

О методе синтеза рисков в управлении безопасностью структурно-сложных систем

Александр В. Бочков, ООО «Газпром газнадзор», Российская Федерация, Москва
a.bochkov@gmail.com



Александр В.
Бочков

Резюме. Цель статьи – показать, что риск для объектов критически важной инфраструктуры (ОКВИ) структурно-сложных систем (ССС) следует рассматривать как многокомпонентный вектор, набор параметров которого может меняться. Реальная оценка уровня безопасности на основе использования риск-ориентированного подхода невозможна без достаточно информативной базы относительно количественных и качественных характеристик факторов рисков и, с другой стороны, данных о состоянии объектов и технологического процессов на них, которые испытывают влияние этих факторов риска. Оценка риска всегда имеет целью определение его количественных показателей, что дает возможность использования ее не только для оценки состояния промышленной безопасности, но и для обоснования экономической эффективности мероприятий, экономических расчетов необходимого возмещения или компенсаций потерянного здоровья рабочим и окружающей среде. **Метод.** Предложен метод синтеза рисков (с использованием игровой постановки задачи противодействия возможным внешним воздействиям различной природы на ОКВИ СССР) как основы создания современных систем мониторинга угроз безопасности функционирования СССР. Особое внимание необходимо уделить влиянию факторов риска на систему сбалансированных показателей безопасности и рисков, поскольку прогнозирование по единичным показателям не дает целостной картины тенденций развития и состояния системы. **Результат.** Сформулированы ключевые методологические положения: от общей постановки задачи управления безопасностью через синтез модели управляемого объекта и его внешних и внутренних связей, решение проблемы выбора приоритетных объектов защиты с точки зрения обеспечения эффективности функционирования и общей безопасности СССР. В качестве основы современных систем мониторинга угроз и рисков безопасности предложена концепция управления рисками, направленная на формирование механизмов, методов и инструментов синтеза, анализа и прогнозирования рисков чрезвычайных ситуаций. **Вывод.** Предложенный метод может быть применен для широкого круга задач первичного анализа, синтеза и количественной оценки рисков ОКВИ и управления безопасностью СССР различного назначения.

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

Для цитирования: Бочков А.В. О методе синтеза рисков в управлении безопасностью структурно-сложных систем // Надежность. 2020. №1. С. 57-67. <https://doi.org/10.21683/1729-2646-2020-20-1-57-67>

Поступила 13.12.2019 г. / После доработки 23.01.2020 г. / К печати 20.03.2020 г.

...есть люди, которые будут комфортнее чувствовать себя в лабиринтах Альп с картой Пиренеев в руках, чем вообще без карты. Конечно, никто не делает этого в прямом смысле, но куда хуже поступают те, кто, имея дело с будущим, полагаются на меры риска. Они предпочитают ущербный прогноз отсутствию прогноза.

Насим Талеб

Введение

Надежность и безопасность являются ключевыми свойствами ССС критического и бизнес-критического назначения, требования к которым постоянно растут. Это обусловлено несколькими факторами.

Во-первых, растут риски аварий и катастроф техногенного характера. Например, по данным, озвученным на известной общеевропейской конференции ESREL, такие аварии составляют 70% от общего количества. Почти каждый десятый пуск ракет-носителей заканчивается аварией, что приводит к последствиям экономического и экологического характера.

Во-вторых, усложнение систем не сопровождается адекватным увеличением показателей безотказности их компонент, что вызывает дефицит надежности и безопасности ССС за отсутствия адекватных структурных решений. Кроме того, растет разнообразие компонент, которые могут использоваться для построения систем, что затрудняет, в свою очередь, поиск вариантов компенсации этого дефицита.

В-третьих, уникальность таких систем как с коротким, так и с длительным временем активного использования, приводит к дефициту достоверной информации относительно реальных значений показателей безотказности их компонент ССС в целом. Острота этого фактора увеличивается пропорционально росту сложности и декларируемой безотказности компонент, например, больших и сверхбольших интегральных микросхем. Кроме того, коммерческий характер производства некоторых элементов и жесткая конкуренция приводят к закрытию или недостоверности информации относительно их безотказности.

С другой стороны, современные методы теории надежности и теории рисков сложных технических систем и соответствующие информационные технологии поддержки принятия решений при их разработке, эксплуатации и реинжиниринга не предоставляют адекватных рекомендаций структурного, функционального и алгоритмического характера. Математические модели классической теории надежности не учитывают в полном объеме многообразие характеристик компонент и вследствие этого фактически не позволяют получить точные решения оптимизационных задач, что приводит к двум видам рисков. Риски, связанные с завышением показателей надежности и

безопасности, могут привести к недопустимому увеличению фактического значения вероятности отказа и аварии, а риски их занижения – относительно действительных – к лишним затратам при разработке и использовании ССС по назначению, что весьма важно, учитывая большую стоимость их производства и владения.

В конце двадцатого века произошли революционные изменения в сфере переработки информации, которые потребовали коренного пересмотра базовых принципов информационного менеджмента. Так, если ранее главное место в информационном обеспечении той или иной деятельности занимали задачи поиска дефицитных данных, то в настоящее время информации стало столько, что наблюдается ее переизбыток. Главными задачами в этих условиях становятся задачи оценивания информации по критериям достоверности, новизны, полезности, а также задачи обеспечения своевременного продвижения информации к конечным потребителям (ЛПР) при обязательном выполнении требований к заданному объему и качеству данных.

Задачи, стоящие перед этими органами управления любой компании или государства, изначально по своей природе непосильны для одного человека или даже целого коллектива. Формирование адекватных управленческих решений требует реализации сложных, распределенных по множеству рабочих мест процедур поиска, хранения и переработки необходимых данных, грамотного сочетания плановой деятельности с деятельностью, вызванной необходимостью быстрой качественной реакции на возникающие непрогнозируемые ситуации.

1. Об уровнях потери устойчивости системы

Управление любой организацией строится по иерархическому принципу. В иерархической системе управления любая подсистема некоторого уровня подчинена подсистеме более высокого уровня, в состав которой она входит и управляется ею. Система управления делится на подсистемы, пока полученная подсистема не перестанет выполнять функции управления, т.е. подсистемой низшего уровня будет подсистема, которая осуществляет непосредственное управление конкретными орудиями труда, механизмами, устройствами или технологическими процессами. Система управления более высокого уровня осуществляет управление технологическими процессами через подсистемы более низких уровней (промежуточных уровней).

Система управления предприятием строится также по многоуровневой структуре. От подсистем, расположенных на более высоком уровне, идет поток управляющей информации к подсистемам, расположенным на более низком уровне, в то же время подсистемы более низкого уровня посылают информацию о текущем состоянии объекта управления подсистемам более высокого уровня. Преимущество иерархической структуры управления предприятием заключается в том, что решение задач управления основывается на базе локальных решений,

принимаемых на соответствующих уровнях иерархии управления. Нижний уровень управления является источником информации для принятия управленческих решений на более высоком уровне. Поток информации от уровня к уровню по количеству информации уменьшается с повышением уровня, но при этом увеличивается ее смысловое (семантическое) содержание.

