УДК 004.413.4:614.8.026.1
Оригинальная статья
Надежность, том 19, №4, 2019 https://doi.org/10.21683/1729-2646-2019-19-4-53-64

О природе рисков в управлении безопасностью структурно сложных систем

Александр В. Бочков, *ООО «Газпром газнадзор», Российская Федерация, Москва*

Александр В. Бочков

Резюме. Цель. *В общем случае риск-ориентированный подход охватывает как вероятностные методы моделирования аварийных процессов и событий, так и детерминистские методы. Использование вероятностных и детерминированных оценок заняло значительное место в исследованиях по повышению безопасности и по совершенствованию эксплуатационных процедур. Однако опыт использования сугубо вероятностного анализа (по сути – однокритериального инструмента) показал, что этот подход охватывает не все необходимые аспекты обеспечения безопасности. Цель статьи – ввести определения (уточнения) самих понятий «анализ» и «синтез», применительно к рискам при исследовании вопросов обеспечения безопасности структурно сложных систем (ССС) и построении систем мониторинга опасностей и угроз их устойчивому развитию.* **Метод.** *В статье с позиций системологии рассматривается методология анализа и синтеза рисков как инструмента создания современных систем мониторинга угроз безопасности функционирования ССС. Приведено сравнение основных концепций управления рисками в ССС, принятыми в настоящее время и показана необходимость их творческого развития. Приведен вид функционала риска, позволяющего определять решение в области обеспечения безопасности величиной математического ожидания потерь с учетом соответствующих поправок.* **Результат.** *Введено понятие «синтез рисков» как единого с анализом инструмента познания, учитывающего существующие связи между элементами исследуемых ССС с точки зрения всей системы как целого. Сформулированы принципы составления полного набора данных, необходимых для принятия решений.* **Вывод.** *Предложенный подход формирует предпосылки к разработке метода синтеза рисков и предполагает создание перспективных экспертно-аналитических систем поддержки принятия решений о безопасности ССС как систем многофункциональных и многоуровневых, предназначенных как для фиксации и анализа каждого конкретного случая (события), так и для прогнозирования тенденций и формирования профилактических мероприятий в случае их необходимости.*

Ключевые слова: *структурно-сложная система, объекты критически важной инфраструктуры, риск, синтез, анализ, безопасность, управление.*

Для цитирования: *Бочков А.В. О природе рисков в управлении безопасностью структурно сложных систем // Надежность. 2019. № 4. С. 53-64. https://doi.org/:10.21683/1729-2646-2019-19-4-53-64*

Поступила 26.08.2019 г. / После доработки 23.10.2019 г. / К печати: 14.12.2019 г.

...Большинство ученых работников стремятся узнать устройство, состав и содержание своего предмета, разлагая его на части. Они пытаются понять, как части соединяются в целое. Иногда это напоминает желание разобрать часы, чтобы понять, что такое время...

Аксенов Г.П. [1]

Введение

Вопросам анализа и оценки рисков посвящено много работ, причем их число стремительно растет в последние годы. Рисунок 1 наглядно демонстрирует рост частоты появления (в количестве на 1 млн слов в год) в англоязычных публикациях слова «риск» с момента его первого упоминания в 1661 году до настоящего времени.

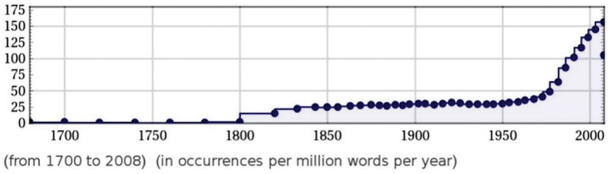

Рисунок 1 – Частота упоминания слова «риск» [2]

Отчасти это связано с общей «модой» на исследования в этой области, отчасти – это ответ на вызовы времени, когда создание человеком большого числа взаимно пересекающихся и частично интегрированных друг в друга систем разного назначения существенно поколебало общую устойчивость развития общества, породило трудно прогнозируемые опасности и угрозы. Появилось даже целое направление в системной инженерии, занимающееся инженерией систем, отдельные части которых могут существовать автономно, были разработаны независимо друг от друга, и тем самым представляют собой полноценную целевую систему. Риск часто выступает как осознанная угроза, следствием чего и является повышенный интерес к нему исследователей. Однако их усилия нередко очень наглядно иллюстрируют слова Г.П. Аксенова, биографа В.И. Вернадского, вынесенные в эпиграф.

В этой связи первостепенную актуальность приобретает задача определения (уточнения) самих понятий «анализ» и «синтез» применительно к рискам. Анализ и синтез – не два разных пути и способа познания, а являются противоположностями одного познающего сознания, разделимыми лишь в абстракции. А. Казеннов [3], например, показывает, что основанием этого единства является их происхождение из практического анализа и из исследования вообще. «…родовым словом для определения анализа, – пишет он, – является не «разделение» (в том числе – мысленное) предмета, а «исследование». А специфическим отличием определения является «различение частей целого и их соотношения друг с другом посредством этого целого». Не расчленение, а различение… Нужно только найти момент тождества «части» и целого, одной части и других «частей».

В то же время отождествление различенных частей друг с другом объединяет предметы (в данном случае – части) в нечто одно, в целое. Но это уже синтез. А определение анализа следует сформулировать так: анализ есть исследование, различающее части предмета и соотносящее их с целым и друг с другом посредством этого целого. Целое в анализе является исходным, опосредствующим все движение исследования. Части же, как правило, выделены уже до данного исследования – предшествующими практическими и теоретическими исследованиями: аналитическими и синтетическими познаниями… синтез: это исследование, рассматривающее соотношение различенных частей предмета и их целого посредством сущности (существенной части) целого. Нахождение такой сущности или существенной части и есть фундаментальное научное открытие, которое проливает новый свет на все предшествующие понятия, выражающие сущность предмета. Она перестраивает всю систему понятий и, соответственно, всю теорию».

При оценке рисков такой подход к их изучению представляется наиболее конструктивным. Особенно важно это при исследовании системы систем и связанной с ней т.н. проблемы критической инфраструктуры, часто обсуждаемой в последние годы [4-9]. Суть этой проблемы заключается в том, что почти во всех важнейших секторах экономики существуют системы, элементы которых настолько далеко разнесены в пространстве (иногда эти системы относят также к классу территориально-распределенных), что экономически практически невозможно полностью защитить все объекты даже какого-либо одного сектора, не говоря уже обо всех секторах системы. Главными вопросами и проблемой лица, принимающего решения (ЛПР) в области обеспечения безопасности функционирования подобных систем является вопрос оценки угроз и рисков, значимых для системы в целом и для ее элементов и определение приоритетности защиты элементов и объектов критической инфраструктуры с учетом ограниченных, как правило, ресурсов, имеющихся в его распоряжении.

Помимо огромных размеров, многие сектора настолько сложны, что технологически и экономически невозможно предвидеть, и просчитать все непредвиденные последствия любого инцидента, независимо от того, был ли инцидент вызван последствиями злонамеренных действий людей, или явился следствием природных бедствий. Как правило, крайне трудно предсказать последствия малых возмущений в одной части критической инфраструктуры для других ее участков. Например, все коммуникации в сети интернет в Южной Африке были полностью прекращены вследствие падения башен-близнецов в результате террористической атаки на США 9 сентября 2001 г., а относительно незначительные неисправности в электрической полезной мощности First Energy в Огайо (США) ускорили блэкаут в августе 2003 года, затронувший 50 миллионов человек за тысячи километров от источника проблемы [10-12].

