Федеральное государственное бюджетное учреждение науки
Институт проблем управления им. В.А. Трапезникова
Российской академии наук

Федеральное государственное бюджетное учреждение науки
Институт прикладной математики им. М.В.Келдыша
Российской академии наук

Федеральное государственное бюджетное образовательное учреждение высшего образования
Российский государственный гуманитарный университет

Научный совет РАН
по теории управляемых процессов и автоматизации

Министерство Российской Федерации
по делам гражданской обороны, чрезвычайным ситуациям и ликвидации
последствий стихийных бедствий (МЧС России)

ПРОБЛЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ

МАТЕРИАЛЫ
XXVI МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ
19 декабря 2018 г., Москва

Под общей редакцией
д.т.н. Калашникова А.О., д.т.н. Кульбы В.В.

Москва
ИПУ РАН
2018

УДК 658.012:658.382.2
ББК 65.9:66.2:68.9
П78

Проблемы управления безопасностью сложных систем : материалы XXVI Междунар. конфер., 19 дек. 2018 г., Москва / под общ. ред. А.О. Калашникова, В.В. Кульбы. – М. : ИПУ РАН. – 2018. – 411 с. – ISBN 978-5-91450-227-7.

Научное издание посвящено различным аспектам проблемы управления безопасностью сложных систем: методам оценивания риска; социальным и экономическим механизмам управления риском; правовому регулированию вопросов безопасности; теории и методам принятия решений; моделированию процессов развития и ликвидации ЧС; планированию и стратегическому управлению в системах обеспечения техногенной, информационной, экономической экологической и природной безопасности; методам построения средств информационной поддержки принятия решений в условиях ЧС и автоматизированных систем управления силами и средствами в условиях ликвидации ЧС различного типа.

Сборник материалов научно-практической конференции предназначен для специалистов, аспирантов и студентов, специализирующихся в области безопасности сложных систем.

Конференция проводится в рамках Федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014—2020 годы»

Труды представлены в авторской редакции

Утверждено к печати Программным комитетом конференции

ISBN 978-5-91450-227-7

I. Общетеоретические и методологические вопросы обеспечения безопасности

Ахромеева Т.С., Малинецкий Г.Г., Кульба В.В., Иванов В.В., Посашков С.А., Торопыгина С.А.

Управление стратегическими рисками энергетического комплекса

Аннотация: Рассматриваются фундаментальные основы и проблемы принятия управленческих решений в научно-инновационном комплексе России на базе компьютерных центров и моделирования. Наряду с глобальными проблемами развития общества показывается, что в мире по сути дела не бывает второстепенных проблем, решение которых требует не меньшего внимания в будущем. Показано, что в настоящее время требуется осознать важность принципиальных решений.

Ключевые слова: стратегия, риск, кризис, проблема, инновации, управленческие решения, горизонт планирования

Постановка проблемы. От неолитической революции к ресурсному переходу

Пока не слишком поздно, не забывайте, что
главное дело жизни – не дело, а жизнь.
Б. Форбс.

Представим себе следующий мысленный эксперимент. Машина времени перенесла нас с нашим знанием истории в эпоху, предшествующую неолитическому кризису. Очевидно желание предупредить наших далеких предков о тяжелых временах, которые ожидают их в самом скором времени. Наверно, мы бы советовали им воспользоваться временем, которое остается до предстоящих перемен, и ресурсами, которые пока есть в распоряжении, для того, чтобы позаботиться о технологиях, которые могут прийти на смену тем, которые ведут в тупик.

Наверно, мы бы не имели успеха у людей того времени. Вероятно, нам рассказали бы, насколько лучше стали копья и луки в последнее время, и как хороши будут их перспективные модели. Другие толковали бы об

алгоритмах коллективных действий, которые позволяют меньшему числу людей убивать больше зверья за меньшее время. Наконец, третьи упрекали бы нас в пессимизме, ссылаясь на волю могущественных богов, которым регулярно приносят жертвы, и которые непременно должны защитить от любых невзгод. Вероятно, мудрые люди объясняли бы нам, что лучшим опровержением наших домыслов и панических слухов является то, что они сами, несмотря ни на что, живы, здоровы и благоденствуют. Думаю, что все наши технологические идеи были бы с гневом отвергнуты сильными, свободными людьми, покорителями бескрайних пространств.

Неолитический кризис оказался очень тяжелым испытанием для человечества. По оценкам ряда исследователей, на этом крутом историческом повороте в живых остался только каждый десятый житель Земли. Именно совершенствование технологий охоты привело к тому, что ресурсная основа для движения по прежнему пути оказалась подорвана. На наш нынешний взгляд, главные технологии того времени удивительно расточительны – на территории нынешней Москвы (около 1000 км^2) хватало места примерно для 50 семей охотников и собирателей. Те, кто в то время выжили и нашли путь в будущее, смогли создать технологии возделывания зерновых культур и методы одомашнивания животных. Именно на этой волне мы и продолжаем развиваться по настоящее время.

Более того – подобные истории повторяются вновь и вновь. Они наглядно показывают, что успех здесь не гарантирован, что если ситуация оценивается неверно и предлагаются не те технологии, которые могут помочь, то трагический финал неизбежен.

В свое время выдающийся историк XX в. Арнольд Тойнби проанализировал судьбу нескольких десятков цивилизаций, о которых мы знаем. Многие из них не смогли дать удовлетворительные Ответы на Вызовы, с которыми они столкнулись, и сошли с исторической сцены. По-видимому, сейчас очень важно осознать тот Вызов, с которым столкнулись мы.

Американский ученый Джаред Даймонд проанализировал коллапсы разных исторических сообществ: «Под коллапсом я подразумеваю резкое падение численности населения и/или потерю политических, экономических, социальных достижений на значительной территории на продолжительное время» [1, стр.9]

Коллапс может быть обусловлен тем, что угроза не осознается или принимаются меры, которые не могут её предотвратить.

Хрестоматийный пример – вымирание сообщества на острове Пасхи – самом удаленном обитаемом участке суши на планете (1300 миль от ближайшего берега). На этом острове в течение столетий вырубались знаменитые гигантские каменные статуи в период между 1400–1600 гг.

В целом остров Пасхи представляет собой самый яркий пример истребления лесов в Океании и один из самых драматичных в мире: лес был вырублен полностью и все виды деревьев исчезли. Последствия не заставили себя ждать: исчезло сырьё, не стало добываемых в лесу дикорастущих съедобных растений, упала урожайность культивируемых злаков.

Сырья не стало совсем, или же оно оказалось доступно лишь в очень ограниченном количестве – это коснулось всего, что изготавливалось из местных пород деревьев и птиц, включая древесину, веревки, кору для производства ткани и перья. Отсутствие строевого леса и канатов привело к остановке работ по транспортировке и установке статуй, равно как и строительства каноэ для далеких морских плаваний», – писал Д. Даймонд. [1, стр. 131]

Жрецы, руководившие жизнью на этом острове, считали главной причиной невзгод, обрушившихся на его обитателей, недовольство богов, а основной технологией, избавляющей от бед – строительство гигантских каменных изваяний, посвященных этим богам.

Неверное понимание ситуации и угроз местными экспертами привело к ошибочным действиям правящей элиты, а эти действия – к трагическому финалу. Цель этих заметок – обратить внимание на неверную оценку многих угроз большинством нашего научного сообщества. Чтобы не произошло коллапса, нам стоит изменить приоритеты нашего научного, технологического, социального и экономического развития.

В большей степени наше научное сообщество повторяет те же ошибки, что и жрецы острова Пасхи – главные проблемы не ставятся, а поэтому их решают не в том темпе и не в том объеме, которого они заслуживают. Так же, как в случае неолитического кризиса, их «оставляют на потом» либо предполагают «решать по мере поступления».

Наглядный пример – выдвинутая создателем Давосского экономического форума Клаусом Швабом и сложившимся там экспертным сообществом концепция *четвертой технологической революции* [2]. В соответствии с этой концепцией, которая сейчас в России и во многих других странах рассматривается, скорее, как дорожная карта желательных перемен, до 2025 г. должен быть пройден 21 поворотный путь. Эти пункты определяют некоторый новый уровень технологического и социального развития. Из них только два относятся к сфере производства (печать автомобилей и печени с помощью 3D-принтеров) и *ни один* не касается сферы ресурсов.

Детальный анализ государственной программы цифровой экономики, в которую предполагается вкладывать по 100 млрд руб. ежегодно, а в общей сложности речь идет о триллионах, показывает, что, собственно, к экономике она не имеет отношения [3].

Вместе с тем, по оценке академика Д.Ю. Пущаровского, добыча ресурсов сегодня обеспечивает почти половину глобального валового продукта. Геология сегодня обеспечивает 70% экспорта России, на территории которой находится 32% полезных ископаемых мира [4].

Расчеты британских ученых показывают, что вес техносферы (состоящей из того, что люди добыли из земли) уже в 30 раз превысил вес биосферы.

Действительно, исполнилось пророчество выдающегося геохимика, мыслителя, философа В.И. Вернадского о том, что человек превратился в геологический фактор, меняющий облик Земли. Но если раньше мы повторяли эти слова с гордостью, то сейчас с большой обоснованной тревогой – хватит ли нам мудрости, чтобы разумно распорядиться теми силами и процессами, которыми научились пользоваться, или опять получится как в сказке про ученика волшебника, который не познакомился с правилами техники безопасности прежде чем взмахнул волшебной палочкой.

Ключевым в ответе на вопрос, что мы считаем важным и опасным, а что нет, является наш *горизонт планирования*. Концепция *устойчивого* (самоподдерживающего sustainable) *развития* советует подумать о следующих поколениях.

Вновь обратимся к оценкам академика Д.Ю. Пущаровского: «Например, за последние пятьдесят лет потребление энергетических ресурсов – в частности, нефти, выросло в десять раз, притом, что население увеличилось в два с половиной раза. Это значит, что темпы потребления этих ресурсов увеличиваются. Встает вопрос, насколько их хватит. Так вот при нынешних темпах мировой добычи – 4,5 млрд тонн, а в России это примерно пятьсот миллионов тонн нефти в год, теперешних запасов хватит на 20-30 лет. При этом, глубина нефтяных скважин за последние 10 лет возросла с 2,6 тысяч метров до 3-х километров, и, соответственно, затраты на добычу одной тонны нефти за это же время увеличились почти в 3 раза. Арктический шельф – весьма заманчивый регион. По некоторым оценкам, здесь сосредоточено около 30% запасов нефти на Земле. Однако добыча нефти из шельфа и из высокоплотных пород предполагает применение новых технологий, а их ресурсы рассматриваются как трудноизвлекаемые.

Не менее важное направление – добыча твердых полезных ископаемых. За последние 100 лет только потребление меди выросло в 37 раз. Если 100 лет назад продуктивными считались месторождения с содержанием меди порядка 13%, то сейчас это число сокращено до 0,2-0,5% [4, стр. 44,45].

Впрочем, добывать всю имеющуюся на Земле нефть не придется. Ключевым здесь является *параметр энергоэффективности* или EROI – «energy return on (energy) invested» – «полученная энергия в расчете на вложенную энергию». Иначе говоря: «энергия, доступная для общества: энергия, используемая для добычи».

К сожалению, параметр EROI со временем драматически уменьшается – имеет место знакомый нефтяникам и экономистам «утес эффективности». Драматическое уменьшение EROI с 100:1 до 25:1, которое имело место для нефти с 1900 по 1975 гг., проявилось в международных делах. Достаточно вспомнить «нефтяной шок» 1973 г., когда впервые развивающиеся страны использовали цены на нефть как оружие против развитых стран. Однако падение с 25:1 до 18:1, произошедшее с 1975 по 1990 гг., уже имело катастрофические последствия для нашей страны. Организованное США падение цен на нефть не позволило профинансировать «перестройку» и повысить жизненный уровень и в совокупности с рядом других факторов оказалось критическим для СССР, привело к крупнейшей геополитической катастрофе XX в.

В 1990 г. EROI для разных стран и месторождений составлял от 18:1 до 10:1, а сейчас приближается к 4:1. А это уже близко к тому пределу, при котором добыча таких энергоресурсов оправдана для сложных развитых индустриальных обществ. Тут уже приходится учитывать, что сейчас в России 1/7 энергии, содержащейся в добытом топливе, идет на его транспортировку, что получение других видов энергии из добытых углеводородов происходит с весьма небольшим коэффициентом полезного действия.

Мы подошли к очень важному рубежу, на котором тактика оказывается вторична, стратегия – гораздо важнее, но главное – осмысление исторической перспективы, которое и позволяет проектировать будущее и направлять события, а не оказываться их удивленной жертвой. Нужен исторический прогноз, контуры которого мы вкратце и обсудим.

Великий философ Иммануил Кант поставил нам три вопроса, на которые следовало бы отвечать мыслителям: «Что я могу знать? Что я должен делать? На что я могу надеяться?» Сегодня, на рубеже ресурсного кризиса, эти вопросы становятся предметом конкретных научных исследований.

Геополитика углеводородов и мировые войны

«Всё моё», – сказало злато.
«Всё моё», – сказал булат.
«Всё куплю», – сказало злато.
«Всё возьму», – сказал булат.
А.С. Пушкин

Сегодня будущее являет себя в концептуальных и математических моделях. Пионерские работы, посвященные анализу глобальных перспектив – *мировой динамике* – были начаты по заказу Римского клуба

Дж. Форрестером и Д. Медоузом [6]. В них мир в целом описывался несколькими макропеременными («параметрами порядка», в терминах синергетики) – численностью населения мира, доступными ресурсами, основными фондами, долей фондов в сельском хозяйстве, уровнем жизни населения. Связи между переменными выбирались таким образом, чтобы как можно точнее воспроизвести траекторию, пройденную мир-системой с 1900 по 1970 гг., а затем полученная система дифференциальных уравнений рассчитывалась на компьютере.

Тогда полученные результаты вызвали шок и привели к созданию экологии, к появлению идей «устойчивого развития» и движения «зеленых». Расчеты показали, что мировую экономику при сохранении намечающихся тенденций и технологий того времени ждет коллапс, и причины его достаточно очевидны. Исчерпание невозобновляемых ресурсов – углеводородов, руд и прочих – снижает эффективность экономической деятельности, товары дорожают, жизненный уровень падает. Кроме того, нарастает загрязнение окружающей среды, – ресурсов для того, чтобы привести её в порядок не хватает. И это также снижает качество жизни.

Сейчас те же результаты вызывают оптимизм у представителей крупных компаний: «почти полвека прошло, а жить стало не хуже, а лучше, и катастрофы не видно». Модели, описывающие валовой внутренний продукт (ВВП) и ряд других показателей показывают, что ВВП Китая, Индии, Бразилии, США экспоненциально растут. Однако это означает не то, что модели неверны. Скорее, они не учитывают важные структурные факторы и кое-где качественные изменения ещё не нашли отражения в количественных показателях, которые дают модели. Мы ненадолго отложим их обсуждение и обратим внимание на исследовательскую программу построения *математической истории*, выдвинутую в 1990-х гг. С.П. Капицей, С.П. Курдюмовым, Г.Г. Малинецким [8]. В её основе лежит математическое моделирование исторических процессов и анализ исторических альтернатив. При этом очень важным становится выявление «исторических аналогов», где в разные эпохи определяющими были одни и те же механизмы. Есть ли исторический аналог у предстоящей нам эпохи?

В ряде работ американских исследователей Л.Г. Бадалян и В.Ф. Криворотова история рассматривается с позиций развития технологий и борьбы за обладание ключевыми ресурсами развития. Победитель в этой борьбе становится *доминантом*, способным навязывать свою волю другим игрокам. При этом доминант заинтересован в расширении сферы своего влияния – в глобализации. Эту стратегию диктует экономическая целесообразность, связанная с эффектом масштаба. Продукция, производимая в бо́льшем количестве, оказывается обычно

существенно дешевле, чем создаваемая в меньшем. Кроме того, расширение и монополизация рынка дают доминанту дополнительные возможности для того, чтобы жить лучше соседей.

В соответствии с теорией выдающегося русского экономиста Н.Д. Кондратьева войны, кризисы, революции связаны с большими циклами технологического обновления (кондратьевскими волнами), занимающими 40-50 лет. В ходе этих циклов происходит смена технологических укладов, определяемых их научными основаниями, новым экономическим пакетом, задающим вектор развития всей социально-экономической системы, локомотивными отраслями экономики.

При этом особенно важным оказывается смена *главного энергоносителя эпохи*. Доминирование Великобритании в начале XX в. было обусловлено тем, что эта страна контролировала мировой рынок угля и связанную с ним инфраструктуру. В каждом крупном порту были английские угольные компании, а все сделки по продаже стратегических товаров должны были заключаться в Лондоне. Тем, кого не устраивало такое положение дел, британский флот, существенно превосходивший военно-морские силы других государств, наглядно показывал их место в мировых делах.

Однако появился новый энергоноситель – нефть и с ним новые «хищники», не отягощенные огромной, дорогой и становящейся всё менее эффективной угольной инфраструктурой – США, Германия и отчасти Россия. Глобальные технологические и экономические сдвиги дают быстро развивающимся странам шанс потеснить доминанта. Первую и Вторую мировые войны специалисты по экономической истории часто называют *войнами нефти против угля*. Исход этой войны для бывшего доминанта плачевен – Англия лишилась многих своих колоний и права монопольной торговли с оставшимися, а потом рухнула и вся мировая колониальная система.

Главным победителем этих войн и следующим доминантом оказалась основная нефтяная держава – США. О масштабах нефтяной инфраструктуры в мире позволяют судить следующие цифры: «из 914127 нефтяных добычных скважин в мире в 1999 г. – 554385 (61% от общего числа мировых скважин!) располагались на территории США, 48258 (5%) – в Канаде, 1685 – в Ираке, 1560 – в Саудовской Аравии, 1120 – в Иране и 790 – в Кувейте.

В целом же на территории США к 1999 г. было пробурено 861384 скважины, из которых 36% являются газовыми и 64% – нефтяными». [5, стр. 144]

Международная политика доминанта со времен Древнего Рима не изменилась. Её принцип: «Разделяй и властвуй». Перекраивая карту мира

колониальные администрации позаботились, чтобы очень большие нефтяные и газовые запасы оказались у очень маленьких государств, которые не могут защитить себя без поддержки доминанта. Наглядный пример – Катар, в котором лишь несколько сотен тысяч граждан, около 2-х миллионов гастарбайтеров и третья позиция в мире по запасам газа.

Доминант слабеет – его доля в глобальном мировом продукте уменьшается, и он уже не может контролировать мировой рынок углеводородов без войн и санкций. Достаточно напомнить спровоцированную американцами ирако-иранскую войну, разгромленную Ливию, блокаду Катара в июне 2017 г., санкции США против Ирана в мае 2018 г., несостоявшийся «Южный поток», «подвешенный» «Северный поток-2». Треть мировых запасов нефти, которыми располагают Россия, Иран и Венесуэла, в настоящее время находятся под санкциями. США активно используют «нефтяное оружие» – создают себе неконкурентные преимущества и пытаются «утопить» тех, кого назначают своими противниками. Они начинают «игру без правил», уже не маскируя своих мотивов: «Ты виноват уж тем, что хочется мне кушать».

В этой связи показательно заявление президента компании «Роснефть», располагающей крупнейшими в мире доказанными запасами нефти (около 25 млрд. баррелей) Игоря Сечина, сделанное в 2015 г.: «Лейтмотив Петербургского форума в этом году – построение экономики доверия. Для «Роснефти», одного из гарантирующих поставщиков на мировом рынке энергоносителей, взаимное доверие прежде всего основывается на безусловном исполнении конкретных обязательств. Продвижению доверия также способствуют взаимные инвестиции, обмен активами, интеграция бизнеса, нахождение взаимовыгодных решений для участников рынка… Политическая конъюнктура появляется и исчезает, а ответственное поведение лидеров отрасли – это наш общий долг и основа для устойчивого развития мировой экономики» [9, стр.31]. Примерно, как в басне И.А.Крылова, в которой ягненок доказывает волку, что соблюдает правила, которые последний уже давно не признает.

США спешат и стремятся затормозить развитие нового центра силы. Китай сейчас вышел на первое место по экспорту высокотехнологичной продукции. Доля стран БРИКС в этом сегменте мирового рынка к 2020 г. должна увеличиться до 1/3, а расходы на научные исследования этой группы стран приближаются к 30% их мирового объема.

У нас на глазах происходит смена главного энергоносителя – место нефти занимает газ. Состоялась сланцевая революция, и мы стоим на пороге газогидратной. Всё это прелюдия к новому переделу мирового рынка и сфер влияния. В логике начала XX в. и борьбы за углеводородные рынки это означало бы прямой путь к войне.

Вот как известные американские исследователи отвечают на главные вопросы:

1. «Можно ли договориться с доминантом? Нет, ибо сговорчивый доминант – не доминант. Запад (как, впрочем, и Восток) упорен генетически и понимает только силу. Впереди игра на годы, вероятно, с выходом на третью мировую.
2. В чем слабость доминанта? В отсутствии солдат, готовых умирать, ибо наемники воюют за деньги, а не за идею. Поэтому нужны слабые противники, которых можно разбомбить или запугать.
3. В чем слабость России? В отсутствии идеологии, за которую готовы жить, а не вымирать. Консерватизм и Русский мир – хорошо, но мало, если всё сводится к замене одного олигарха на другого». [11, стр.37]

Наступает время булата, серьезных экзаменов для разных цивилизаций, которыми являются войны. К сожалению, ядерное оружие не является в нашем случае идеальным и эффективным сдерживающим фактором. В кибервойнах, при разных вариантах биологического нападения вообще неясно, кто же нападает. Никто не отменял использование «мягкой силы», экономических, информационных, когнитивных войн, подкупа элит.

Если в рамках традиционной экономической логики мы движемся к мировой войне, то надо менять эту логику.

Геоэкономика и гуманитарно-технологическая революция

Если это работает, то оно устарело.
С. Бир

В послании Федеральному Собранию РФ 01.03.2018 г. в качестве главной задачи президент РФ обозначил *преодоление отсталости*. Нашей стране очень важно не остаться в прошлом. Классик писал, что политика является концентрированным выражением экономики. Будущая экономика может снять сегодняшние геополитические проблемы.

Надежду на это дает переход от индустриального к постиндустриальному обществу и разворачивающаяся у нас на глазах *гуманитарно-технологическая революция* [3].

В самом деле, индустриальная эпоха предполагала массовое производство, потребление, культуру, занятость, образование, оружие массового поражения, гигантские предприятия и электростанции, вовлечение в хозяйственную деятельность всех доступных ресурсов. В эту эпоху численность людей на Земле N росла по гиперболическому закону $N(t) \approx (t_f - t)^{-1}$, где t_f – *время обострения* или *точка сингулярности* $t_f \approx 2025$ год. Именно макроэкономические показатели были ведущими –

валовый внутренний продукт, объемы производства и торговли. Можно сказать, что воплощался императив «человека для экономики». При этом главным противоречием, определяющим развитие политической системы, было противоречие между немногочисленными собственниками (капиталистами) и многочисленными рабочими (пролетариями). Первые владели основными фондами – результатами накопленного труда, вторые – собственным трудом, без которого основные фонды мертвы. Эти противоречия порой заканчивались революциями, социальные издержки которых оказывались очень велики.

Однако ситуация изменилась. В странах-лидерах технологического развития из 100 человек 2 человека работают в сельском хозяйстве и кормят себя и всех остальных, 10 – в промышленности, 13 – в управлении. Встает вопрос о том, чем должны заниматься оставшиеся 75 человек. Именно этот вопрос определяет вектор развития общества, его будущее. Голодные накормлены, социальная структура общества изменилась. Мы приходим к императиву «экономика для человека». Как и предсказывал в 1970-х гг. американский социолог Дэниел Белл нормой становятся постоянные перемены, внедрение изобретений, создание новых технологий, развитие и использование достижений науки. На первый план выходят высокотехнологичный и инновационный сектор экономики.

Машинам уже удалось поручить тяжелый физический труд и, вероятно, в недалеком будущем они возьмут на себя рутинную умственную работу.

Людей всё чаще заменяют роботы. По прогнозам всемирного экономического форума в 2025 г. 52% работ будут выполняться роботами. Роботизация стремительно проходит в Китае, куда поставляется треть всех роботов мира. Очень красноречиво распределение числа роботов, приходящихся на 10 тысяч рабочих: Южная Корея – 631, Германия – 309, Япония – 303, США – 189, Испания – 160, Австралия – 83, Китай – 68, ЮАР – 28, Бразилия – 10, Индия – 3, Россия – 3.

Новая индустриализация России и роботизация её промышленности сейчас являются важнейшими направлениями преодоления отставания России от стран-лидеров мирового технологического развития. К сожалению, именно это направление «выпало» из государственной программы развития цифровой экономики РФ.

Роботизация приводит к тому, что из-за автоматизации труда, судя по прогнозу, к 2022 г. в мире будет потеряно 75 млн рабочих мест. Но она же приведет к появлению 133 млн рабочих мест. Людей понадобится не меньше, а больше.

Что будет энергетическим фундаментом постиндустриальной реальности? Разбор динамики и перспектив каждого сектора мировой энергетики требует отдельного обсуждения. Поэтому здесь стоит провести только экспертную оценку выдающегося физика, лауреата Нобелевской

премии Ж.И.Алфёрова. По его оценке, 1% солнечной энергии, падающей на Сахару, будет вполне достаточно для того, чтобы удовлетворить все энергетические потребности человечества в ближайшие десятилетия. Вопрос состоит в том, чтобы повысить КПД солнечных батарей и создать эффективную инфраструктуру, обеспечивающую передачу энергии. По мысли Ж.И.Алфёрова, будущее за сверхпроводящими кабелями, погруженными в жидкий водород. Несмотря на большие технологические сложности, эта перспектива представляется вполне реальной.

Здесь следует обратить внимание на стратегическую энергетическую инициативу, выдвинутую в своё время Бараком Обамой. В соответствии с ней, к 2050 г. потребление нефти, газа и угля в этой стране должно сократиться вдвое. Без сжигания углеводородов должно к этому времени получаться более 35% энергии и более 65% электричества.

Для решения этой задачи предполагалось тысячи квадратных метров пустыни Аризоны и Невады покрыть солнечными батареями. Этот проект оценивался в $500 млрд. и детально прорабатывался. Администрация Дональда Трампа, во многом ориентирующаяся на «старую экономику», на нефтегазовые компании притормозила этот проект. Тем не менее, перспектива такого «энергетического маневра» остается и у США, и у других стран.

По мнению Ж.И.Алфёрова, у энергетики нет термоядерного будущего. Судя по 60 с лишним годам усилий в этой области, термоядерная энергетика требует огромных, дорогих, сложнейших установок, требующих исключительно точного управления. Это на много порядков сложнее, чем создание и эксплуатация атомных реакторов. Кроме того, осуществление управляемого термоядерного синтеза требует в различных вариантах от 100 до 500 миллионов градусов в реакторе. Это удивительно высокие температуры в земных условиях, создание которых требует огромных усилий. Достаточно напомнить, что температура поверхности Солнца 5000°, а его короны около двух миллионов.

По мнению Ж.И. Алфёрова, и атомные станции для выработки электроэнергии в ближайшие десятилетия уступят солнечным собратьям. Утилизация радиоактивных отходов и наработка плутония оказались гораздо более тяжелыми проблемами, чем это представлялось на заре развития атомной энергетики.