Все решения, принимаемые для управления производством, делятся на регламентные и случайные. К регламентным решениям относятся решения, которые принимаются регулярно с определенной периодичностью, поэтому большая часть процедур, связанных с выполнением этих решений, поддается автоматизации. Случайные решения принимаются в результате непредвиденных обстоятельств и поэтому не поддаются надежному информационному обслуживанию.

В крупных производственных объединениях для руководителей верхнего уровня управления создаются специализированные системы контроля исполнения директивных вышестоящих и собственных решений (индикативные системы). Это позволяет руководителям сосредоточить свое внимание на стратегических вопросах, на исполнении перспективных задач и долгосрочных плановых работах за счет повышения скорости получения стратегической информации, широты и глубины анализа на основе информационной группировки сведений.

Таким образом, для организации оптимальной системы управления безопасностью в СССР необходима интеграция научно-технических результатов и информационных ресурсов и разработка методики комплексного анализа устойчивости функционирования и методических основ комплексной системы управления рисками компании. Внедрение подобной системы повысит обоснованность решений не только в области прогнозирования угроз возникновения внештатных и кризисных ситуаций различных типов и масштабов, но и в области решения задач оценки эффективности вложений в направления обеспечения безопасности и устойчивого функционирования системы. Комплексный анализ взаимосвязанных рисков позволит дать обоснование необходимых и достаточных уровней безопасности опасных объектов и производств исходя из их важности для решения широкого спектра задач управления.

В настоящее время существует ряд подходов к оценке кризисной (предкризисной) ситуации на некотором объекте (системе), которые с системной точки зрения базируются на решении задач классификации состояний исследуемой частично управляемого динамического объекта (системы) в условиях риска и неопределенности или другими словами – на оценке последствий прогнозируемых сценариев развития текущего состояния в последующие.

С позиций системологии потеря устойчивости развития системы проявляется на нескольких иерархически связанных уровнях, каждый из которых требует отдельного обстоятельного анализа.

Первый уровень – уровень «прочности» (сложная конструкция должна состоять из устойчивых элемен-

тов) – связан с устареванием оборудования, отставанием уровня квалификации персонала от скорости развития современных технологий и истощением ресурсов на которых работает система.

Второй уровень – уровень «надежности» (сохранение работоспособности целого в условиях отказа части элементов) – обеспечивается главным образом дублированием элементов, узлов, подсистем.

Третий уровень – уровень «живучести» – связан со способностью системы активно противодействовать внешним угрозам.

Четвертый уровень – уровень «самоорганизации» – проявляется в адаптивных свойствах системы по «подуровням»:

- а) «гомеостазис» – поддержание «в норме» целостности системы и ее жизненно важных функций;
- б) «обучение, тренинг» – выработка новых методов функционирования для обеспечения способности решать более сложные задачи в будущем;
- в) «преадаптация» (предвидение, интеллект) – подготовка «впрок» оптимизированных планов, механизмов и ресурсов для разрешения кризисных и предкризисных ситуаций, которые не произошли, но возможны в будущем;
- г) «перерождение» – формирование в недрах старой системы «новой» системы, функционирующей по «новым» правилам, в которых старая система существовать не сможет.

Кроме того, как уже упоминалось ранее, ситуационное управление принципиально базируется на том факте, что значительная часть информации представлена в виде текстовых сообщений в средствах массовой информации или других изданиях и имеет внеплановый непрогнозируемый характер. Поскольку эта информация уникальна и изменчива во времени, аналитические структуры компании зачастую не способны оценить ее достоверность, новизну и полезность. Нередко вследствие этого информация переходит в разряд т.н. «слабо формализованных угроз» (т.е. угроз, которым свойственны неопределенность и динамичность исходных данных и знаний), для которых характерны:

- большое количество информации, которая имеет символическую природу;
- не существует математической постановки задачи и формального алгоритмического решения, а если и существует, то пространство поиска решения очень велико и найти его за допустимое время и с имеющимися ресурсами практически невозможно;
- для решения задач требуются эвристики – утверждения, основанные на экспериментальных данных, интуиции; цель их применения – найти более рациональное решение, а не точное математическое, путем исключения заранее непригодных решений.

Несмотря на то, что в последнее время доля слабо формализуемых угроз (появление новых информационных и социальных технологий, террористические и военные риски, вопросы изменения ценовой политики, новые технологии, миграционные процессы и т.п.) растет, что не может не отражаться, в том числе, и на

комплексной безопасности, оценке и анализу этих угроз уделяется недостаточно внимания.

Вместе с тем накапливается опыт создания систем пополнения знаний, появляются модели, позволяющие различать просто информационный шум от информационной атаки или информационного обозначения поступающих событий. В частности, меняется лексика и частотный характер сообщений до «критических» событий и после. Информация имеет, как правило, многоаспектный характер, существуют т.н. «классификаторы проблем» и, тем самым, кроме идентификации угроз накапливаются и систематизируются знания относительно того, какая проблема «цепляет» другие проблемы в соответствии некоторыми сценариями.

Только комплексный анализ взаимосвязанных рисков ССС в целом и входящих в нее подсистем, позволит дать обоснование необходимых и достаточных уровней безопасности опасных объектов и производств исходя из их важности для решения широкого спектра задач управления.

Следует также отметить, что в практике экономико-математического анализа, применяемого в настоящее время, существует засилье методов, происхождение которых вызвано успешным решением тех или иных физико-технических задач. Вместе с тем тезис «классической науки» о беспристрастности законов природы (безусловной воспроизводимости их в жизни) не выдерживает критики. Практические решения часто носят «разовый», «неповторимый» характер, поэтому математика для «жизни» методологически принципиально более сложная, чем, математика для «физики».

При всем уважении к физико-техническим и другим естественнонаучным задачам, изучаемым в них явлениям присуща подчиненность объективным природным закономерностям и независимость от чьих-либо субъективных действий и от чьих-либо интересов. Сознательное вмешательство в развитие «физического мира» сводится, выражаясь математическим языком, к заданию тех или иных «параметров» при использовании неизменных общих закономерностей. Познание физических процессов направлено на выявление и анализ относящихся к ним скрытых причинно-следственных отношений и, тем самым, затрагивает лишь аналитический уровень познания.

Анализ систем не включает в себя ни оценки познанного, ни рассмотрения каких-либо действий, совершаемых познающим субъектом на основании приобретенной информации. Истинный анализ беспристрастен – он не должен указывать, каким должен быть изучаемый объект (каким было бы «хорошо» ему стать), и какие действия следовало бы предпринять для его изменения в том или ином направлении. Тем самым, критерием завершения анализа систем как этапа системного познания является установление непротиворечивости данных, полученных после формализации фактов, и корректности процедур выводов из них.

Вместе с тем исследование большинства явлений, происходящих в реальном мире, вызвано именно необходимостью активного сознательного «пристрастного» изменения познающим субъектом объектов познания,

в частности, необходимостью конструирования таких объектов, которых не было ранее. При этом надо уметь прогнозировать деятельность и вытекающий из нее результат с учетом того, что «другие не спят», т.е. работать в условиях конкуренции в постоянном поиске оптимальных (приемлемых) решений.