По сути, существующая инфраструктура уязвима просто потому, что она содержит так много очень тесно взаимосвязанных между собой компонентов, что для большинства технических консультантов, аналитиков и ЛПР, определяющих политику ее безопасности, это становится неразрешимой задачей.

Понятие структурной сложности, как и понятие системы вообще, до сих пор не нашло однозначного определения. Вместе с тем современные требования к построению систем обеспечения безопасности и эффективности их функционирования были и остаются достаточно высокими. Как следствие, возникают задачи выбора приоритетных объектов оснащения из их генеральной совокупности и оптимального распределения имеющихся в распоряжении владельца системы (собственника, государства) финансовых и материальных ресурсов на их защиту. О понятии оптимальности в приложении к задачам синтеза риска мы поговорим позже. Прежде всего, необходимо разобраться с понятием риска, его онтологией. Измерять можно только то, что четко определено, хотя А. Эйнштейн утверждал, что «мир понятие не количественное, а качественное».

Люди избавились бы от половины своих неприятностей, если бы договорились о значении слов…

Рене Декарт

1. О природе риска и подходах к обеспечению безопасности

Риск – это понятие, возникающее на стыке понятий надежности и безопасности. Сама по себе техника, производственные системы не рискуют. Рискует всегда человек. Надежность – свойство технического объекта безотказно функционировать непрерывно со 100% уровнем эффективности. При анализе надежности главный критерий – критерий отказа, который делит все на «да» (работоспособное состояние) и «нет» (неработоспособное состояние). Надежность зависит, если можно так выразиться, от внутренних свойств и характеристик объекта (качества изготовления, его наработки на отказ, технологических особенностей, требований к эксплуатации и т.п.). Безопасность – свойство того же объекта выполнять свои функции без нанесения ущерба обслуживающему персоналу, окружающей среде и пр. Безопасность зависит уже от свойств внешних (окружающая среда, угрозы, квалификация персонала). Кроме того, безопасность – это одновременно и ощущение, и состояние. Состояние безопасности определяется развитием соответствующих технологий, а оценивается с помощью математических методов моделирования; оно основано на анализе и оценке рисков и эффективности различных мер, средств и механизмов защиты. Ощущение безопасности – это психологические реакции человека на угрозы и риски, и психологическое же восприятие достаточности мер защиты; то, что называется уровнем приемлемого риска (т.е., от каких угроз человек готов не защищаться, какие ущербы для него являются допустимыми). В том смысле, что ощущение безопасности может субъективно меняться, можно согласиться с высказыванием американского криптографа, писателя и специалиста по компьютерной безопасности Брюса Шнайдера: «Безопасность – это процесс, а не результат». Но это совсем не означает, что у процесса обеспечения безопасности нет цели. Цель обеспечения безопасности – достигнуть такого состояния защищенности человека и окружающей среды, которое соответствует его субъективному ощущению опасности (т.е., приемлемому уровню риска). Для достижения этой цели применяют т.н. «риск-ориентированный подход».

Риск появляется как оценка опасности для человека, выполняющего работу с помощью технических устройств. Поскольку и при рассмотрении надежности, и при рассмотрении безопасности есть скрытые дефекты и неопределенности места и времени возникновения отказов и опасностей, риск часто трактуют как влияние неопределенностей на достижение поставленных человеком-оператором целей деятельности. Конкретика возникает, когда рассматривается конкретный механизм (объект, промышленное предприятие, корпорация и т.п.), который человек использует для реализации целей деятельности в определенной среде (которая, в свою очередь, характеризуется наличием угроз, природными особенностями, наличием конкурентов, имеющих свои цели и т.п.)

В живых системах, например, неустойчивость используется целесообразно – это одна из самых важных движущих сил эволюции. Можно сказать, что высокая адаптивность живых организмов является следствием их неустойчивости. Известный сторонник «управляемой неустойчивости» Насим Талеб, также неоднократно подчеркивал, что многоуровневая избыточность – главное свойство естественных (живых) систем, управляющее риском [13]. Как и в живых системах, неустойчивые процессы в системах обеспечения безопасности – залог их адаптивности к изменяющимся угрозам и опасностям.

С некоторой оговоркой можно сказать, что риск служит наилучшей мерой для количественного описания опасности. Это понятие широко используется в современной литературе и часто подразумевает совершенно различный смысл. В наиболее общем случае риск характеризуется: вероятностью возникновения неблагоприятного воздействия, вероятностью того, что возникает неблагоприятное воздействие именно данного типа и вероятностью того, что данный тип воздействия вызывает определенную величину отклонений состояния субъекта воздействия от его динамического равновесия. То есть, риск – векторная величина, которая может описывать опасности разного вида и куда все его значения, приведенные выше, входят составными частями. Так как основные вопросы, обсуждаемые ниже, так или иначе связаны с обеспечением безопасности промышленных объектов, то там, где это не оговорено особо, под термином «риск» мы будем понимать риск техногенного или, более конкретно, промышленного происхождения.

Первым приближением, в вопросах, связанных с обеспечением безопасности, чаще всего является требование достижения пренебрежимо малого или «нулевого» риска, связанного с той или иной, как правило, производственной, деятельностью. Поэтому системы безопасности, которые создавались и использовались в промышленности, чаще всего являлись инженерными решениями, направленными на выполнения требования абсолютной безопасности. Основной принцип, используемый для создания этих систем – т.н. принцип **ALAPA** (As Low As Practicable Achievable). Согласно этому принципу, необходимо повышать промышленную безопасность любыми средствами и независимо от достигнутого уровня, если это технически осуществимо. Иными словами, согласно ALAPA необходимо создавать технические меры безопасности, которые предотвращали бы аварийные ситуации, т.е. сводили на нет саму возможность возникновения и развития аварии. Усложнение технологий привело к тому, что часто просто немыслимо предугадать все возможные сценарии развития аварии и, соответственно, предусмотреть инженерные и организационные решения для их предотвращения, что лишний раз показали аварии в Чернобыле и Фукусиме. Все это потребовало принципиально нового подхода в решении задач обеспечения безопасности. В последнее три десятилетия этим вопросам было посвящено значительное количество работ, которые убедительно подтвердили уже ставшее аксиоматическим утверждение о том, что достижение абсолютной безопасности невозможно.

Философия риска, основанная на концепции абсолютной безопасности, с необходимостью пришла к концепции приемлемого риска. Концепция приемлемого риска потребовала отказа от принципа ALAPA и прохода к новому принципу **ALARA** (As Low As Reasonable Achievable). Согласно ALARA, необходимо достижение определенного уровня безопасности, который должен определяться исходя из социальных и экономических условий развития общества. Для аварий, риск от которых выше приемлемого, необходимо использовать инженерные решения для их предотвращения и ослабления последствий, а для тех аварий, риск от которых меньше, только меры по ослаблению последствий. Реализация этого принципа, например, для атомной энергетики нашла отражение в соответствующих положениях по обеспечению безопасности. Для ССС также вводится понятие приемлемого (предельно допустимого) риска как риска, уровень которого допустим и обоснован исходя из экономических и социальных соображений. Хотя полноценных методик определения приемлемого риска для опасных промышленных объектов ССС до настоящего времени нет, можно сказать, что в настоящее время решение задач безопасности сводится к тому, чтобы на основании определенных критериев ответить на вопрос о том, какими средствами и до какого уровня необходимо снижать риск в той или ивой области производственной деятельности, чтобы безопасность как человека, так и окружающей среды была оптимальной.