У каждого известного нам типа генерации электроэнергии есть свои недостатки, и инженеры и ученые вкладывают огромные усилия, чтобы скомпенсировать их тем или иным способом. Будущее покажет, кто здесь добьётся наибольших успехов. Тем не менее, уже сегодня очевидно, что электроэнергию следует производить там, где наиболее удобно, а затем передавать её туда, где она особенно нужна. Это требует энергетической инфраструктуры нового поколения.

Значение энергосистем всегда было велико. На Нюрнбергском процессе немецкого генерала Хейнца Гудериана спросили, что не было учтено немецким генеральным штабом при планировании нападения на СССР. Он ответил, что германские стратеги недооценили два фактора – культурный уровень и образованность советского солдата, а также значение единой энергетической системы нашей страны.

Американский футуролог Олвин Тоффлер несколько десятилетий назад предсказал выход энергетической системы на новый уровень, позволяющий при необходимости «меняться местами» производителям и потребителям энергии. Это особенно важно для возобновляемых источников энергии – солнечных, ветровых, приливных электростанций. Появился новый термин «протребление энергии = производство + потребление». «Умные сети» забирают энергию домохозяйств, когда у них возникает избыток мощности, и возвращают её, когда в этом есть потребность. Именно здесь компьютерные управляющие системы особенно важны. Новая энергетическая реальность позволяет выдвигать проекты разработки *Глобального энергетического объединения* (ГЭО). С таким проектом выступил в сентябре 2015 г. председатель КНР Си Цзяньпин на Генеральной ассамблее ООН.

В самом Китае Государственная электросетевая компания (State Grid Corporation of China SGCC) занимает монопольное положение на рынке транспортировки и реализации энергии в стране. Она является крупнейшим в мире поставщиком электроэнергии и занимает второе место в списке крупнейших компаний мира Fortune Global 500 с выручкой 348,9 млрд.

Проект ГЭО увязывается с другим китайским проектом, предусматривающим участие многих других стран – «Один пояс – один путь». Предполагается, что проект ГЭО завершиться до 2070 г., а в его реализацию будет вложено $38 трлн ($27 трлн – в производство энергии и $11 трлн – в сети).

Важнейшая цель проекта ГЭО – добиться того, чтобы к 2070 г. доля электроэнергии, получаемой от чистых источников, составляла 90% (25% – ветровая энергетика, 41% – солнечная, 13% – гидроэнергетика и 7% будет приходиться на геотермальную энергетику, биомассу и другие источники). Сейчас доля энергии, получаемой в результате сжигания угля, нефти и газа, составляет около 80%. По плану ГЭО к 2070 г. эта зависимость должна быть снята.

К сожалению, в настоящее время Россия двигается «против течения». При установленной мощности 239 ГВт пиковое потребление составляет 190 ГВт, около 50 ГВт – лишние, которые можно было бы продавать на мировом рынке, имей мы соответствующую инфраструктуру. После реформы РАО ЕЭС, которую связывают с именем А.Б.Чубайса,

направленной на то, чтобы остановить рост цен, был получен обратный эффект. В последние 10 лет рост цен на электроэнергию опережает инфляцию, а сами цены уже стали выше, чем в ряде стран, которым Россия продает газ, и которые используют его для производства электроэнергии. Она выше, чем в 15 штатах США и в 6 странах ЕЭС.

В настоящее время Единая российская энергосистема состоит из 70 региональных энергосистем, которые образуют 7 объединенных энергетических систем, причем одна из них работает изолированно.

В советской энергетике минимизировались расходы на производство электроэнергии по всей стране. Сейчас генерирующие мощности находятся в руках собственников, и каждая энергосистема стремится стать самодостаточной. Цена на энергию растет и уже многие предприятия начинают строить свои генерирующие мощности. Мир идет к интеграции энергосетей, к повышению эффективности генерации, к снижению цены энергии, а мы движемся в противоположном направлении.

В настоящее время широко обсуждается идея правительства о повышении цены на энергию. Суть этой идеи в том, что домохозяйства должны оплачивать энергию по существующей цене лишь за 300 кВт·ч в месяц, то, что свыше – по повышенному тарифу, а начиная с 500 кВт·ч. – вообще по «экономически обоснованному».

При капитализме есть два способа увеличить прибыль производителей, тем более, если они являются монополистами. Это либо снижение цены, приводящее к увеличению объёма продаж, либо наоборот – повышение цены, приводящее к снижению продаж. Почему же мы опять двигаемся по худшему пути?

Кроме того, дешевое топливо и электроэнергия являются «допингом» для развития промышленности, в котором так нуждается наша страна, инструментом для преодоления отсталости.

Геокультура и новые экологические ниши

Тот, кто не хочет прибегать к новым
средствам, должен ожидать новых бед.
Ф. Бэкон

Вернемся к моделям мировой динамики и подумаем, чем мы можем помочь нашим детям и внукам (а может быть и себе?), как смягчить неизбежно и достаточно быстро надвигающийся ресурсный кризис.

Из анализа модели мировой динамики, проведенного в 1970-х гг. группой профессора В.А.Егорова, следует озаботиться проблемой отходов и создать соответствующую отрасль промышленности. Территории, занятые свалками промышленных отходов занимают в России около 4 млн гектаров, что равно площади таких стран, как Швейцария или Голландия,

вдвое превышает площадь Словении или Израиля и в 4 раза площадь Кипра. В России уже накоплено около 1000 т отходов на одного человека.

Если в странах-лидерах перерабатывается 95% создаваемых отходов и 5% захоранивается на полигонах. Протесты в Подмосковье и сопредельных регионах в 2018 г. показывают неудовлетворительный технологический уровень этой отрасли экономики в России, которая в других странах (некоторые из которых закупают отходы) дает большие прибыли.

Это особенно досадно, потому что в СССР этой отрасли уделялось серьёзное внимание, и её технологический уровень в сравнении с другими странами был достаточно велик. Много эффективных технических решений было предложено и в новой России. Однако мало иметь хорошие технологии, их надо широко и масштабно внедрять и вновь ставить во главу угла интересы большинства населения, а не сверхприбыли капиталистов и криминальных авторитетов.

Здесь возникает принципиальный вопрос, касающийся целеполагания и проектирования будущего. Технологии и промышленные, и социальные, и управленческие кардинально зависят от уровня культуры. Это особенно важно в высокотехнологичных отраслях, в частности, в атомной и космической промышленности. Подобно тому, как академик Д.С.Лихачёв говорил о культурном пространстве, об экологии культуры, сейчас можно говорить об экологии технологий.

Теория самоорганизации, и в частности её раздел, часто называемый *субъективной синергетикой*, наглядно показывает, что управление при наличии множества параметров не может быть эффективным (человек может следить не более, чем за 5-7 медленно меняющимися переменными), а задачи многокритериальной оптимизации зачастую неразрешимы. Например, до недавнего времени эффективность деятельности губернатора должна была оцениваться по 47 параметрам – человек не мыслит в пространстве такой размерности. Ещё более удивительна ситуация со стратегическим планированием, закон о котором был принят в России. Эксперты утверждают, что по этому поводу уже принято более 57 тысяч официальных документов. Это говорит о *кризисе целеполагания* и исключает деятельность по эффективному стратегическому планированию.

В настоящее время в России создается *распределенная сеть ситуационных центров* субъектов федерации, федеральных министров и крупнейших компаний. Из приведенных примеров следует, что в отсутствие ясного целеполагания и алгоритмов отделения главного (ведущих переменных, параметров порядка) от второстепенного можно снизить качество государственного управления, загрузив аппарат ненужной или второстепенной информацией. В известном военном

принципе, призывающем сосредоточить усилия на главном, решающем направлении, есть свой глубокий смысл.

На пути в будущее нас поджидает ещё одна опасность – препоручить управление социальными процессами или рядом вооружений машинами. Мы привыкли к тому, что поисковики присылают нам статьи, исходя из предыдущих запросов и нашей активности в сети. И иногда они «указывают» удивительно точно.

Следующий этап, о котором всё чаще говорят эксперты в связи с развитием «интернета вещей» и «интернета моделей», это появление «цифровых двойников». Под последними понимаются сущности, содержащие наиболее важную информацию о реальных объектах и субъектах, их своеобразные компьютерные модели, которые в недалекой перспективе будут давать прогноз о реакции моделируемого объекта на различные управляющие воздействия. Это дает возможность небольшим элитарным группам перехватывать управление, что может сделать мир гораздо более неустойчивым, чем сейчас. О том, что со временем эта проблема встает в полный рост и человечество окажется перед очень серьезным выбором, предупреждал ещё в 1950-х гг. создатель кибернетики Норберт Винер.

В начале XVII в. выдающийся философ Френсис Бэкон сформулировал чеканную формулу «Знание – сила». Однако до настоящего времени алгоритмы и инструменты работы с накопленным знанием во многом остались прежними, разве что гаджеты заменили гусиные перья. Вероятно, в постиндустриальную эпоху нам придется «взять производную» от бэконовской мудрости: «*знание о знании в наступающую эпоху становится стратегическим ресурсом*».

В современном мире знание становится субъектным, – книги всё чаще оказываются мертвым грузом, а принципиальными становятся люди, представляющие и воплощающие в себе онтологии целых областей, знающие и умеющие пользоваться накопленной информацией и ясно представляющие карту нашего незнания. Заботы о «цитируемости» и «публикационной активности», длительный «патентный поиск», традиционные инструменты, связанные с «интеллектуальной собственностью» и «авторским правом», остаются в далеком прошлом. Стоит привести только две цифры, показывающие, что мы уже оказались в другой реальности. В среднем более 100 новых химических веществ синтезируются «каждый день». В поиске новых средств борьбы против рака участвовало более 10 миллионов компьютеров, огромное количество математических моделей и баз данных. Кто же является «автором» выдающегося результата, полученного в ходе этой масштабной работы? Поэтому на пути в будущее принципиальное значение приобретает *стратегическое управление знаниями, технологиями, программами,*

прогнозами, проектами, что требует нового поколения информационных технологий и человеко-машинных систем. Без этого не удается, в частности, отстроив «новую энергетическую парадигму».

С 1950-х гг. годов почти 30 лет мир жил с иллюзией будущего изобилия, строил «общество потребления». Это отражают и экономические теории, и измерительные инструменты, популярные в то время. Мы до сих пор говорим о мериле благополучия. Но ведь в него входят «услуги», в том числе и финансовые. И многократные продажи от одного посредника к другому могут его значительно увеличить.

Очевидно, никакие «финансовые маневры» тут не помогут, и приходит время принципиальных решений. Есть поговорка: «Вам шашечки или ехать?». И применительно к нашей непростой ситуации можно перефразировать: «*Жить в «мире одноразовых стаканчиков» – вещей быстро выходящих из строя, либо пользоваться качественными добротными вещами длительного и сверхдлительного пользования*». В последнем случае есть шанс смягчить надвигающийся ресурсный кризис либо избежать его.

В настоящее время ведущие мировые бренды сознательно ухудшают качество и снижают ресурс своих изделий. Этим занимаются «гарантийщики» – специалисты, обеспечивающие, чтобы изделие выходило как можно скорее после окончания гарантийного срока. В России дилеры мирового лидера автомобильного рынка фирмы Toyota рекомендуют сменить автомобиль через три года после его покупки. Это прямая дорога к кризису, путь в тупик.

Этот новый курс, ориентированный не на экономический рост и расширенное воспроизводство («линейная экономика») в Европе называют «*циклической экономикой*».

Очень много возможностей, чтобы пойти по этому пути уже сеть. И «углеродная пауза» – подарок человечеству – должна была бы использоваться для того, чтобы перейти от линейной к циклической экономике. Человечество не настолько богато, чтобы покупать «дешевые», быстро выходящие из строя вещи. Кроме того, для такого перехода уже есть много технологических возможностей.

Например, сейчас офисные здания строятся с расчетом на 40-50 лет после чего их надо сносить. В тоже время здания, которые должны служить 100-200 лет, стоят не намного дороже. Вполне реально увеличить гарантийный пробег легковых автомобилей до 1 миллиона километров. Холодильник «ЗИЛ» во многих семьях прослужил по 50-60 лет, в то время как современные японские модели обычно ориентированы на замену или серьезный ремонт через 3 года. Эксперты в области холодильной промышленности показали, что «ЗИЛ»у требовалось на каждую калорию холода втрое меньше энергии, чем современным японским моделям.

Представим себе, что наша страна начала производить именно такие долговечные холодильники отличного качества, служащие не 3, а 60 лет. Очевидно, в 20 раз можно будет уменьшить число предприятий, занимающихся этим, в 20 раз число потребных ресурсов и втрое потребление энергии, необходимой для эксплуатации. Да, и в мире нашлось бы, наверно, много желающих иметь дело с такой техникой. А ведь речь можно вести не только о холодильниках и офисах, но и обо многих других товарах и сооружениях. Это был бы сильный ответ на санкции Запада.

Пластиковая бутылка, брошенная в лесу, будет разлагаться 200 лет, отравляя окружающую среду, памперсы – 500 лет. В мире нет места для одноразовой посуды (вспомним гигантские «мусорные острова» в океане). Посуда должна быть либо многоразовой, либо биоразлагаемой. В Швейцарии молоко продают в стеклянных бутылках, которые в ходе эксплуатации в среднем проходят 24 цикла использования. Швейцарцы берегут свою страну.

Наверно, и нам, рассматривая энергетические проблемы, стоит заглянуть хотя бы на полвека в будущее и подумать, чем мы сможем сегодня помочь следующим поколениям, которых ждут, судя по всему, нелегкие времена.

P.S. Рассматривая проблему энергоресурсов и ресурсов в целом, мы обсудили инновационный ответ на этот вызов. Однако если взглянуть с точки зрения эволюции, то проблема представляется ещё более масштабной.

У каждого вида на планете есть своя экологическая ниша. Таковыми были и у абсолютных хищников, которые доминировали в истории. Ряд могущественных древних цивилизаций погибли, потому что их ниши оказались исчерпаны либо в силу несовершенства технологий, либо из-за климатических изменений, либо из-за того, что несущая способность территории оказалась значительно превышена (вспомним неолитический кризис). Поэтому может быть очень большую пользу будущим поколениям могут принести технологии освоения экологических ниш, пока не занятых человеком. История учит, что выход на новый социальный, технологический, организационный уровень часто был связан с тем, что люди приходили на «неудобья», где до них не жили. Что же может стоять «неудобьями» и перспективой XXI в., о которых стоит подумать сейчас?

– *Северная Евразия*. До настоящего времени удается освоить лишь побережья морей, океанов, рек (вспомним Северный завоз). Эффективных технологий освоения внутриматериковых территорий, где должны быть свои большие возможности и источники развития, по сути, нет. Но они вполне могут появиться и дать человечеству шанс.

– *Поверхность и глубины океанов*. Сейчас проходится важный рубеж – объем продовольствия выращиваемого и производимого в море, становится больше, чем на суше. Поэтому будущее может оказаться связано с новым уровнем освоения этой стихии.
– *Космическое пространство.* Отказ от космической экспансии, от масштабных пилотируемых программ в последние 40 с лишним лет так или иначе привел к замедлению научно-технического развития. Движение в сторону виртуальной реальности, заменившей освоение космоса не только кое-что дает, но и очень многое отнимает. Поэтому стоит всерьёз отнестись ко всё чаще звучащим призывам вернуться к звездам.

Видимо попытки «инноваторов» доисторической эпохи заняться выращиванием зерновых и одомашниванием животных и вложить небольшие имевшиеся ресурсы именно в это не встретили поддержки и понимания у современников. Но именно они и открыли двери в Будущее.

Работа была поддержана программой фундаментальных исследований президиума РАН, проект 3.2 «Разработка фундаментальных основ прогнозирования, экспертизы и принятия управленческих решений в научно-инновационном комплексе России на базе информационного и компьютерного моделирования и когнитивных центров», а также грантами РФФИ 18-011-00567 и 18-511-00008.

Литература:

1. *Даймонд Дж. Коллапс.* Почему одни общества выживают, а другие умирают. – М.: АСТ:МОСКВА, 2008. – 762с. – (Philosophy).
2. *Шваб К.* Четвертая промышленная революция. – М.: Издательство «Э», 2017. – 208с. – (Top Business Awards).
3. Контуры цифровой реальности: Гуманитарно-технологическая революция и выбор будущего / Под ред. В.В. Иванова, Г.Г. Малинецкого, С.Н. Сиренко. – М.: ЛЕНАНД, 2018. – 314с. – (Будущая Россия, №28).
4. «Природа хранит тайны своих «лабораторий»» // Знание-сила, 2018, №10. С.44-50.
5. *Анпилогов А.* Мир на пике – Мир в пике. – М.: Селадо, 2015. – 392с.
6. *Форрестер Д.* Мировая динамика. – М.: ООО Издательство АСТ; СПб: Terra Fantastica, 2003. – 379с. − (Philosophy).
7. *Махов С.А.* Динамическая макромодель стран БРИКС с учетом торговли. Препринт ИПМ им. М.В. Келдыша РАН, №139 за 2017 г., − 20с.
8. *Капица С.П., Курдюмов С.П., Малинецкий Г.Г.* Синергетика и прогноза будущего. 2-е изд. – М.: Эдиториал УРСС, 2001. – 288с.

9. *Бадалян Л.Г., Криворотов В.Ф.* История. Кризисы. Перспективы. Новый взгляд на прошлое и будущее. Изд. 2-е. – М.: Книжный дом «ЛИБРОКОМ», 2012. − 288с. – (Синергетика: от прошлого к будущему №50).
10. *Сечин И.* Нефтяные рынки: риски или новые возможности // Эксперт, 2018, №23 (1077), с.26-31.
11. *Бадалян Л.Г., Криворотов В.Ф.* Конец истории или Новое Средневековье // 2014, октябрь-ноябрь (176), с.36-57.
12. Роботы и работа // Русский репетитор, 2018, 8-22 октября, с.56-57.
13. Иванов В.В., Малинецкий Г.Г. Россия: XXI век. Стратегия прорыва. Технологии. Образование. Наука. Изд. 2-е. – М.: ЛЕНАНД, 2017. – 304с. – (Будущая Россия №26).
14. Рециклинг ресурсов – первый шаг к экологическому социализму / Под ред. Г.И. Цуцкаревой. – М.: ЛЕНАНД, 2018. – 432с. – (будущая Россия №27).
15. *Комаров С.М.* Цивилизация старьевщика // Химия и жизнь, 2013, №13, с.2-7.

Шульц В.Л, Кульба В.В., Чернов И.В., Шелков А.Б.

Комплекс программ автоматизации сценарного анализа процессов управления обеспечением региональной безопасности

Аннотация: Приведено описание структуры и ключевых функций пилотной версии специализированного программно–аналитического комплекса, осуществляющего информационную поддержку процессов формирования и исследования альтернативных сценариев развития социально – политической ситуации с целью оценки эффективности управленческих решений по обеспечению социальной стабильности.

Ключевые слова: управление, региональная безопасность, социальная стабильность, информационная поддержка, сценарный анализ, моделирование, знаковые графы

В современных условиях повышение эффективности управления обеспечением региональной безопасности и социальной стабильности, являющейся важнейшей ее составляющей, становится ключевой, критически важной стратегической задачей государственной политики России. Сегодня особенно серьезную угрозу представляют собой попытки использования западными странами во главе с США существующих в российском обществе экономических, социальных, политических,

этнических, религиозных и иного рода противоречий в своекорыстных целях, провоцирования столкновений определенных (в том числе – крупных) социальных групп (этносов, классов, религиозных общин и т.д.), а также финансовой, методической, организационной и информационной поддержки сепаратистских движений, организаций и групп радикального толка, проповедующих экстремизм и терроризм. В качестве инструмента влияния на внутреннюю ситуацию в России странами Запада практически открыто используются СМИ и социальные сети, морально и материально стимулируемая извне значительная часть так называемой несистемной оппозиции, различные неправительственные, некоммерческие, образовательные, гуманитарные, правозащитные, экологические и иные подобного рода организации, накачиваемые Госдепом США финансами фонды, «советы», «общественные движения» и т.п. [1,2].

В сложившейся ситуации повышение эффективности управления обеспечением социальной стабильности становится одной из ключевых, стратегических и критически важных для обеспечения поступательного развития российского общества и государства задач.

В этих условиях повышается роль методологии сценарного анализа, базирующейся на процессах разработки и исследования имитационных моделей и обеспечивающей эффективную информационную поддержку процессов планирования, подготовки и реализации организационных и информационных мер по противодействию различным угрозам дестабилизации внутренней ситуации в стране или ее территориальных образованиях на различных уровнях государственного управления.

Основы методологии использования сценарного подхода в области исследования поведения сложных систем на базе математических и графовых моделей специального типа, а также совершенствования технологии управления их развитием, впервые были сформулированы в 60-х годах прошлого столетия и отражены в работах Ф. Робертса (F. Roberts), Дж. Форрестера (J. Forrester), Д. Медоуза (D. Meadows) и ряда других ученых [3-5]. Представленные в настоящей работе результаты являются развитием данной методологии в направлении разработки формализованных методов анализа и синтеза альтернативных сценариев развития ситуации в социально-политической сфере, а также технологий моделирования и автоматизации процессов их генерации с целью повышения эффективности информационной поддержки процессов управления обеспечением социальной стабильности.

Основная задача, решаемая в рамках сценарного подхода, заключается в формировании необходимых исходных данных для подготовки и принятия эффективных стратегических и оперативных решений, а также комплексном опережающем анализе последствий реализации этих решений при различных условиях. Таким образом, сценарий развития

исследуемой системы или конкретной проблемной ситуации является необходимым промежуточным звеном между этапами целеполагания, формирования, а также реализации конкретных управленческих решений, направленных на достижение поставленных целей.

Процессы управления обеспечением социальной стабильности в своей основе базируются на результатах комплексного анализа широкого спектра социально-экономических, политических и др. показателей (индикаторов), позволяющих оценивать сложившуюся социально – политическую ситуацию в государстве и обществе, а также риски ее дестабилизации. Различные, используемые в процедурах информационной поддержки процессов подготовки и реализации управленческих решений, показатели после соответствующей обработки с определенной степенью достоверности позволяют оценивать уровень социальной напряженности в обществе, прогнозировать и вырабатывать адекватные меры по предотвращению различных негативных социальных и общественных проявлений.

В рамках процессов управления обеспечением социальной стабильности наиболее важными задачами сценарного анализа являются:

- анализ эффективности стратегических и тактических решений по обеспечению региональной безопасности в целом и социальной стабильности в частности;
- диагностика и идентификация угроз социальной стабильности и «окон» уязвимости региональных социально – экономических систем;
- комплексная оценка потенциальной опасности угроз социальной стабильности и тяжести последствий их реализации (снижение неопределенности);
- оценка эффективности превентивных планов и упреждающих решений по предотвращению возникновения социальных конфликтов;
- разработка и анализ эффективности решений по противодействию информационным угрозам социальной стабильности (внешним и внутренним деструктивным информационным воздействиям);
- оценка эффективности процессов контроля и оперативного управления противодействием угрозам;
- анализ эффективности решений по недопущению эскалации социальных конфликтов и их разрешению;
- анализ эффективности решений по устранению последствий конфликтов и приведших к его возникновению причин;
- корректировка стратегии противодействия угрозам социальной стабильности.

Проведенный анализ существующих средств моделирования показал, что для генерации сценариев развития социально–экономических систем

целесообразно использовать аппарат знаковых графов, который позволяет работать с данными как качественного, так и количественного типа [6].

Математическая модель знаковых, взвешенных знаковых, функциональных знаковых орграфов, т.е. ориентированных графов, является расширением классической графовой модели. Кроме орграфа *G(X,E)*, где *X* – конечное множество вершин, а *E* – множество дуг графа, в модель включаются дополнительные компоненты. В частности, вводится множество параметров вершин $V = \{ v_i, i \le N = \|X\| \}$. В соответствие каждой вершине x_i ставится ее параметр $v_i \in V$. Вводится также функционал преобразования дуг *F(V, E)*, т.е. в соответствие каждой дуге ставится либо знак, либо вес, либо функция.

На расширенных таким образом орграфах вводится понятие импульса и импульсного процесса в дискретном временном пространстве. Импульсом $P_i(n)$ в вершине x_i в момент времени $n \in N$ называется изменение параметра в этой вершине в момент времени *n*:

$P_i(n) = v_i(n) - v_i(n-1)$.

Значение параметра в вершине x определяется соотношением:

$$v_i(n) = v_i(n-1) + \sum_{j=1, j\neq i}^{N} F\left(v_i, v_j, e_{ij}\right) P_j(n-1) + P_i^0(n) \cdot$$

Здесь $P_i^0(n)$ – внешний импульс, вносимый в вершину e_i в момент времени *n*.

Из двух последних конечно–разностных уравнений легко получить уравнение для импульса в исследуемом процессе:

$$P_i(n) = \sum_{j=1, j\neq i}^{N} F\left(v_i, v_j, e_{ij}\right)\left(P_j(n-1) + P_i^0(n)\right) \cdot$$

Содержательно параметрами вершин графа являются ключевые показатели (факторы), описывающие состояние и динамику развития ситуации в социально-политической или социально-экономической сферах, структура знакового графа отражает причинно–следственные взаимосвязи между ними. Совокупность значений параметров вершин в графовой модели описывает конкретное состояние исследуемой ситуации в определенный момент времени. Изменение значений параметров вершин графа порождает импульс и интерпретируется как переход исследуемой системы из одного состояния в другое. Управление развитием системы моделируется изменением структуры и подаваемыми импульсами в определенные вершины графа.

Основной целью разработанного программного комплекса является автоматизация процессов сценарного исследования региональных

социально-экономических систем и синтез альтернативных сценариев их поведения (развития ситуации на различных временных горизонтах) в условиях неопределенности под воздействием внешних и внутренних угроз социальной стабильности. Разработанный комплекс программ работает под управлением ОС MS Windows.

Программный комплекс обеспечивает автоматизацию решения следующих функциональных задач:

1. *формирования графовых моделей* в виде совокупности вершин и направленных дуг между ними, который обеспечивает хранение и доступ к моделям, используя древовидную структуру, запись наименований моделей в виде длинных имен, удаление, копирование, перенос и объединение моделей, как в древовидной структуре, так и внутри древовидного каталога;
2. *модификации моделей* пользователем в визуальном режиме (drug-and-drop): добавление и удаление вершин и дуг, придание дугам веса и его изменение, придание дугам временных задержек прохождения импульса и «разрывов» в тактах моделирования (веса дуг могут быть заданы десятичными положительными и отрицательными числами, арифметическими и стандартными функциями от величин значений факторов вершин и проходящих по дугам импульсов);
3. *хранения структуры моделей и результатов моделирования* в одном из наиболее распространенных форматов – DBF, что облегчает их возможное использование в других приложениях (наличие распространенных средств доступа к форматам хранения: ODBC, OLE DB);
4. *моделирования (модельного исследования)*: проведение поэтапного моделирования с заданием количества шагов на каждом этапе, возврат процедуры моделирования на заданное количество шагов с восстановлением предыдущего состояния модели, возможность внесения изменений в ходе моделирования (добавление, удаление и изменение параметров вершин и дуг), изменение величин импульсов и значений в вершинах знакового графа на любом этапе моделирования;
5. *решения обратной задачи:* формирования сценариев управленческого воздействия для целенаправленного и заданного изменения свойств моделируемых объектов, систем и процессов, т.е. решения обратных задач для целей планирования и управления развитием социально–экономических систем и обеспечением региональной безопасности в условиях неопределенности;
6. *выдачи результатов моделирования:* результаты сценарных исследований выдаются программным комплексом в текстовой

форме на естественном языке (с использованием встроенной функции автоматического формирования текстового описания полученных сценариев развития социально–экономических систем), в табличной форме (с помощью экспорта полученных результатов в стандартные таблицы MS Excel), а также в графической форме с абсолютным или относительным масштабированием (включая предоставление сравнительных графиков результатов моделирования и динамики изменения значений вершин графовой модели) с возможной привязкой к картам геоинформационных систем.