2. Замечания об оптимальности

Здесь уместным становится методологическая проработка вопроса «что такое оптимально?». Содержательные представления об оптимальности в условиях конфликтов (т.е. в условиях различия интересов) возникли и развиваются достаточно давно. Во многих исследованиях представление о конфликте и об оптимальности в условиях конфликтов является ведущим в том смысле, что отказ от их рассмотрения делает беспредметным все исследование. Достаточно сослаться на такие явления, как боевые конфликты, политическая борьба, конкуренция в экономике и т.п. Наличие конкуренции в корне меняет существо прогнозных оценок, в том числе и прогнозных оценок достижений тех или иных направлений бизнеса.

Поясним сказанное на примере системы уравнений Лотки-Вольтерра, предназначенной для изучения явления «конвергентной эволюции» (отбора наиболее перспективных направлений развития, в частности):

$$\begin{cases} dN_1/dt = \varepsilon_1 \times N_1 - \gamma_{12} \times N_1 \times N_2 - \gamma_{11} \times N_1^2 = UP_1(N_1, N_2) \times N_1; \\ dN_2/dt = \varepsilon_2 \times N_2 - \gamma_{21} \times N_2 \times N_1 - \gamma_{22} \times N_2^2 = UP_2(N_1, N_2) \times N_2. \end{cases} \quad (1)$$

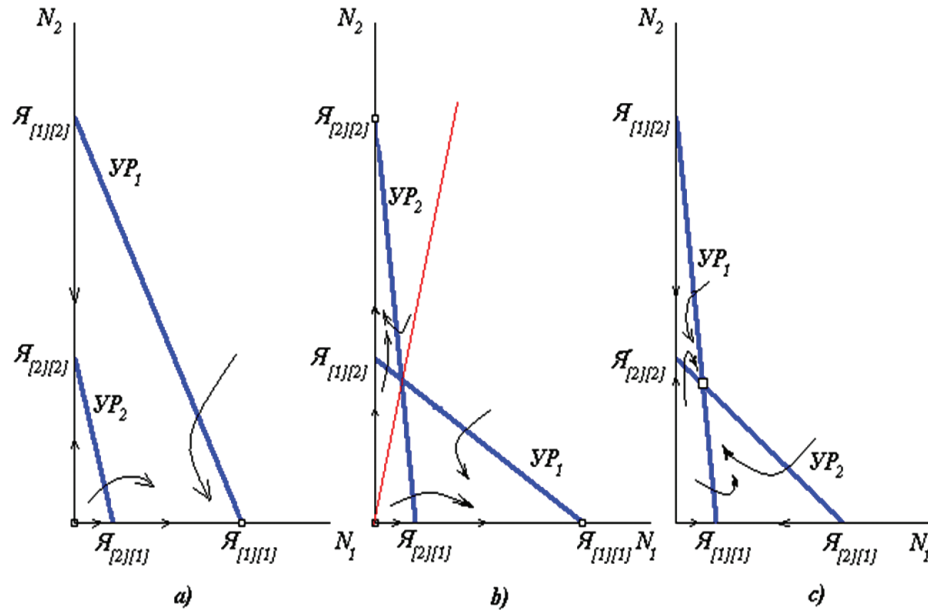
Первые коэффициенты в правых частях уравнений ε_1 и ε_2 – скорости экономического роста капиталов двух конкурирующих направлений, вторые γ_{12} и γ_{21} – уровень межвидовой конкуренции (воздействия внешних конкурентов, «чужих»); третьи γ_{11} и γ_{22} – являются показателями внутривидовой конкуренции (воздействия внутренних конкурентов, «своих») – развитие собственного производства уменьшает дефицит продукции, то есть снижает цены на товар, тем самым замедляя рост производства). Здесь N_1 и N_2 – размеры соответствующих конкурирующих капиталов.

Обозначим через $Y_{[a][b]}$ координаты пересечения линейных уравнений $UP_a(N_1, N_2)$ с осями переменных $(0, N_b)$:

$$Y_{[1][1]} = \frac{\varepsilon_1}{\gamma_{11}}, Y_{[1][2]} = \frac{\varepsilon_1}{\gamma_{12}}, Y_{[2][1]} = \frac{\varepsilon_2}{\gamma_{21}}, Y_{[2][2]} = \frac{\varepsilon_2}{\gamma_{22}}. \quad (2)$$

В зависимости от значений этих четырех коэффициентов и начальных значений капиталов $N_1(0)$ и $N_2(0)$ система (1) допускает решения трех типов, описывающих три различных исхода конкурентной борьбы (рис. 1).

Случай (а). Если одновременно выполняются $Y_{[1][1]} > Y_{[2][1]}$ и $Y_{[1][2]} > Y_{[2][2]}$, то первый вид бизнеса, безусловно, вытесняет своего оппонента независимо от «стартовых» начальных условий (см. рис. 1а). Реализуется сценарий «отбора» сильнейшего, у слабейшей стороны нет шансов на выживание.



Y_{P1} и Y_{P2} – изоклины вертикальных и горизонтальных касательных, соответственно.

Рисунок 1. Фазовые портреты системы Лотки-Вольтерра

Случай (b). Если $Y_{1[1][1]} > Y_{2[1][1]}$ и $Y_{2[2][2]} > Y_{1[2][2]}$ то снова имеется только один победитель, но который из двух – это уже зависит от начальных условий (см. рис. 1b).

В этом случае антагонизм конкурентов настолько силен, что факторы самоограничения не играют существенной роли. Случай (b) отличается от предыдущего случая тем, что «слабейшая» сторона получает шанс победить за счет «численного превосходства»: требуется наличие соответствующего «стартового капитала», помещающего победителя с предпочтительной для него стороны от сепаратриссы, проходящей через точку фазовой плоскости (0,0) и точку пересечения изоклин вертикальной и горизонтальной касательных. Этот случай описывает ситуации на рынке, когда главную роль играет факт того, достаточно ли «критическая масса» стартового капитала для того, чтобы задавить конкурента «в зародыше», не дать ему вырасти до того уровня, когда с ним придется «считаться» (делить рынок).

Случай (c). Внутривидовая борьба для обоих конкурентов настолько сильна (каждый занят решением проблем торможения роста капитала вследствие «внутренних проблем»), что конкуренция среди «своих» превышает давление со стороны «чужаков» (при $Y_{2[2][2]} < Y_{1[2][2]}$ и $Y_{1[1][1]} < Y_{2[1][1]}$).

В этом случае возможно длительное сосуществование обеих конкурирующих сторон на рынке (см. рис. 1c). При этом имеется единственное устойчивое решение, при котором скорости воспроизводства новых элементов конкурирующих сторон компенсируют торможение, оказываемое сочетанным воздействием факторов внутренней и внешней конкуренции.