Анализ риска является единственной возможностью исследовать те вопросы безопасности, на которые не может быть получен ответ из статистики, как, например, аварии с малой вероятностью реализации, но с большими потенциальными последствиями. Конечно, анализ риска не является решением всех задач обеспечения безопасности, однако только используя его, можно сравнить риски от различных источников опасности, выделить наиболее существенные из них, выбрать наиболее эффективные и экономичные системы по увеличению безопасности, разработать мероприятия по снижению последствий аварий и т.д.

В зарубежной печати наряду с понятием «анализ риска» (Risk Analysis) иногда пользуются методом **PRA** (Probabilistic Risk Analysis, вероятностная оценка риска), утвержденным NRC (Nuclear Regulatory Commission, Комиссия по ядерному регулированию США). Принципиального различия между ними нет, хотя считается, что PRA преимущественно нацелен на анализ аварий с низкой вероятностью, однако при помощи PRA часто исследуются события и с широким спектром вероятности возникновения. В отечественной литературе такого разделения не существует.

В настоящее время процедуру анализа риска можно условно разделить на две основные составные части и несколько промежуточных, каждая из которых характеризуется своими проблемами и использует присущие ей методы и модели: оценка и управление. Важно при этом помнить, что вопросы анализа риска нельзя рассматривать отдельно от игровой постановки. Риск, как динамическая характеристика, зависящая от времени, средств и информации, сведена к «двумерным оценкам» вероятности и ущерба.

Забыто, что прежде всего существует принципиальное различие между стохастическими факторами, приводящими к принятию решения в условиях риска, и неопределенными факторами, приводящими к принятию решения в условиях неопределенности. И те, и другие приводят к разбросу возможных исходов результатов управления.

Но стохастические факторы полностью описываются известной стохастической информацией, эта информация и позволяет выбрать лучшее в среднем решение. Но основные формулы в анализе риска (АР) извращены, упрощены, забыта их принадлежность к теории игр. Причин этому несколько. Слово риск стало «модным», в итоге специалисты «ухватились за термин» не понимая, откуда он происходит, какие аксиомы в этот термин «положены». В итоге экономисты, страховщики, экологи, и другие много лет плодят ложные научные результаты исходя из ложных ими придуманных определений. Иногда («ложь» на «ложь» дает «истину») получают приемлемые результаты. Но это, как правило, касается только статических и стационарных случаев (где работает теория «надежности»), но никак не динамических случаев. Для ряда приложений нужно было, чтобы формула была «попроще», чтоб ее понимали развивающиеся страны, вступающие, например, в МАГАТЭ. В итоге риск как динамическая характеристика, зависящая от времени, средств и информации, свелась к двумерным снимкам фотографий, в которых присутствует только вероятности

и ущерб. Дело было отдано «войскам гражданской обороны» (ныне МЧС), не имеющим тогда соответствующего научного «потенциала» и выступающим как «заказчики» НИР. Наиболее влиятельные Министерства (Минсредмаш, МинОбщемаш), в общем, имели собственные представления о риске, которые в целом значительно отличались друг от друга. На формирование мнения, что задачи анализа риска разрешимы за счет «статистики» наблюдаемых явлений, подавляющее влияние оказали западные ученые (TNO из Нидерландов другие). Влияние было настолько сильным, что в современном анализе рисков были оставлены «теория прочности» и «теория надежности». Но были задавлены на корню исследования по «теории живучести», «теории гомеостазиса», адаптивные теории, включая «теорию выбора решений», «теорию перспективной активности», «теорию рефлексий», «теорию самоорганизующихся систем».

Применительно к неопределенным факторам подобная информация отсутствует. В общем случае неопределенность может быть вызвана либо противодействием разумного противника (более сложный случай – связанный с рефлексиями противника (террористическая угроза)), либо недостаточной осведомленностью об условиях, в которых осуществляется выбор решения.

Выбор решений при наличии недостаточной осведомленности относительно условий, в которых осуществляется выбор, принято называть «играми с природой». В терминах «игры с природой» задача принятия решений может быть сформулирована следующим образом. Пусть лицо, принимающее решение, может выбрать один из M возможных вариантов своих решений: $X_1, X_2, \ldots, X_M$ и пусть относительно условий, в которых будут реализованы возможные варианты, можно сделать N предположений: $Y_1, Y_2, \ldots, Y_N$. Оценки каждого варианта решения в каждых условиях (X_m, Y_n), где $m = 1 \ldots M$, $n = 1 \ldots N$, известны и заданы в виде матрицы выигрышей лица, принимающего решения: $A=A(X_m, Y_n)=\left| A_{mn} \right|$.

Предположим вначале, что априорная информация о вероятностях возникновения той или иной ситуации Y_n отсутствует. Теория статистических решений предлагает несколько критериев оптимальности выбора решений. Выбор того или иного критерия неформализуем, он осуществляется ЛПР субъективно, исходя из его опыта, интуиции и т.п. Рассмотрим эти критерии.

Критерий Лапласа. Поскольку вероятности возникновения той или иной ситуации Y_n неизвестны, будем их все считать равновероятными. Тогда для каждой строки матрицы выигрышей подсчитывается среднее арифметическое значение оценок. Оптимальному решению будет соответствовать такое решение, которому соответствует максимальное значение этого среднего арифметического, т.е.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M} \left(\frac{1}{N} \sum_{n=1}^{N} A_{mn} \right).$$

Критерий Вальда. В каждой строчке матрицы выбираем минимальную оценку. Оптимальному решению соответствует такое решение, которому соответствует максимум этого минимума, т.е.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M} \left(\min_{1 \le n \le N} \left(A_{mn} \right) \right).$$

Этот критерий очень осторожен. Он ориентирован на наихудшие условия, только среди которых и отыскивается наилучший и теперь уже гарантированный результат.

Критерий Сэвиджа. В каждом столбце матрицы находится максимальная оценка $\overline{A}_n = \max_{1 \le m \le M} \left(A_m \right)$ и составляется новая матрица, элементы которой определяются соотношением $R_{mn} = \overline{A}_n - A_{mn}$. Это размер сожалений, что при стратегии Y_n сделан не оптимальный выбор X_m.

Величину R_{mn} называют риском, под которым понимают разность между максимальным выигрышем, который имел бы место, если бы было достоверно известно, что наступит самая выгодная ситуация $\overline{Y}_n$ для лица, принимающего решения, и реальным выигрышем при выборе решения X_m в условиях Y_n.

Эта новая матрица называется матрицей рисков. Далее из матрицы рисков выбирают такое решение, при котором величина риска принимает наименьшее значение в самой неблагоприятной ситуации, т.е. $\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M} \left(\max_{1 \le n \le N} \left(R_{mn} \right) \right)$.

Сущность этого критерия заключается в минимизации риска. Как и критерий Вальда, критерий Сэвиджа очень осторожен. Они различаются разным пониманием худшей ситуации: в первом случае – это минимальный выигрыш, во втором – максимальная потеря выигрыша по сравнению с тем, чего можно было бы достичь в данных условиях.

Критерий Гурвица. Вводится некоторый коэффициент α, называемый «коэффициентом оптимизма», $0<\alpha<1$. В каждой строке матрицы выигрышей находится самая большая оценка $\max_{1 \le n \le N} \left(A_{mn} \right)$ и самая маленькая $\min_{1 \le n \le N} \left(A_{mn} \right)$.