Единый доступ к отдельным моделям или их фрагментам (слоям) осуществляется посредством организации общих папок в локальной сети либо единого рабочего пространства в облачных сервисах в глобальной сети.

Программный комплекс позволяет осуществлять по телекоммуникационным каналам экспорт промежуточных или итоговых данных моделирования в ситуационные центры органов регионального управления.

С использованием комплекса программ автоматизации сценарного анализа разработана базовая мультиграфовая модель управления противодействием комплексным деструктивным информационным воздействиям и проведено сценарное исследование эффективности процессов управления региональной безопасностью и противодействием информационным угрозам социальной стабильности в регионах Российской Федерации в условиях обострения противоречий между странами Запада и Россией [7].

В частности, проведен сценарный анализ эффективности противодействия проявлениям религиозно – политического экстремизма в рамках решения задач обеспечения региональной безопасности. Результаты проведенных исследований показали, что использование сценарного анализа в управлении социальной безопасностью позволяет диагностировать и идентифицировать внешние и внутренние угрозы социальной стабильности в обществе, обеспечивать комплексную оценку потенциальной опасности угроз, достоверно оценивать эффективность принимаемых решений по управлению региональной безопасностью и противодействию угрозам социальной стабильности, а также формировать заключения о наиболее вероятных направлениях развития динамических процессов в социальной сфере в условиях неопределенности.

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 1607–00245 А «Модели и методы управления региональной безопасностью на основе сценарного подхода».

Литература:
1. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Сценарный анализ в управлении геополитическим информационным противоборством. – М.: Наука, 2015. – 542 с.
2. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Управление региональной безопасностью на основе сценарного подхода. - М.: ИПУ РАН, 2014. – 163 с.
3. *Робертс Ф.С.* Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам. – М.: Наука, 1986. – 497 с.
4. *Форрестер Д.* Мировая динамика. – СПб.: Изд-во АСТ, 2003 – 379 с.
5. *Медоуз Д.Х., Медоуз Д.Л., Рандерс Й. Беренс В.В.*III. Пределы роста. – М.: Изд-во МГУ, 1991. – 208 с.
6. Модели и методы анализа и синтеза сценариев развития социально – экономических систем: в 2-х кн. / Под ред. В.Л. Шульца, В.В. Кульбы. – М.: Наука, 2012. – Кн. 1 – 304 с., кн. 2 – 358 с.
7. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Информационное управление в условиях глобализации. – М.: ИПУ РАН, 2017. – 130 с.

Цыганов В.В.

Пределы роста и глобальная финансовая олигархия

Аннотация: Рассмотрена проблема перемещения Глобального центра капитала (ГЦК), создаваемого глобальной финансовой олигархией, в условиях пределов роста. Указанная олигархия создает в стране пребывания ГЦК наилучшие условия для формирования одномерных людей, ценности которых увязаны с деньгами, как средством увеличения потребления. Однако, при достижении пределов экономического роста и потребления, одномерные люди проявляют недовольство, инициируя социально-политическую нестабильность. Проблема усугубляется противоречием между ними и носителями традиционных (многомерных) ценностей. В результате олигархия вынуждена переместить ГЦК в другую страну. В этом суть проклятия пределов роста для глобальной олигархии. С другой стороны, элита страны пребывания ГЦК стремится подавить страны-конкуренты, чтобы сохранить своё привилегированное положение. Это ведет к усилению международной напряженности, цветным революциям и войнам.

Ключевые слова: капитал, олигархия, общество, потребление, ценности, пределы роста, нестабильность, революция, война

Глобальная финансовая олигархия (ГФО) - группа семейных кланов, которые добились практически полного контроля над мировой финансовой системой и правящими элитами многих стран. ГФО создает Глобальный центр капитала (ГЦК), который базируется, в основном, в избранной ею стране [1]. Для своего удобства, ГФО создает в стране пребывания ГЦК наилучшие условия для замены традиционных (многомерных) человеческих ценностей монетарными [2]. В результате, формируется общество потребления, состоящее из одномерных людей, ценности которых увязаны с деньгами, как единственным средством увеличения потребления [3]. Однако, при достижении пределов экономического роста и связанного с ним потребления, одномерные люди единодушно проявляют недовольство, инициируя социально-политическую нестабильность в стране пребывания ГЦК [4].

В прошлом перемещения ГЦК инициировались угрозами стабильности, вызванные внешними факторами. Эта нестабильность усиливалась изнутри одномерными людьми, их недовольством пределами экономического роста. Если социально-экономическое управление страной было неадекватным (как во времена Горбачева), то пределы экономического роста затрагивали широкие народные массы и приводили к массовому недовольству. Нередко одномерные люди направляли это недовольством в выгодное для них русло (например, для осуществления цветной революции) [4]. Порождаемая всем этим нестабильность в прошлом приводила к перемещению ГЦК [2]. Например, в XV веке центр глобальной олигархии, ростовщичества и геополитики находился в Венеции, которую называли «хозяйкой всего золота христианского мира». Все европейские государи, чеканящие собственные монеты, зависели от Венеции.

С началом эпохи географических открытий были проложены новые морские пути на Восток, была открыта Америка, португальцы открыли путь в Индию вокруг Африки. В Европу на португальских и испанских каравеллах стали прибывать невиданные прежде сокровища из Америки и Индии, золото, серебро, пряности. Средиземноморские торговые пути не выдерживали конкуренции. Прямой угрозой ГЦК в Венеции стала война Камбрейской лиги в 1509-1517 гг. Венецианские олигархи понимали, что большие европейские государства (в том числе Испания и Франция) могут раздавить крошечную Венецию. В качестве средства самозащиты ими была изобретена идея протестантской Реформации, осуществленная Лютером, Кальвином и Генрихом VIII. В результате Европа получила полтора столетия религиозных войн и «малое средневековье» с кульминацией в точке Великого Кризиса XVII века. Например, население

Германии после этих войн сократилось на две трети. В это время Венеция действовала как раковая опухоль, планирующая собственные метастазы. И самыми богатыми государствами Европы в это время стали не Испания и Португалия, а Нидерланды. Самым процветающим городом Европы тех времен был Антверпен. Дело в том, что из Венеции банкиры, которые контролировали все финансовые потоки Европы, перебирались в протестантские страны. Банкирам было гораздо легче найти общий язык с лютеранами и кальвинистами, чем с католиками.

С другой стороны, в начале XVI в. роль ГЦК могла перейти к Испании – стране с самой высокой природной сельскохозяйственной рентой в Европе, в которую стекались золото и серебро из покоренных провинций в Америке. Однако формированию монетарных ценностей и одномерных людей препятствовал католицизм. Кроме того, пределы роста их потребления и накопления одномерных людей в Испании были связаны с ограниченностью природной (сельскохозяйственной и горнодобывающей) ренты. А в это время на севере континентальной Европы развивался технологический уклад, связанный с новыми ремеслами. Этот уклад позволял расширить пределы роста потребления и накопления одномерных людей. Это привело к миграции капитала из Испании на север, в Нидерланды, имеющие лучший климат на севере континентальной Европы (поскольку климат в Европе улучшается с востока на запад) [1]. Испанские власти решили бороть с её организаторами - одномерными людьми с помощью инквизиции. Символично, что напротив Золотой башни в Севилье, куда сгружали золото и серебро галеонов, прибывших из Америки, на другом берегу Гвадалквивира располагалась резиденция Великого инквизитора.

Инквизиция свирепствовала и в Нидерландах. Художественное описание этого дано в книге Шарля де Костера «Легенда о Тиле Уленшпигеле». В результате одномерные люди мигрировали со своими деньгами к главному конкуренту Испании - в островную Англию. Туда же переправились и венецианские олигархи. Переселение в Англию т.н. Венецианской партии совпадает с разрывом короля Генриха VIII с католической церковью. Так ГЦК на три столетия переместился в Британию. Нельзя сказать, что все в Англии приняли венецианцев с большой любовью. Например, В.Шекспир изобразил венецианского ростовщика в образе Шейлока в своей пьесе «Венецианский купец». Но взаимовыгодные интересы заставили многих представителей английского дворянства забыть о кодексе рыцарской чести. Союз венецианских банкиров-маранов и части родовитой английской аристократии закреплялся перекрестными браками.

Таким образом, жители мокрой лагуны - венецианские олигархи присмотрели себе болото и остров, выходящие в Северную Атлантику —

Голландию и Британские острова. Здесь они смогли создать базу для своих семейных богатств и идеологии. В результате, в конце XVI века в Нидерланды и на Британские острова из Венеции перебралась, как сегодня бы сказали, финансовая элита Европы, бывшая тогда ГФЭ.

Поскольку перемещение ГЦК наносит ущерб странам-конкурентам, их элиты всячески противодействуют этому традиционным способом – подавлением соперников. Например, власти Испании всячески старались препятствовать вышеописанному перемещению ГЦК путем давления на страны-конкуренты, что привело к усилению международной нестабильности. А поскольку главным конкурентом Испании стала Британия, то это привело к их многовековому противостоянию. В частности, на море оно было отмечено походом Непобедимой армады в 1588г., и завершилось лишь Трафальгарским сражением в 1805г. Война за Испанское наследство в 1702-1713 г. была первым геополитическим конфликтом мирового масштаба и последним поражением соперников Британии за право быть страной пребывания ГЦК — Испании и Голландии.

Выбор страны пребывания ГЦК. ГФО заинтересована в том, чтобы ГЦК находился в самой сильной стране, чтобы диктовать свою волю всему миру. Поэтому ГФО заинтересована в однополярном мире во главе со страной пребывания ГЦК (например, в США). До недавнего времени так и было. Оставалось только обеспечивать социально-экономическую стабильность в самой стране пребывания ГЦК (т.е. в США). Однако в США, как и в предыдущих странах пребывания ГЦК, возникла проблема пределов роста и социально-экономического застоя. Ведь в США живет около 300 млн человек, являющихся носителями монетарных ценностей. И их недовольство ограничением потребления изливается не только на окружающих, но и на американских политиков, ожесточенную борьбу которых мы сегодня наблюдаем. «Как я много раз говорил, в стране (США – прим. ИА REX) идет гражданская война и ожесточение сражающихся растет», - писал А. Бродский 12.06.2018г. Эта внутриполитическая борьба пагубно сказывается на международной стабильности, необходимой для работы ГФО («Большие деньги любят тишину»). Причем, по мере роста недовольства и взаимного ожесточения, рычагов стабилизации внутриполитической обстановки в США у ГФО становится все меньше: кто может управлять сотнями миллионов американцев, слившихся в протестном экстазе?

Кроме того, мир стал многополярным, и США уже не могут диктовать свою волю. В этих условиях, ГФО может пойти на то, чтобы переместить ГЦК в одну из стран – лидеров многополярного мира, социально-экономическая обстановка в которой более стабильна, чем в США. В первую очередь, к таким лидерам многополярного мира можно отнести

Россию и Китай. Социально-экономическую стабильность в этих странах, даже в условиях пределов роста, обеспечивают традиционные (многомерные) ценности (в том числе религиозные). В России ими являются православие, патриотизм и коллективизм. В Китае – конфуцианство и др. Поскольку от перемещения ГЦК потеряет американская элита, то ей необходимо противодействовать этому традиционным способом – подавлением соперников [2]. Поэтому американская элита развязала против России долгосрочную холодную войну, а против Китая – долгосрочную торговую войну.

К лидерам многополярного мира можно будет отнести и Британию, после выхода её из Евросоюза и восстановления независимости от брюссельской бюрократии. Социально-экономическая обстановка в этой стране более стабильна, чем в США, вследствие многочисленности носителей традиционных (многомерных) ценностей, таких как вера в монархию. Да и численность населения Британии почти в 5 раз меньше, чем США. А после выхода из Евросоюза оскудеет и приток мигрантов. Соответственно, ГФО может меньшими средствами поддерживать и даже увеличивать уровень потребления британского населения, чтобы обеспечить внутреннюю стабильность.

Переместить ГЦК в Британию проще ещё и потому, что в Лондоне до сих пор находится один из главных центров управления глобальной экономикой. К тому же ГЦК располагался там в течение многих веков. Ведь, как бы ни была сильна королева, Британия по существу – не монархия. Это олигархия, построенная по типу Венеции в период расцвета. Б. Дизраэли, прежде чем стать премьер-министром Британии, написал роман «Конингсби», в котором виги-аристократы 1688 года признаются в своем намерении сделать Британию «аристократической республикой» по модели Венеции, с «венецианской конституцией» и королями в роли дожей. А поскольку для ГФО важно, чтобы ГЦК находился в «сильной» стране, элите Британии надо любой ценой формировать её имидж как бесстрашного лидера западного мира (хотя бы на словах, как в деле Скрипалей). Удивительно, но поражения, потери, загнивание самой Британии не уменьшают ее роли в геополитических делах. Как удается кучке развратных аристократов на этом острове строить козни против всего мира? Ведь Британия перестала быть «мастерской мира». Флот внушителен, но его возможности переоцениваются. Армия третьеразрядна. Но англичане научились от венецианцев механизмам овладения капиталом и властью [1]. А в умении плести интриги, организовывать заговоры, разжигать войны и стравливать народы, в искусстве загребать жар чужими руками, как это делали венецианцы, с англичанами сейчас никто не сравнится.

Строго говоря, следует рассмотреть и возможность перемещения ГЦК в обезлюженный лимитроф (от лат. limitrophus «пограничный») - государство, образовавшееся после 1917 года на территории, входившей в состав Российской империи, а затем, в начале 1990-х годов, — в состав СССР (Эстония, Латвия, Литва, Украина). Пример – Украина с её богатым природным потенциалом (например, самыми толстыми в мире слоями чернозема), повально уезжающей на заработки за границу квалифицированной молодежью и вымирающими в результате реформ МВФ пенсионерами. Однако, для перемещения ГЦК необходимо завершить оболванивание оставшегося местного населения (как это произошло в Хазарии [2]), окончательно зачистить его от возможного протестного электората и обеспечить приток мигрантов из неблагоприятных регионов мира (например, из Израиля, подвергающегося все более угрожающему давлению, как со стороны окружающих арабских государств, так и изнутри, со стороны палестинцев). На первый взгляд, вариант перемещения ГЦК в лимитроф типа Украины крайне маловероятен, в силу подверженности последнего влиянию сильных соседей. Но даже если ГФО не развалит Россию, как СССР, ГЦК в Украине может не только состояться, но и удержаться за счет «свежих» идей глобальной олигархии. Заметим, что потенциальный ГЦК в Украине должен иметь выход к морю. А для этого, учитывая чувствительную утрату Крыма, требуется сохранить Одессу в составе Украины. Не потому ли первая группа израильских колонистов во главе с И. Гекко (Беркутом) уже высадилась в Одессе?

Перемещение ГЦК и глобальная нестабильность. Процесс перемещения ГЦК занимает значительное время и приводит к международной нестабильности. Например, миграция ГЦК в Британию привела к её многовековой вражде с Испанией. Миграция ГЦК из Британии в США была инициирована Первой мировой войной. Её следствием стала Великая депрессия 1929-1933гг. Окончательно ГЦК закрепился в США лишь после Второй мировой войны. Поэтому, чтобы обеспечить международную стабильность, необходимо исследовать возможности перемещения ГЦК из США мирным путем. При этом, во избежание потрясений, надо предупреждать страны - кандидаты на роль страны пребывания ГЦК о проклятии пределов роста.

Литература:

1. *Цыганов В.В., Бородин В.А., Шишкин Г.Б.* Механизмы овладения капиталом и властью. – М.: Университетская книга, 2004.-768с.
2. *Цыганов В.В., Бородин В.А., Шишкин Г.Б.* Преемник: механизмы эволюции России. - М.: Академический проект. 2007.- 396с.

3. *Цыганов В.В.* Адаптивные механизмы и высокие гуманитарные технологии. - М.: Академический проект. 2012. - 378с.
4. *.Цыганов В.В, Шульц В.Л.* Социология общественной безопасности. – М.: Наука, 2014. - 415с.

Кереселидзе Н.Г.

Обобщенная дискретная модель Информационной Войны с ограничениями и задача ее управляемости

Аннотация: Построена дискретная обобщенная математическая и компьютерная модель информационной войны с ограничениями. Для полученной обобщенной дискретной системы информационной воны поставлена специфическая задача управляемости подавления информационной войны миротворческой стороной.

Ключевые слова: обобщенная дискретная модель, информационная война, информационные потоки, информационные адепты

1. Введение. В различных центрах принятии решении по стратегической безопасности в последнее время вопросам информационного противостояния уделяют немалое внимание. Безусловно что принятые решения обеспечиваются соответственными финансовыми и материальными ресурсами. Эти ресурсы очевидно не малые и посему их объем должно быть рассчитано оптимальными методами. Так, например, три года назад Министериал Совета Европы учредил специальную группу «Стратегическое коммуникация с Востоком» - **EastStratCom,** https://euvsdisinfo.eu (19.10.2018, 18: 10), для информационного противостояния, а в 2018 году бюджет этой оперативной группы был увеличен до 1,1 миллиона Евро. Президент Евросоюза **Дональд Туск**, сообщивший о росте бюджета, не упомянул об обоснований выделенных финансов, но очевидно, что этому предшествовало экспертная работа специалистов по оптимальному распределения средств.

В работе предлагается один из подходов научного исследования процессов информационной войны, на основе которого возможно принятие оптимального решения по управлению информационного противостояния. Заметим, что в термин «Информационная война» мы будем использовать для обозначения информационного противостояния двух антагонистических сторон. Стороны используют логос - слово, как оружие, для дискредитации, дезинформации противника и т.п. Третьей стороной в Информационной Войне выступает миротворческая сторона,

целью которой является подавление противостояния антагонистических сторон.

Построение обобщенной модели Информационной Войны диктуются следующими соображениями. Можно выделить два подхода в математическом и компьютерном моделировании информационной войны, которые применялись ранее. Это, с одной стороны, исследования с помощью модели количество людей, которые восприняли распространенную информацию противоборствующей стороны, тем самым стали адептами - приверженцами этой информации. При другом подходе с помощью модели исследуются потоки информаций распространенные сторонами информационной войны. Т.е. моделируются потоки информации. При этом в моделях информационных адептов не учитываются в явном виде информационные потоки, и наоборот, в моделях информационных потоках нет места для адептов распространяемых информации. Поэтому, для более адекватного описания процессов Информационной Войны целесообразно совместное использование этих подходов. В работе представлена модель, построенная на основе этого единого подхода, объединяющая совместное описание и адептов, и потоков. На основе полученной дискретной обобщенной моде ставится специфическая задача управляемости Информационной Войны. Представленное исследование и доклад выполнен при финансовой поддержке научного гранта №YS17_78 «Автоматизированная Информационная Система Информационной Войны» Национального Научного Фонда Шота Руставели Грузии. This work was supported by Shota Rustaveli N ational S cience F oundation o f G eorgia (SRNSFG) gr ant №YS17_78.

2. Дискретная модель информационных адептов. Для построения дискретной модели воспользуемся непрерывной моделью рекламной компании **А.А. Самарского** и **А.П. Михайлова** приведенная в работе [1]:

$$\frac{dx(t)}{dt} = [\alpha_1(t) + \alpha_2(t)x(t)]\left(X_0 - x(t)\right), \tag{1}$$

$$x(t)|_{t=0} = 0. \tag{2}$$

Дискретный аналог модели (1),(2)

$$n_{i+1} = -\tau\alpha_2 n_i^2 + (1 - \tau\alpha_1 + \tau\alpha_2 N)n_i + \tau\alpha_1 N. \tag{3}$$

$$n_0 = 0. \tag{4}$$

будем называть дискретной моделью Самарского-Михайлова. В (1),(2) X_0 - количество людей в обществе, где распространяется информация

рекламного характера о неком товаре, $x(t)$- количество людей воспринявших эту информацию (адепты) в момент времени t, $\alpha_1(t)$– интенсивность информационной (рекламной) кампании. $\alpha_2(t)$– интенсивность информационной (рекламной) кампании адептов, которые также начинают распространять полученную информацию о товаре. В дискретной модели Самарского-Михайлова (3),(4) N количествотало индивидуумов в сообществе которые получают информацию о некотором событий. (4) является начальным условием и указывает на то, в начале процесса никто не является адептом той информации, которая еще не распространена. Измерение количество адептов происходит в дискретные моменты времени $t_i = i * \tau$ и равно n_i, где τ является шагом между соседними дискретными моментами, $i = 0,1,2,...,m$, а процесс рассматривается на отрезке времени $[0; m \times \tau = T]$. α_1 является коэффициентом интенсивности распространения информации посредством целенаправленной кампанией, а α_2 коэффициент интенсивность распространения информации на межличностном уровне.

Компьютерная реализация дискретной модели Самарского-Михайлова в среде MatLab для различных значении коэффициентов интенсивности распространения информации показывает, что при увеличении значений этих величин число адептов приближается к числу индивидуумов в сообществе. Таким образом, описываемый моделью процесс управляем и в качестве управляющих параметров можно принять коэффициенты α_1, α_2. Вместе с тем, нужно отметить, что в дискретной модели Самарского-Михайлова в явном виде не присутствует количество распространяемой информаций, т.е. информационный поток, с помощью которого и происходит рекрутирование адептов.

3. Дискретная модель Информационных Потоков с ограничением. В математическом моделировании информационной войны достаточно развит и другои подход, в котором основном описываются информационные потоки распространяемые участниками Информационной Войны (Чилачава Т., Кереселидзе Н. [2], Мишра Бимал Кумар, Праджапати Афекша [3] и др.). В этих моделях, по предложению профессора Т. Чилачава, две стороны распространяют друг против друга информационные потоки дезинформации и дискредитации, а третья сторона – миротворческая, призывает их прекратит информационную войну.

Для построения дискретной модели потоков с ограничениями мы воспользуемся непрерывной моделью предложенной в работе [4]. Дискретный аналог непрерывной модели имеет вид:

$$\begin{cases} N_{10}^{i+1} = N_{10}^{i} + \tau\alpha N_{10}^{i}\left(1 - \dfrac{N_{10}^{i}}{I_1}\right) - \beta\tau N_3^{i}, \\ N_{20}^{i+1} = N_{20}^{i} + \tau\alpha N_{20}^{i}\left(1 - \dfrac{N_{20}^{i}}{I_2}\right) - \beta\tau N_3^{i}, \\ N_3^{i+1} = N_3^{i} + \tau\gamma\left(N_{10}^{i} + N_{20}^{i}\right)\left(1 - \dfrac{N_3^{i}}{I_3}\right). \end{cases} \quad (5)$$

$$N_{10}^{0} = N_{10}, \quad N_{20}^{0} = N_{20}, \quad N_3^{0} = N_{30} \quad (6)$$

где (6) начальные условия; I_1, I_2, I_3 уровень развития информационных технологии соответствующих сторон, в силу чего они не могут распространить объем информаций превышающие эти величины; α - коэффициент агрессивности антагонистических сторон; γ - коэффициент миротворческой готовности антагонистических сторон; γ - коэффициент миротворческой активности третьей стороны; N_{10}^{i}, N_{20}^{i}, N_3^{i} -распространенная информация в момент времени i первой, второй и третьей стороны соответственно. Вычислительный эксперимент по исследованию свойств дискретной модели с ограничениями показал, что соответствующая система управляема и третья сторона может подавить информационное противостояние антагонистических сторон увеличивая значения коэффициента своей миротворческой активности, которая, по сути, и является управляющим параметром. Завершение, или подавление информационной войны характеризуется выходом на нуль количества информации, которую распространяют антагонистические стороны - $N_{10}^{i^*} = 0$, $N_{20}^{i^{**}} = 0$. Заметим, что в дискретной модели с ограничениями (5),(6) со своей стороны отсутствует количество адептов, которые безусловно возникнут в результате распространения информации сторонами.

4. Обобщенная дискретная модель Информационной Войны с ограничением. В дискретной модели Информационной Войны с ограничением основной упор делается на информационные потоки, и в ней не присутствуют адепты информации. С другой стороны, в дискретной модели типа Самарского-Михайлова не присутствую информационные потоки, однако имеются адепты этих информационных потоков. Построим обобщенную дискретную модель Информационной Войны, в которой будут присутствовать и потоки, и адепты, для этого используем также методы, использованные в работе [5] .