Эти модели используются, в частности, для прогнозирования перспектив относительно однородных технологий, конкурирующих между собой, (например,

вследствие принадлежности различным собственникам), но и имеющих «общего врага». Например, для газовой промышленности таковыми являются ядерная энергетика, возможно, другие альтернативные виды энергетике, химическая промышленность материалов, замещающих газ, используемый как сырье для синтеза и т.д.

Как видно даже из анализа приведенной выше упрощенной аналитической модели – использование средств «технического анализа» экономических данных, построенного на различных моделях регрессии не корректно всегда. По крайней мере, в условиях, когда доминирующим фактором является не динамика предыдущей успешности, а факторы, определяющие конкурентоспособность старых (проверенных) технологий на фоне развивающихся новых технологий (и «своих» и «чужих»), в условиях их борьбы за одного и того же ограниченного по возможностям потребителя, необходимы методы анализа конкурентных систем.

3. Алгоритм синтеза функции риска

В статье [2] предлагался алгоритм решения задачи распределения ресурсов, предназначенных для защиты объектов критической инфраструктуры от террористических атак, на основе субъективных экспертных оценок. Покажем, как от качественных экспертных оценок можно перейти к количественным оценкам угрозы, используя алгоритм, названный ранее синтезом рисков.

Итак, рассмотрим некоторый (k -й) объект CCC.

В результате предполагаемого воздействия некоторого уровня интенсивности этому объекту, через его полный (или частичный) выход из работоспособного состояния, будет нанесен определенный ущерб. Обозначим его через X .

С учетом того, что не каждое воздействие априори приводит к разрушениям, профиль защиты k -го объекта может быть описан интервальными представлениями посредством задания четырех матриц:

$$Q_{\min}^{[k]}(i, j), Q_{\max}^{[k]}(i, j), X_{\min}^{[k]}(i, j), X_{\max}^{[k]}(i, j), \quad (3)$$

где $i(i=0, 1, \dots, I^{[k]})$ – уровень защиты k -го объекта (нулевой уровень ($i=0$) соответствует текущему состоянию защиты).

Интерпретация элементов матрицы такова: если на указанный объект k с уровнем защиты i будет осуществлено воздействие с уровнем интенсивности j , то с вероятностью от $Q_{\min}^{[k]}(i, j)$ до $Q_{\max}^{[k]}(i, j)$ ССС будет нанесен ущерб величиной от $X_{\min}^{[k]}(i, j)$ до $X_{\max}^{[k]}(i, j)$.

Ясно, что величины (3) будут расти по мере роста уровня интенсивности воздействия j и будут снижаться по мере возрастания уровня защищенности объекта i .

Очевидно, что защита на любом уровне требует определенных материальных затрат как со стороны собственника объекта, так и государства. Обозначим величину затрат на создание и поддержание защиты объекта k на i -ом уровне как $Y^{[k]}(i^{[k]})$.

Поскольку суммарный ресурс, выделяемый на защиту всех объектов, ограничен, должно выполняться неравенство:

$$\sum_k Y^{[k]}(i^{[k]}) \leq Y, \quad (4)$$

где Y – сумма всех затрат на защиту объектов при условии, что для каждого объекта k выбран вариант системы защиты $i^{[k]}$.

В случае природных воздействий, у которых, в отличие от воздействий, организуемых человеком, не существует преимущества выбора цели и варианта воздействия, то есть, природа неизбирательна (как и технологические отказы), «оптимальный» профиль защищенности объектов мог бы быть достигнут посредством последовательного выполнения следующего алгоритма:

Шаг 1. Оценить вероятности $\lambda^{[k]}(j)$ воздействия на каждый k -ый объект j -го уровня интенсивности;

Шаг 2. Рассчитать медианное значение риска от реализации воздействия на k -ый объект j -го уровня интенсивности при $i^{[k]}$ -ом варианте реализации системы защиты объекта:

$$R[k; i^{[k]}] = \sum_{j=0}^J \left\{ \lambda^{[k]}(j) \times \left(\frac{Q_{\min}^{[k]}(i^{[k]}, j) + Q_{\max}^{[k]}(i^{[k]}, j)}{2} \right) \times \left(\frac{X_{\min}^{[k]}(i^{[k]}, j) + X_{\max}^{[k]}(i^{[k]}, j)}{2} \right) \right\}; \quad (5)$$

Шаг 3. Определить величину предотвращенного риска на единицу вложенных в защиту средств – $\theta[k, i^{[k]}]$:

$$\theta[k, i^{[k]}] = \frac{R[k, i^{[k]}]}{Y^{[k]}(i^{[k]})}; \quad (6)$$

Шаг 4. Выбрать для каждого k -го объекта максимальное из значений $\theta[k, i^{[k]}]$:

$$\theta[k, i^{*[k]}] = \max_{i^{[k]}} \{ \theta[k, i^{[k]}] \}, \quad (7)$$

т.е. при выбранном варианте $i^{*[k]}$ наблюдается максимальное снижение риска на единицу вложенных средств для k -го объекта.

Шаг 5. Составить ранжированный перечень объектов, располагая их по убыванию величины показателя $\theta[k, i^{*[k]}]$, и отсчитать первые \tilde{K} объектов в списке такие, что суммарные затраты на их защиту вкладываются в выделенные средства Y , а на $(\tilde{K}+1)$ -ый объект ресурсов не хватает.

Суть вышеприведенной процедуры проста и понятна: нет смысла изыскивать средства на дополнительную защиту тех объектов, которым ничто не грозит (величины угроз $\lambda^{[k]}(j)$ малы). Также нецелесообразно защищать дополнительно те объекты, временная потеря работоспособности которых практически не сказывается на величине суммарных потерь собственника объектов (соответственно, малы $X_{\max}^{[k]}(i^{[k]}, j)$). И, наконец, дополнительная защита нецелесообразна на тех объектах, которые уже защищены настолько хорошо, что снижение потерь может быть принципиально достигнуто, но неадекватно большими средствами (т.е. малы значения $\theta[k, i^{*[k]}]$).

Ключевым моментом описанного выше алгоритма является составление ранжированного перечня объектов по критерию минимизации математического ожидания потерь на единицу вложенных средств в их защиту (в их устойчивое функционирование).

В формуле (5) четко прослеживается необходимость сбора и оценки данных по трем компонентам:

- по величинам потерь, вызванных реализацией воздействий $X_{\min}^{[k]}(i, j)$, $X_{\max}^{[k]}(i, j)$;
- по показателю «агрессивности среды функционирования» $\lambda^{[k]}(j)$;
- по зависимости рисков от типов объектов k .

Величины потерь X , вследствие того, что объекты ССС не являются автономными предприятиями, должны отражать системный эффект (или социально-экономический мультиэффект), который существенно возрастает в зависимости от того, какие из потребителей продукции объекта, подвергнувшегося воздействию, пострадают из-за снижения его работоспособности.

Следовательно, необходимо рассматривать не средние, а верхние границы показателей ущербов и ввести в рассмотрение дополнительно четвертый компонент – показатель важности непрерывного функционирования объекта в связи с каскадным эффектом усиления последствий потери работоспособности объекта для других объектов экономики.