Они умножаются соответственно на α и $(1-\alpha)$ и затем вычисляется их сумма. Оптимальному решению будет соответствовать такое решение, которому соответствует максимум этой суммы, т.е.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M} \left(\alpha \times \max_{1 \le n \le N} \left(A_{mn} \right) + (1-\alpha) \times \min_{1 \le n \le N} \left(A_{mn} \right) \right).$$

При (α=0) критерий Гурвица трансформируется в критерий Вальда. Это случай крайнего «пессимизма». При (α=1) (случай крайнего «оптимизма») человек, принимающий решение, рассчитывает на то, что ему будет сопутствовать самая благоприятная ситуации. «Коэффициент оптимизма» α назначается субъективно, исходя из опыта, интуиции и т.п. Чем более опасна ситуация, тем более осторожным должен быть подход к выбору решения и тем меньшее значение присваивается коэффициенту α.

Важно, что к анализу рисков этот критерий не имеет отношения. Разве только к субъективному восприятию «случайных» и «добровольных» рисков.

Как же считать риски?

Из вышесказанного следует, что оценка риска возможна только при наличии альтернатив выбора. Если существует всего один единственный вариант выбора, то риск автоматически равен нулю и разброс платежей является лишь характеристикой неуправляемой природной среды. Впрочем, надо заметить, альтернатива всегда присутствует в виде отказа принимать решение.

В каких-то случаях отказ принимать какое-то решение может давать оптимум по столбцам и тогда появятся не нулевые риски в вариантах за счет выбора неправильного решения. Например, выгодно не играть в казино, чем играть, придерживаясь какой-то стратегии. Напротив, в шахматах есть смысл играть даже в случае единственного (вынужденного) хода. Например, когда противник объявляет «шах», закрыться нечем, а отступление возможно только на единственную клетку – риск также нулевой, поскольку отказ играть – автоматическое поражение.

Наличие оценок вероятностей $\sum_{n=1}^{N} p_n = 1$ для описания состояния природной среды $p_1 = p(Y_1)$, $p_2 = p(Y_2)$, …, $p_N = p(Y_N)$ позволяет отказаться от выбора самого неблагоприятно случая при использовании критерия Сэвиджа, и записать искомое решение в виде:

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{N} p_n \times \left(\max_{1 \le n \le N}\left(A_{mn}\right) - A_{mn}\right)\right),$$

что является более правильной формулой.

Для случая, когда для любой пары (X_m, Y_n) платеж определяется только размером потерь $A_{mn}=B–C_{mn}$ имеем:

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times \left(B - C_{mn}\right)\right) =$$

$$= B + \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times C_{mn}\right).$$

Для случая, когда уровень потерь при оптимальном варианте для условий Y_1, Y_2, …, Y_N не зависит от n и равен $\overline{C}$, тогда:

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times \left(B - C_{mn}\right)\right) =$$

$$= B - \overline{C} + \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times C_{mn}\right).$$

Только в этом случае решение действительно будет определяться величиной математического ожидания потерь. Но с поправкой на B и $\overline{C}$. Неучет этих поправок содержится во множестве работ. Обычно принимают B и $\overline{C}$ равными нулю. Например, в экологии улучшать «воздух» ничего не стоит (не приносит прибыли), и если никто не заболел, то оптимальный ущерб принимается за 0.

К тем же оценкам приводит Критерий Байеса:

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times A_{mn}\right) =$$

$$= \left(B = 0; \overline{C} = 0\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times C_{mn}\right).$$

В целом, проблема обеспечения безопасности и анализа рисков объектов ССС в условиях изменения состава и интенсивности угроз устойчивому развитию отрасли не теряет своей актуальности на протяжении длительного времени. Требования безопасности, установленные для объектов высокой и средней категории опасности, порой высоки, и существенно повышают возможности собственников объектов. Как следствие, возникает вопрос ранжирования объектов внутри заданных категорий для определения очередности оснащения объектов требуемыми средствами защиты. Для этого необходимо задать критерий, относительно которого будет определяться важность (и, соответственно, порядковый номер) того или иного объекта в ранжированном перечне.

Используемые методы ранжирования объектов основаны на математическом моделировании, экспертных оценках, теории принятия решений и интервальном оценивании. В той или иной мере они учитывают интересы организаций, эксплуатирующих эти объекты, государственных надзорных органов, страховых компаний. Вместе с тем, имеющиеся на сегодняшний день методы ранжирования (например, ранжирование объектов по защищенности от ЧС на железнодорожном транспорте, ранжирование объектов опасных производственных систем газораспределения и др.) не учитывают особенности структурной связности объектов ранжирования и важности работы конкретного объекта для смежных систем и подсистем.

Задача ранжирования объектов ССС является типовой задачей теории измерения некоторых сложных синтетических свойств объектов. Формально решение задачи сводится к построению некоторой функции ценности, полезности, связывающей измеряемое свойство с более простыми измеряемыми в натуральных величинах ресурсными показателями (факторами). Функция ценности используется как для решения задач выбора некоторого наилучшего варианта из множества альтернатив, так и для решения более композиционных задач, типа задачи формирования портфеля заказов на выполнение работ при ограничениях на ресурсы (объемы финансирования создания или модификации объектов). Факторы, через которые строятся ранги, часто измеряются не в количественных, а в качественных шкалах, поэтому требуется использование методов экспертных оценок и экспертных технологий для построения зависимостей между полезностью и первичными ресурсными факторами. В связи с развитием компьютерной техники появилась возможность оценивания объектов, факторы описания которых задаются с погрешностью, что требует разработки специфического аппарата статистической обработки первичных данных и использования инструментария нечеткой логики. Существенной чертой решения задач ранжирования является

адаптивный характер процедур принятия решений выбора оптимальных вариантов, при которых для построения окончательной формулы функции ранжирования требуется проведение нескольких циклов согласования экспериментальных данных и экспертных предпочтений.

В данном контексте оценка риска является тем этапом, на котором определяются неблагоприятные последствия, связанные с той или иной производственной деятельностью. И прежде необходимо идентифицировать источники опасности, для чего нужно определить границы исследуемой системы. Другими словами, необходимо знать, какие источники включать в рассмотрение, а какие нет при оценке риска в регионе или от конкретной исследуемой системы. Жестких правил здесь нет и быть не может. Однако на сегодняшний день существует ряд разработанных положений, которые должны быть учтены при исследовании вопросов безопасности. Наиболее полно сформулированные положения по определению границ исследуемых региональных или крупных промышленных систем можно найти в разных источниках. Международные организации отмечают тот факт, что при оценке риска даже от одной конкретной технологии в различных странах в большинстве случаев получают различные значения. Поэтому для облегчения сбора и обработки данных должен быть принят единый набор терминов и положений для описания энергетических и промышленных систем и их основных компонент [14].

2. Замечания о категории риска

Основными моментами в оценке риска является подробное описание источника опасности и определение связанного с ним возможного ущерба. Существуют различные модели источников опасности, которые позволяют определить вероятность того или иного развития аварии и определить соответствующую мощность выброса опасных веществ в окружающую среду. В зависимости от типа источника выделяют три категории риска.