При построении обобщенной дискретной модели Информационной Войны надо учесть расслоение общества первой и второй сторон. Когда первая сторона распространяет "свою" - т.н. "официальную" информацию, то адептами этой информации становится часть общества, как в самой первой стороне - ${}_{11}^{i}N$, так и второй стороны - ${}_{21}^{i}N$. Адепты ${}_{11}^{i}N$, ${}_{21}^{i}N$ будут распространять угодную первой стороне информацию в количестве N_{11}^{i}, N_{21}^{i} соответственно. Аналогично, адепты второй стороны внутри себя - ${}_{22}^{i}N$, и в первой стороне ${}_{12}^{i}N$. Эти адепты будут соответственно распространять информацию, угодной второй стороне в количестве N_{22}^{i}, N_{12}^{i} соответственно.

$$
\begin{cases}
N_{10}^{i+1} = N_{10}^{i} + \tau\alpha N_{10}^{i}\left(1-\dfrac{N_{10}^{i}}{I_1}\right) - \beta\tau N_{3}^{i}, \\
N_{20}^{i+1} = N_{20}^{i} + \tau\alpha N_{20}^{i}\left(1-\dfrac{N_{20}^{i}}{I_2}\right) - \beta\tau N_{3}^{i}, \\
N_{3}^{i+1} = N_{3}^{i} + \tau\gamma\left(N_{10}^{i} + N_{20}^{i}\right)\left(1-\dfrac{N_{3}^{i}}{I_3}\right), \\
{}_{11}^{i+1}N = {}_{11}^{i}N + \tau\left(\alpha_3 N_{10}^{i} + \alpha_4 N_{11}^{i}\,{}_{11}^{i}N\right)\left(1-\dfrac{{}_{11}^{i}N}{{}_{1}N}\right), \\
{}_{12}^{i+1}N = {}_{12}^{i}N + \tau\left(\alpha_5 N_{20}^{i} + \alpha_6 N_{12}^{i}\,{}_{12}^{i}N\right)\left(1-\dfrac{{}_{12}^{i}N}{{}_{1}N}\right), \\
{}_{21}^{i+1}N = {}_{21}^{i}N + \tau\left(\alpha_7 N_{20}^{i} + \alpha_8 N_{21}^{i}\,{}_{21}^{i}N\right)\left(1-\dfrac{{}_{21}^{i}N}{{}_{2}N}\right), \\
{}_{22}^{i+1}N = {}_{22}^{i}N + \tau\left(\alpha_9 N_{10}^{i} + \alpha_{10} N_{22}^{i}\,{}_{22}^{i}N\right)\left(1-\dfrac{{}_{22}^{i}N}{{}_{2}N}\right), \\
N_{11}^{i+1} = N_{11}^{i} + \tau\alpha_{11} N_{11}^{i}\left(1-\dfrac{{}_{11}^{i}N}{{}_{1}N}\right){}_{11}^{i}N + \tau\alpha_{12} N_{10}^{i}\left(1-\dfrac{N_{11}^{i}}{I_{11}}\right), \\
N_{12}^{i+1} = N_{12}^{i} + \tau\alpha_{13} N_{12}^{i}\left(1-\dfrac{{}_{12}^{i}N}{{}_{1}N}\right){}_{12}^{i}N + \tau\alpha_{14} N_{20}^{i}\left(1-\dfrac{N_{12}^{i}}{I_{12}}\right), \\
N_{21}^{i+1} = N_{21}^{i} + \tau\alpha_{15} N_{21}^{i}\left(1-\dfrac{{}_{21}^{i}N}{{}_{2}N}\right){}_{21}^{i}N + \tau\alpha_{16} N_{20}^{i}\left(1-\dfrac{N_{21}^{i}}{I_{21}}\right), \\
N_{22}^{i+1} = N_{22}^{i} + \tau\alpha_{17} N_{22}^{i}\left(1-\dfrac{{}_{22}^{i}N}{{}_{2}N}\right){}_{22}^{i}N + \tau\alpha_{18} N_{10}^{i}\left(1-\dfrac{N_{22}^{i}}{I_{22}}\right).
\end{cases}
\qquad (7)
$$

С начальными данными (8).

$$\begin{cases} N_{10}^0 = N_{10}, \quad N_{20}^0 = N_{20}, \quad N_3^0 = N_{30}, \\ N_{11}^0 = 0, \quad N_{12}^0 = 0, \quad N_{21}^0 = 0, \quad N_{22}^0 = 0, \\ {}_{11}^{0}N = 0, \quad {}_{12}^{0}N = 0, \quad {}_{21}^{0}N = 0, \quad {}_{22}^{0}N = 0. \end{cases} \tag{8}$$

5. Управляемость дискретной системы Информационной войны с ограничениями. В дискретной модели Информационной Войны с ограничениями (7), (8) т.н. "полезная" информация для первой и второй стороны соответственно равно:

$$N_1^i = N_{10}^i + N_{11}^i + N_{22}^i, \tag{9}$$

$$N_2^i = N_{20}^i + N_{21}^i + N_{12}^i. \tag{10}$$

Количество информаций (9), (10) третья сторона своей активностью должна обратить в "нуль", это и есть управляемость системы. Т.е. для первой и второй сторон должны наступить моменты времени, когда будут выполнены следующие условия:

$$N_1^{i^*} \le 0, \quad N_2^{i^{**}} \le 0. \tag{11}$$

Здесь i^*, i^{**} первые же значения моментов времени, для которых справедливо (11), а для $\forall k \ge i^* \,\&\, \forall l \ge i^{**}$ имеем $N_1^k \le 0, \quad N_2^l \le 0$. Задача управляемости тем самым сводится в нахождении тех значении миротворческой активности третьей стороны - γ и уровня IT третьей стороны - I_3, что бы система, которая описывается соотношениями (7) была переведена из состояния (8) в состояние (11). При этом особенность этого управляемости в том, что значения i^*, i^{**} не связаны с друг другом, т.е. свободны. Для установления управляемость системы (7),(8),(11) была составлена программа и в среде MatLab, с помощью компьютерного эксперимента доказана управляемость дискретной системы Информационной Войны с ограничениями.

Литература:

1. *Самарский* А.А., *Михайлов А.П*. Математическое моделирование: Идеи. Модели. Примеры. Первое издание -1997г., второе исправленное издание - 2005 г. - М. Физматлит. 320 с.
2. *Chilachava T., Kereselidze N.* Non-preventive continuous linear mathematical model of information warfare. Sokhumi State University Proceedings, Mathematics and Computer Sciences vol. 7. 2009, № 7. p. 91 – 112.

3. *Bimal kumar Mishra, Apeksha Prajapati*. Modelling and Simulation: Cyber War. International Conference o n C omputational I ntelligence: Modeling Techniques and Applications (CIMTA) 2013. Procedia Technology 10 (2013) 987 – 997. Elsevier.
4. *Кереселидзе Н.Г.* О соотношениях уровней информационных технологий сторон в обобщенной математической модели информационной войны игнорирования противника. // Труды XXI международной конференций "Проблемы управления безопасностью сложных систем". Москва, Декабрь, 2013, с. 173-175.
5. *Kereselidze N.* Combined continuous nonlinear mathematical and computer models of t he I nformation Warfare.// International journal of c ircuits, systems and signal processing, Volume 12, 2018, pp. 220-228.

Комков Н.И., Лазарев А.В., Чекаданова М.В.

Адаптационный механизм управления разработкой и созданием высокотехнологичной продукции

Аннотация: Рассматриваются условия, тормозящие ускоренное развитие высокотехнологичных отраслей. Для их устранения предлагается механизм адаптации известных организационных форм (особая экономическая зона, кластер, субсидии и др.) и экономических методов управления (программно-целевое управление, управление проектами) с учетом процессов развития управленческого сектора радиоэлектронной промышленности.

Ключевые слова: высокие технологии, кластер, особая экономическая зона, программно-целевое управление, управление проектами, адаптация

Инновационная модернизация отечественной экономики в большинстве правительственных документах, отражающих проблемы развития, рассматривается как основное направление перехода к новому технологическому укладу и устойчивому социально-экономическому развитию. Это направление часто ограничивается рассмотрением динамики потенциала высокотехнологичной продукции, создаваемой на основе учитываемых Росстатом передовых производственных технологий (ППТ). Анализ динамики ППТ за последние 10 лет свидетельствует об увеличении почти в 2 раза числа созданных ППТ при одновременном росте объемов финансирования НИР почти в 4 раза.

Вместе с тем доля отечественных инновационных технологий на мировых рынках составляет всего 1%, а доля ВВП РФ в мировом объеме едва превышает 2% [1]. Признание ведущей роли высоких технологий в

увеличении валовой добавленной стоимости, достигнутой промышленно развитыми странами, а также невозможность ресурсной ориентации экономики обеспечения стабильно высоких темпов роста ВВП при высокой волатильности мировых цен на ресурсы (углеводороды, металлы, древесина и др.), экспорт которых составлял более половины доходов бюджета РФ, потребовало увеличения доли ППТ в общем объеме создаваемых инновационных технологий. Однако, в конце 90-х годов прошлого века необходимость роста доли высокотехнологичной продукции рассматривалось руководством страны как возможность увеличения доходов от экспорта этой продукции, способной заменить ожидавшееся ограничение доходов от экспорта ресурсов. Наметившееся отставание отечественного научно-технологического уровня предполагалось компенсировать за счет импорта высокотехнологичной продукции. При этом доля затрат на науку и технологии стабилизировалась на уровне 1% от ВВП, а размер затрат отечественных компаний в этом объеме составлял всего около 20%. Стабильно низкое финансирование российской науки в 90-х годах, приоритетная поддержка налоговой системой стратегии ресурсно-экспортной ориентации отечественной экономики и другие меры привели к банкротству и утрате своего потенциала для ряда высокотехнологичных предприятий в области станкостроения, электронного машиностроения и радиоэлектронной промышленности, формировавших отечественный рынок высокотехнологичной продукции. Поэтому пожелания увеличения разработки высоких технологий и доли высокотехнологичной продукции при отсутствии защиты отечественных предприятий от растущего импорта этой продукции и неблагоприятной налоговой политики для создания технологий высоких переделов привели не только к закрытию многих высокотехнологичных предприятий (например, объединения по созданию обрабатывающих центров в г. Иваново и др.), но и к частичному распаду научно-технологического потенциала. Намерения руководства страны повысить этот потенциал носили декларативный характер и не учитывали всей совокупности факторов-тормозов в данной области.

Изменения в общем прогрессивном подходе к намерению развивать высокотехнологичные разработки, обозначились в начале 2000-х годов и были связаны с ростом внимания и поддержки высокотехнологичных отраслей, ориентированных на интересы ВПК. Постепенно вырабатывались организационно-экономические меры содействия гражданских высокотехнологичных производств в форме особых экономических зон, кластерных образований, грантовой поддержки рядом созданных фондов (РГНФ, РФФИ, РНФ), включая венчурные структуры.

Одновременно при подготовке утверждаемых правительством документов по проблемам научно-технологического развития [2-4], сопровождаемых низкими объемами финансирования содержались

призывы к концентрации ресурсов на разработке высоких технологий. Тот факт, что такие призывы звучат регулярно с начала XXI века, но объемы создаваемых ППТ растут незначительно, а ожидание прорывных успехов в этой области постоянно откладывается, свидетельствует о том, что необходимо пересмотреть сложившуюся парадигму к управлению разработкой и созданием высоких технологий.

Несмотря на отсутствие значительных позитивных успехов в увеличении доли высокотехнологичной продукции, в отдельных отраслях обозначились локальные успехи (медицинское оборудование, электроника, арктические технологии судостроения, станкостроение, фармацевтика и др.). Эти успехи во многом достигнуты на основе совмещения созданных организационных форм поддержки (кластеры, особые экономические зоны и др.) и использования современных методов целевого управления.

В основе новой парадигмы к управлению разработкой и созданием высоких технологий целесообразно направленно использовать существующие организационно-экономические формы с учетом особенностей конкретных процессов исследований и разработки высоких технологий и адаптации к этим особенностям известных механизмов целевого управления программами и проектами. К числу важных особенностей процессов исследований и разработки высоких технологий относятся следующие:

1) обязательное восстановление на постоянной основе потенциала основных звеньев и их связей в рамках полного инновационного цикла, начиная с фундаментальных исследований, теоретико-прикладных исследований, практических разработок, инжиниринговых услуг и освоения отечественными компаниями;
2) оценка в динамике потенциала конкурентоспособности технологий;
3) оптимальное управление интенсивностью выполнения работ, целевых проектов и программ;
4) стимулирование «ответственного исполнителя» работ, целевых проектов и программ, содействующее их выполнению «точно в срок с заданным качеством и согласованными затратами»;
5) контроль целевого расходования средств, достижение ключевых результатов и передача завершенных результатов заказчику. Варианты механизмов управления работами, проектами и программами изложены в работах [5,6].

Адаптация методов целевого управления сложными процессами и организационных форм их поддержки с учетом особенностей процессов управления разработками и созданием высоких технологий применительно к разработке высокотехнологичного медицинского оборудования, а также к разработке сложных технологий, используемых в арктической зоне

России, позволяет надеяться на успешную и полезную реализацию изложенной ранее парадигмы и в других областях разработки высоких технологий.

Литература:

1. *Кулакин Г.К.* Анализ и оценка организационно-технологического потенциала среднесрочного горизонта планирования // Научные труды ИНП РАН. – М.: Макс-Пресс, 2016. – С. 399–420.
2. Президентский указ «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». 7 мая 2018 г. [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/events /president/news/57425. – Заглавие с экрана. – (Дата обращения: 25.08.2018).
3. Стратегия научно-технологического развития (утв. Указом Президента РФ от 1 декабря 2016 г. № 642) [Электронный ресурс]. – Режим доступа: http://www.garant.ru/products/ipo/prime/doc/71451998/. – Заглавие с экрана. – (Дата обращения: 14.02.2017).
4. Прогноз научно-технологического развития до 2030 года (утв. Правительством РФ). 10 июля 2018 г. [Электронный ресурс]. – Режим доступа: http://legalacts.ru/doc/prognoz-nauchno-tekhnologicheskogo-razvitija-rossiiskoi-federatsii-na-period/. – Заглавие с экрана. – (Дата обращения: 10.09.2018).
5. *Комков Н.И., Бондарева Н.Н., Романцов В.С., Диденко, Н.И., Скрипнюк Д.Ф.* Методические основы управления развитием компаний. – М., 2015. – 520 с.
6. *Комков Н.И., Луговцев К.И., Якунина Н.В.* Информационная технология формирования и управления реализацией инновационных проектов // Проблемы прогнозирования. – 2012. – № 3. – С. 118–132.

Горелова Г.В., Кузьминов А.Н., Калиниченко А.И.

Имитация конкуренции и конфронтации систем, когнитивное моделирование

Аннотация: Эффективность управленческих решений зависит от их взвешенности и своевременности. Это особенно важно в условиях конкуренции систем или конфронтации сторон для обеспечения безопасности одной из систем/сторон. Предлагается использовать разработанный инструментарий когнитивного моделирования сложных систем для имитации структуры, состояния и поведения взаимодействующих сложных систем, для предвидения возможного развития ситуаций в них. Это позволит разрабатывать и обосновывать управленческие решения, направленные на снижение риска от конкуренции/конфронтации.

Ключевые слова: конкуренция, конфронтация, безопасность, имитация, когнитивное моделирование, принятие решений

Введение. Роль и значение научного обоснования решений органов государственного, военного управления, управления конкурирующими компаниями, фирмами и т.п. в настоящее время существенно возрастают [2]. Конкуренция сторон, противоборство, конфронтация враждующих сторон, группировок, социальных и политических систем, всё, что обозначим понятием «противостояние», происходит по причине столкновения интересов, целей, убеждений, взглядов, принципов и др. Полная противоположность интересов и полярность позиций приводит стороны к состоянию открытого противоборства, жесткому непримиримому противостоянию. Частичное совпадение интересов заставляет искать компромиссные решения. Но стремление отстоять как можно больше из «своих» интересов и не дать партнеру возможности реализовать его интересы за счет ущемления «своих» интересов определяет цели и средства каждой из противостоящих сторон. Очевидно, что осуществление действий, способствующих безопасности, эффективному достижению «своей» цели, требует, в первую очередь, принятия обоснованных стратегических управленческих решений. Стратегическое управление строится на элементах стратегического взаимодействия, когда результаты действий отдельной стороны (агента) зависят от действий одного или нескольких других сторон (агентов), которые должны действовать в условиях противостояния, в условиях внутренней и внешней конкуренции. Поэтому правильная оценка потенциала той или иной стратегии обеспечения устойчивого преимущества стороны должна быть основана на глубоком понимании конкурентных взаимодействий, на способности руководителей, управленцев обосновывать применяемую стратегию, анализируя, прогнозируя, оценивая ее возможные результаты.

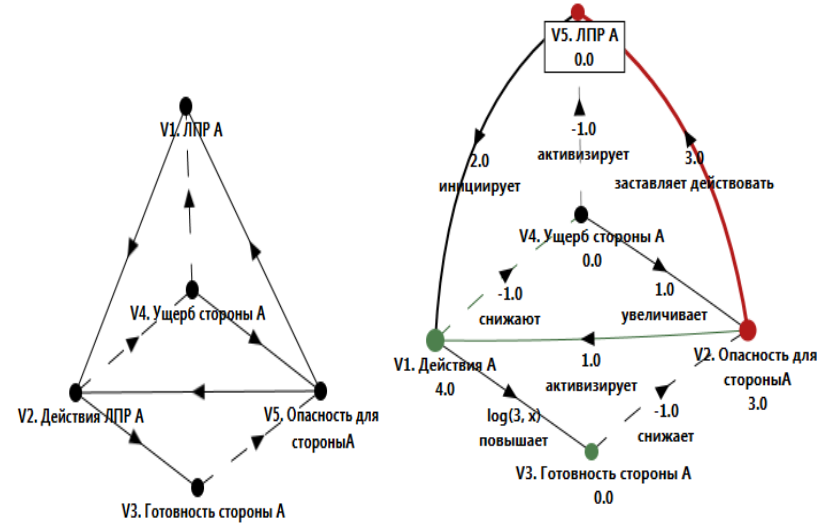
Обоснование может базироваться на имитационном моделировании условий, ситуаций, на предвидении возможного поведения сторон. Современное имитационное моделирование структуры, поведения, взаимодействия сложных систем, которыми являются, в том числе, противостоящие стороны, строится на привлечении разнообразных методов описания, объяснения, прогнозирования развития систем, обоснования и выбора лучших решений по управлению. В соответствии с этим разработка системы моделей и последовательности методов для решения задач имитационного моделирования противостояния является актуальной проблемой. Предлагается в качестве имитационного моделирования применять методологию и инструментарий когнитивного моделирования сложных систем [3,4].

Целью данной работы было исследование проблемы взаимодействия (противостояния) сторон в ее постановке с позиций когнитивного моделирования и с использованием возможностей авторской программной системы CMSS (Cognitive Modeling Software System), фрагмент которой представлен [4]. Новая программная система является развитием предшествующей программной системы когнитивного моделирования ПСКМ [5], которая на начальных этапах разрабатывалась в след работам ИПУ РАН. Теория и практика когнитивного моделирования сложных систем развивалась как на базе работ российских, так и зарубежных авторов. Автором были проведены исследования в разных предметных областях (социотехнической, социально-экономической, геополитической и др.) [4], подтвердившие применимость и эффективность разработанного инструментария когнитивного имитационного моделирования к исследовании сложных систем. Основное отличие имитационного моделирования, названного когнитивным моделированием сложных систем, от других вариантов когнитивного моделирования в когнитивных науках состоит в совокупности решаемых на когнитивной модели системных задач, а не только в задаче помочь разработать когнитивную модель в форме concept map, mind map, и др. Отличие также заключается в назначении – для исследования социотехнических, экономических, социальных, геополитических и др. сложных систем, а не только личности и его процессов познания; отличие состоит и в объекте исследования – паре «объект-субъект» (сложная система-личность, лицо принимающее решение, исследователь, наблюдатель) для учета риска человеческого фактора на этапах исследования и внедрения результатов исследования.

Основные положения. Рассмотрим постановку задачи взаимодействия двух, трех и более сторон (пока абстрактные стороны A, B, C, …) в общем виде, моделируя и фиксируя результаты рассуждений и исследований с помощью разработанной программной системы CMSS [7], одновременно иллюстрируя некоторые ее возможности.

Обобщенную когнитивную модель взаимодействия сторон будем строить, моделируя ее из блоков – когнитивных моделей, которые назовём «базовыми». На рис. 1 изображена модель из 5 вершин для стороны A, один из вариантов, в котором учтены факты наличия у каждой стороны: лица, принимающего решение ($V1$ ЛПР), опасности для стороны ($V5$), возможности ущерба при возникновении опасности ($V4$), готовности стороны противостоять опасности ($V3$) и необходимости действий ЛПР ($V2$) для снижения опасности и ущерба от неё. При разработке когнитивной модели возможен более простой ее вариант в виде когнитивной карты рис. 1а, в которой учтены только вершины V и

отношения *E* между ними в виде положительных (увеличение/уменьшение сигнала в *Vi* приводит к увеличению/уменьшению сигнала в *Vj*; сплошные линии) и отрицательных дуг (увеличение/уменьшение сигнала в *Vi* приводит к уменьшению / увеличению сигнала в *Vj*; штрихпунктирные линии) – это знаковый ориентированный граф $G=<V,E>$ [3-6].



\+ а) б)

Рис.1. – Когнитивная модель причинно-следственных связей вершин стороны А, возможности разработки и представления ее с помощью CMSS

При более глубоком погружении в проблему возможно представление когнитивной модели в виде рис. 1.б - функционального векторного параметрического графа [6], когда определены функции на дугах (например, $f_{23} = aX \bullet X$), весовые коэффициенты (например, w_{51} = 3,0) и параметры или веса вершин (например, вес вершины задан равным 5) Возможно раскрашивать вершины и дуги, изображать их разной величины/толщины, выделять рамкой вершину (вершины), на которой необходимо сосредоточить внимание, обозначать действие некоторых или всех дуг, убирать все обозначения и видеть когнитивную модель только как когнитивную карту а), возможно изменение номеров вершин – все эти действия учитывают психологические особенности исследователя, помогая ему осознавать и моделировать изучаемую проблему. Модель системы в виде матрицы отношений m×m дает возможность проводить анализ свойств когнитивной модели.

На рис. 2 изображена когнитивная модель взаимодействия трех сторон: конкурирующих А и В и стороны С, союзной А.

Модель рис. 2 построена путем операций объединения отдельных структур А, В и С. Заметим, возможны и другие способы комбинаций взаимодействия сторон А, В, С. Зависит от конкретных исследуемых объектов.

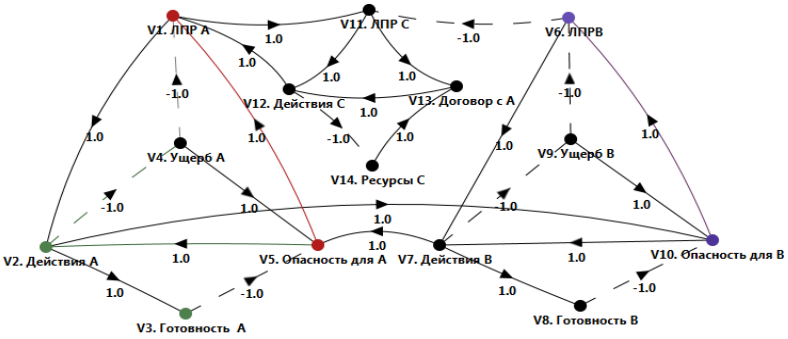


Рис.2. – Когнитивная модель G_1 взаимодействия двух конкурирующих сторон А и В в присутствии «союзной» для А стороны С

Методология когнитивного моделирования сложных систем, разрабатываемая в [3,4], включает в себя анализ свойств когнитивной модели, таких, как: 1) анализ циклов и путей, 2) анализ устойчивости (структурной и к возмущениям); позволяет провести: 3) симплициальный анализ модели, 4) импульсное моделирование развития ситуаций (научное предвидение вариантов будущего развития системы) и ряд других исследований, дающих возможность судить о соответствии/несоответствии модели реальной сложной системе.

Анализ циклов и путей. На рис. 3 представлены результаты вычислительного эксперимента по определению циклов модели G_1. Для наглядности на рис. 3 выделен наибольший из циклов. Этот цикл отрицательный (нечетное число отрицательных дуг), стабилизирующий.

Анализ устойчивости. Структура модели G_1содержит 21 цикл, из них – 13 отрицательных (рис. 3), что свидетельствует о структурной устойчивости модели [4]. Поскольку максимальный по модулю корень характеристического уравнения матрицы отношений модели G_1 $|M|=1{,}34>1$, то это свидетельствует о неустойчивости к возмущению и по начальному значению [4,5].

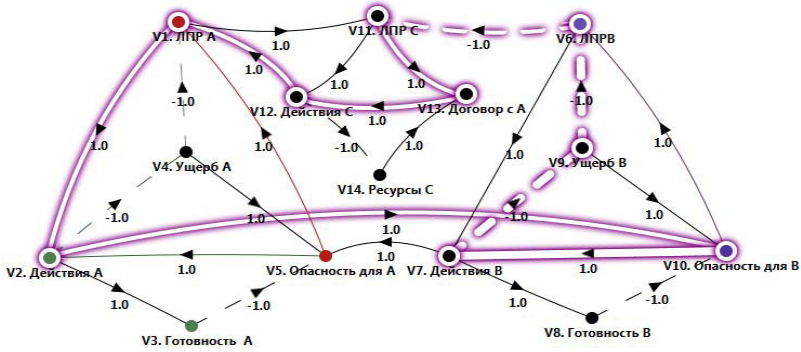


Рис. 3 – Определение циклов когнитивной модели G_1

Симплициальный анализ (анализ q-связности). Этот анализ топологических свойств графа G_1 предназначен для выявления цепочек q-связи симплексов [1,4]. Результаты этого анализа позволяют выявить «дыры» между блоками (симплексами), следовательно, слабые места сложной системы, изображенной когнитивной моделью.

Рис. 4 показывает 2 симплекса: образованный вершиной *V*2, которая является причиной взаимосвязи вершин *V*3 *V*4, *V*10 (соответствующая строка матрицы отношений), и образованный вершиной *V*1, связующей вершины *V*3, *V*4, *V*12 (соответствующий столбец матрицы отношений).

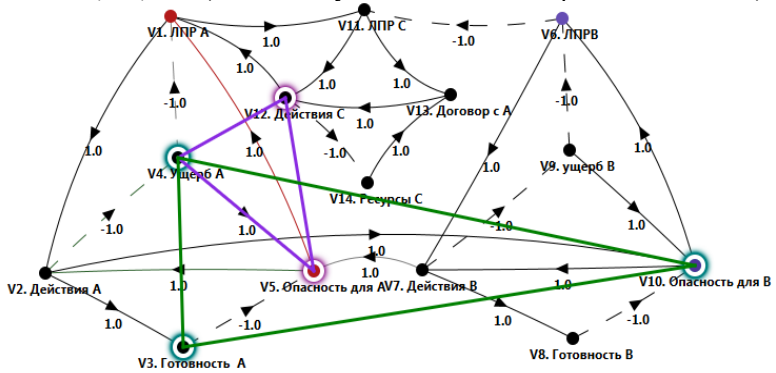


Рис. 4 – Фрагмент результатов симплициального анализа модели G_1

Сценарный анализ, предвидение возможных тенденций развития ситуаций на модели. Производится путем импульсного моделирования [5,6]. На рис. 5. изображены тенденции развития ситуаций в предположении начала действий всех сторон, вносятся воздействия q_A=+1, q_B=+1, q_C=+1. Представлены результаты 10 шагов моделирования; возможно любое увеличение/уменьшения количества шагов, зависит от конкретного объекта исследования и решений экспериментатора.

Заключение. Приведенный пример исследования абстрактной модели противостояния систем с помощью CMSS проиллюстрировал не только ряд ее возможностей, но, главное, обозначил те исследовательские задачи, которые должны и могут решаться на когнитивных моделях сложных систем. Все это отличает CMSS от многих современных программных систем когнитивного моделирования, которые, в основном, предназначены только для разработки когнитивных карт. Методология когнитивного моделирования сложных систем [4] и CMSS могут быть использованы не только в исследовательских целях, но и для автоматизированного теоретического обучения непосредственных исполнителей (например, ЛПР А). CMSS может быть элементом интеллектуальных систем поддержки принятия решений, в сфере когнитивных наук относится к направлению «Искусственный интеллект».

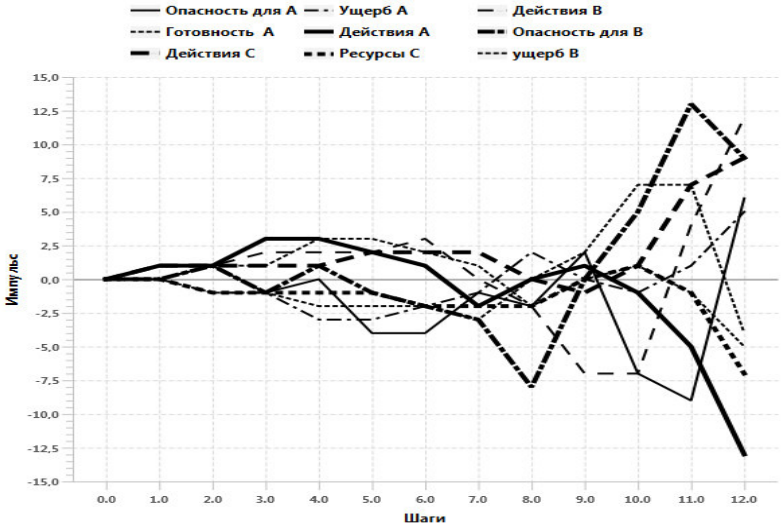


Рис. 5 – Сценарий развития ситуаций при внесении возмущений в вершины действий всех сторон

Литература:

1. *Akin R. H.* Combinatorial Connectivies in Social Systems. An Application of Simplicial Complex Structures to the Study of Large Organisations / R. H. Atkin. - Interdisciplinary Systems Research. 1997.
2. *Богданов О.А., Смирнов А.А., Ковалев Д.В.* Имитационное моделирование противоборства в воздушно-космической сфере / *О.А.Богданов, А.А Смирнов, Д.В. Ковалев* // Программные продукты и системы. - 2015. – С.160-165.