И, наконец, дополнительно требуется ввести пятый компонент, необходимый для адекватного ранжирования объектов в случае террористического воздействия на объекты. Необходимость его введения обусловлена тем, что если воздействие, все-же, носит активный и

целенаправленный характер, при этом у него имеются неизвестные ни экспертам службы безопасности, ни компетентным органам государства факторы ценности и приоритеты, смещающие значения $\lambda^{[k]}(j)$ от «средневзвешенных по отрасли». Иногда эти «дополнительные» ценности носят специфический характер: террористы, например, склонны к чрезмерному кровопролитию и захвату заложников, ритуальным убийствам и т.д. Часто системная значимость охраны конкретных объектов временно возрастает во время пребывания на них первых лиц государства, министров, особенно во время пуска политически важных производственных объектов не только международного, но и регионального уровня внутри страны. Можно достаточно долго анализировать факторы, требующие учета специфики той или иной преступной деятельности, но важен сам факт: преступность действует исходя из собственных представлений о результативности и осуществимости атак. Тем самым происходит смещение приоритетов выбора целей – для террористов важна не только и не столько экономическая война, не столько важен ущерб, наносимый собственнику объектов (как конкуренту, как «оружию» влияния на сопредельные государства и т.п.), сколько достижение через нанесение ущерба объектам данной CCC каких-то других целей.

Учесть эти обстоятельства поможет пятый компонент – корректирующий коэффициент $\mu^{[k]}$, изначально равный для всех объектов единице, и который может быть, по мнению ЛПР или экспертов, увеличен таким образом, чтобы повысить приоритет включения именно k -го объекта в список объектов, оснащаемых дополнительными мерами защиты по причинам, не учитываемым общими для всех объектов правилами. В какой-то степени целесообразность введения показателя $\mu^{[k]}$ становится более понятна из следующей интеграционной модели моделей.

Итак, пусть \tilde{Z} – оценка суммарного ресурса, имеющегося у сил, заинтересованных в нарушении безопасности объектов CCC. Если $\tilde{Z} < Z$, то защищающаяся сторона недооценивает возможности воздействия, если $\tilde{Z} > Z$, то, напротив, имеет место переоценка интенсивности воздействия.

Далее рассмотрим активное воздействие как наиболее непредсказуемый случай. Будем считать, что на момент выбора атаки нарушитель имеет собственные представления о количестве ресурсов, выделяемых собственником системы на охрану своих объектов, то есть, у него имеются некоторые представления и о том, как мог измениться известный ему «нулевой вариант».

Нарушители обладают правом выбора целей, и они способны выбирать наборы объектов, которые будут ими атакованы. Пусть их выбор базируется на их собственной модели ожидаемого ущерба, то есть, в их распоряжении имеются четыре аналогичные (3) матрицы для каждого из объектов: $\tilde{Q}_{\min}^{[k]}(i, j)$, $\tilde{Q}_{\max}^{[k]}(i, j)$, $\tilde{X}_{\min}^{[k]}(i, j)$, $\tilde{X}_{\max}^{[k]}(i, j)$ и свое представление о том, сколько ресурсов \tilde{Y} потрачено собственником на защиту всех объектов CCC. Аналогично, если $\tilde{Y} < Y$, то противник недооценивает возможности защиты объектов и, если

$\tilde{Y} > Y$, то он их переоценивает. Очевидно, что оценки $\tilde{Q}_{\min}^{[k]}(i, j)$, $\tilde{Q}_{\max}^{[k]}(i, j)$, $\tilde{X}_{\min}^{[k]}(i, j)$, $\tilde{X}_{\max}^{[k]}(i, j)$ также могут быть нарушителями как завышены, так и занижены, тем не менее, в соответствии со своим правом выбора, они выбирают такой набор объектов для атаки и такие варианты подготовленности нарушителей для каждого объекта, при которых наносится максимальный ущерб.

Обозначим через $\delta^{[k]}(i, j)$ характеристическую функцию, которая означает, что против k -го объекта с ожидаемым уровнем защиты $i(i=0, 1, \dots, I^{[k]})$ выбрана атака уровня $j(j=0, 1, \dots, J^{[k]})$. Если для всех $i(i=0, 1, \dots, I^{[k]})$ значения $\delta^{[k]}(i, j)$ равны нулю, то j -ый объект не будет подвержен атаке уровня j . Если при всех j и всех i значения $\delta^{[k]}(i, j)$ равны нулю, то k -й объект при предполагаемом противником варианте целеполагания полностью выбывает из списка целей.

Если для некоторого \tilde{i} значение $\delta^{[k]}(\tilde{i}, j(\tilde{i})) = 1$, мы считаем, что объект k с уровнем защиты 0 выбран противником как цель для атаки уровнем подготовленности $j(\tilde{i})$.

Перечисленные свойства записываются системой равенств:

$$\begin{cases} \forall k \forall i \forall j \delta^{[k]}(i, j) \times (1 - \delta^{[k]}(i, j)) = 0, \\ \forall k \left(\sum_{i=0}^{I_k} \sum_{j=0}^{J_k} \delta^{[k]}(i, j) - 1 \right) \times \left(\sum_{i=0}^{I_k} \sum_{j=0}^{J_k} \delta^{[k]}(i, j) \right) = 0. \end{cases} \quad (8)$$

Учитывая, что

$$\forall j \sum_{i=0}^{I_k} \sum_{k=1}^K \delta^{[k]}(i, j) = N_j \quad (9)$$

и дополняя (8), (9) системой ограничений мы получаем оценку суммарного ущерба, наносимого объекту:

$$\tilde{R} = \sum_k \sum_{i=0}^{I_k} \sum_{j=0}^{J_k} \left\{ \delta^{[k]}(i, j) \times \left(\frac{\tilde{Q}_{\min}^{[k]}(i^{[k]}, j) + \tilde{Q}_{\max}^{[k]}(i^{[k]}, j)}{2} \right) \times \left(\frac{\tilde{X}_{\min}^{[k]}(i^{[k]}, j) + \tilde{X}_{\max}^{[k]}(i^{[k]}, j)}{2} \right) \right\}. \quad (10)$$

Обозначим \tilde{R} как $\tilde{R}(Var_i, Var_j)$, подчеркивая, что \tilde{R} зависит как от варианта защиты объектов Var_j , так и от варианта воздействия Var_i . Ищем максимум \tilde{R} для всех вариантов воздействий, удовлетворяющих ограничениям, при рассмотрении всех вариантов оснащения дополнительной защитой в качестве параметров:

$$\tilde{R}^*(Var_i) = \max_{Var_j} \{ \tilde{R}(Var_i, Var_j) \}. \quad (11)$$

Тем самым постулируется, что противник (природа) выбирает самый худший для защищающейся стороны вариант. Следовательно, задача защиты сводится к ограничению множества выбора вариантов воздействия – ищется такое усиление объектов, которое минимизирует $\tilde{R}^*(Var_i)$. То есть, задача управления безопасностью сводится к поиску равновесного значения \tilde{R}^{**} :

$$\tilde{R}^{**} = \min_{Var_i} \{ \tilde{R}^*(Var_i) \}. \quad (12)$$

Предлагаемая постановка имеет типовой вид задач теории игр. Решением этой задачи является равновесие по Нэшу – седловая точка (Var_{js}, Var_{js}) :

$$\tilde{R}^{**} = \tilde{R}(Var_{js}, Var_{js}). \quad (13)$$

В этой точке «обороняющейся стороне» не выгодно менять стратегию оснащения Var_{js} , поскольку вне этой стратегии у противника появляются возможности для нанесения более «чувствительных» воздействий. Одновременно, активной атакующей стороне не выгодно менять свой план $Var_{js}(Var_{js})$, так как любое изменение приводит к снижению суммарных ущербов, которые он стремится нанести объектам CCC, а через них – государству в целом.