Обычный риск связан с нормальной работой предприятия. В условия нормальной работы включаются и аварии с незначительным ущербом, которые происходят довольно часто. Эта категория риска характеризуется вероятностью реализации равной или близкой к единице. В большинстве случаев обычный риск либо является неотъемлемой частью самого производственного процесса, либо легко контролируется. Источники такого риска обычно описываются мощностью выброса или утечки в окружающую среду, связанные с нормальной работой либо с каким-то происшествием. Оценка мощности выброса или утечки для работающих предприятий может быть произведена на основании измерений либо результатов опыта работы аналогичных предприятий.

Другие две категории риска связаны с авариями на производстве, при транспортировке или хранении опасных веществ. Под аварией при этом понимается событие с низкой вероятностью осуществления (например, менее одного за все время жизни предприятия), но со значительными или даже катастрофическими последствиями. При анализе аварийных ситуаций обычно рассматриваются возможные сценарии развития аварии. При этом должны быть учтены такие факторы, как тип инициирующего события, количество имеющегося опасного вещества, эффективность аварийных систем безопасности и многие другие. Обычно существует большое число возможных сценариев развития аварии и поэтому в оценке риска необходимо определить весь спектр возможных сценариев и их вероятности. Величины вероятности могут при этом изменяться от 10^{-6} до 10^{-8} событий в год. Более редкие события настолько трудно оценить, что считают, что они практически невероятны.

Периодический риск связан с теми авариями, которые довольно часто повторяются, но вызывают ограниченный ущерб, куда могут входить даже человеческие жертвы. Это вовсе не означает, что такие аварии являются планируемыми. Они, конечно, нежелательны, и для предотвращения их создаются и используются системы безопасности. Однако несмотря на эти меры, такие аварии могут происходить, и риск, связанный с ними, имеет довольно широкий диапазон значений в зависимости от типа производственной деятельности. Причиной таких аварий является обычно нарушение технологического процесса, неверное использование оборудования и ошибки персонала. Для оценки риска этой категории частота аварий и другие необходимые параметры оцениваются при помощи стандартных статистических методов на основе имеющихся данных.

Гипотетический риск связан с авариями, которые, как считается, могут происходить с очень малой вероятностью, но приводить к очень большим последствиям. Для такого класса аварий характерно отсутствие либо недостаточное количество статистических данных. Однако из-за их огромного потенциального ущерба невозможно просто ждать, пока наберется достаточный практический опыт. Поэтому в этих случаях производят анализ гипотетических аварий с целью определения вероятности реализации этой аварии и оценки возможных ее последствий. Обычно недостаток статистических данных относится к поведению крупной промышленной или энергетической системы в целом. Поэтому такой анализ проводится либо при помощи экспертной оценки, либо методом «деревьев событий», где вероятность гипотетической аварии может быть предсказана на основе возможных неисправностей или отказов в работе отдельных узлов или механизмов, по которым имеются соответствующие статистические данные.

Следует помнить о том, что для оценки риска нет необходимости использовать чрезмерно усложненные модели из-за больших неопределенностей и осреднений, возникающих при расчете. Кстати, нахождение величины неопределенности и диапазона возможных значений риска является еще одной составной характеристикой риска вообще. Так, по мнению различных экспертов, неопределенность в оценке риска от аварий на промышленных предприятиях может составлять один и даже достигать двух порядков величины. Это связано с недостатком базы знаний по широкому кругу технических, экологических и социальных факторов, которые необходимо учитывать в

анализе риска. Есть даже заключения, основанные на анализе точности и неопределенности при определении риска, что модели переноса, позволяющие получить значение концентрации опасного вещества в исследуемом месте с точностью 10% (максимум 20%) вполне приемлемы.

3. Замечания о системе мониторинга

Таким образом, устойчивое функционирование и развитие любой ССС зависит от влияния большого числа внешних и внутренних факторов, в том числе факторов негативного воздействия. Для мониторинга и оценки этих факторов и принятия решений, направленных на снижения негативных последствий их проявления, повсеместно внедряются т.н. системы сбалансированных показателей (Balanced Scorecard), ключевых показателей эффективности (КПЭ) (количественно характеризующих факторы рисков, которым подвержена система) из числа которых выбираются стратегические целевые показатели (СЦП), количественно отражающие стратегические цели функционирования системы и представляющие собой базовые экономические и производственные показатели, которые характеризуют эффективность ее развития (опосредовано их недостижение характеризует уровень существующих угроз и степень их реализации в рассматриваемый промежуток времени).

На основе этих показателей строятся системы мониторинга угроз и рисков, позволяющие собирать данные об изменениях и проводить анализ эффективности функционирования системы по нескольким сотням показателей в организационном, продуктовом, географическом и других разрезах на суточном, квартальном и годовом горизонте планирования. Считается, что результаты анализа позволяют осуществлять «управление по отклонениям», акцентируя внимание на проблемных областях каждого объекта управления посредством «светофорной» индикации. Однако по мере накопления данных возникает проблема интерпретации сигналов этих сотен «светофорных индикаторов». Не очевидно, что считать «хорошим» или «плохим» сигналом в целом для системы, если, например, половина из индикаторов «горит» зеленым цветом, а половина «красным». Как квалифицировать ситуацию, если «зеленых» индикаторов немного больше, чем «красных» и т.п. Неочевидна также связь анализируемых индикаторов с показателями высокого уровня (СЦП) и степени их влияния на достижение целевых значений СЦП, утвержденных руководством компании. Возникает так называемый эффект «больших данных», когда аналитики не успевают обработать накапливающуюся информацию, а стандартные статистические методы просто перестают работать.

Кроме того, система мониторинга угроз и рисков, построенная на основе анализа трендов изменения показателей, не способна предсказывать кризисы и ситуации с негативной динамикой. Такие события редки и протекают, как правило, при различном прогнозном фоне, а в случае анализа рядов исторических данных редких событий имеют место дискретные динамические вероятностные процессы.

Целью анализа ССС как объекта прогнозирования в области обеспечения безопасности функционирования и устойчивости развития является построение такой прогностической модели динамики ситуаций, возникающих при ее функционировании, которая позволит с помощью вычислительных экспериментов и подбора приемлемых параметров уменьшать степень неопределенности дат событий и их масштаба, то есть, получать прогнозную информацию об объекте прогнозирования за счет выявления скрытых закономерностей, которые указывают либо на изменения состояния объекта, либо на закономерности изменений параметров внешней среды, существенно влияющей на его функционирование (так называемые законы изменчивости «прогнозного фона»).

Из-за дискретной природы кризисных ситуаций использование аппарата анализа данных, основанного на классических законах больших чисел, некорректно. Сходимость по вероятности в реальности практически никогда не наблюдается, за исключением статистики, накопленной в системах массового обслуживания. Панель индикаторов, реализованная в виде «светофора», построенного на основе использования дисперсии как основного показателя, может в течение всего года указывать на нормальное состояние, когда на самом деле система переходит в область предкризисных значений.

Кроме того, при официально декларируемой иерархической системе показателей, как правило, отсутствует однозначная функциональная связь и взаимное влияние показателей нижнего и верхнего уровня.