3. *Горелова Г.В., Мельник Э.В., Радченко С.А.* Анализ взаимодействия сложных систем на имитационных динамичных когнитивных моделях // Сб. материалов 8-й междунар. научно-практ. мультиконф. «Интеллектуальные и многопроцессорные системы. Искусственный интеллект – 2007». – Таганрог: Изд-во ТРТУ, 2007. Т1. – С.17-22.
4. Инновационное развитие социо-экономических систем на основе методологий предвидения и когнитивного моделирования. Коллективная монография / Под ред. Г.В.Гореловой, Панкратовой Н.Д. - Киев: Изд-во «Наукова Думка», 2015.- 464 с.
5. *Casti J.* Connectivity, co mplexity a nd cat astrophe i n l arge-scale s ystems / J.Casti.- Chichester-New York-Brisbane-Toronto, 1979.–216 p.
6. *Кульба В.В.* Сценарный анализ динамики поведения социально-экономических систем (Научное издание) / В.В. Кульба, Д.А. Кононов, С.С. Ковалевский, С.А. Косяченко, Р.М. Нижегородцев, И.В. Чернов. – М.:ИПУ РАН, 2002. – 122 с.
7. Программа для когнитивного моделирования и анализа социально-экономических систем регионального уровня. Свидетельство о государственной регистрации программ для ЭВМ № 2018661506 от 07.09.2018.

Усманова Т.Х., Исаков Д.А.

Новая парадигма развития системы электроэнергетики России в условиях интеграции в мировое хозяйство

Аннотация: Предмет/ тема. Процессы интеграции в мировое хозяйство развиваются на основании глобальных соглашений, формирования новой Парадигмы и внедрения концепций взаимодействия инфраструктурных элементов общества. Современное взаимодействие крупных корпораций и холдингов в мировом сообществе привело к противоречивым трансформациям. В таких условиях организационные процессы могут способствовать развитию сложных социотехнических систем, ориентированных на результат. Раскрытие проблем в крупных системах в условиях интеграции в мировое хозяйство позволяет глобальным структурам более эффективно для участников формировать тарифную политику. В статье рассматривается взаимодействие системы электроэнергетики на смежные отрасли, в частности промышленных структур.

Ключевые слова: электроэнергетика, парадигма, тарифная политика, регулирование, интеграция

За последние годы развитие экономики, основанная на Стратегии социально-экономического развития страны также значительно затрагивает деятельность топливно-энергетического комплекса (ТЭК). В свою очередь ТЭК влияет на развитие всех смежных отраслей народного хозяйства. В связи этим роль ТЭК в повышении темпов развития экономики страны занимает центральную позицию. [1]

«В 2013 – 2015гг. в производстве электроэнергии в стране наблюдался спад, вызванный экономическим кризисом и падением потребления. В 2016г. по данным ОАО «СО ЕЭС» потребление электроэнергии увеличилось, её выработка составила 1071,7 млрд. кВт, что на 2,1 % больше, чем в 2015 году» [5]. Однако, по мнению Минэнерго РФ росту потребления энергии в 2016г. в условиях продолжавшегося падения общего производства способствовала достаточно холодная зима и в, большей степени это сказалось на увеличении потребления энергии населением. При этом промышленность, особенно энергоемкие отрасли, будучи основными потребителями электроэнергии, не увеличили потребление энергии.

Макроэкономические показатели Министерства экономического развития и Правительства РФ накануне кризиса 2013 – 2015гг. строили оптимистические прогнозы. А именно, рост ВВП должен был составить на среднесрочную перспективу 2-3%, который должен был привести к ежегодному росту потребления электроэнергии 3-4% в год. Существенные изменения в институциональной структуре промышленности за анализируемый период показали то, что происходило постепенное их банкротство, слияние или поглощение крупными глобальными корпорациями и холдингами. В вязи с этим прогнозы Минэкономразвития и Минэнерго РФ были снижены до 2-3% роста потребления. Тем не менее, под влиянием положительных прогнозов роста экономики вместо модернизации действующих энергетических мощностей началось создание новых. Так в 2011-2016 гг. были введены в эксплуатацию 24 ГВт мощностей. В таблице 1 приведена информация о потреблении топливно-энергетических ресурсов на одного занятого в экономике страны.

Таблица 1. Потреблено топливно-энергетических ресурсов на одного занятого в экономике страны по видам экономической деятельности

№		2012	2013	2014	2015	2016
1	Всего в экономике страны	13,0	12,8	13,1	13,0	12,6
2	В том числе по видам деятельности					
3	Сельское хозяйство, охота и лесное хозяйство	2.9	2.4	2.8	2.5	3.0

№		2012	2013	2014	2015	2016
4	Рыболовство, рыбоводство	8.3	7.9	7.7	7.2	11.6
5	Добыча полезных ископаемых	62,9	63,9	72,8	72,8	72,5
6	Обрабатывающие производства	29,0	28,9	28,7	27,9	27,1
7	Производство и распределение электроэнергии, газа и воды	30,1	28,9	30,5	32,2	32,0
8	Строительство	2,2	2,3	2,3	2,7	3,6
9	Транспорт и связь	21,0	20,5	20,1	19,6	18,6
10	Прочие виды деятельности	8,8	8,5	8,7	8,7	8,0
Источник: Росстат. (Величина показателя по Российской Федерации меньше величины показателя по отдельным видам экономической деятельности из-за изменения в них пропорции объема конечного потребления топливно-энергетических ресурсов (в тоннах условного топлива) и численности занятых.						

Как видно из таблицы 1, по многим отраслям экономической деятельности наблюдается рост потребления электроэнергии. При этом в условиях дальнейшего закрытия или ликвидации промышленных предприятий, низкого роста экономики в стране сформировался большой избыток энергетической мощности, и сохраняется тенденция его увеличения. Основной проблемой закрытия или ликвидации промышленных структур считается ежегодный рост тарифов на электроэнергию. Не отвечающая требованиям интересов Российской Федерации, Парадигма развития энергетики показала всю свою негативную сторону.

При этом в России продолжается развитие инвестиционной деятельности в системе топливно-энергетического комплекса в виде ввода новых мощностей, так как проекты, как правило, формируются от 3 до 10 лет [3]. Ввод дополнительных мощностей, которые были запланированы на увеличение спроса на электроэнергию со стороны предположенного роста потребления промышленных структур, пришелся на эпоху их значительного сокращения. В то же время ОАО «Системный оператор» планировал, что в 2017-2020гг. будут введены в эксплуатацию еще 13 ГВт мощностей и выведены из эксплуатации старые 8 – 9 ГВт мощности. Следовательно, НП «Совет рынка» считает, что к имеющимся избыточным мощностям 24 ГВт добавится не менее 18 ГВт. За последние годы происходит увеличение потребления по видам экономической деятельности за последние 2016-2017 годы. Однако, существующее развитие на основе старой Парадигмы развития системы

электроэнергетики показало свою не проработанность, не совершенное регулирование экономикой страны и формирование не эффективной тарифной политики в целом.

В условиях интеграции экономик в мировое хозяйство и в частности в ЕврАзЭс в настоящее время, происходит формирование единой электроэнергетической сети. Однако, процессы интеграции происходят также под большим давлением со стороны участников мирового энергетического рынка и разработчиков энергетической политики в мировом сообществе. [2] Не только в системе электроэнергетики происходят притеснение российских корпораций и холдингов. Приведем некоторые примеры конфликта интересов в интеграционных условиях.

Недавно Россия подала в ВТО контрапелляционную жалобу по спору с ЕС и его государства члены – меры в отношении «энергетического сектора» (так называемый третий энергопакет). «Речь идет о мерах, решение по которым было вынесено третейской группой не в пользу России. Контрапелляция подается в том случае, если одна из сторон спора подает апелляцию. По правилам ВТО, в ближайшее время стороны также должны будут представить ответы на претензии друг друга», — отметили в министерстве.

В свою очередь в сентябре ЕС подал апелляционную жалобу на решения третейской группы в пользу России. Она затрагивает выигранные российской стороной претензии к применению на территории ЕС и его государств-членов норм третьего энергопакета. РФ в 2014 году начала процедуру разбирательства в ВТО по третьему энергопакету ЕС. Третий энергопакет подразумевает, что собственниками расположенных в регионе магистральных трубопроводов не могут быть компании, которые занимаются добычей газа. Эти требования создавали препятствия для строительства, например, «Южного потока», от которого пришлось отказаться. В августе текущего года Всемирная торговая организация сообщила, что не поддержала возражения РФ против требований третьего энергопакета ЕС по разделению управления компаниями по добыче, сбыту и транспортировке газа, а также по преференциям, предоставляемым ЕС поставщикам сжиженного природного газа (СПГ). Вместе с тем Минэкономразвития РФ тогда же сообщило, что ВТО поддержала Россию в ключевых моментах этого спора. В частности, организация признала неправомерными количественные ограничения поставок газа из РФ по газопроводу OPAL, включая 50-процентное использование его мощностей, а также нормы ЕС о продаже газа на бирже и дискриминацию операторов ГТС под контролем иностранцев в Литве, Венгрии и Хорватии, сообщало МЭР РФ.

Приведем другой пример, который появился в процессе интеграции энергетической системы. В средствах массовой информации появилась статья под заголовком «Предлагается отнять у «Газпрома» трубопроводную сеть России». Центр стратегических разработок (ЦСР) предлагает отстранить «Газпром» от контроля над единой системой газоснабжения (ЕСГ) и монополии на экспорт трубопроводного газа. Об этом говорится в докладе центра «Перспективы развития газового рынка России». «В проекте доклада смоделированы несколько сценариев. В каждом из них «Газпром» утрачивает контроль над единой системой газоснабжения и монополию на экспорт трубопроводного газа – в оптимальном варианте последняя также передается государству.

В течение ряда лет тарифообразование в системе электроэнергетики не отвечает интересам реального российско-ориентированного производства. Как показывает практика, энерготарифы растут медленнее, чем инфляция, но счета за электроэнергию составляют значительную статью расходов для потребителей: населения и производственных структур. При этом тарифы растут быстрее, чем цены на продукцию всех отраслей промышленности. За последние годы в рамках существующей Парадигмы, не отвечающей целям и задачам экономического роста России, средняя цена на электроэнергию выросла в 3 раза, при параллельном росте тарифов других естественных монополий и стала главным фактором банкротства, слияния и поглощения многих производственных структур.

Существующая Парадигма развития системы электроэнергетики позволяла формировать новые инвестиционные проекты в рамках договоров поставки мощностей (ДПМ). При этом, построенные 20-25 гигаватт мощностей были созданы по договорам поставки мощностей, на основании которых все инвестиции должны возвращаться в течение 15 лет под 14-17% годовых. Данные договоры рассматривались как генеральное направление развития электроэнергетики и обеспечили ввод в действие новых мощностей. При этом договоры поставки мощности не обеспечили обратной связи: электропотребление не растёт, мощности продолжают вводиться, а все расходы по их реализации ложатся на потребителя (в большей степени на промышленные структуры, особенно те, где больше энергоемкости в деятельности и энергозатрат) электроэнергии не только не сокращают возможности роста общего производства, но и являются тормозом и причиной их несостоятельности.

При этом на экономический рост оказывает давление и то, что часть тепловых станций, построенные во времена плановой экономики СССР, мощность которых составляет 27,6 ГВт, находится в сверхаварийном состоянии из-за отсутствия средств на ремонтные работы. Однако тепловые станции также требуют расходы на собственное поддержание, так как они обслуживают целые микрорайоны и промышленные

территории во многих городах, обеспечивая экономическую безопасность в целом.

Одним из серьезных крайностей переходной экономики является формирование структуры гарантирующих поставщиков. По мнению экспертов и самих энергетиков, гарантирующие поставщики ничем не владеют, но выставляют счета, рассчитанные по высоким тарифам. Самые высокие тарифы [6] в тех регионах, где гарантирующие поставщики наиболее активно пользуются своим монопольным положением. ФАС фиксирует, что «негативные явления, препятствовавшие развитию конкуренции в 2015г, сохранились и в 2016г».

В последнее время много возникает спорных тем о сущности «Эталона затрат» и «Эталона необходимой валовой выручки (НВВ)». Эксперты считают, что в условиях низких стандартов в оплате труда и социальной защите населения и работающих, эти два эталона могут загнать системы электроэнергетики на более сложные компенсационные процессы. В условиях существования «узкого места» для вывода денежных средств из системы электроэнергетики «Эталон затрат» и «Эталон НВВ» могут оказаться инструментом или механизмом очередного пресса в экономических процессах. Поэтому научное обоснование нововведений также требуют обоснования и отражения, в сформированной новой парадигме для системы электроэнергетики. [4]

В настоящее время формирование ценообразования и тарифообразования в менеджменте компаний энергетического комплекса не могут отличаться совершенством. Так как конфликт интересов ТЭК, производственных структур и ЖКХ с каждым годом растет и растет все больше и больше. Не ведётся методологическая и методическая системная работа по оптимизации затрат в системе энергетики. В каждом отдельно взятом регионе используются различные модели и способы по необоснованному увеличению тарифов.[5]

Таким образом, происходят особые процессы интеграции крупных социально-экономических систем в глобальную энергетическую сеть путем их расщепления и формируя новые перекосы, на почве старых нерешенных проблем. Принципы «разделяя, властвуй!» в данном случае формируют «высокие технологии» интеграционных процессов, которые могут привести к дальнейшим перекосам в рамках создания Единой энергетической сети в рамках ЕАЭС. Существующая Парадигма не отвечает требованиям развития системы энергетики, поэтому возникает необходимость формирования новой Парадигмы с учетом интересов коренного населения Российской Федерации, а не в ущерб развития человеческого потенциала и капитала в стране.

Литература:
1. Восстановление экономического роста в России. Научный доклад ИНП РАН / В.В. Ивантер, и др. // Проблемы прогнозирования. 2016. № 5 (158). С. 3-17. U RL: https://elibrary.ru/item.asp?id=28163872 (Дата обращения: 10.10.2018)
2. *Исаков Д.А.* Управление рисками развития муниципальных экономических систем. Москва, 2010.
3. *Комков Н.И.* Условия структурно-инновационной политики развития экономики России. МИР (Модернизация. Инновации. Развитие). 2017. Т. 8. № 1 (29). С. 80-87.
4. *Николаев В.А., Исаков Д.А.* Методология стратегического анализа рисков социальных систем. Аудит и финансовый анализ. 2014. № 1. С. 316-318.
5. *Усманова Т.Х., Исаков Д.А.* // Интеграция фундаментальной и прикладной науки для развития инноваций в производстве. М. Экономика. Бизнес. Банки. 2018. Т. 7. С. 66-78
6. *Усманова Т.Х., Исаков Д.А.* //Научно-технологическое развитие в России в условиях внедрения цифровой экономики. // М.: Издательский дом «Научная библиотека», Экономика и управление: проблемы, решения. 2018. Т. 7. № 5. С. 101-105.

Тюрин С.А.

О стратегическом соперничестве в киберпространстве: «Cyber Strategy – 2018»

Аннотация: Рассмотрено содержание «Cyber Strategy – 2018» US DoD. Проанализированы основные положения стратегии с позиций проблематики управления социотехническими системами в целом. В частности, сопоставляются некоторые аспекты «tradecraft» в сочетании с характерными особенностями развития таковых предметных областей.

Ключевые слова: киберпространство, стратегия, стратегическое соперничество, интенция, «tradecraft»

Исследования тенденций развития киберсреды представляется одной из наиболее интересных проблем управления безопасностью, в том числе в контексте «Стратегии в киберпространстве» Министерства обороны США 2018 (US DoD «Cyber Strategy – 2018»), которая действует в рамках реализации приоритетов Стратегии национальной безопасности и

Стратегии национальной обороны Соединенных Штатов в киберпространстве и представляет собой видение Министерством обороны США ответа на существующие угрозы кибербезопасности [1].

Эксперты и аналитики Министерства обороны Соединенных Штатов рассматривают киберпространство, как виртуальную цифровую среду, обладающую характеристиками открытости и децентрализованности. Вопросы изучения влияния кибер- или информационного пространства на все виды деятельности различных акторов представляют собой еще недостаточно изученную междисциплинарную область – этим обусловлены как повышенное внимание к подобного рода проблемам, так и необходимость выработать единый словарь для дальнейших исследований по данной тематике. В этом контексте соответствующие действия должны рассматриваться в рамках представлений об усилиях, направленных на укрепление возможностей всех видов вооруженных сил Соединенных Штатов выполнять задачи с учетом непрерывного характера взаимодействия всех акторов в киберпространстве, а также в условиях реальной обстановки (through cyberspace).

Так, одним из основных направлений разработки и реализации новых возможностей в киберпространстве являются задачи предотвращения возникновения и противодействия вредоносной активности, которая ввиду единства информационного пространства становится одной из наиболее значимых проблем для успешного выполнения функций и задач. Предполагается также, что подобная активность способна привести к возникновению крупного инцидента в киберпространстве, который трактуется как событие происходящее в (или осуществляемое при помощи) компьютерной сети, способное само по себе (в группе связанных с ним событий) привести к очевидному ущербу интересам национальной безопасности, навредить иностранным отношениям или экономике Соединенных Штатов или нанести удар по общественному доверию, гражданским свободам или общественному здоровью (public health) и безопасности населения, и нанести значительный ущерб критически важной инфраструктуре Соединенных Штатов, для чего прорабатываются возможности взаимодействия с различными агентствами и частными структурами в целях взаимного информирования и недопущения применения воздействий результатов вредоносных усилий.

Наиболее важными с точки зрения национальных интересов США являются задачи сохранения ценности собственных разрабатываемых и внедряемых технологий, как и недопущение дестабилизации работы правительства и рыночных механизмов, оспаривания демократических процессов, таким образом киберпространству дается оценка, как среде, обладающей возможностями для реализации вреда практически всем жизненно важным областям функционирования государства, как лишь при

помощи технических средств Интернета, так и в совокупности с воздействием другими методами в случае кризиса, в том числе и наступательными возможностями армии при возникновении «действительного» боевого конфликта.

В представлении экспертов и аналитиков Министерства обороны Соединенных Штатов, ключевые противостоящие США акторы в киберпространстве удерживаются «ниже уровня вооруженного конфликта» (below the level of armed conflict), однако некоторые конкурирующие субъекты пошли на усиление вредоносной активности, разворачивая кампании в киберпространстве, несущие долгосрочные стратегические риски для США, поэтому стратегический подход к осуществлению успешного соперничества в киберпространстве нацелен, как на повседневные мероприятия в сети, так и шире – на построение более летальных вооруженных сил, которые в свою очередь реализуют свойства масштабируемости, хорошо адаптируются к стремительно изменяющимся условиям и обладают разнообразием характеристик в целом для предоставления максимальной гибкости вооруженным силам Соединенных Штатов. В контексте долгосрочного стратегического соперничества обозначенные усилия произведения инноваций со скоростью, превышающей конкурентов США, сводятся к нахождению решений с «быстродействием машины» (to operate at machine speed) на стыке возможностей, предоставляемых коммерческим сектором, и собственного потенциала Министерства обороны Соединенных Штатов. Особое внимание уделяется также повседневному соперничеству в киберпространстве с использование уникальных навыков и умений, которыми обладают партнеры и союзники США, а также разработке норм ответственного поведения государств в киберпространстве, в том числе с привлечением работы международных экспертиз ООН.

Реформа Министерства обороны Соединенных Штатов рассматривается в ключе обеспечения осведомленности сотрудников на всех уровнях о возможностях и изменениях информационного пространства, а также большей подотчетности всех действий сотрудников для последующего использования этих сведений в целях оптимизации деятельности. Для реформы кадров предлагается совместно со всеми министерствами и агентствами США наращивать усилия по распространению научных, технических, инженерных, математических дисциплин и изучения иностранных языков на уровне начального и среднего образования по всей территории Соединенных Штатов для будущего инкорпорирования наиболее одаренных представителей заинтересованной молодежи в систему программы по развитию «киберпотенциала нации».

Стратегия в киберпространстве Министерства обороны США 2018 нацелена на опережающее реагирование, повседневное конкурирование и подготовку к войне при помощи создания более летальных вооруженных сил, расширения альянсов и партнерств, реформирования Министерства обороны Соединенных Штатов и развития кадрового потенциала при активных действиях по оспариванию и сдерживанию конкурентов США. В совокупности, рассматриваемые выше взаимодополняющие друг друга мероприятия, как утверждается, позволят Министерству обороны США конкурировать, сдерживать соперников и побеждать в киберпространстве.

Перспективами развития, по мнению автора, могут быть такие акценты рассмотрения проблематики, как «tradecraft», «интенция» с различных позиций (например, кибер-физических систем, управления социально-экономическими системами и т.д.).

В докладе приводятся примеры некоторых сопутствующих интеграционных компонентов предметной области [2-7].

Литература:

1. Summary de partment o f de fense c yber s trategy 2018 / *Department of Defense Cyber Strategy.* - URL*:* https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf (Дата обращения 08.11.2018)
2. *Рожнов А.В., Скорик Н.А.* Информационно-аналитическое обеспечение предпроектных исследований и системная интеграция: проблемные вопросы формирования задела и внедрения единых технологий / Труды 17-й Международной конференции «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта (CAD/CAM/PDM-2017, Москва). - М.: ИПУ РАН, 2017. С. 296-300.
3. *Рожнов А.В., Лобанов И.А., Скорик Н.А., Цыпелев В.В.* О нечёткой стратегии интеграции компонентов в интересах накопления опыта эволюционного моделирования проблемно-ориентированной системы управления на начальных этапах жизненного цикла / Труды 15-ой международной конференции «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта» (CAD/CAM/PDM-2015, Москва). - М.: ООО "Аналитик", 2015. С. 345-348.
4. *Ryvkin S., Rozhnov A., Lychev A., Lobanov I., and Fateeva Y.* Multiaspect modeling o f infrastructure solutions at energy landscape as virtual semantic environment / Proceedings - 2017 International Conference on Optimization of Electrical and Electronic Equipment, OPTIM 2017 and 2017 International Aegean Conference on Electrical Machines and Power Electronics, ACEMP 2017. B rasov, R omania: I nstitute o f E lectrical a nd E lectronics E ngineers (IEEE), 2017. P. 935-940.

5. *Гудов Г.Н., Рожнов А.В., Лобанов И.А.* Анализ практик «посткибератак» в критических сегментах инфраструктуры электроэнергетики / Труды 25-й Международной конференции "Проблемы управления безопасностью сложных систем" (Москва, 2017). - М.: РГГУ, 2017. С. 401-405.
6. *Лобанов И.А., Слепко Г.Е., Тюрин С.А.* Исследование иерархически упорядоченных сетей при поиске альтернативных путей и управлении взаимодействием информационных потоков / Тезисы докладов 16-й Всероссийской научной конференции «Нейрокомпьютеры и их применение» (Москва, 2018). - М.: МГППУ, 2018. С. 395-396.
7. *Тюрин С.А., Губин А.Н.* О методе контрактур и пределах свободы в цифровую эпоху / Тезисы докладов 16-й Всероссийской научной конференции «Нейрокомпьютеры и их применение» (Москва, 2018). - М.: МГППУ, 2018. С. 393-394.

Мачкин П.И.

Проблемы резкого ускорения процессов современного развития сложных систем и пути их высокоэффективного решения

Аннотация: В докладе приведена краткая характеристика трех главных глобальных проблем, возникших на современном этапе развития сложных систем, и представлены предложения по их высокоэффективному решению на основе уже созданных и реализованных на практике отечественных технических решений.

Ключевые слова: сложная система, информационная технология, семантический анализ, энтропия информации, энтропийная оценка, автоматизированная система

Краткая характеристика трех главных глобальных проблем современного этапа развития сложных систем

На современном этапе развития сложных систем возникли три главные глобальные проблемы, требующие их срочного решения:

- первая – это резкое ускорение протекания социально-экономических процессов в сложных системах, вызванных, прежде всего, активным переходом на цифровые способы и методы обработки информации во всех видах и сферах человеческой деятельности;

- вторая – это резкое увеличение объема свалившейся на человека информации (обусловленное активным переходом на цифровые способы и

методы обработки информации во всех видах и сферах человеческой деятельности), которую он должен обрабатывать и принимать на ее основе управленческие решения;

- третья – это необходимость срочной перестройки моделей управления государством и управления бизнесом, с тем чтобы сформированные в результате новые система управления государством и система управления бизнесом смогли вовремя реагировать на проходящие сейчас глобальные изменения в социально-экономическом развитии общества, чтобы нам в России не застыть и не оказаться отброшенными на обочину современного развития общества.

В наиболее общем виде постановку этих трех глобальных проблем современного этапа развития сложных систем, возникших в последние годы и проявляющихся во всех экономически развитых странах мира, и в России в том числе, и требующих срочного их решения, сформулировал президент Сбербанка России Греф Г.О. в одном из своих выступлений на панельной дискуссии на тему: «Бизнес и государство: модели партнерства в цифровую эпоху» на Гайдаровском форуме-2018, состоявшемся в российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС) [1]. При этом длительность видеофильма об этой панельной дискуссии составляет 1 час 56 мин. 04 сек., но для рассмотрения темы настоящего доклада, особенно важной является первая часть выступления Грефа Г.О. на указанную в [1] тему, она представлена в этом видеофильме с момента 9.25 по 17.25.

Во время этого своего выступления он подчеркнул главный тезис о том, что в современной действительности человек уже просто не успевает обрабатывать резко возросший поток информации. Возникло ключевое противоречие между линейной характеристикой мыслительной деятельности человека и его возможностей по обработке информации и резким экспоненциальным ростом сваливающейся на него информации, которую человек должен обрабатывать и принимать управленческие решения. Этот свой вывод он подкрепил очень простым, но чрезвычайно убедительным графиком резкого экспоненциального роста объема информации, требуемого для обработки и принятия решений (Рис. 1).

При этом Греф Г.О. особо подчеркнул, что человечество находится сейчас на переломе колена этой экспоненты, и дальше экспоненциальный рост объема информации, требуемого для обработки и принятия решений, будет только лишь усиливаться. Возникла, как он заявил, глобальная проблема, требующая решения, и этого решения человечество пока что не придумало.

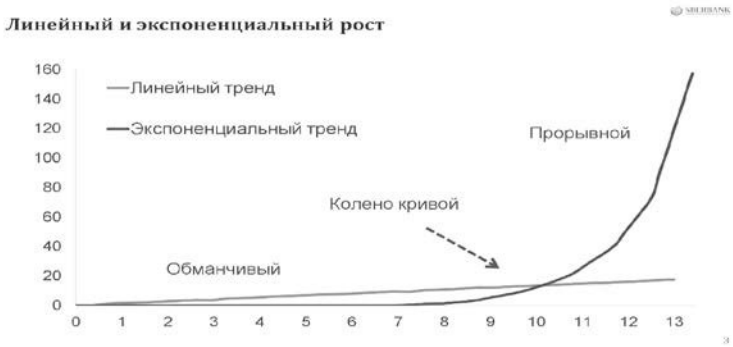


Рис. 1 – График Грефа Г.О.

