализации функций мониторинга и противоаварийной защиты при заданных исходных данных вероятность безопасного функционирования системы в течение года составит 0.998, а в течение 5 лет – превысит 0.99. Это – высокий уровень безопасности, т.е. уровень 0.01 за 5 лет может служить ориентиром допустимого риска! В свою очередь, за счет своевременной реакции на результаты периодического контроля процессов, связанных с хранением, подачей, отпуском и дренажными сбросами выветренного конденсата и дизельного топлива, вероятность безопасного функционирования в течение года составляет 0.79, а в течение 5 лет – 0.30. Последнее означает, что в процессах, связанных с хранением, подачей, отпуском и дренажными сбросами выветренного конденсата и дизельного топлива, за 5 лет реально возникнет хотя бы одна потенциально опасная ситуация, потребующая применения мер противоаварийной защиты. Риск наступления такой ситуации составляет около 0.70, что означает острую необходимость поиска новых путей повышения безопасности с оценкой эффективности по результатам моделирования.

Пример 2. Учитывая важность «человеческого фактора» в вопросах пожарной безопасности гипотетичного объекта, в противодействии различного рода угрозам для опасного производства, зададимся частотой возникновения скрытых или явных угроз 1 раз в месяц, среднее время развития угрозы (от появления первых признаков критичной ситуации до пожара или аварии) – 1 сутки. Рабочая смена – 8 часов. Системный контроль объекта – 1 раз за смену, положим, средняя длительность системного контроля – 10 мин. (предполагается, что при выявлении первых признаков нарушений целостности восстановление объекта ожидается также за 10 минут, что в реальности – далеко не так (учтем далее в примерах 3-6)). Полагается, что работники средней и высокой квалификации способны к выявлению признаков критичной ситуации после их появления, а низкоквалифицированные – к этому неспособны. Пусть далее работники средней квалификации могут допускать ошибки в среднем не чаще 1 раза в месяц, а работники высокой квалификации – не чаще 1 раз в год. Как влияет учет квалификации работников на прогнозируемые риски нарушения целостности за год и за 10 лет эксплуатации объекта?

Результаты моделирования. Результаты прогноза показывают: риски для неквалифицированных работников (ошибающихся чаще 1 раза в месяц) свидетельствуют о неизбежности нарушений с вероятностью, близкой к 1. Риск нарушения для специалистов средней квалификации за год составит около 0.007, за 10 лет – 0.067, а для специалистов высокой квалификации – за год 0.0006, за 10 лет – 0.0058.

Пример 3. Сосредоточимся на анализе ошибок высококвалифицированных специалистов Повышая адекватность моделирования, в дополнение к исходным данным примера 2 учтем, что время восстановления нарушенной целостности системы составит не 10 минут, а 1 сутки (что более адекватно характеризует противодействие большинству угроз, развивающихся в течение суток и более, но не охватывает быстрореализуемых угроз, например, в результате умышленного поджога или взрыва).

Какие скрытые знания могут быть извлечены из результатов прогнозирования рисков для этих видоизмененных исходных данных?

Извлеченные знания. Результаты фрагмента ФР, рассчитанные по моделям, изложенным выше, показывают: риск нарушения целостности возрастет с 0.0006 (за год) до 0.0119 (за 20 лет) – см. рис. 9 сверху. При этом средняя наработка на нарушение целостности с возможным ущербом составит 493 года, т.е. около 0.002 раз в год. Если сравнивать с изначальной наработкой на ошибку (1 раз в год), это – почти в 500 раз больше. А, если сравнить с изначальной частотой инцидентов (1 раз в месяц), частота нарушений с возможным ущербом становится меньше в 6000 раз! И такой эффект достигнут за счет предпринимаемых мер контроля, мониторинга и восстановления целостности в случае выявления признаков развития угроз.

Рис. 9 Результаты моделирования для примеров 3 и 4

Если сравнивать с экспоненциальной аппроксимацией процессов с той же частотой, для которой риск нарушения целостности будет расти с уровня 0.002 (за год) до 0.04 (за 20 лет), отличие в 3.3 – 3.4 раза. Чтобы почувствовать, насколько это много, достаточно констатировать, что для построенной ФР граница допустимого риска 0.002 будет достигнута не за 1 год прогноза (как для экспоненциальной аппроксимации), а за 3 года, т.е. период эффективного функционирования в 3 раза выше!

Пример 4. На опасном производстве критичные операции осуществляются специалистами во взаимодействии (т.е. в режиме резервирования, один контролирует и подстраховывает действия другого). Формально они действуют как параллельные элементы с резервированием – см. рис. 3. Тем самым учет такого взаимодействия позволяет повысить адекватность моделирования. Рассмотрим показатели функционирования такой системы (все исходные данные для каждого из параллельных элементов – те же, что в примере 3).