Задача в такой постановке теоретически имеет очень большую размерность, обладает большой комбинаторной сложностью, но вполне решается вследствие монотонности используемых критериев и линейности систем ограничений.

Основные проблемы решения этой задачи имеют скорее информационно-технологический, а не математический характер:

- для каждого k -го объекта необходимо иметь оценки последствий возможных воздействий разной интенсивности j , что часто не достижимо практически;
- для всей CCC требуется рассмотрение рисков, которым подвергаются объекты, в комплексе возможных, в том числе и слабо формализуемых угроз: оптимизация защиты тем более эффективна, чем более точно оцениваются потенциальные возможности воздействия (а они неоднородны как в технологическом, так и в региональном аспекте).

В рамках рассмотренной постановки, учитывающей комплексное воздействие, кардинально меняется понимание оценки эффективности систем защиты. Для активного воздействия, в силу ограниченности ресурсов, доступных преступному миру, естественно ожидать от него перемещение целеполагания с хорошо защищенных объектов (с малой ожидаемой результативностью воздействий) на менее защищенные объекты (с большей результативностью, но при меньших разовых ущербах). Очевидно, что нерационально дополнительно защищать объекты, которые никто не атакует. Возможно, потому и не атакуют, что ведется плановая работа по усилению охраны.

Еще одним ключевым элементом рассматриваемой задачи является то, что поиск эффективных решений с обеих сторон лежит в значительной мере в информационной плоскости:

- преступник, готовясь к атаке на объект, в идеале ищет сообщников, которые помогли бы ему выбрать цель приложения сил, достижимую при его уровне подготовленности и оснащенности;
- система защиты способна была бы оказать большее концентрированное противодействие, если бы знала о намерениях преступности.

Поэтому при описании вышеприведенной процедуры для активного воздействия неоднократно подчеркивается,

что речь идет только об оценках с обеих сторон. Из-за неустрашимой неопределенности оценок в качестве решения задачи о выработке стратегии и тактики усиления защиты объектов CCC от возможных противоправных действий, включая террористические акты и атаки диверсионных групп, целесообразно «заглубить» игровую постановку [3]. При этом заглублении должны «идеализироваться возможности противника» и ужесточаться характеристики возможных потерь, например, путем перехода от медианных оценок рисков к максимальным.

В заключение заметим, что на этапе решения задачи оценки рисков необходимо установить связи анализируемых показателей безопасности с показателями высокого уровня (например, стратегическими целевыми показателями) и степени их влияния на достижение целевых значений этих показателей. Контроль объекта мониторинга должен быть организован таким образом, чтобы можно было вовремя провести управленческие решения, если состояние объекта приближается к опасной зоне. Данная задача распадается на ряд подзадач, так как в вертикально интегрированных компаниях есть несколько центров принятия решений на разных уровнях управления. Перспективными при решении данной задачи могут оказаться методы оценки надежности достижения целевых показателей и методы группового анализа [3, 4].

4. Об индикаторах предкризисных ситуаций

Вычисление параметров, описывающих уровни конкуренции, требует, помимо использования стратегического «коридорного» прогноза, создания системы мониторинга «слабо формализуемых» угроз устойчивому функционированию и развитию CCC, т.е. разработки индикаторов предкризисных ситуаций.

Очевидно, что разработка индикаторов предкризисных ситуаций – сложнейшая многоуровневая задача и не может укладываться в одну какую-то универсальную схему, поэтому дальнейшее развитие системы стандартизации и методологического обеспечения управления безопасностью в CCC предполагает рассмотрение ряда направлений дополнительных исследований по разработке индикаторов предкризисных ситуаций, которая должна вестись в «частных» исследовательских парадигмах с использованием различных теоретических подходов и моделей:

- информационно-логический подход;
- энергетический (балансовый) подход;
- балансовый подход (программно-целевое планирование);
- индикация состояния системы на основе моделей группового поведения элементов систем;
- индикация состояния системы на основе измерения корреляционных связей в динамике показателей элементов системы;
- индикация состояния системы на основе моделей «серого ящика» (нейронные сети, метод опорных векторов и т.п.).

Кратко поясним суть упомянутых подходов.

Информационно-логический подход. В этом подходе сущность «критическая ситуация» C описывается в виде логической функции – объединения возможных частных «эталонных» реализаций логикой «ИЛИ»:

$$C = \bigcup_n C^{[n]}. \quad (14)$$

Каждая критическая ситуация $C^{[n]}$ описывается некоторым достаточно большим подмножеством информационно-логических признаков (подобно ключевым словам в тексте). Описания эти в общем случае не однозначны, возможны «синонимы», пропуски «подразумеваемых» признаков и т.п. Как правило, признаки разделяются на три категории: индикаторы состояния самой исследуемой системы X , индикаторы «нейтральной» внешней среды (природной среды) p и индикаторы деятельности потенциального противника («конкурента») Y :

$$C^{[n]} = F^{[n]} \left\{ X^{[n,1]}, \dots, X^{[n,K(n)]}; p^{[n,1]}, \dots, p^{[n,L(n)]}; Y^{[n,1]}, \dots, Y^{[n,M(n)]} \right\}. \quad (15)$$

Предкризисная ситуация (угроза критической ситуации) диагностируется как неполный набор индикаторов, близкий к одному или нескольким «эталонным» наборам аргументов функции $F^{[n]}$. При этом предполагается, что решающая система способна оценивать вероятности перерастания угроз в реальные критические ситуации. Здесь нужны модели природных явлений и модели поведения конкурентов в ответ на реализацию тех или иных управляющих решений.

Подобный подход развивается в теории конфликтующих структур и в теории эвристик в многошаговых позиционных играх [5], в теории принятия решений [6], в ряде областей применения искусственного интеллекта [7] (медицинские диагностические системы и другие системы распознавания образов). В любом случае при этом подходе реализуется некоторая автоматизация формирования гипотез [8] и некоторые механизмы «размывания» образа «эталона» [9].

Описания моделей сценариев предкризисных ситуаций оформляются в виде деревьев (сетей) событий (отказов), иллюстрирующих логику развертки сценариев [10]. Синонимия (конкуренция или замещение рисков) моделируется в виде вложенных друг в друга функций сверток информационных признаков $F^{[n]}$, начиная со сверток первичных признаков в более крупные агрегативные признаки [6]. При большом количестве первичных признаков зачастую используется иерархическое устройство словарей признаков [11].