Предложения по высокоэффективному решению трех главных глобальных проблем современного этапа развития сложных систем

Наши предложения по высокоэффективному решению трех главных глобальных проблем современного этапа развития сложных систем, на основе информационной технологии семантического анализа и энтропийной оценки обрабатываемой, с использованием средств электронной вычислительной техники информации (СемАн-технологии) [2 - 5], были озвучены мною во время проведения на Гайдаровском форуме-2018 открытой лекции проф. Черниговской Т.В. на тему: «Искусственный интеллект – вызов для человечества». Модератором этого мероприятия выступил А.Б.Чубайс, который предоставил мне возможность для выступления по теме лекции Черниговской Т.В. [6]. Длительность видеофильма об этой открытой лекции составляет 1 час 57 мин. 35 сек., мой вопрос автору лекции и краткое выступление с предложениями по решению поставленных в ее лекции глобальных проблем в этом видеофильме представлены в течение 4 минут, с момента 1.42.17 по 1.46.07 [6].

При этом доказательством высокой эффективности практического применения СемАн-технологии для решения этих проблем и задач является очень простой факт, который можно охарактеризовать здесь в следующем виде:

- перестройка системы управления государством и бизнесом с опорой при этом на линейный характер деятельности существующих в настоящее время иерархических административных организационных структур в различных видах и сферах человеческой деятельности будет невозможной из-за действия объективных факторов ограничения линейного характера деятельности людей в составе этих организационных структур;

- однако за счет того, что в СемАн-технологию заложен механизм формализованного описания процесса мыслительной деятельности человека, то построение на ее основе программно-информационных комплексов различной информационно-вычислительной мощности и назначения для автоматизированного решения задач формирования объективных прогнозов развития существующих знаний и разработки новых знаний в какой-либо конкретной сфере человеческой деятельности и в соответствующей ей области знаний, или в группе областей знаний, позволит тем самым резко повысить производительность труда и качество решения этих задач (совершенно недостижимое для линейного характера деятельности людей в составе существующих в настоящее время организационных структур) [2, 3];

- за счет того, что современная вычислительная техника и созданные на ее основе программно-информационные комплексы различной информационно-вычислительной мощности и назначения, объединенные в различные сети и структуры, позволяют во много крат быстрее по времени и больше по объему обрабатывать различную информацию, чем мозг человека, то заложив в основу построения этих программно-информационных комплексов разработанные нами алгоритмы и процедуры СемАн-технологии (реализующие фактически процесс мышления человека и формирования им своих умозаключений), можно в реальности создать требуемый высокоэффективный инструментарий автоматизированного решения двух указанных выше фундаментальных задач по формированию объективных прогнозов и разработке новых знаний в различных видах и сферах человеческой деятельности [4];

- а так как проблема формирования новых знаний является главной для всех отраслей экономики (в том числе и для всех отраслей шестого технологического уклада), то создание универсального инструментария по автоматизированному формированию новых знаний в различных отраслях экономики будет являться, во-первых, фактически новой отраслью экономики, и, во-вторых, базовой фундаментальной основой функционирования всех остальных отраслей экономики шестого технологического уклада [5].

Литература:

1. *Греф Г.О.* Какие технологические тренды сформируют наше ближайшее будущее // Панельная дискуссия на тему: «Бизнес и государство: модели партнерства в цифровую эпоху», Гайдаровский форум-2018, РАНХиГС, 17.01.2018г. // Адрес видеофильма в Интернете: https://www.youtube.com/watch?v=QiLiTU4pHdw (дата обращения: 18.04.2018).

2. *Заличев Н.Н.* Энтропия информации и сущность жизни», Москва, Издательство «Радиоэлектроника», 1995, 192 с.
3. *Заличев Н.Н., Мачкин П.И.* Комплексная технология прогноза развития знаний*, Н*аучно-практический журнал «Биржа интеллектуальной собственности», № 4 (апрель), 2005, с. 23-31.
4. *Заличев Н.Н., Мачкин П.И.* СемАн-технология – научно-технологический прорыв в становлении информационного общества // В сборнике трудов научно-технического конгресса по безопасности «Безопасность – основа устойчивого развития регионов и мегаполисов». Пленарное заседание и итоговые материалы тематических конференций и круглых столов; доклады и сообщения, переданные в Секретариат (Программный комитет) конгресса. Россия, Москва, 15-16 ноября 2005 года. М.: ООО «Научно-издательский центр "Инженер"», 2006, 276с., с. 91-110.
5. *Мачкин П.И.* О создании в цифровой экономике совершенно новой отрасли – автоматизированного формирования новых знаний // *Проблемы* управления безопасностью сложных систем. Труды XXV международной научной конференции, Москва, декабрь 2017г. // Под ред. Н.И.Архиповой и В.В.Кульбы, М.: РГГУ, 2017, 652 с, с. 202-205.
6. *Черниговская Т.В.* Искусственный интеллект – вызов для человечества // Открытая лекция, Гайдаровский форум-2018, РАНХиГС, 18.01.2018 г. // Адрес видеофильма лекции в Интернете: https://www.youtube.com/watch?v=5hz4mHblync (Дата обращения: 18.04.2018).

II. Проблемы обеспечения экономической и социально-политической безопасности

Неизвестный С.И.

Проблемы социальной и информационной безопасности проекта «Цифровая экономика»

Аннотация: Представлен нарратив некоторых аспектов социальной и информационной безопасности проекта «Цифровая экономика», объектом которого является сложная многоуровневая система.

Ключевые слова: цифровое общество, информационная и социальная безопасность, развитие и деградация

Проект «Цифровая экономика» (правильнее говорить о мероприятиях реализации Программы «Цифровая экономика») [1], несомненно, является одним из сложнейших проектов России общенационального масштаба. Этот проект является подтверждением того, что мы находимся в хронологическом периоде развития общества, который некоторые специалисты относят к четвертой промышленной революции.

Каждая промышленная, технологическая революция сопровождалась значительным противодействием со стороны сторонников предыдущих технологий. Это противодействие было и на структурном, и на функциональном, и на социальном уровнях. Причин, порождающих в связи с этим проблем, несколько: традиции, привычки, инерционность населения, непродуманность осуществления собственно переходов на новые технологии, отсутствие глубокого системного анализа рисков и последствий их реализации, связанных со скачкообразными изменениями в жизни общества и т.д. Одним из ярких примеров такого противодействия – движение луддитов, «восстания» против машин в начале 19-го века, было вызвано массовым сокращением занятого трудоспособного населения, утратой традиционных профессий, аргументацией деградации человека как вида. Или другой пример – массовые забастовки начала 80-х годов прошлого столетия преподавателей системы образования Японии, вызванные разрешением правительства использовать ПК учащимися в

учебных заведениях (кстати, и сейчас подавляющее большинство школьников Японии не знают таблицы умножения).

Некоторые специалисты антропологи-когнитивисты считают что, промышленные революции ускоряют процесс умственной и физической деградации человека, как популяции [2-3]. Сегодня набирает распространение тренд «жить одним днем, получать максимум от жизни сегодня». В США популярный аргумент в пользу такой жизненной стратегии выглядит с точки зрения развития человечества весьма странно: «Почему я должен заботиться о правнуках, если они обо мне не заботятся?»

Как правило, все промышленные революции приводили к увеличению нагрузки на окружающую среду, вызывали ускорение нарушения естественного баланса в биосфере. Одно из следствий этого тот факт, что около 50% школьников РФ в возрасте 14 лет имеют хронические заболевания, к окончанию школы это количество возрастает до 90-95% [3].

Промышленные революции увеличивают разрыв между духовным и техническим развитием человечества, тем самым увеличивая вероятность самоуничтожения цивилизации.

Цифровизация общества как составляющая промышленной революции существенно отличает четвертую от предшествующих революций. Принципиальное отличие состоит в том, что цифровизация переводит производство свободного времени человека совершенно на новый высокий уровень. Человек получает в свое распоряжение большие объемы свободного времени, что делает актуальным вопросы целеполагания его использования. Эта проблема имеет глобальный масштаб и ее решение в принципе определяет направление развития человека, да и стратегию выживания человечества в целом.

Следующее отличие касается резкого скачка увеличения производительности труда и его качества, с одной стороны, и значительного роста структурной безработицы – с другой. Эта проблема рождает следующую: потребность переквалификации большого числа трудоспособного населения и необходимость перестройки системы образования, которая в нынешнем варианте ориентирована на формирование знаний сегодняшнего и вчерашнего и практически не формирует знания завтрашнего дня.

Цифровизация бизнеса идет в условиях глобализации, что рождает ещё одно отличие: переход к цифровому бизнесу приводит к усилению социальной поляризации общества, к усилению разрыва между бедными и богатыми.

В условиях цифровизации основной объем делопроизводства, коммуникаций, функциональной реализации бизнеса и государственных структур осуществляется с использованием разнообразной информации,

больших данных, которые пронизывают все общество. Это также отличает четвертую революцию от предыдущих, обостряя проблему информационной безопасности общества.

В переходе на цифровую экономику имеется содержательный казус: с одной стороны цель цифровизации - замещение человека роботами, автоматами, автоматизированными системами, с другой стороны цель государства и бизнеса – сохранение рабочих мест и создание новых. Т.е. главная проблема цифровизации - социальная, проблема утилизации трудовых ресурсов (до 2024 года - несколько миллионов трудоспособных людей). Решение ее ложится на плечи основной критической инфраструктуры государства – системы образования. Но эта критическая система - система с отложенным результатом на 5-10 лет. Как перевести работу этой системы с подготовки специалистов качественно и быстро выполняющих типовые действия к формированию компетентности творчества (к активизации способностей творчества, заложенных природой) и сформировать принципиально новые профессии? Проблема утилизации трудовых ресурсов при переходе к цифровой экономике связана с проблемой улучшения качества образовательного процесса средней и высшей школы, проблемой принципиального изменения системы подготовки специалистов цифрового общества.

Цифровизация может вернуть человеку приоритет творческой составляющей в его труде. Изначально, от рождения в любом человеке присутствуют творческие способности. Промышленные революции с одной стороны позволили повысить производительность труда, с другой – привели к резкой дифференциации на людей, занимающихся творчеством и на людей, выполняющих однотипно повторяющиеся действия, приводящих к атрофии креативную составляющую в работе. Осознание этого явления позволит системно перейти к цифровизации, решая проблему безработицы, путем активизации, заложенной в человеке от природы, творческого начала и развития созидательной деятельности. Вернувшись к этим истокам, можно активизировать отношение к человеку как к личности, но не как к бездуховному исполнительному механизму. Естественно это требует от управленцев реинжиниринга управленческой культуры, организационного потенциала и системы формирования компетенций. Игнорирование данного процесса в цифровизации бизнеса может дискредитировать саму сущность цифровизации и привести к значительным социальным проблемам. Чтобы упредить данные проблемы, необходимо принципиально изменить систему формирования компетентности специалистов, вовлекаемых в процесс цифровизации, прежде всего специалистов управления сложными системами. Современные тенденции к сокращению сроков обучения, к переходу на дистанционные формы, к замене педагогов на тренинг-роботов,

использование вчерашних знаний, позавчерашних методологий и стандартов приводит к падению качества подготовки специалистов. А самая важная составляющая процесса образования, педагогического процесса – воспитание, формирование культуры управления – выхолащивается. Воспитание тяжело поддается цифровизации.

Цифровизация дает толчок высокоинтеллектуальным когнитивным технологиям управления вследствие чего в управлении сложными системами должно наступить кардинальное изменение. Это изменение затронет, прежде всего, передачу части управленческого процесса управления сложными системами, связанную с принятием решений с системным привлечением неструктурированных данных (которые в настоящее время используются лишь фрагментарно и влияют на эти решения опосредовано через интуицию менеджера или его измененное состояние сознания). Технологически особое значение в данном аспекте применения цифровизации в управлении приобретет отрицательная обратная связь [4] обеспечивающая сходимость (устойчивость) процесса управления.

Перевод реальных процессов управления сложными системами в гибридный вариант в результате цифровизации (основной объем принятия управленческих решений будет реализовываться в результате цифровых когнитивных технологий с привлечением комплексных АИС, ИИ, многопараметрического моделирования и фази-логики: т.е. в среде виртуальной реальности) принципиально выведет на ведущее место управление информационной безопасностью [1]. Естественно переход на цифровые технологии предъявляет высокие требования к надежности, бесперебойности, защищенности всех операций с информацией. Так, например, при полном переходе на безбумажный цифровой документооборот, малейший сбой может привести к остановке, параличу всего предприятия, отрасли, что повлечет за собой большие материальные, финансовые, репутационные потери и дискредитацию цифровых технологий в целом. Особенно важным становится обеспечение надежности цифровизации в банковской сфере, медицине, транспорте [5]. Аналитики перехода к цифровой экономике (см. например.[6]) подчеркивают необходимость перераспределения ресурсов между разработкой, внедрением и сопровождением (обеспечением непрерывности и защиты работы) процессов цифрового бизнеса. Цифровизация актуализирует процесс определения надежности источников информации и надежности данных. В этой связи существенно диверсифицируется роль доверия в управлении информационной безопасностью. С одной стороны изменяется /ограничивается/ круг доверительных связей, с другой – доверие на уровне творческих личностей должно быть глубоким, взаимный. Внешне это выглядит парадоксально:

кажется, что превращение «в цифру» значительно снижает субъективный человеческий фактор, обезличивает многие бизнес-процессы и должно приводить к снижению роли доверия между участниками проектной деятельности. Однако качество, надежность и результаты цифровизации сильнейшим образом зависят от качества входной информации, качества ресурсов, процессов и методологии преобразования этой информации.

Цифровизация усиливает процессы глобализации и при сохранении текущих тенденций рыночной экономики в мире будет приводить к дальнейшему увеличению расслоения общества на богатых и бедных.

В целом внедрение цифровизации – это не техническая проблема, а методологическая и социальная.

Цифровизация экономики в значительной степени переводит реальный мир человеческой деятельности в виртуальный. Человечество еще недостаточно сориентировалось в этом надвигающемся виртуальном мире, многие его стороны непонятны, неопределенны с точки зрения права, юриспруденции, выработки новых законов, регулирующих деятельность физических, юридических лиц, организаций, отраслей в цифровом виде. Непроработанность экономических, юридических полей в виртуальной составляющей нашего нового гибридного мира, приводит к нарушению целостности установившихся процессов реального мира, к возрастанию значимости информационной и социальной безопасности общества.

Литература:

1. Программа «Цифровая экономика. Россия 2024». АНО «Цифровая экономика». Информационная безопасность [Электронный ресурс]. – Режим доступа: https://data-economy.ru/security - (Дата обращения: 15.08.2018).
2. *Савельев С.В*. Возникновение мозга. М.: «Веди», 2010, с. 310.
3. *Бояринцев В.И.* Деградация человека [Электронный ресурс] – Режим доступа: https://public.wikireading.ru/117701 - (Дата обращения: 15.08.2018).
4. *Клименко Э.Ю., Неизвестный С.И.* Цикл статей «Рычаги стратегического управления портфелем проектов». Статья шестая. Положительная и отрицательная обратная связи. Управление проектами, № 1, 2012, с. 16-28.
5. *Kitaev A., Mironova I., Pogodaeva A., Sokolov D., Guseva E.* R ailway station 2 .0: a n ew p attern for th e d evelopment o f th e d igital r ailway. International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 2, p. 85-96.
6. *Kupriyanovsky V., Dunaev O., Fedorova N., Namiot D., Kupriyanovsky Yu.* On intelligent mobility in the digital economy. International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 2, p. 46-63.

Чилачава Т.И., Почхуа Г.Р.

О возможности разрешения конфликта посредством экономического сотрудничества

Аннотация: В работе рассматривается новая нелинейная математическая модель экономического сотрудничества между двумя политически взаимно противоборствующими сторонами (возможно страны или страна и её субъект), которая учитывает экономическое или другого типа сотрудничество между частями населений сторон, направленное на сближение сторон и мирное разрешение конфликта. В модели подразумевается, что процесс экономического сотрудничества свободен от политического давления, т.е. правительства сторон и третья внешняя сторона не вмешивается в этот процесс. Получена динамическая система, описывающая динамику частей населений сторон, ориентированных на сотрудничество. В модели также предполагается, что обе стороны имеют нулевой демографический фактор, т.е. сумма сторонников и противников сотрудничества неизменна. В случае постоянства коэффициентов модели найдены особые точки нелинейной системы дифференциальных уравнений. Изучен вопрос устойчивости решений. В случае некоторой зависимости между постоянными коэффициентами модели, найден первый интеграл и точное аналитическое решение. Полученное точное решение позволяет в пределах данной математической модели и зависимости между ее коэффициентами, определить условия при которых экономическое сотрудничество сможет мирно разрешить политический конфликт (большинство населений сторон желают разрешения конфликта).

Ключевые слова: математическая модель разрешения конфликта, динамическая система, устойчивость решений, точное решение

Как известно, математики Роберт Ауманн и Томас Шеллинг в 2005 году получили Нобелевскую премию по экономике за цикл научных работ „Понимание проблем конфликта и сотрудничества с помощью анализа в рамках теории игр“. Роберт Ауманн в своей лекции при получении премии 8 декабря 2005 года отметил, что: «Войны и другие конфликты являются одним из основных источников человеческих страданий. Так что, целесообразно посвятить эту лекцию одной из наиболее насущных и глубоких вопросов, стоящих перед человечеством: войны и мира», а Томас Шеллинг подчеркнул, что: «Самым захватывающим событием прошлой

половины века является то, которое не произошло. Мы наслаждались шестьюдесятью годами без ядерного оружия, взорванного в гневе».

Один из авторов сингапурского «экономического чуда» Ли Куан Ю уверен, что «Если Вам нужен экономический рост, то с соседями лучше не воевать, а торговать».

Как известно, в последние годы широкое распространение получило математическое моделирование в социальной сфере, в социологии, в демографии, в истории, в конфликтологии, в описании информационных войн, процессов ассимиляции народов, глобализации и т.д. [1,2].

Предлагаемая нами новая нелинейная математическая модель экономического сотрудничества между двумя противоборствующими сторонами имеет вид:

$$\begin{cases} \dfrac{dN_1(t)}{dt} = -\alpha_1(t)(a - N_1(t))(b - N_2(t)) + \beta_1(t)N_1(t)N_2(t) \\ \dfrac{dN_2(t)}{dt} = -\alpha_2(t)(a - N_1(t))(b - N_2(t)) + \beta_2(t)N_1(t)N_2(t) \end{cases} \quad (1)$$

$$N_1(0) = N_{10},\ N_2(0) = N_{20}, \quad (2)$$

где $N_1(t)$ - число граждан первой стороны в момент времени t, желающих или уже находящихся в экономическом сотрудничестве и склонных к последующему мирному разрешению конфликта,

$N_2(t)-$ число граждан второй стороны в момент времени t, желающих или уже находящихся в экономическом сотрудничестве и склонных к последующему мирному разрешению конфликта, $\alpha_1(t), \alpha_2(t)-$ коэффициенты агрессивности (отчуждения) сторон, $\beta_1(t), \beta_2(t)-$ коэффициенты сотрудничества сторон, $a, b-$ населения соответственно первой и второй сторон, которые в модели предполагаются неизменными (нулевой демографический фактор).

Мы предполагаем, что относительно слабыми и сильными условиями разрешения конфликта являются:

$$\begin{cases} \dfrac{a}{2} < N_1(t) \le a \\ \dfrac{b}{2} < N_2(t) \le b \end{cases} \qquad t \ge t_* \quad (3)$$

$$\begin{cases} \dfrac{2a}{3} \le N_1(t) \le a \\ \dfrac{2b}{3} \le N_2(t) \le b \end{cases} \qquad t \ge t_{**} \quad (4)$$

Рассмотрим случай постоянных коэффициентов модели

$$\alpha_1(t) = \alpha_1 = const > 0,\ \alpha_2(t) = \alpha_2 = const > 0,$$
$$\beta_1(t) = \beta_1 = const > 0,$$
$$\beta_2(t) = \beta_2 = const > 0, \tag{5}$$

Система нелинейных дифференциальных уравнений (1), в случае (5) имеет следующие стационарные (особые) точки:

$M_1(a;0)$, которая при выполнении неравенства $\alpha_1\beta_2 - \alpha_2\beta_1 > 0$ является неустойчивым узлом, а при выполнении противоположного неравенства $\alpha_1\beta_2 - \alpha_2\beta_1 < 0$ - гиперболическим седлом;

$M_2(0;b)$ - при выполнении неравенства $\alpha_1\beta_2 - \alpha_2\beta_1 < 0$ является неустойчивым узлом, а при выполнении противоположного неравенства $\alpha_2\beta_1 - \alpha_1\beta_2 < 0$ - гиперболическим седлом.

При выполнении равенства $\alpha_1\beta_2 - \alpha_2\beta_1 = 0$ в первой четверти фазовой плоскости решений мы получим кривую, каждая точка которой

$$M_3(q; \frac{\alpha_1 b(a-q)}{\beta_1 q + \alpha_1(a-q)}),\ 0 < q < a \tag{6}$$

является особой.

Предположим, что имеет место соотношение

$$\alpha_1\beta_2 - \alpha_2\beta_1 = 0, \quad \frac{\alpha_1}{\beta_1} = \frac{\alpha_2}{\beta_2} = p \tag{7}$$

Тогда система (1), с учетом (5), (6) перепишется в следующем виде

$$\begin{cases} \frac{dN_1(t)}{dt} = -\beta_1[p(a - N_1(t)(b - N_2(t)) - N_1(t)N_2(t)] \\ \frac{dN_2(t)}{dt} = -\beta_2[p(a - N_1(t))(b - N_2(t)) - N_1(t)N_2(t)] \end{cases} \tag{8}$$

Из (8), с учетом начальных условий (2), легко получить первый интеграл системы дифференциальных уравнений

$$N_2(t) = N_{20} + \frac{\beta_2}{\beta_1}(N_1(t) - N_{10}) \tag{9}$$

Далее, подставляя (9) в первое уравнение (1), для функции $N_1(t)$ получим следующее дифференциальное уравнение

$$\frac{dN_1(t)}{dt} = pa(-\beta_1 b + \beta_1 N_{20} - \beta_2 N_{10}) +$$
$$+ [\beta_1 pb + \beta_2 pa + \beta_1(1-p)N_{20} - (1-p)\beta_2 N_{10}]N_1(t) + \tag{10}$$
$$+ (1-p)\beta_2 N_1^2(t)$$

с начальным условием (2).

Рассмотрим некоторые частные случаи.

1. $p = 1$

Тогда решение задачи Коши (10), (2) имеет вид

$$N_1(t) = \frac{1}{\beta_1 b + \beta_2 a}[\beta_1(bN_{10} + aN_{20} - ab)\exp[(\beta_1 b + \beta_2 a)t] + \quad (11)$$

$$+ a(\beta_1(b - N_{20}) + \beta_2 N_{10})]$$

Анализ решения (11), показывает, что при

$$bN_{10} + aN_{20} < ab$$

$$\frac{dN_1(t)}{dt} < 0, \quad \frac{dN_2(t)}{dt} < 0,$$

при

$$bN_{10} + aN_{20} = ab$$

$$\frac{dN_1(t)}{dt} = 0, \quad \frac{dN_2(t)}{dt} = 0,$$

$$N_1(t) = N_{10}, \quad N_2(t) = N_{20}$$

при

$$bN_{10} + aN_{20} > ab$$

$$\frac{dN_1(t)}{dt} > 0, \quad \frac{dN_2(t)}{dt} > 0$$

$$N_1(t_*) = a, \quad t_* = \frac{1}{\beta_1 b + \beta_2 a}\ln\frac{a[\beta_1 N_{20} + \beta_2(a - N_{10})]}{\beta_1(bN_{10} + aN_{20} - ab)}$$

2. $p \neq 1$

$$\delta^2 = pa[\beta_2 N_{10} + (b - N_{20})\beta_1] \quad (12)$$

$$\varepsilon = \beta_1 pb + \beta_2 pa - \beta_1(p-1)N_{20} + (p-1)\beta_2 N_{10} \quad (13)$$

В первом случае

$$\varepsilon^2 = 4\delta^2(p-1)\beta_2, \quad (14)$$

что возможно только при $p > 1$, решение (10) имеет вид

$$N_1(t) = \frac{N_{10} + \frac{\varepsilon}{2}[N_{10} - \frac{\varepsilon}{2(p-1)\beta_2}]t}{[(p-1)\beta_2 N_{10} - \frac{\varepsilon}{2}]t + 1} \quad (15)$$

при этом, согласно (13), при $p > 1, \ \varepsilon > 0$

$$\lim_{t\to\infty} N_1(t) = \frac{\varepsilon}{2(p-1)\beta_2} \quad (16)$$

Во втором случае

$$\varepsilon^2 < 4\delta^2(p-1)\beta_2, \quad (17)$$

то возможно только при $p > 1$, решение (10) имеет вид

$$N_1(t) = \frac{\varepsilon}{2(p-1)\beta_2} + q\frac{N_{10} - \frac{\varepsilon}{2(p-1)\beta_2} - q\tan((p-1)q\beta_2 t)}{q + (N_{10} - \frac{\varepsilon}{2(p-1)\beta_2})\tan((p-1)q\beta_2 t)}$$

при этом, согласно (13), при $p > 1$, $\varepsilon > 0$.

В третьем случае

$$\varepsilon^2 > 4\delta^2(p-1)\beta_2 \tag{18}$$

$$N_{11} = \frac{\varepsilon}{2(p-1)\beta_2} - \frac{\sqrt{\varepsilon^2 - 4\delta^2(p-1)\beta_2}}{2|p-1|\beta_2} \tag{19}$$

$$N_{12} = \frac{\varepsilon}{2(p-1)\beta_2} + \frac{\sqrt{\varepsilon^2 - 4\delta^2(p-1)\beta_2}}{2|p-1|\beta_2}$$

$$N_1(t) = \frac{N_{12}(N_{10} - N_{11}) - N_{11}(N_{10} - N_{12})\exp\{t\frac{(1-p)}{|p-1|}\sqrt{\varepsilon^2 - 4\delta^2(p-1)\beta_2}\}}{N_{10} - N_{11} + (N_{12} - N_{10})\exp\{t\frac{(1-p)}{|p-1|}\sqrt{\varepsilon^2 - 4\delta^2(p-1)\beta_2}\}}$$

Если $p > 1$, тогда

$$N_1(t) = \frac{N_{12}(N_{10} - N_{11}) - N_{11}(N_{10} - N_{12})\exp\{-t\sqrt{\varepsilon^2 - 4\delta^2(p-1)\beta_2}\}}{N_{10} - N_{11} + (N_{12} - N_{10})\exp\{-t\sqrt{\varepsilon^2 - 4\delta^2(p-1)\beta_2}\}}$$

$$\lim_{t\to\infty} N_1(t) = \frac{\varepsilon + \sqrt{\varepsilon^2 - 4\delta^2(p-1)\beta_2}}{2(p-1)\beta_2} \tag{20}$$

Если же $p < 1$

$$N_1(t) = \frac{N_{12}(N_{10} - N_{11}) - N_{11}(N_{10} - N_{12})\exp\{t\sqrt{\varepsilon^2 - 4\delta^2(p-1)\beta_2}\}}{N_{10} - N_{11} + (N_{12} - N_{10})\exp\{t\sqrt{\varepsilon^2 - 4\delta^2(p-1)\beta_2}\}}$$

$$\lim_{t\to\infty} N_1(t) = \frac{\varepsilon + \sqrt{\varepsilon^2 + 4\delta^2(1-p)\beta_2}}{2(1-p)\beta_2} \tag{21}$$

Анализ полученного точного решения (11) – (21) позволяет в пределах данной математической модели и некоторых зависимостей между ее коэффициентами, определить условия при которых экономическое сотрудничество сможет мирно разрешить политический конфликт (большинство населений сторон желают разрешения конфликта).