Извлеченные знания. Результаты фрагмента ФР, рассчитанные по моделям, изложенным выше, показывают (см. рис. 9 снизу): риск нарушения целостности возрастет с 0.0000003 (за год) до 0.00014 (за 20 лет). При этом средняя наработка на нарушение целостности составит 663 года, т.е. около 0.0015 раз в год, что на 32.6% реже, чем в примере 2. А, если сравнить с изначальной частотой инцидентов (1 раз в месяц) частота нарушений становится меньше в 8000 раз!

Если сравнивать с экспоненциальной аппроксимацией процессов с той же частотой, для которой риск нарушения целостности возрастет с 0.0015 (за год) до 0.03 (за 20 лет), отличие – от двух сотен до 5000 раз! Для построенной, более адекватной ФР граница допустимого риска 0.002 будет достигнута не за 1.3 года прогноза (как для экспоненциальной аппроксимации), а за 195 лет, т.е. период эффективного функционирования в 150 раз выше! И такой эффект достигнут за счет взаимной подстраховки высококвалифицированных специалистов.

Пример 5. Сложная система из 9 объектов, обслуживаемых высококвалифицированными специалистами. Чем крупнее производство – тем более высокие риски ожидаются. Но насколько эти риски высокие?

Положим, на каждом из объектов задействованы специалисты, взаимно контролирующие и подстраховывающие свою деятельность. Их деятельность моделируется с использованием идей раздела 4 – см. рис. 10. Большая адекватность достигается усложнением структуры системы до 9 подсистем. Безопасность системы обеспечивается, если «И» в 1-й подсистеме, «И» во 2-й … «И» в 9-й подсистеме безопасность обеспечена. Исходные данные - те, же, что и в примере 4.

Извлечение скрытых знаний. Результаты фрагмента ФР, рассчитанные по моделям, изложенным выше, показывают (см. рис. 10 вверху): риск нарушения целостности возрастет с 0.000003 (за год) до 0.0013 (за 20 лет). При этом средняя наработка на нарушение целостности составит 283 года, т.е. около 0.0035 раз в год, что в 2.3 раза чаще, чем в примере 3. Т.е. существенное усложнение структуры привело к тому, что частота нарушений возросла в 2.3 раза. А, если сравнить с изначальной частотой инцидентов (1 раз в месяц) частота нарушений становится меньше в 3430 раз!

Рис. 10 Результаты моделирования для примеров 5 и 6

Если сравнивать с экспоненциальной аппроксимацией процессов с той же частотой, для которой риск нарушения целостности возрастет с 0.0035 (за год) до 0.07 (за 20 лет), отличие – от 54 до 1167 раз! Для построенной, более адекватной ФР граница допустимого риска 0.002 будет достигнута не за 7 месяцев прогноза (как для экспоненциальной аппроксимации), а за 24 года, т.е. период эффективного функционирования почти в 41раз выше!

Пример 6. Анализ нарушений для сложной системы, безопасность контролируется среднеквалифицированными специалистами. Наличие «человеческого фактора» существует из-за того, что далеко не всегда и везде удается привлечь высококвалифицированных специалистов. Насколько риски возрастут, если в системе примера 5 используются не высококвалифицированные специалисты, а специалисты средней квалификации?

Извлечение скрытых знаний. Результаты фрагмента ФР, рассчитанные по моделям, изложенным выше, показывают (см. рис. 7): риск нарушения целостности возрастет с 0.0009 (за год) до 0.25 (за 20 лет). При этом средняя наработка на нарушение целостности составит 24 года, т.е. около 0.04 раз в год, что на порядок меньше, чем для высококвалифицированных специалистов примера 4.

Если сравнивать с экспоненциальной аппроксимацией процессов с той же частотой, для которой риск нарушения целостности возрастет с 0.04 (за год) до 0.55 (за 20 лет), отличие – от 2.2 до 44.4 раз! Для построенной, более адекватной ФР, граница допустимого риска 0.002 будет достигнута не за месяц прогноза (как для экспоненциальной аппроксимации), а за 2 года, т.е. период эффективного функционирования почти в 24 раза выше.

Важное замечание: во всех примерах для моделирования использованы правдоподобные исходные данные, свойственные различным предприятиям опасного производства (например- частота возникновения скрытых или явных угроз со стороны «человеческого фактора» - 1 раз в месяц). Они никак не «подгонялись» под нормативные допустимые риски для опасного производства (10^{-3} – 10^{-7} опасных событий в год и реже). Но в результате применения более адекватных моделей получены эффекты с выходными оценками рисков, очень близкими к нормативным. Разница – лишь в том, что в итоге возможно построение зависимостей (от чего и в какой степени зависит интегральный риск), с помощью которых возможно решение задач синтеза.