Описание деревьев событий – прерогатива экспертов, однако в последнее время проявляется устойчивый интерес к описанию сложных слабо формализуемых решений экспертов с помощью «генетических» алгоритмов и других эвристических методов, сочетающих поиск наилучшего описания сложной системы (предкризисной ситуации в ней) и ограниченную логику эволюционного отбора [12].

Энергетический (балансовый) подход. В деятельности любой компании прослеживается три компонента:

ресурсная компонента, научно-технологическая (производственная) компонента и внешнеэкономическая (рыночная) компонента.

Из этих представлений количество проданного товара может быть оценено следующей формулой

$$T = E \times K_{\text{пл}} \times K_{\text{план}}, \quad (16)$$

где E – энергия, необходимая для производства товара; коэффициент полезного действия ($K_{\text{пл}}$) ($0 \leq K_{\text{пл}} \leq 1$) – отражает эффективность производства товара (научно-технологический уровень производителя); коэффициент качества плана ($K_{\text{план}}$) меньший единицы указывает на то, что продукт произведен, но оказался невостребованным (или проданным по меньшей цене), например, из-за действий конкурентов на рынке (появление альтернативных источников энергии), или каких-то внешнеполитических (внешнеэкономических) обстоятельств (риски неплатежей, перенос энергоемких, загрязняющих окружающую среду производств в страны третьего мира и других).

Этот подход позволяет разрабатывать индикаторы угроз критических ситуаций на языке вероятностей срыва потока мощности производства товаров. Особое место при этом подходе уделяется определению «узких мест», определяющих предельные скорости потоков товаров (принцип Гаузе, «узкое горло Пауэлла» и другие), и показатели которых используются при анализе продуктивности самовоспроизводящихся систем с учетом «внутривидовой» и «межвидовой» конкуренции [13].

Балансовый подход (программно-целевое планирование). Методами сетевого (календарного) планирования можно рассчитать зависимости вероятностей выполнения тех или иных работ от объемов выделенных ресурсов R и выделенного времени T . По физическим причинам существуют минимальные значения T_{min} и R_{min} , ниже которых работа невыполнима в принципе. Поэтому для более вероятного выполнения работ создаются «резервы» времени и ресурсов и с учетом этих резервов предполагается соблюдение графика исчерпания времени и ресурсов в зависимости от оставшегося объема работ.

Анализируя динамику расхода времени и средств, уместно в качестве индикаторов использовать данные, свидетельствующие о приближении показателей исполнения работ, не лежащих на «критических» путях в сетевых графиках, к показателям критических работ. Угроза образования большого количества новых критических путей по ресурсам и/или времени может служить индикатором предкризисной ситуации.

Все обсужденные подходы предполагают усложняющуюся детализацию описания динамики системы в парадигме адаптивного управления, то есть, анализируются уровни отклонения от выбранного планового графика деятельности изучаемой системы так, как будто только «внешние» факторы (природа, конкуренция) выбивают систему из устойчивого равновесия, и надо измерить вероятность выхода за некоторый барьер устойчивости.

Вместе с тем возможны ситуации, в которых удерживать «равновесие» невозможно или нецелесообразно,

и требуется перестройка структуры системы – поиск «жизни по-новому».

Индикация состояния системы на основе моделей группового поведения элементов систем. В последнее время для предсказания поведения экономических систем часто используются «полевые» модели на основе уравнений Ланжевена и уравнений Фоккера-Планка. Эти уравнения описывают динамику элементов системы как некоторый «рой частиц», на который действуют два типа факторов: факторы дрейфа, смещающие «центр тяжести» под действием внешней силы, а также диффузионные факторы, отражающие уровни свободы перемещения частиц внутри роя. В моделях разрабатываются индикаторы разрушения целостности «роя» или его вырождения. Модельные индикаторы носят оценочный характер, поскольку опираются, главным образом, на справедливость законов больших чисел (теорию больших отклонений при случайных блужданиях).

Отмечается близкая связь «полевых» моделей с прикладной теорией катастроф [14], в частности показывается близость таких индикаторов, как «учащение больших отклонений – сокращение времени выхода контролируемых показателей из «коридоров», замедление «скорости релаксации системы к равновесным состояниям», «вырождение матрицы устойчивости Гессе».

Индикация состояния системы на основе измерения корреляционных связей в динамике показателей элементов системы. В этих постановках основанием для классификации критической ситуации является изменение устойчивых (например, корреляционных, причинно-следственных, ассоциативных, информационных) связей между элементами системы. Для анализа взаимосвязанного экономического поведения крупных подсистем (дочерних предприятий) представляет интерес применения разработок в области анализа гендерных (семейных) отношений, а также математической теории комплиментарности этносов Гумилева [15].

Индикация состояния системы на основе моделей «серого ящика» (нейронные сети). Нейросетевая классификация состояний сложной системы основана на выявлении информационных признаков и связей между ними, соответствующих наиболее часто встречающимся конструкциям критических ситуаций. Получение решающих правил осуществляется посредством «обучения на примерах».

Поскольку законы распределения критических ситуаций не известны, требуется большое количество параметров для их описания и большое количество примеров, поэтому при решении задач классификации «критическая ситуация – некритическая ситуация» используются те или иные методы упрощения.

Для моделирования стохастических процессов наиболее эффективны следующие нейросетевые решения: вероятностные нейронные сети [16], самоорганизующиеся карты Кохонена [17] и динамически подстраиваемые под изменяемую статистику алгоритмы, описывающие

координаты «эталонов» критических ситуаций в виде растущего «нейронного газа», распространяющегося по пространству описания примеров [18].

Заключение

Все вышесказанное, а также требования системного подхода к исследованию перечисленных в статье задач, естественно приводит к необходимости моделирования системы обеспечения безопасности ССС как развивающейся системы [19]. Любой объект исследования, дополненный, если необходимо, определенными связями с другими развивающимися объектами, в частности, с субъектами исследования, можно интерпретировать в виде такой системы. Понимание этого обстоятельства способствует все более активному развитию этого направления в различных отраслях науки [19-23].

Экспертные оценки показывают, что суммарный эффект от применения всех доступных средств ситуационного анализа (идентификация опасной деятельности, декларирование безопасности, планирование действий при аварии, информирование населения о возможной чрезвычайной ситуации) по снижению аварийности и внеплановых потерь может достигать 10–15 %. Например, быстрое законодательное принятие странами Европейского сообщества основных положений Директивы Seveso (1982) [24] позволило снизить аварийность в развитых странах в 4–8 раз (от 400 аварий, в том числе 75 крупных, в 1983 г., до 70, в том числе 21 крупной, в 1989 г.). При этом предлагаемые меры информационного и организационного характера станут более действенными, если все составляющие системы управления производственной безопасностью в части прогнозирования, предотвращения и локализации последствий ситуаций с негативными последствиями будут работать в соответствии с едиными регламентами и стандартами. Следовательно, необходим процесс постепенной актуализации состояния информационного, нормативно-методического и прогнозно-аналитического обеспечения деятельности в области производственной безопасности как на уровне системообразующих корпораций, так и на уровне государства.