Как следствие, необходим корректный первичный анализ многолетней статистики, и уже на основе этого анализа можно дать заключение – возможна ли разработка адекватного исследуемой задаче инструмента прогнозирования и какая доля случайности дат возникновения неблагоприятных ситуаций и их масштабов может быть с его помощью устранена. Также очевидно, что, поскольку истинные законы распределения анализируемых случайных процессов и, главное, факторы их определяющие, будут непрерывно корректироваться (любая высокотехнологичная система, изменяется быстрее, чем накапливается адекватная статистика), необходимо использовать критерии, «свободные от распределений». В частности, например, в качестве критериев достижения прогностической цели следует взять не величины отклонений модельных и реальных данных, а критерии, используемые в методах классификации и распознавания образов. Например, в качестве измерения точности прогноза можно использовать величины ошибок предсказания первого и второго родов для различных классов и типов ситуаций, причем, если удастся, в зависимости от классов физического объекта и в зависимости от значения параметров прогнозного фона. Второе обстоятельство очень важно, поскольку, например, некорректно складывать статистику аварийности различных времен года, так как в различные сезоны технологические процессы протекают по-разному.

Надежное выполнение системой своих функций характеризуется сохранением некоторых заданных характери-

стик (отражаемых в соответствующих значениях СЦП и КПЭ) в установленных пределах. На практике полностью избежать отклонений невозможно, однако необходимо стремиться к минимизации отклонений текущего состояния от некоторого заданного идеала – цели, заданной, например, в виде значений СЦП первого уровня.

Мера угрозы недостижения заданных значений СЦП первого уровня (по сути, мы снова говорим о риске), рассматривается в данном случае как переменная величина, представляющая собой функцию относительно текущего положения системы: она увеличивается при приближении оцениваемой ситуации к некоторой допустимой границе, после достижения которой система не может выполнить свои обязательства и достичь соответствующих заданных целевых значений СЦП первого уровня.

Общая математическая постановка обсуждаемой задачи: пусть задано множество признаков текущей ситуации X (например, текущих значений КПЭ, факторов риска и т.п.), множество допустимых реализаций ситуаций Y (например, текущее значение СЦП первого уровня больше (или меньше) предыдущего и т.п.), и существует целевая функция y^*: $X \to Y$, значения которой $y_i = y^*(x_i)$ известны только на конечном подмножестве объектов $\{x_1,\ldots,x_l\} \subset X$ (например, соответствующие текущему значению СЦП первого уровня значения КПЭ). Пары «объект-ответ» (x_i, y_i) – прецеденты. Совокупность пар $X_l = \sum_{i=1}^{l} x_i, y_i = 1$ составит обучающую выборку. Требуется по выборке X_l восстановить зависимость y^*, то есть, построить решающую функцию $A: X \to Y$, которая приближала бы целевую функцию $y^*(x)$, причем не только на объектах обучающей выборки, но и на всем множестве X. Поскольку при этом решающая функция A должна допускать эффективную компьютерную реализацию, возможно называть ее также алгоритмом.

Условно существует два класса объектов, с которыми приходится сталкиваться специалистам в области автоматизации управления: «простые» и «сложные». «Простыми» являются объекты, точные математические модели которых, например, в виде системы алгебраических уравнений или модели линейного программирования, при учете всех необходимых количественных факторов, влияющих на поведение объекта, пригодны для реализации на ЭВМ выбранного класса и вполне адекватны объекту. «Сложные» объекты управления имеют следующие главные отличительные особенности: не все цели выбора управляющих решений и условия, влияющие на этот выбор, могут быть выражены в виде количественных соотношений; отсутствует, либо является неприемлемо сложным, формализованное описание объекта управления; значительная часть информации, необходимая для математического описания объекта, существует в форме представлений и пожеланий специалистов-экспертов и т.п. Построение точных математических моделей «сложных» объектов, пригодных для реализации и эксплуатации на современных ЭВМ, либо затруднительно, либо часто вообще невозможно.

Но это не означает, что задача не имеет решения. В общем случае возможных направлений поиска может быть два. Первое – попытаться применить нетрадиционный математический аппарат для построения модели, учитывающей все особенности объекта и пригодной для реализации. Второе – строить не модель объекта, а модель управления объектом (т.е., моделируется не сам объект, а человек-оператор в процессе управления объектом). По своей сути алгоритм в этом случае связан с построением поля структуры данных и анализом его эффектов, включая и уточнение самой структуры. В любых данных одновременно присутствует и порядок, и беспорядок. Поскольку исключающее ИЛИ «построить» трудно, возможна реализация идеи построения решающих правил (далее – решатель) на монотонных функциях, задающих сетевой порядок [15, 16].

Геометрический смысл решателя достаточно прост: необходимо так подобрать признаки, сохраняя свойства частного порядка, чтобы объекты на подмножестве признаков разделились. Это – классическая задача дискретной математики о нахождении логической функции, и решается она десятками различных способов, в основе которых лежит метод разложения любой логической функции в суперпозицию более простых функций. Методы решения с оптимизацией при всех успехах эвристической математики, как правило, приводят к большому перебору вариантов, что не гарантирует оптимальность найденных решений. Методы построения оптимальных (содержащих меньше переменных, или с непересекающимися сомножителями в логических суммах) формул для частично заданных логических функций имеют алгоритмы комбинаторной сложности с экспоненциальным ростом затрат вычислительных ресурсов от размеров решаемых таблиц (как по количеству переменных, так и по количеству обучающих объектов).

4. Принципы составления полного набора данных

Исходя из вербального определения «рискованное действие – это дело, затеянное на удачу в надежде на успех», собственно, вытекает идеология оценок, анализа и управления рисками. Что в данном определении присутствует? Первое – наличие, как минимум, двух исходов – «успешный», на который имеется надежда, и «неуспешный», при котором затеянное не свершается или свершается в меньшем масштабе. В тех редких случаях, когда имеется только два исхода, рисковая ситуация описывается платежной матрицей (табл. 1).

Таблица 1 – Платежная матрица

	Успешный исход	Неуспешный исход
Выгода (платеж за действие)	X_0	X_1
Мера возможности реализации	p_0	$p_1=1-p_0$

Недополученная выгода (X_0–X_1) называется, как правило, ущербом, а величина математического ожидания недополученной прибыли – риском R:

$$R = p_0\left(X_0 - X_0\right) + p_1\left(X_0 - X_1\right) = p_1\left(X_0 - X_1\right). \quad (1)$$

В случае, когда возможна угроза реализации неуспешных исходов с различными ущербами (X_0–X_n), риск исчисляется по формуле:

$$R = \sum_{n=1}^{N} p_n\left(X_0 - X_n\right). \quad (2)$$

Формула (2) может быть корректно применима для текущей оценки рискового действия только в тех случаях, когда это действие «обратимо», то есть, когда имеется возможность повторить это действие достаточно большое число раз для того, чтобы обеспечить сходимость «по вероятности».

При анализе слабо формализуемых угроз такая ситуация не наблюдается.

Во-первых, как правило, исследователям ничего не известно о возможности или невозможности появления «новых» сценариев с неуспешными исходами, кроме тех, что внесены в анализируемую платежную матрицу (табл. 1). Поэтому, хотя и должно выполняться классическое условие $\left(p_0 + \sum_{n=1}^{N} p_n = 1\right)$, но величины $p_n(n=0, \ldots, N)$ – это не вероятности (probability (вероятность) – апостериорные вероятности, подсчитанные частоты), а возможности (likelihood (правдоподобие) – априорные вероятности, предполагаемые пропорции реализации исходов).