Литература:
1. *Чилачава Т.И.*, *Дзидзигури Ц.Д.* Математическое моделирование. Тбилиси, 2008, 440 с.
2. *Chilachava T.* Mathematical Model of Economic Cooperation Between the Two Opposing Sides.. IX International Conference of the Georgian mathematical union, Book of Abstracts, Batumi - Tbilisi, 2018, pp. 96-97.

Касабов Г.А., Жеков В.И.

Экономическая дискуссия на тему "Закон рынков Сея"

Аннотация: В данной статье рассматриваются три слоя диалектики на основе ее материалистического понимания и трех ее уровней.

Ключевые слова: потребности, поиск, рынок, занятость, процент, деньги, кризис, экономика, продукты, полезность, труд, стоимость

В начале дискуссии припомним три слоя диалектики:

- Первый слой связан с объективной диалектикой процессов в рыночном хозяйстве;
- Второй слой относится к субъективной диалектике как продукту отражения рыночной объективной диалектики в научных знаниях рыночных процессов;
- Третий слой имеет прямое отношение к тому, что субъективная диалектика и диалектические законы как метод познания „не совпадают целиком с диалектическими законами развития познаваемых объектов" [1]. Этот слой ярче всего демонстрирует фальсификации и несоответствия теоретиков рыночного фундаментализма.

Анализ теории Сея и современных апологетов фундаментальной рыночной теории показывает, что эта теория занимает в некоторых экономических институтах почетное место. В то же время с непонятным воодушевлением и завидным рвением правящая элита Болгарии ориентирована именно на эту модель экономики – называемую рыночной, либеральной. Однако, здесь не учитывается степень риска, который возникает при рыночном фундаментализме в Болгарии.

Закон рынков Сея

«Трактат политической экономии» по словам самого Сея – это только «упрощенное, схематизированное и очищенное от ненужных абстракций» учение Смита. Но приводя в порядок «безграничный хаос верных идей» из

«Богатства народов», Сей в то же время добавил к ним и некоторые собственные теории, наиболее известной из которых является «Теория сбыта» или, как ее еще называют «Теория рынков».

Согласно этому закону Сея «*предложение порождает свой собственный спрос*» [2, С.21]. Эта дефиниция закона рынков цитируется во всех учебниках, хотя сам Сей «... никогда не использовал фразу «*предложение порождает свой собственный спрос*» при формулировании своего закона рынков**;** *эти слова*, – как заметил М. Блауг, – *изобретение Кейнса* и никогда до него не использовались (здесь и везде курсив мой – Г.К.)» [3, с.141-142]. К этому можно добавить, что в своей «Теории сбыта», в которой, как считают экономисты, формулируется этот *закон рынков*, Сей никогда не использовал не только фразу «предложение порождает свой собственный спрос», а даже и ключевые слова этой фразы – «спрос» и «предложение».

Но проблема не в том, что Кейнс при формулировании закона Сея употребил *свою* фразу, а в том, что эта фраза выражает определенную *мысль*, которой в «Трактате» Сея *нет*. Какой же *смысл* вложил Кейнс в свою фразу «предложение порождает свой собственный спрос»? На этот вопрос сам Кейнс отвечает так**:** «Предложение, – пишет он, – само порождает спрос в том *смысле*, что *совокупная цена спроса равна совокупной цене предложения* для всех уровней производства и занятости» [2, с.18].

Раз «совокупная цена спроса *равна* совокупной цене предложения», значит в рыночной экономике *каждый* продукт, который предлагается на рынке, «находит себе покупателя», т.е. *реализуется* на рынке. Таким образом, *смысл* фразы Кейнса «*предложение порождает свой собственный спрос*» состоит в том, что в рыночной экономике *каждый* произведенный продукт *реализуется* на рынке. Но такой *мысли* в «Трактате» Сея *нет*. Напротив, в своей «Теории сбыта» он акцентирует на том, что в рыночной экономике на некоторых рынках «большое количество товаров *не* находят себе покупателей», т.е. *не* реализуются на рынке. Именно в этом Сей видит проблему, решению которой он посветил 5 главу «Трактата» с заглавием «Теория сбыта».

Между прочим, Кейнс при формулировании *закона рынков* Сея, употреблял и эту фразу («*совокупная цена спроса равна совокупной цене предложения*»), которая до него никогда не использовалась, т.е. и эта фраза является изобретением Кейнса. Так, например, он пишет**:** «И так, *закон Сея* (*совокупная цена спроса на продукцию в целом равна совокупной цене предложения* для любого объема производства) равносилен предположению, что не существует препятствий к достижения полной занятости» [2, с.21].

В экономической литературе закон Сея представлен в *двух* вариантах**:** *тождество* Сея и *равенство* Сея. В обоих случаях экономисты пытаются доказать, что согласно закону Сея «предложение порождает свой собственный спрос».

Тождество Сея

В книге М. Блауга „Экономическая мысль в ретроспективе" имеется раздел с названием «Закон рынков Сея». В этом разделе есть только *одна* фраза из «Трактата» Сея, состоящая из *трех* слов**:** «*продукты уплачиваются за продукты*», а все остальное представляет свободное сочинение на тему**:** «Что означает утверждение «предложение создает свой собственный спрос?» – утверждение, которое, как отмечает и сам М. Блауг, не принадлежит Сею.

Именно эти три слова, по мнению М. Блауга, раскрывают сущность закона Сея. В своей книге он пишет**:** «*Продукты уплачиваются за продукты* во внутренней торговле так же, как и во внешней – вот *суть закона рынков Сея*. Столь простая мысль произвела фурор, не совсем утихший и по сей день. Утверждение о том, что «продукты уплачиваются за продукты» ни в коей мере не тривиально. В каком-то смысле это начало глубокого макроэкономического анализа" [3, с.136].

Выражение «продукты уплачиваются за продукты» является тривиальным для рыночной экономики *бартерного* типа, но *не* и для *денежной* экономики, а именно такую – *денежную* – экономику имеет в виду Сей, когда изрекает свою культовую фразу.

Все видят, что в *денежной* экономике *продукты* покупаются за *деньги*, а не за продукты, но Сей утверждает, что они покупаются за *продукты*, а не за деньги. В своем «Трактате» Сей отмечает**:** «Покупка всякого *продукта* не может совершиться иначе как на ценность другого *продукта* ... Деньги исполняют лишь временную роль в процессе обмена**;** как только состоялись сделки, всегда оказывается, что за *продукты* заплачено только *продуктами*» [4], а не деньгами.

В экономике *бартерного* типа каждый *продает* свой и *покупает* чужой продукт на одном и том же *месте* и в одно и то же *время*, а в *денежной* экономике эти два акта *отделены* друг от друга во времени и пространстве.

В *первом* случае, т.е. в *бартерной* экономике, никто не может продать свой товар, без того чтобы купить какой-то другой, т.е. «все *продавцы неизбежно являются покупателями*», а это, как принято считать, означает, что в *бартерной* экономике «предложение создает свой собственный спрос».

В экономической литературе, как и в учебниках экономической теории, часто подчеркивается, что «справедливость закона Сея не вызывает

сомнений в отношении экономики, основанной на натуральном обмене, когда продукты производства непосредственно обмениваются друг на друга» [5]. Никто не сомневается в том, что в рыночной экономике *бартерного* типа, в которой продукты покупаются за продукты, а не за деньги, все «*продавцы неизбежно являются покупателями*», а это, как уже отмечалось, для экономистов означает, что в *бартерной* экономике закон Сея действует.

Сомнения возникают во *втором* случае, когда рыночная экономика рассматривается в более сложной форме – как *денежная* экономика, в которой, как это видно всем, кроме Сея, продукты покупаются за *деньги*, а не за продукты.

В денежной экономике «никто, – как отмечает Маркс, – не может продать, без того, чтобы кто-нибудь другой не купил. Но никто не обязан немедленно покупать только потому, что сам что-то продал» [6]. Если кто-то продал, но не купил, или продал больше, чем купил, тогда кто-то другой не сможет продать, или не сможет продать все, что он произвел. Поэтому в *денежной* экономике утверждение «все *продавцы неизбежно являются покупателями*», а значит и Сам закон Сея, вызывает известные сомнения.

Эти сомнения, по мнению многих экономистов, рассеивает Сей. Для него *деньги* это только «... *повозки*, перевозящие ценность продуктов. *Все назначение* их в том, чтобы *перевезти* к вам ценность продуктов, которые покупатель продал, чтобы купить у вас ваши продукты» [4]. Деньги для Сея имеют только *одно предназначение – перевозить* ценность продуктов, но сами они ценности *не* имеют.

По мнению Сея, всякая вещь ценна не сама по себе, а только по отношению к *потреблению*. «Если люди признают за предметом определенную ценность, – пишет Сей, – то лишь в отношении его употребления**:** что ни на что не годится, тому и не дают никакой цены» [4]. Но деньги, по его мнению, не представляют никакой ценности по отношению к *потреблению*. «В самом деле, – спрашивает Сей, – зачем вам деньги? Не правда ли, затем, чтобы купить на них сырые материалы для вашей промышленности или съестные припасы для вас самих. Из этого вы сами видите, что *вам нужны не деньги*, *а продукты*» [4].

Но раз «вам нужны не деньги, а продукты», а деньги это только «*повозки*, перевозящие ценность продуктов» (или, как пишет Самуэльсон, «*смазочный материал*, облегчающий обмен» [7] ценностями, а *не* сама *ценность*), значит и в *денежной* экономике «продукты покупаются за *продукты*», а не за деньги**:** нельзя за то, что имеет какую-то ценность (т.е. за продукты) платить тем, что не имеет никакой ценности (т.е. деньгами). Таким образом, в рыночной экономике, независимо от формы, в которой она рассматривается – простой (как *бартерная* экономика) или более сложной (как *денежная* экономика) – «все *продавцы неизбежно являются*

покупателями», т.е. получается, что закон Сея действует и в *денежной* экономике.

Эта нетривиальная мысль Сея, состоящая из трех слов, буквально воспроизводится и другими ортодоксальными экономистами. Например Рикардо пишет**: «***Продукты* всегда покупаются за *продукты* или услуги**;** деньги служат только мерилом, при помощи которого совершается этот обмен. Какой-нибудь отдельный товар может быть произведен в излишнем количестве, и рынок будет до такой степени переполнен, что не будет даже возмещен капитал, затраченный на этот товар. Но это не может случиться одновременно со всеми товарами» [8]. Дж.Ст. Милль также отмечает**:** «То, что образует собою *средства платежа за товары*, – это сами *товары*. Средства каждого лица для оплаты продукции других состоят из тех товаров, которыми оно владеет. *Все продавцы неизбежно ... являются покупателями*» [9].

Как это видно, по мнению Д. Рикардо и Дж.Ст. Милля в *денежной* экономике «продукты покупаются за *продукты*», а не за деньги. Отсюда следует, что и в *денежной* экономике, как и в бартерной, «*все продавцы неизбежно являются покупателями*» и, следовательно, закон Сея действует.

В этом *грубом* варианте закон рынков Сея третируется как *тождество* Сея, поскольку то, что *предлагается* на рынке одним индивидом, является *спросом* другого индивида**:** предложение = спросу. Если «совокупная цена спроса *равна* совокупной цене предложения», то *тождество* Сея соблюдается.

Равенство Сея

В другом варианте закона Сея, известный как *равенство Сея*, спрос воспринимается как «поток доходов, который может *прерываться* или иметь *утечку*, так что какая-то часть произведенной продукции может оказаться *нереализованной*». При этих условиях совокупный спрос *не* поглащает *все* произведенные продукты, «совокупная цена спроса» *не равна* «совокупной цене предложения» и тождество Сея *не* выполняется.

Но такая ситуация, как утверждают ортодоксальные экономисты, вызывает реакцию на денежном рынке, в результате которой «всякий индивидуальный акт воздержания от потребления равнозначен тому, что труд и материальные средства, высвобождаемые из сферы потребления, направляются на производство капитальных благ» и равновесие, таким образом восстанавливается.

В экономике частного сектора, состоящая только из двух секторов – домохозяйства и фирмы – *совокупный* спрос включает в себя спрос на *потребительские* блага и на *инвестиционные* блага. Когда домохозяйства сберегают *больше*, чем это необходимо фирмам для инвестиций, т.е. когда

появляются *излишние* сбережения, спрос на *потребительские* блага *уменьшается*, но на *инвестиционные* блага – *увеличивается* (увеличение в *сбережениях* домохозяйств в классической денежной теории означает увеличение *денежного предложения*, а это *уменьшает* равновесный *процент*, в результате чего спрос на инвестиционные блага повышается), так что величина *совокупного* спроса *сохраняется*, но структура его меняется, а вместе с тем меняется и структура национального продукта. Выходит, что в рыночной экономике «сам процесс производства создает *эффективный* спрос, необходимый для того, чтобы поглотить *всю* выпущенную продукцию» [10], т.е. в конечном счете закон Сея действует и в этом случае, но *не* как *тождество*, а как *равенство*, допускающее временное *расхождение* между совокупным спросом и предложением.

В этом варианте закона Сея экономика может *временно* отклоняться от своего потенциала и когда это происходит, *естественные силы рынка* восстанавливают нарушенное равновесие**:** экономика возвращается к своему потенциалу, приобретая *новую* структуру при *прежнем* уровне цен.

В классической, как и в кейнсианской, теории в экономике частного сектора единственным условием *реализации* национального продукта является *равенство* между *сбережениями* домохозяйств и *инвестициями* фирм (S = I). Кейнс не отрицает, что при S = I экономика оказывается в равновесие, а просто считает, что установление этого равенства является *случайностью*, а не нормой.

При полной занятости ресурсов домохозяйства могут увеличить свои сбережения что изменит только *структуру* совокупного спроса, а значит и национального продукта, но не и их *величины*. Национальный продукт с *новой* структурой будет тоже *реализован* на рынке, поскольку при увеличении сбережений домохозяйств *нарушенное* равенство между сбережениями и инвестициями *восстанавливается* благодаря изменениям, происходящим на денежном рынке.

Таким образом, выходит что *реализация* национального продукта при полной занятости ресурсов осуществляется не при строго определенной его *структуре*, а при строго определенном соотношении между S и I. Если это соотношение равно 1 ($S/I=1$), то национальный продукт будет *реализован* на рынке при любой его структуре**.** В противном случае, когда $S/I>1$, какая-то часть национального продукта не поглощается совокупным спросом, т.е. не реализуется на рынке и возникает *безработица*, а когда $S/I<1$, появляется *инфляция*.

Неудивительно, что при таком подходе представляется возможным *повышение уровня национального производства* и занятости *без увеличения производства* материальных благ. Так, например, во время Великой депрессии Кейнс писал**:** «Если бы казначейство наполняло старые бутылки банкнотами, закапывало их на соответствующей глубине в

бездействующих угольных шахтах, заполняло эти шахты доверху городским мусором, а затем, наконец, предоставляло бы частной инициативе ... выкапывать эти банкноты из земли, то безработица могла бы полностью исчезнуть» [2, С.108]. К этой – шокирующей – мысли он добавил**:** «Разумеется, более целесообразно было бы строить жилые дома и т. п., но если этому препятствуют политические и практические трудности, то и предлагаемый вариант лучше». Из этих слов становится ясно, что существуют *различные* варианты повышения уровня национального производства и занятости – «строительство жилых домов» или создание каких-то *других* материальных благ, а в крайнем случае можно вообще не создавать никакие дополнительные блага и ликвидировать безработицу, если для безработных создать стимулы для выкапывания банкнот, которые казначейство закопало в бездействующих угольных шахтах, заполняя их доверху мусором. Таким образом, выходит, что национальный продукт, создаваемой при *полной* занятости ресурсов, может быть *реализован* при *любой структуре* этого продукта. Цитируемое выше высказывание Кейнса является красноречивой иллюстрацией этого утверждения.

Вообще, в экономике проблема реализации возникает только в связи с актом воздержания населения от потребления. Если, например, допустить, что население не воздерживается от потребления и *весь* свой доход тратит за потребление, то доход населения не будет *прерываться* и не будет никакой *утечки* из него. При этих условиях совокупный спрос будет *равен* совокупному предложению и никакой проблемы реализации не возникнет. Но это не так. Например, в схемах простого воспроизводства Кене и Маркса население не воздерживается от потребления, расходует на потребление *весь* свой доход и никакой утечки из этого дохода нет, но не смотря на это, как показывают эти схемы, *реализация* национального продукта *осуществляется* только при установлении в экономике строго определенных количественных соотношений между разнородными по натуральной форме благами, т.е. *реализация* национального продукта осуществляется только при *строго определенной структуре* этого продукта.

При полной занятости ресурсов может *производиться* национальный продукт с *различной* структурой, но *воспроизводится* только *один* из них, который *реализуется* на рынке. В этом состоит экономический смысл понятия „*воспроизводство*“, которое Ф. Кене *ввел* в экономическую науку**.** *Воспроизводство и реализация* национального продукта осуществляется только при *строго определенной структуре* этого продукта. Именно эта идея (которая по словам Маркса «....была в высшей степени гениальной, бесспорно, самой гениальной из всех какие только выдвинула до сего

времени политическая экономия» [12]) содержится в „Экономический таблице" Ф. Кенэ.

Конечно, когда национальный продукт *реализуется* на рынке, $S = I$, но отсюда не следует обратный вывод**:** если $S = I$, то национальный продукт будет *реализован* на рынке. При *реализации* национального продукта, устанавливается *равенство* между *рыночной* ценой каждого продукта и его *естественной* ценой (между *ценой* продукта и его *стоимостью*, если использовать терминологию Маркса), а также и *равенство* между *сбережениями* и *инвестициями*. Например, национальный продукт, который отражен в схеме простого воспроизводства Маркса, *реализуется* на рынке. В этой схеме рыночная цена каждого продукта *равна* его естественной цене, а сбережения домохозяйств *равны* инвестициям фирм (при *нулевых* сбережениях населения чистые инвестиции фирм тоже равны *нулю*). Но это не означает, что, если все продукты будут продаваться по их *естественным ценам*, то национальный продукт будет *реализован*. Точно такой – *обратный* – вывод, как известно, сделал Прудон в своей теории о „конституированной" стоимости. По этому поводу Маркс писал**:** „Вместо того чтобы говорить, как все люди**:** в хорошую погоду можно встретить много гуляющих, г-н Прудон отправляет своих людей гулять, чтобы обеспечить им хорошую погоду."[13].

Прудон *перевернул* причинно-следственную связь. Тоже самое делается в классической и кейнсианской теориях, когда утверждается, что, если $S = I$, то национальный продукт будет *реализован* на рынке при любой его структуре. Когда *реализация* национального продукта осуществляется *независимо* от его структуры, как это утверждается в указанных выше теориях, понятие „воспроизводство" *обессмысливается* и поэтому оно *исчезло* из словаря экономической науки.

Полезность и ценность в учении Сея

Учение Сея о *ценности* благ, созданное им в том же «Трактате», лежит в основе его «Теории рынков». Поэтому следует уточнить что же представляет *ценность* продукта в учении Сея?

«Способность известных предметов удовлетворять разным потребностям человека, – пишет Сей, – я позволю себе назвать полезностью (потребительной стоимостью)» [4]. Производство, пишет Сей, « ... есть создание, но не материи, а *полезности* ... Вот в каком смысле надо понимать слово производство и в каком оно будет употребляться в этом сочинение. Производство не создает материи, но создает *полезность*» [4]. Но если в рыночной экономике «производство создает полезность» и именно в этом смысле «надо понимать слово производство», то откуда же берется *ценность* продукта и есть ли вообще какое-то различие между

полезностью продукта (потребительной стоимостью) и его *ценностью* (стоимостью)?

«Производство создает полезность», но, так как «эта *полезность*, – как отмечает Сей, – *сообщает предметам ценность*» [4], значит все то, что создается в сфере производства, представляет какую-то *ценность*. Но ценность это богатство. Именно поэтому Сей обобщает свою теорию *ценности* следующим образом**:** «Я, – пишет Сей, – скажу так**:** производить предметы, имеющие какую-нибудь *полезность*, значит производить *богатство*, так как *полезность* предметов составляет первое основание их *ценности*, а ценность есть богатство» [4].

В учении Сея о *ценности* все то что имеет *полезность*, представляет какую-то *ценность*, т.е. *нет* никакого *различия* между *полезностью* продукта и его *ценностью*. Но это означает, что в его «Теории рынков» *каждый* произведенный *продукт* представляет какую-то *ценность*, поскольку продуктов, не имеющих *полезности* не бывает.

Никто не выносит на рынок вещи, *не имеющие* полезного приложения, т.е. вещей, не имеющих *полезности* на рынках нет. Но раз «эта *полезность* сообщает предметам *ценность*», значит на рынке нет и ничего другого, кроме различных *ценностей*. Поэтому у Сея возникает вопрос**:** почему на рынке какой-то отрасли, на котором предлагаются *абсолютно одинаковые* ценности, имеющие *одну и ту же полезность*, одни ценности покупаются, а другие *такие же* ценности не находят для себя покупателей, т.е. не покупаются. Именно решению этой проблемы, как уже отмечалось, и посвящена «Теория сбыта» Сея.

Такая проблема, например, никогда не возникает в экономической теории Маркса, потому что согласно его учению в рыночной экономике каждая *ценная* вещь имеет какую-то *полезность*, но не каждая *полезность* является *ценной* вещью. Это предполагает, что *не все* продукты, которые предлагаются на рынке, имеют *ценность* и поэтому в теории Маркса не может возникнуть такой вопрос**:** « Откуда берется такое большое количество товаров, которые *не покупаются* одни за другие?». Ясно, что в учении Маркса потребители покупают те продукты, которые имеют ценность, и отказываются покупать другие продукты, которые ценности не имеют. Неясно другое, а именно**:** почему потребители покупают *одни* продукты и отказываются покупать *другие* в том случае, когда *все* продукты, которые предлагаются на рынке, представляют какие-то *ценности* – как это в учении Сея. Именно это и объясняет Сей в своей «Теории рынка».

Продукт труда *всегда* имеет какую-то *полезность*, т.е. способность обслуживать какую-то человеческую потребность, независимо от того кем он создается – первобытным человеком, крепостным крестьянином, рабом или наемным работником, т.е. *полезность* продукта является вечным и

естественным свойством продукта. Но *ценность* продукта – это такое свойство, которое возникает и существует только в рамках *рыночного* хозяйства. Свойство *ценности* возникает только тогда, когда *частные* производители создают продукты, предназначенные для обслуживания *общественной* потребности, т.е. потребности *других*, неизвестных им потребителей, а не потребности самих производителей. Ценность, следовательно, является *скрытом* моментом производства («на лбу стоимости не написано что это такое» [14]), потому что в самом процессе *производства* не возможно установить имеет ли продукт, созданный *частным* производителем, способность обслуживать *общественную* потребность, т.е. потребность других, *неизвестных* ему потребителей. Это можно выявить только *после* процесса производства, когда продукт выносится из процесса производства на рынок для его участия в обмене на другие продукты.

Если продукт, который появился на рынке, *принят* в обмен на какой-то другой продукт, значит *частный* производитель этого продукта *еще в процессе производства* создал продукт, способный обслуживать определенную *общественную* потребность, т.е. создал *ценность*. Таким образом, этот продукт, который принят в обмен на другой продукт, *имеет* не только *полезность*, но и *ценность*, которая *создалась* еще в процессе производства, но *проявилась* после этого процесса – на рынке, в процессе обмена. Поэтому *разменная стоимость* является *формой проявления* ценности продукта, а *не* самой *ценностью* этого продукта.

Если же продукт *частного* производителя *не* принимается в обмен на другие продукты, значит он *не* способен обслуживать *общественную* потребность в этом продукте и, следовательно, *не* имеет никакой *ценности*, даже если в его производстве было израсходовано огромное количество ресурсов. Этот продукт, который не принят в обмен на какой-то другой продукт, *имеет полезность*, поскольку он способен обслуживать определенную человеческую *потребность*, но *не имеет* никакой *ценности*, так как он не способен обслуживать *общественную* потребность в этом продукте.

«Теория сбыта» в «Трактате» Сея

Сей, как это уже отмечалось, считал, что в *денежной* экономике *продукты* покупаются не за деньги, а за *продукты*. Поэтому создавая *данный продукт*, его производитель тем самым создает *средство для оплаты других продуктов* – продуктов, создающих другими производителями, имеющие ценности, различные от ценности данного продукта. Отсюда следует, что «один только факт производства товара в тот самый момент, как он произведен, открывает сбыт для *других* товаров» [4]. Другими словами, предложение каждого товара, который выносится на

рынок, создает спрос на *другие* товары, а *не* собственный спрос. Но в экономической литературе, как уже отмечалось, утвердилось мнение о том, что «согласно закону Сея каждое предложение создает свой *собственный* спрос» [10].

«Предприниматели в разных отраслях промышленности, – пишет Сей, – говорят обыкновенно, что не трудно произвести, а трудно продать, что можно всегда произвести достаточное количество товаров, если легко найти им верный сбыт» [4]. В этом *первом* изречении Сея из его «Теории сбыта» уже сформулирована проблема этой теории**:** «*не трудно произвести, а трудно продать*». Затем эта проблема выражается в более конкретной форме**:** «... Откуда берется такое *большое количество товаров*, которые иногда загромождают обращение, потому что *не находят себе покупателей*? Почему же эти товары *не покупаются* одни за другие?» [4]. На этот вопрос, как пишет Сей, обычно отвечают так**:** «*Нельзя продать*, потому что *денег мало*. Но здесь, – отмечает Сей, – следствие принимается за причину. Нельзя, следовательно говорить**:** нельзя продать, потому что *мало денег*, а надо сказать так**:** нельзя продать, потому что *мало других продуктов*» [4].

Если какой-то продукт *не продается*, значит *средств для оплаты* этого продукта *мало*. Но *средством оплаты* каждого продукта, как считает Сей, являются *не деньги,* а *другие продукты* – продукты *других* производителей, производящие *другие* ценности. Поэтому «нельзя говорить**:** нельзя продать, потому что мало денег, а надо сказать так**:** *нельзя продать, потому что мало других продуктов*»

«Денег, – подчеркивает Сей, – *всегда довольно*, чтобы служить обращению и взаимному обмену других ценностей, если только эти ценности действительно существуют ... Когда какого-нибудь товара очень много и он не находит себе покупателей, то *причина* этого вовсе *не в том*, *что недостаток денег останавливает продажу*» [4]. Но если *не* «недостаток денег», то что же тогда в теории Сея «останавливает продажу» товаров? Почему же на некоторых рынках «большое количество товаров не находит себе покупателей»?