Вообще, задача мониторинга функционирования сложного «организма» корпорации – ключевая задача управления безопасностью. Этот мониторинг, если использовать аналогии, подобен профилактическим терапевтическим мероприятиям в медицине. В отличие от диспетчерского управления, которое призвано оперативно реагировать на изменение ситуации, локализовать возникновение внештатных ситуаций, иногда решать задачу (если пользоваться той же аналогией) «хирургического» вмешательства, центр мониторинга (а в перспективе сеть центров для получения объективной информации о происходящих в ССС изменениях) призван предвидеть возникновение негативных тенденций в окружении ССС, в ее внутренних процессах, чтобы предложить «лечение», которое поможет избежать перерастания обнаруженных угроз во внештатные и кризисные ситуации.

Библиографический список

1. **Бочков, А.В.** О природе рисков в управлении безопасностью структурно сложных систем [Текст] / А.В. Бочков // Надежность. – 2019. – № 4, С. 54-66. – URL: <https://doi.org/10.21683/1729-2646-2019-19-4-54-66>.
2. **Бочков, А.В.** Решение задачи распределения ресурсов, предназначенных для защиты объектов критической инфраструктуры от террористических атак на основе субъективных экспертных оценок [Текст] / А.В. Бочков, И.А. Ушаков // Надежность. – 2015. – № 1. – С. 88-96. – URL: <https://doi.org/10.21683/1729-2646-2015-0-1-88-96>
3. **Bochkov, A.V.** Dynamic Multi Criteria Decision Making Method for Sustainability Risk Analysis of Structurally Complex Techno-Economic Systems [Text] / A.V. Bochkov, N.N. Zhigirev, V.V. Lesnykh // Reliability: Theory & Applications, Vol. 1, № 2(25), 2012, June, p.36-42.
4. **Bochkov, A.V.** Development of Computation Algorithm and Ranking Methods for Decision-Making under Uncertainty [Text] / A.V. Bochkov, N.N. Zhigirev: Ram M., Davim J. (eds) // Advanced Mathematical Techniques in Engineering Science. – CRC Press. – Series: Science, Technology and Management. – 2018. – May, 17. – P. 121-154.
5. **Лефевр, В.А.** Конфликтующие структуры [Текст] / В.А. Лефевр. – М.: Сов. радио, 1973.
6. **Мушик, Э.** Методы принятия технических решений [Текст] / Э. Мушик, П. Мюллер. – М.: Мир, 1990.
7. **Попов, Э.В.** Статические и динамические экспертные системы [Текст] / Э.В. Попов, И.Б. Фомин, Е.Б. Кисель и др. – М.: Финансы и статистика, 1996. – 315 с.
8. **Гаек, П.** Автоматическое образование гипотез: математические основы общей теории [Текст] / П. Гаек, Т. Гавранек. – М.: Наука, 1984.
9. Нечеткие множества и теория возможностей [Текст]. – М.: Радио и связь, 1986. – 408 с.
10. **Подиновский, В.В.** Парето-оптимальные решения многокритериальных задач [Текст] / В.В. Подиновский, В.Д. Ногин. – М.: Наука, 1982. – 256 с.
11. **Жамбю, М.** Иерархический кластер-анализ и соответствия [Текст] / М. Жамбю. – М.: Финансы и статистика, 1988. – 342 с.
12. **Price, K.V.** Genetic Annealing [Text] / K.V. Price // Dr. Dobbs's Journal. – 1994. – Oct. – Vol. 19. – № 11. – P. 117.
13. **Эбелинг, В.** Физика процессов эволюции [Текст] / В. Эбелинг, А. Энгель, Р. Файстель. – М.: Эдиторал УРСС, 2001. – 328 с.
14. **Гилмор, Р.** Прикладная теория катастроф: в 2-х томах [Текст] / Р. Гилмор. – М.: Мир, 1984.
15. **Гуц, А.К.** и др. Математические модели социальных систем: уч. пособие в 2-х томах [Текст] / А.К. Гуц, В.В. Коробицын. – Омск: ОмГУ, 2000.
16. **Specht, D.** Probabilistic Neural Networks [Text] / D. Specht // Neural Networks. – 1990. – № 1.
17. **Kohonen, T.** Self-Organizing Maps [Text] / T. Kohonen. – Springer-Verlag, 1995.
18. **Fritzke, B.** A growing neural gas network learns topologies [Text] / B.A. Fritzke: G. Tesauro, D.S. Touretsky and T.K. Leen (eds) // Advanced in Neural Information Processing Systems 7, MIT Press, Cambridge MA, 1995.
19. **Глушков, В.В.** Моделирование развивающихся систем [Текст] / В.В. Глушков, В.В. Иванов, В.М. Яненко. – М.: Наука. Главная редакция физико-математической литературы, 1983. – 350 с.
20. **Николис, Г.** Самоорганизация в неравновесных системах / Г. Николис, И. Пригожин: под ред. Ю.А. Чизмажева. – М.: Мир, 1979. – 512 с.
21. **Реутов, А.П.** Системная модель как отношение обобщенных качеств – упорядоченности, надежности и эффективности: в кн.: Вопросы кибернетики (управление развитием систем) [Текст] / А.П. Реутов, Р.Г. Савченко, Р.М. Суслов: под ред. А.П. Реутова, Р.М. Суслова. – М.: 1979. – С. 5–34.
22. **Романовский, Ю.М.** Процессы самоорганизации в физике, химии и биологии [Текст] / Ю.М. Романовский. – М.: Знание, 1981. – 48 с.
23. **Ganti, T.** A theory of Biomedical supersystems and its application to problems of natural and artificial biogenesis [Text] / T. Ganti. – Budapest: Akademiai, 1979. – 136 p.
24. Директива о предотвращении тяжелых аварий (Севезо III). Директива 2012/18/ЕС Европейского Парламента и Совета от 4 июля 2012 г. о контроле крупных аварий, связанных с опасными веществами. [Электронный ресурс]. – URL: http://phase1.pprdeast2.eu/assets/files/Publications/SevesoIII_Directive_RUS.pdf (дата обращения: 17.02.2017).

Сведения об авторе

Александр В. Бочков – доктор технических наук, начальник отдела анализа и ранжирования объектов контроля Администрации ООО «Газпром газнадзор», Российская Федерация, Москва, e-mail: a.bochkov@gmail.com

Вклад автора в статью

Автором предложен метод синтеза рисков (с использованием игровой постановки задачи противодействия возможным внешним воздействиям различной природы на объекты критически важной инфраструктуры) как основы создания современных систем мониторинга угроз безопасности функционирования структурно сложных систем. Сформулированы ключевые методологические положения: от общей постановки задачи управления безопасностью через синтез модели управляемого объекта и его внешних и внутренних связей, решение проблемы выбора приоритетных объектов защиты с точки зрения обеспечения эффективности функционирования и общей безопасности структурно сложной системы.