Во-вторых, приходится считать, что различных сценариев слишком много, и каждый из них имеет пренебрежительно малую вероятность реализации. Собственно, в жизненном процессе реализуется только один единственный сценарий – тот, который реализуется в реальности. Поэтому неуспешные исходы должны группироваться в классы. Первая процедура при разбиении исходов на классы осуществляется по признаку эквивалентности ущербов, что опять-таки неправильно с позиций классической теории вероятностей: величины оценок возможностей $p_g(g=0, \ldots, G)$, где индекс g указывает на группу исходов, зависят от субъективного восприятия ущерба (значимости ущерба). В результате анализируется распределение «псевдовероятностей» по шкале исследователя, а не по шкале природы явления.

В-третьих, часто решение о вступлении в рискованное действие реализуется лишь один раз, поэтому сомнительно использовать вероятностные имитационные инструменты анализа типа метода Монте-Карло.

В-четвертых, часто приходится решать задачу выбора рискованного действия из множества альтернативных вариантов, чтобы исключить риски неприемлемого уровня. Оценочная функция, соответствующая случаю недопущения ущерба ниже теоретически возможного, предполагает, что от действий, для которых существует хотя бы один сценарий $\tilde{n}$, при котором ущерб $\left(X_0 - X_{\tilde{n}}\right)$ превышает заданный уровень, надо отказаться. Оценочная функция, соответствующая политике «крайней осторожности», строится на основе минимаксного критерия.

Для оценки угроз такой критерий, впрочем, трудно признать пригодным для использования – редкие сценарии с большими ущербами отменили бы любую деятельность кроме «безнаказанной». Поэтому на практике приходится «сглаживать» ситуацию, что делается несколькими путями.

Первый – оценивать ущербы и риски, занимая «уравновешенную» позицию. Предполагается, что на практике реализуются варианты между точками зрения крайнего оптимизма (только успех, а другого не может быть) и крайнего пессимизма (прикладываются максимальные усилия на предотвращение и/или смягчение ущербов от угрозы, но все равно реализуется наихудший из возможных сценариев реализации угрозы).

Второй – угадать и корректировать пропорции, в которых ожидаются возможные реализации сценариев угроз, для этого необходимо «периодически» оценивать текущее состояние, тенденции изменения и прогнозируемые состояния угроз. То есть, речь идет о построении адаптивной схемы корректировки платежных матриц.

Это разделение крайне важно, так как различные источники информации имеют различную специфику воздействия на оценки рискованных действий.

Так, например, «компетентные источники» могут уточнять текущее состояние – вплоть до внесения новых альтернатив реализаций угроз (столбцов платежных матриц). Но отслеживание динамики состояния угроз для них не является основным видом деятельности. Научно-технологические источники достаточно уверенно могут дать предельные характеристики прогнозируемых величин (скажем, даты промышленного освоения той или иной технологии).

А вот оценки тенденций, оценки скоростей нарастания или ослабления угроз можно получать только путем анализа показателей внештатных и кризисных ситуаций.

Основанием для создания мониторинговых модулей могут служить многочисленные факты, указывающие на то, что, прежде чем сформируется угроза большого масштаба (например, крупного землетрясения), этому предшествует серия угроз меньшего масштаба (учащающиеся мелкие толчки).

Экспертно-аналитическая система должна быть многофункциональной и многоуровневой системой, предназначенной как для фиксации и анализа каждого конкретного случая (события), так и для прогнозирования тенденций и формирования профилактических мероприятий, если таковы ожидаются. Ожидание тех ситуаций, которые требуют действий, типично для служб пожарной охраны, МЧС, скорой медицинской помощи. В случае же слабо формализуемых угроз стационарного характера негативных событий нет «по определению», поэтому об этих угрозах система узнает из компетентных источников, сообщающих об этих угрозах в дополнение к их основной деятельности, либо из СМИ, когда об угрозе говорят все, «кому не лень». Между «компетентными источниками» и «общедоступными СМИ» имеется ши-

рокий спектр источников информации типа «материалы выставок и конференций», публикации научных изданий и специалистов, местная пресса (заведомо более близкая к субъектам и объектам угроз) и т.п.

Все источники информации, таким образом, выстраиваются в некоторую двумерную шкалу. Первое измерение отражает комплиментарность источника информации: «свой», «приближенный», «нейтральный», аффилированный с конкурентами, «недружественный». Второе измерение отражает уровень специализации (компетентности) источника информации. Например, к мнению специалиста (узкоспециализированного журнала) в его области естественно относиться с большим доверием, но с меньшим доверием в более широкой области, поскольку такой источник, «очевидно», будет переоценивать факты и результаты из своей области, и принижать значимость фактов и результатов из смежных областей, рассматривая их в качестве конкурентов. Оценивая ту или иную информацию, поступающую от источника по соответствию реальности (на потоке ретроспективных данных), мы можем сформировать отношение к источнику как к некоторому инструменту измерения, классификации, распознавания той или иной ситуации.

Большое разнообразие альтернативных источников информации требует проведения их сравнительного анализа и, по возможности, отбора и оптимизации задолго до того, как принять решение об использовании их в практической работе системы обеспечения безопасности.

Для этого необходим ответ на ключевой вопрос, а именно: по каким критериям оценивать источники, чтобы обеспечить сравнимость результатов их использования? В качестве технических критериев качества источников можно использовать показатели полноты и точности [17, 18].

Коэффициент полноты *ComplMcl* метода классификации *Mcl* равен доле правильно классифицированных объектов класса C из тестирующей выборки $\{X\}^{\in C \Rightarrow \in C}$ к полному количеству объектов класса C, находящихся в ней $\{X\}^{\in C}$:

$$ComplMcl = \frac{\{X\}^{\in C \Rightarrow \in C}}{\{X\}^{\in C}}. \quad (3)$$

Коэффициент точности *ExactMcl* метода классификации *Mcl* равен доле правильно классифицированных объектов класса C из тестирующей выборки $\{X\}^{\in C \Rightarrow \in C}$ к полному количеству объектов этой выборки, которые были классифицированы как принадлежащие классу C:

$$ExactMcl = \frac{\left|\{X\}^{\in C \Rightarrow \in C}\right|}{\left(\left|\{X\}^{\in C \Rightarrow \in C}\right| + \left|\{X\}^{\in C}\right|\right)}. \quad (4)$$

Коэффициент полноты связан с ошибками первого рода – неправильной классификацией объектов, принадлежащих классу C. Коэффициент точности корреспондируется с ошибками второго рода – классификациями ложных объектов как принадлежащих классу C.

Хороший метод классификации должен допускать меньше ошибок, то есть, иметь большие значения *ComplMcl* и *ExactMcl*. Однако 100% результат достигается лишь на специально подготовленных «эталонных» массивах данных. На практике же редко наблюдается одновременное превышение величинами *ComplMcl* и *ExactMcl* значения 70% [19, 20].

Повышение надежности оценок для формирования обучающих выборок требует наличия объясняющих компонент, что вытекает из аналитического характера деятельности.

В практике мы фактически наблюдаем два типа оценок:

• оценки собственно экспертов-источников;

• оценки, рассчитываемые из близости размещения текстов, поступающих от источников, по близким рабочим местам.

То есть, окончательную оценку качества источников требуется проводить по «конечному результату». В качестве интегральных критериев доверия к источнику информации предлагаются следующие показатели:

• среднее время наработки критического количества ошибок источника;

• среднее время наработки критического соотношения ошибок первого и второго рода, совершенных на базе данных источника.