Выводы

1. Анализ нормативных документов показал: для адекватного прогнозирования рисков важна не конечная частота нарушений целостности, а частота изначальных разнородных событий, ведущих к нарушениям, в т.ч. связанных с «человеческим фактором». Использование именно этой суммарной частоты, на порядки превышающей предоставляемую стандартной статистикой частоту произошедших нарушений, предоставляет возможность научного обоснования эффективных упреждающих мер для обеспечения целостности системы в условиях разнородных угроз.

2. Предложенные способы повышения адекватности прогнозирования рисков для сложных структур учитывают применительно к каждому из критичных элементов помимо характеристик разнородных угроз еще и характеристики мер контроля, технического обслуживания и своевременной реакции на начальные признаки развития угроз и позволяют осуществлять построение ФР времени между соседними нарушениями системной целостности и расчет средней наработки системы на нарушение целостности.

3. Проведенные исследования рисков по результатам моделирования сложных систем количественно доказали, что прогнозирование рисков с помощью частоты нарушений и соответствующей экспоненциальной аппроксимации времени между нарушениями – это грубый и бесперспективный инженерный способ. Его применение пресущественно искажает вероятностные оценки рисков и не способно обеспечить эффективное противодействие угрозам (отклонения в оценках рисков могут составлять десятки-сотни тысяч процентов (!)). За счет применения более адекватных моделей к анализу «человеческого фактора» доказана возможность снижения частоты нарушений в тысячи раз до уровня 10^{-3} – 10^{-7} раз в год (!) по сравнению с изначальной частотой инцидентов порядка 1 раз в месяц. Сравнение при одинаковой расчетной частоте нарушений показало, что по сравнению с адекватной ФР риски при оценках с помощью экспоненциальной аппроксимации оказываются завышенными в сотни-тысячи раз (!). А для задаваемого допустимого риска прогнозируемый период эффективного функционирования при экспоненциальной аппроксимации оказывается в десятки-сотни раз меньше.

Литература

[1] Kostogryzov A.I. “Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ).” Proceedings of the 34-th Annual Event of the Government Electronics and Information Association (GEIA), Engineering and Technical Management Symposium, USA, Dallas, pp.63-70, 2000.

[2] Костогрызов А.И., Нистратов Г.А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М. Изд.”Вооружение, политика, конверсия”, 2004, 2-е изд.-2005.- 395с.

[3] Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: ВПК, 2008. – 404с.

[4] Григорьев Л.И., Кершенбаум В.Я., Костогрызов А.И. Системные основы управления конкурентоспособностью в нефтегазовом комплексе – М.:НИНГ, 2010, 374с.

[5] K.Kolowrocki and J.Soszynska-Budny “Reliability and Safety of Complex Technical Systems and Processes”, DOI:10.1007/978-0-85729-694-8, Springer-Verlag London Limited, 2011, 405p.

[6] Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. “Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex

systems", Proceedings of the 1st International Conference on Transportation Information and Safety （ICTIS 2011), Wuhan, China, pp. 845-854, June 2011

[7] Kostogryzov A., Nistratov A., Nistratov G. "Applicable Technologies to Forecast, Analyze and Optimize Reliability and Risks for Complex Systems" // Proceedings of the 6st International Summer Safety and Reliability Seminar, Poland, Volume 3, Number 1, pp. 1-14, September 2012

[8] Andrey Kostogryzov, George Nistratov and Andrey Nistratov, "Some Applicable Methods to Analyze and Optimize System Processes in Quality Management", Total Quality Management and Six Sigma, InTech, pp. 127-196, August 2012. Available from: http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management

[9] Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. "Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes", American Journal of Operations Research, Special Issue, Volume 3, Number 1A, pp.217-244, January 2013, Available from: http://www.scirp.org/journal/ajor/

[10] Безопасность России. Человеческий фактор в проблемах безопасности – М.: Знание, 2008 – 704с.

[11] Акимов В.А., …, Костогрызов А.И., …, Махутов Н.А., …, Соколов И.А., Степанов П.В. и др. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Фундаментальные иследования проблем техногенной безопасности./Под ред. Махутова Н.А./ – М.:МГОФ «Знание», 2013, - 576с.

[12] Kostogryzov A., Nistratov G. and Nistratov A., 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*

[13] Костогрызов А.И., Костеренко В.Н., Тимченко А.Н., Артемьев В.Б. Основы противоаварийной устойчивости угольных предприятий. Библиотека горного инженера.Том 6 «Промышленная безопасность». Книга 11. - М.: Изд-во «Горное дело» ООО «Киммерийский центр», 2014. – 336с.

[14] Алешин А.В, …, Костогрызов А.И., …, Соколов И.А., Степанов П.В. ,…, Фортов В.Е., … Шойгу С.К. и др. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности./Под ред. Махутова Н.А. – М.:МГОФ «Знание», 2015, - 936с.