Заключение

Таким образом, в части задачи построения системы мониторинга безопасности и прогнозирования рисков ССС следует рассматривать возможность одновременного использования двух базовых показателей ее развития: рисков развития (в качестве которых могут использоваться количественные показатели, определяющие неблагоприятное сочетание вероятностей возникновения опасных процессов и их последствий – ущербов – в экономическом и научно-технологическом развитии компании на заданном прогнозном отрезке времени) и эффективности комплексных мероприятий в процессе развития (количественный показатель, определяющий повышение стратегически важных уровней экономического и научно-технического развития компании на прогнозном отрезке времени за счет формирования и проведения корпоративной политики по базовым приоритетным направлениям, методам, критериям и системам реализации прогнозов с учетом стратегических рисков развития).

Для адекватной оценки текущего состояния системы необходимо иметь:

• полную систему индикаторов состояния системы и внешней (конкурентной) среды (описание позиции);

• генератор конечного обозримого количества возможных сценариев развития системы (ходы «своих» «фигур», «нейтральные» ходы «природы» и антагонистические ходы «фигур» «противника»);

• функцию оценки состояния (выигрыш – улучшение позиции – ухудшение позиции – проигрыш).

При этом, не дожидаясь наступления «проигрыша» (при ухудшении оценки текущего состояния, или же когда конкуренты предпринимают нерассмотренные ранее ходы), необходимо искать новые сценарии развития, поскольку

все рассмотренные ранее варианты приводят к проигрышу или вероятность благоприятных последствий чрезвычайно мала. Вследствие того, что в развитии любой системы присутствуют активные противники (конкуренты), частично управляемые внутренние факторы (техногенная и антропогенная аварийность) или неуправляемые факторы (природные бедствия и катастрофы) все сценарии носят вероятностный характер. Поэтому даже при плавном изменении состояния системы (в котором невозможно получить крупный проигрыш в короткое время) необходимо учитывать фактор накопления случайностей и разрабатывать индикаторы оценки близости исследуемой системы к границам потери устойчивости развития.

Библиографический список

1. **Аксенов Г.П.** Вернадский [Текст] / Г.П. Аксенов. – М.: Молодая гвардия, 2015. – 526[2] с.: ил. – (Жизнь замечательных людей).

2. По материалам: Word frequency history based on a Google Books sample of one million books in English; Michel, J.-B., Y. K. Shen, A. P. Aiden, A. Veres, M. K. Gray, The Google Books Team, J. P. Pickett, D. Hoiberg, D. Clancy, P. Norvig, J. Orwant, S. Pinker, M. A. Nowak, and E. L. Aiden. «Quantitative Analysis of Culture Using Millions of Digitized Books» Science 331 (2011).

3. **Казеннов А.С.** К пониманию единства анализа и синтеза [Электронный ресурс] / А.С. Казеннов. – URL: http://www.smyrnyh.com/?page_id=686. – Дата доступа: 18.08.2019.

4. Critical Infrastructure Security. Assessment, Prevention, Detection, Response [Text] / Edited By: F. Flammini (2012). // WIT Transactions on State-of-the-art in Science and Engineering (ISBN 978-1-84564-562-5). – 2012. – Volume 54. – 325 p.

5. National Infrastructure Protection Plan [Text]. – U.S. Department of Homeland Security, 2009. – 100 p. – (Available at www.DHS.gov).

6. National Strategy for the Physical Protection of Critical Infrastructure and Key Assets [Text]. – U.S. Department of Homeland Security, 2003. – (Available at www.DHS.gov).

7. **Dudenhoeffer D.D.** CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis [Text] / D.D. Dudenhoeffer, M.R. Permann, M. Manic: In L.F. Perronc, F.P. Wieland, J. Liu, B.G. Lawson, D.M. Nicol & R.M. Fujimoto (Eds) // Proceedings of the 2006 Winter Simulation Conference. – Institute of Electrical and Electronics Engineers, Piscataway, NJ, 2006. – P. 478-485.

8. **Perrow C.** Normal Accidents [Text]. – Princeton University Press, Princeton, NJ, 1999. – 450 p.

9. **Ramo J.C.** The Age of the Unthinkable [Text]. – Little, Brown & Company, New York, NY, 2009. – 280 p.

10. National Research Council, The Internet Under Crisis Conditions: Learning from September II. National Academics Press. – Washington, DC, 2003. – (Available at www.nap.edu).

11. August 14th Blackout: Causes and Recommendations. – U.S.-Canada Power System Outage Task Force, April 2004. – P. 12. – (Available at https://reports.energy.gov).

12. **Рябинин И.А.** Надежность и безопасность структурно-сложных систем [Текст] / И.А. Рябинин. – СПб.: Изд-во С.-Петерб. Ун-та, 2007. – 276 с.

13. **Taleb N.N.** Antifragile: Things That Gain from Disorder (Incerto) [Text] / N.N. Taleb // Series: Incerto (Book 3). – Random House Trade Paperbacks: Reprint edition (January 28, 2014). – 544 p.

14. **Радаев Н.Н.** Методические аспекты задания требования, оценки и обеспечения защищенности объектов газовой отрасли от противоправных действий [Текст] / Н.Н. Радаев, В.В. Лесных, А.В. Бочков: Монография. – М.: ООО «ВНИИГАЗ», 2009. – 164 с.

15. **Bochkov A.V.** Development of Computation Algorithm and Ranking Methods for Decision-Making under Uncertainty [Text] / A.V. Bochkov, N.N. Zhigirev : In: Ram M., Davim J. (eds) // Advanced Mathematical Techniques in Engineering Science. Series: Science, Technology and Management. – 2018. – May, 17. – P. 121-154.

16. **Бочков А.В.** Использование метода опорных векторов для поиска скрытых закономерностей в задачах классификации ситуаций, описываемых оцененными вопросниками [Текст] / А.В. Бочков, Н.Н. Жигирев // Proceedings 8th DQM International Conference Life Circle Engineering and Management ICDQM-2017. – 2017. – June 29-30. – P. 43-71.

17. **Корнеев В.В.** Интеллектуальная обработка данных [Текст] / В.В. Корнеев, А.Ф. Гареев и др. – М.: Нолидж, 1999.

18. **Salton G.** Automatic Text Processing [Text] / G.Salton. – Addison-Wesley Publishing Company, Inc., Reading, MA, 1989.

19. **Гареев А.Ф.** Решение проблемы размерности словаря при использовании вероятностной нейронной сети для задач информационного поиска [Текст] / А.Ф. Гареев // Нейрокомпьютеры: разработка, применение. – 2000. – №1. – С. 60-63.

20. Global Trends 2015: A Dialogue About the Future With Nongovernment Experts [Электронный ресурс] / This paper was approved for publication by the National Foreign Intelligence Board under the authority of the Director of Central Intelligence. Prepared under the direction of the National Intelligence Council. NIC 2000-02, December 2000. – URL:http://infowar.net/ cia/publications/globaltrends2015/ http://www.futurebrief.com /globaltrend2015.pdf.

Сведения об авторе

Александр В. Бочков – кандидат технических наук, заместитель начальника отдела анализа и ранжирования объектов контроля Администрации ООО "Газпром газнадзор" (Москва, Россия). e-mail: a.bochkov@gmail.com

Вклад автора в статью

Автор выполнил сравнение основных концепций управления рисками и показал необходимость их творческого развития. Предложен вид функционала риска, позволяющего определять решение в области обеспечения безопасности величиной математического ожидания потерь с учётом некоторых поправок. Автором введено понятие «синтез рисков» и сформулированы предпосылки к разработке соответствующего метода.