На этот жгучий для Сей вопрос в «Теории сбыта» есть «прямой и лаконичный ответ**:** «Известных продуктов *слишком много*, потому что *недостает других*. Выражаясь проще, многие *меньше купили*, потому что сами меньше выработали» [4]. Таким образом, известного продукта «слишком много» не потому, что *производители* предложили его в «*большем* количестве, чем он требуется» потребителям (как это у Смита и Рикардо), а потому, что *потребители* его «*меньше* купили», чем надо. Иначе говоря, в теории Сея *несоответствие* между производством и потреблением выражается в том, что *потребление* не соответствует *производству*, а не наоборот – как это в учении Смита и Рикардо.

Сей, в отличии от некоторых современных экономистов, видит, что в рыночной экономике на некоторых рынках иногда появляется «*большое количество товаров*, которые *не находят себе покупателей*». Но что можно сказать о спросе и предложении тех товаров, которые «не находят себе покупателей»? Каждому, в том числе и Сею, ясно что если какие-то товары «не покупаются», значит нет спроса на эти товары и их предложение, следовательно, *не* создало свой *собственный* спрос. Но как тогда понимать утвердившееся в экономической литературе мнение о том, что «согласно закону Сея *каждое* предложение создает свой *собственный* спрос»?! Достаточно только поставить такой вопрос и сразу же становится ясно почему «изобретение» Кейнса («предложение порождает свой собственный спрос») не встречается *ни в одной* работе ортодоксальных экономистов, а только в учебниках экономики.

И так, мы приходим к выводу о том, что никакого «закона рынков Сея» в «Трактате» Сея нет, а то что принято считать законом Сея, является, как точно выразился М. Блауг, «изобретением Кейнса». Конечно «Теория рынков» – это новая, созданная Сеем теория. Но эта теория Сея (как и другие его теории) не дополняет и не развивает, а искажает учение Сея.

Центральное место в «Теории рынков» занимает *мысль* Сея о том, что «*продукты покупаются за продукты*». Если эту мысль убрать из «Теории рынков», то не будет и самой этой теории. Можно только удивляться тому, что эта грубая и примитивная мысль Сея, которую он выразил в 1803 году, продолжает впечатлять современных экономистов и воспринимается ими как «начало глубокого макроэкономического анализа».

Литература:

1. *Косичев А.Д.* „Философские проблемы „Капитала" К.Маркса" Изд. МГУ,1968 г.
2. *Кейнс, Дж.* Общая теория занятости, процента и денег. Петроком,1993 г., с.21.
3. *Блауг М.* Экономическая мыслъ в ретроспективе. Академия народного хозяйства. Москва, Дело ЛТД, 1994.
4. Сей Ж-Б. Трактат по политической экономии. 5глава. Теория сбыта URL: http://ek-lit.narod.ru/saysod.htm (Дата обращения: 01.11.2018)
5. *Пезенти А.* Очерки политической экономии капитализма. Издательство "Прогресс", 1976, с. 586 – 587.
6. *Маркс К. и Энгельс Ф.,* Соч., 2изд., т.23, с.124.
7. *Самуэльсон П., Нордхаус В.* Экономика. Издание пятнадцатое. Москва 1997, с.72.
8. *Рикардо Д.* Соч. Т. 1, с.240.

9. *Милль Дж.Ст*. Принципы политической экономии. Цитируется по Кейнсу, Общая теория занятости, процента и денег. Петроком,1993г., с.16.
10. *Селигмен Б.* Основные течения современной экономической мысли. Издательство Прогресс, Москва, 1968г., с. 497
11. *Кейнс Дж.* Общая теория занятости, процента и денег. Петроком,1993г., с.108.
12. *Маркс К.* Теории за принаденатa стойност, т.1, М., 1931г., с.73
13. *Маркс К и Энгельс Ф*. Соч.т.4, с.95
14. *Маркс К.* Капиталът т.1, Партиздат, София, 1988г, с, 94.

Горелова Г.В., Саак А.А.

Имитационное моделирование социальной безопасности молодежи

Аннотация: Актуальной проблемой развития современной России является обеспечение социальной безопасности молодежи, как стратегического ресурса общества. В работе проанализированы факторы, определяющие состояние социальной безопасности молодежи, и государственная молодежная политика. Поставлены вопросы определения ее влияния на будущее социальной безопасности молодежи. Предложено использовать имитационное когнитивное моделирование для исследования проблем социальной безопасности. Приведен пример когнитивного имитационного моделирования.

Ключевые слова: молодежь, социальная безопасность, имитационное моделирование, когнитивный подход

Состояние социальной безопасности молодежи в обществе находится в прямой зависимости от качества и уровня жизни населения и не может быть обеспечено только действиями властных институтов. Она требует благоприятных социально-экономических условий. В современной России, в условиях смены собственности, перехода к рынку, трансформации ценностных ориентиров молодежи еще не выработана эффективная социальная политика, как в отношении всего населения, так и в отношении динамичной его части – молодежи [8]. Существуют угрозы безопасности для разных социальных слоев молодежи вследствие возникновения и развития резких качественных изменений в образе жизни. Ущемляются жизненно важные социальные права и интересы личности: права на труд, профессию, гарантированную заработную плату, на бесплатное

образование, здравоохранение, отдых. Социальная государственная политика должна регулировать отношения между обществом и личностью в целом.

Для анализа социальной безопасности молодежи и оценки результативности социальной государственной политики предлагается использовать когнитивное моделирование сложных систем [1,2+], которое позволит имитировать структуру и поведение системы «Социальная безопасность молодежи».

Поскольку социальная безопасность молодежи зависит от качества жизни, воспользуемся данными работы [7, с.100] - рис.1, в которой был представлен ряд результатов когнитивного анализа качества жизни молодежи, и дополним его данными по безопасности молодежи.

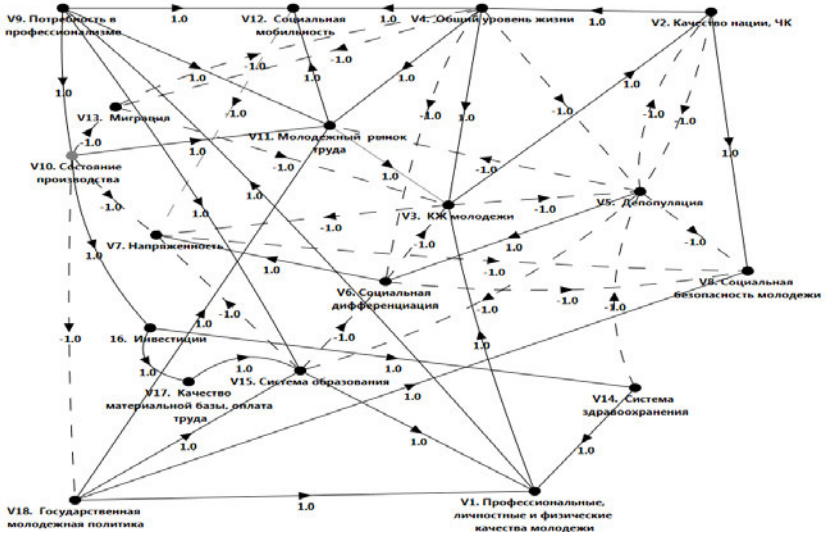


Рис. 1 – Когнитивная карта *G*1 «Качество жизни молодежи»

Социальная безопасность молодежи помимо зависимости от качества жизни определяется еще другими базовыми факторами, такими, как: уровень жизни молодежи, образ жизни молодежи, правовое обеспечение безопасности молодежи, система общественной безопасности, борьбы с правонарушениями и преступностью; система социальной защиты населения, страхования, пенсионного обеспечения; политическая обстановка. От безопасности молодежи зависит национальная безопасность страны [4]. В соответствии с названными факторами разработана когнитивная карта *G*2 (рис. 2).

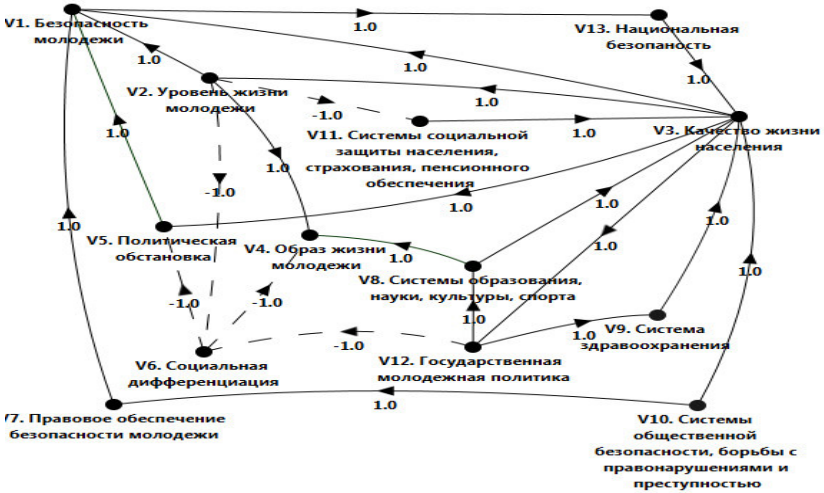


Рис. 2 – Когнитивная карта *G*2 «Социальная безопасность молодежи»

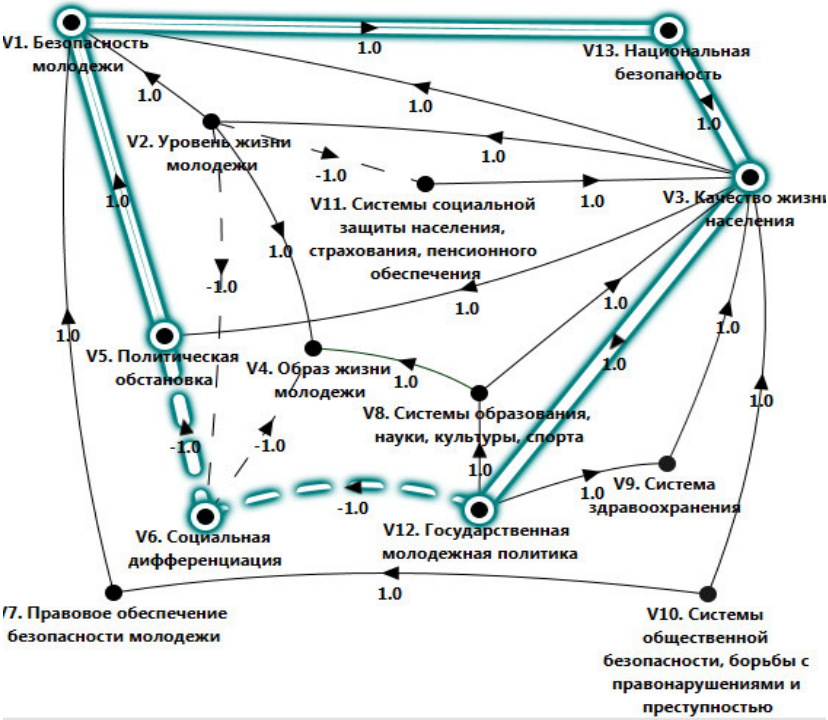
Композиция *G*2 с когнитивной картой *G*1 представляет собой возможную структуру сложной системы «Безопасность молодежи» (не изображена здесь из-за громоздкости). Возможно провести когнитивный анализ «блоков» *G*1 и *G*2 в отдельности. Рисунки 3-6 иллюстрируют некоторые результаты такого анализа на модели *G*2.

Для обоснования управленческих решений, которые могут быть приняты после когнитивного моделирования, важно проанализировать устойчивость модели, ее пути и циклы, провести сценарное моделирование [1,2,3].

Для проведения такого анализа была использована специальная программная система когнитивного моделирования сложных систем [5].

Анализ циклов и структурной устойчивости когнитивной модели. На рис. 3 изображен один из циклов модели *G*2 и обозначены другие циклы. Всего в модели 8 циклов, из них – один отрицательный (стабилизирующий). Поскольку отрицательных циклов – нечетное число, то модель является структурно устойчивой [1].

На когнитивной модели было проведено сценарное моделирование [1,3,4] путем внесении возмущений (импульсов) в отдельные вершины и в совокупности вершин. На рис. 4 изображены часть графиков импульсных процессов, соответствующих сценарию №1, в предположении успешного действия Государственной молодежной политики, и сценарию №2, в предположении роста социальной дифференциации и противодействующей ей государственной молодежной политики и системы социальной защиты населения.



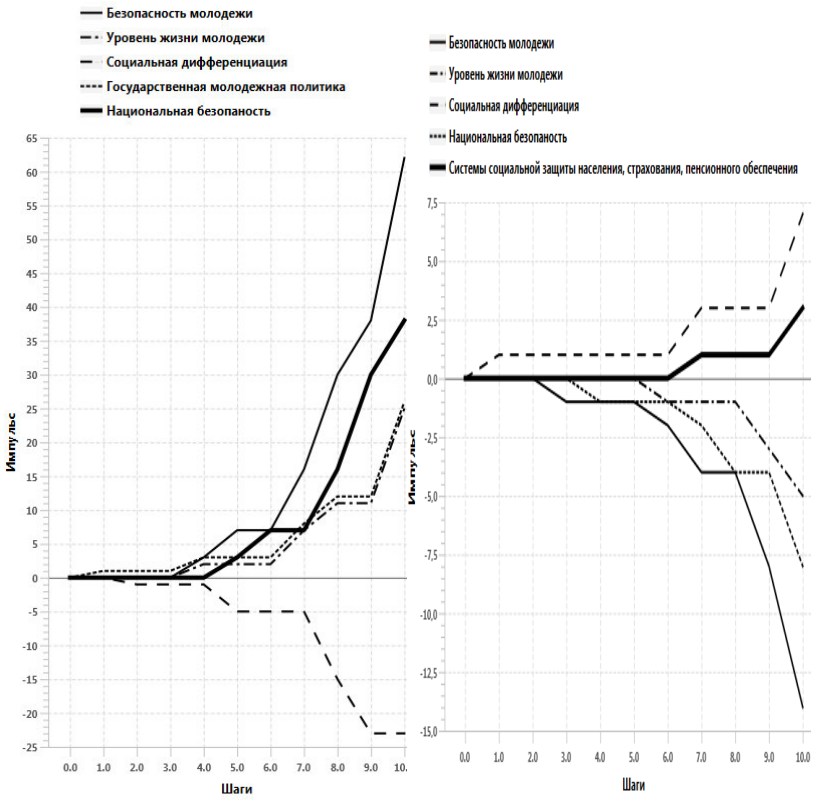
Циклы. Всего: 8. Отрицательных: 1. Положительных: 7.

+ (4.0) V1 -> V13 -> V3 -> V2 -> V1
+ (2.0) V1 -> V13 -> V3 -> V2 -> V6 -> V5 -> V1
+ (3.0) V1 -> V13 -> V3 -> V1
+ (2.0) V1 -> V13 -> V3 -> V12 -> V6 -> V5 -> V1
+ (4.0) V1 -> V13 -> V3 -> V5 -> V1
- (1.0) V2 -> V11 -> V3 -> V2
+ (3.0) V3 -> V12 -> V8 -> V3

Рис.3 – Анализ циклов и структурной устойчивости модели *G*2

Как видно из рис. 4 для сценария №1 характерны положительные тенденции развития ситуаций в системе, Государственную молодежную политику можно считать успешной. Для сценария №2 тенденции развития ситуаций неблагоприятны. Растущей социальной дифференциация не могут противостоять только существующие система социальной защиты и государственная молодежная политика.

На рис. 4 изображены процессы 10 шагов моделирования. Увеличение количества шагов, как показал вычислительный эксперимент, не показывает изменений тенденций развития ситуаций.



Сценарий №1 *Сценарий №2*

Рис. 4. – Графики импульсных процессов в предположении успешности Государственной молодежной политики

Заключение. В рамках данного исследования мы следовали принципу композиции когнитивных моделей, отображающих разные аспекты изучаемой проблемы, через вершины, общие разным моделям. Такая декомпозиция слабоструктурированной проблемы облегчает изучение сложной системы.

Возможности имитационного когнитивного моделирования социальной безопасности молодежи позволяют разрабатывать различные сценарии развития ситуаций на когнитивных картах, которые дают основание для оценки и рекомендации желаемых стратегий развития этой системы.

Литература:
1. *Горелова Г.В.* Когнитивный подход к исследованию занятости молодежи на рынке труда / Г.В.Горелова, Каурова О.В., Саак А.А., В.А. Вишнякова //Социальная политика и социология. – 2017. –Том 16, №1(120). – С. 18-27.
2. Инновационное развитие социо-экономических систем на основе методологий предвидения и когнитивного моделирования. Коллективная монография / Под ред. Г.В.Гореловой, Панкратовой Н.Д. - Киев: Изд-во «Наукова Думка», 2015.- 464 с.
3. *Кульба В.В.* Сценарный анализ динамики поведения социально-экономических систем (Научное издание) / В.В. Кульба, Д.А. Кононов, С.С. Ковалевский, С.А. Косяченко, Р.М. Нижегородцев, И.В. Чернов. – М.:ИПУ РАН, 2002. – 122с.
4. Общая теория национальной безопасности / Под общ. ред. А. А. Прохожева. М.: Изд-во РАГС, 2005. 344 с.
5. Программа для когнитивного моделирования и анализа социально-экономических систем регионального уровня. Свидетельство о государственной регистрации программ для ЭВМ № 2018661506 от 07.09.2018.
6. *Саак А.А.* Причинный анализ и когнитивное моделирование качества жизни молодежи / А.А. Саак // Вестник адыгейского государственного университета. Серия «Экономика». – 2018, Вып.1 (215). – С.96-108.
7. *Саак А.А.* Исследование взаимосвязи качества жизни молодежи с социально-экономической средой / А.А. Саак // Проблемы экономики и юридической практики. - 2018, №1. – С. 57-60.
8. *Фомченкова Г.А.* Институализация безопасности молодежи в условиях трансформации российского общества: дисс. докт. соц. наук/ Г.А. Фомченкова. – Санкт-Петербург, 2014. -407.

Косачев Ю.В.

Стратегия эффективной деятельности интегрированной структуры, участвующей в экономическом развитии региона

Аннотация: Рассматривается возможность организации эффективной экономической деятельности региональной интегрированной структуры. С использованием математического моделирования показано, что реализация компромиссного решения способствует развитию и региона и интегрированной структуры, и, как следствие, повышению их экономической безопасности.

Ключевые слова: интегрированная финансово-промышленная структура, экономическая безопасность, экономическая эффективность, региональная структура, инвестирование, налоги на прибыль

Вертикально интегрированные финансово-промышленные структуры (ФПС) обладают возможностью получения дополнительного прироста своей эффективности не только за счет увеличения затрат, но и за счет “правильной” организации взаимодействия предприятий, интегрированных внутри структуры. Это является одной из глубинных причин стремления к интеграции различных фирм, предприятий и организаций. В работе [1] с использованием математического моделирования показано, что при выполнении определенных условий появляется возможность разработки оптимальной инвестиционной программы. К наиболее важным условиям относятся: *во-первых*, необходимость учета длительных мотиваций участников-инвесторов, для чего требуется рассмотрение инвестиционного процесса как нестационарного, *во-вторых*, обеспечение независимости финансово-экономической деятельности участников структуры – предприятий, банков и других при выборе объемов выпуска, кредитов, цен, и т.д. Реализация оптимальной инвестиционной программы обеспечивает участникам получение максимальных гарантированных дисконтированных доходов на всем планируемом интервале [2].

Несколько иначе дело обстоит с региональными интегрированными структурами (РФПС), расположенными на территории региона. В работе [3] обсуждаются вопросы взаимодействия РФПС с руководством региона, отмечается актуальность этого процесса для обеих сторон. Очевидно, что к оптимальным в этом случае (выгодным как корпорациям, так и региону) можно отнести лишь согласованные компромиссные решения. В качестве такого решения в данной работе предлагается введение балансирующей льготной ставки платежей по региональному налогу на прибыль корпорации. Следует отметить, что наиболее чувствительно этот вопрос задевает интересы финансовой организации – банка в составе РФПС. В соответствии с существующим законодательством регионам предоставляется право установления территориальных ставок налога на прибыль с учетом своих местных задач и условий. При этом, чрезмерная ставка подрывает стимулы к росту производства; с уменьшением ставки, наоборот, растет прибыль хозяйствующих субъектов, но падает доход регионального бюджета.

В этом контексте предоставление льгот по ставкам налога на прибыль банка может стать стимулирующей мерой по обеспечению

заинтересованности вхождения банка в состав РФПС и организации ее эффективной деятельности. Основной вопрос заключается в обосновании такой балансирующей льготной ставки платежей по налогу на прибыль банка, при которой региональный бюджет не потеряет много доходов, а банку будет выгодно кредитовать производственный сектор.

Пусть *А* – производственное предприятие, *Б* – банк, *В* – сбытовое предприятие в составе структуры, $[t_0,T]$ – планируемый временной интервал их деятельности.

Введем следующие обозначения:

θ_0^A - ставка платежей в региональный бюджет по налогу на прибыль предприятия *А*; $\theta_0^Б$ - ставка платежей по налогу на прибыль банка *Б*; θ_0^B - ставка платежей по налогу на прибыль *В*, вертикально связанного с производителем *А*.

Прибыль предприятий *А*, *В* и *Б* в момент $t \in [t_0,T]$ от торговли с потребителем *В* после расчетов по кредитам составит величину:

$$\begin{aligned}
&\tilde{\pi}^A(t) = (1-\theta_0^A)[\xi\, g(x(t)) - \tau K(t)] - K(t);\\
&\tilde{\pi}^B(t) = (1-\theta_0^B)\,\Delta\pi^B(t) - \alpha_0 \Delta\pi^B(t), \qquad (1)\\
&\tilde{\pi}^Б = (1-\theta_0^Б)[(1-\xi)(\alpha_0+\omega)\, g(x(t)) + \tau K(t)],
\end{aligned}$$

где $\Delta\pi^B(t) = (1-\xi) g(x(t))$; ξ - трансфертная цена (ниже рыночной) продажи продукции *А* предприятию *В*; τ - внутрикорпоративная банковская процентная ставка по кредиту $K(t)$, которая ниже рыночной; $g(x(t))$ - функция дохода производителя *А* от торговли на рынке продукта по рыночной цене p_0:

$$g(x(t)) = \beta \left(\frac{p_0}{1+\beta}\right)^{\frac{1+\beta}{\beta}} \cdot [\varphi(x(t))]^{-\frac{1}{\beta}} - P; \qquad (2)$$

α_0, ω - доли акций *В*, которыми обладает банк в момент *t*; α_0, β - const.

$\varphi(x(t))$ – функция затрат производителя *А*; *P* – постоянные издержки.

Прибыль банка *Б* в момент *t* складывается из процентов по кредитам, выдаваемым производителю *А*, и дивидендов по акциям предприятия *В*, которыми в момент *t* владеет банк:

Предполагается, что участники корпоративной структуры выполняют условия оптимальной программы совместного финансирования производителя, при которых они получают максимальные гарантированные доходы на интервале $[t_0,T]$. С учетом ставок регионального налога на прибыль, моменты переключения оптимальных этапов инвестиционной программы будут:

$$\widetilde{t}_1 = \mathrm{T} - \frac{1}{\mu_1}\ln\frac{\xi\theta^{A}G(x)}{\xi\theta^{A}G(x)-\mu_1};\quad \widetilde{t}_0^{*} = t_1\ \frac{(\xi-\varepsilon\theta^{Б})-\dfrac{1}{\theta^{A}t_1G(x)}}{(\xi-\varepsilon\theta^{Б})+\varepsilon\theta^{Б}\mu_0 t_1};$$

$$\widetilde{t}_1^{*} = \mathrm{T} - \frac{1}{\mu_0}\ln\frac{\varepsilon_0\theta^{Б}G(x)}{\varepsilon_0\theta^{Б}G(x)-\mu_0}; \qquad (3)$$

$$\theta^{Б}=1-\theta_0^{Б},\ \theta^{A}=1-\theta_0^{A},\ \varepsilon=\tau(1-\xi)\alpha_0\frac{q_0}{q_1},\ q_0=\omega+\alpha_0\geq 0,\ q_1=\omega-\alpha_0\tau\geq 0,$$

μ_0, μ_1 – коэффициенты дисконтирования соответственно банка и производителя, μ_0, μ_1 = const; $G(x)$ – функция, характеризующая темп роста доходов производителя A при вложении в снижение его затрат финансового ресурса x, $G(x)=\dfrac{dg(x)}{dx}$.

Решением оптимизационной задачи для банка $Б$ является его максимальный гарантированный доход, который составляет величину

$$\widetilde{J}_0(T) = \theta^{Б}\{(1-\xi)[\alpha_0(1+\tau)J_0^{13}+q_0J_0^{24}]+\tau W\lambda_0^{13}\} = (1-\theta_0^{Б})\widetilde{\widetilde{J}}_0; \qquad (4)$$

$$\widetilde{\widetilde{J}}_0=(1-\xi)[\alpha_0(1+\tau)J_0^{13}+q_0J_0^{24}]+\tau W\lambda_0^{13};\quad \lambda_0^{i}=-\frac{1}{\mu_0}\left(e^{-\mu_0\widetilde{t}_{iк}}-e^{-\mu_0\widetilde{t}_{iн}}\right);$$

$$J_0^{i}=\int_{\widetilde{t}_{iн}}^{\widetilde{t}_{iк}} g(x)\,e^{-\mu_0 t}dt;\qquad J_0^{ik}=J_0^{i}+J_0^{k};\qquad \lambda_0^{ik}=\lambda_0^{i}+\lambda_0^{k}.$$

$\lambda_0^{ik}=\lambda_0^{i}+\lambda_0^{k}$, $\widetilde{t}_{iн}$, $\widetilde{t}_{iк}$ - время начала и окончания i-го этапа инвестиционной программы, (i = 1 ,..,4), W – свободный ресурс банка, направляемый на кредитование производителя A под процент τ, либо на приобретение дополнительных акций потребителя B.

Выражение (4) определяет достаточно сложную зависимость критерия эффективности банка $\widetilde{J}_0(T)$ от ставки налога $\theta_0^{Б}$, так как этот параметр входит и в пределы интегрирования $\widetilde{t}_i$ функции дохода банка на каждом i-м этапе оптимальной инвестиционной программы. Однако, в работе [1] показано, что вариации аргумента функции $\widetilde{t}_i(\theta_0^{Б})$ вокруг некоторого его постоянного значения, не могут существенно повлиять на значение самой функции. Это значит, что с некоторой небольшой погрешностью можно рассматривать зависимость (4) как линейную функцию относительно ставки $\theta_0^{Б}$.

Итак, при ставке регионального налога на прибыль банка $\theta_0^{Б}$ его максимальный доход, за период [t_0,T], составит величину $\widetilde{J}_0(\theta_0^{Б})$.

Допустим, что за тот же период банк имеет возможность получить максимальный гарантированный доход $I_0 > \widetilde{J}_0(\theta_0^Б)$, но не в группе, а при независимой альтернативной деятельности. (Обоснование этой доходности должно производиться независимыми аудиторскими службами с учетом расчетов самого банка.) Мы хотим оценить изменение $\Delta\theta_0^Б$ ставки налога на его прибыль таким образом, чтобы выполнялось:

$$\widetilde{J}_0(\theta_1^Б) = I_0, \text{ где } \quad \theta_1^Б = \theta_0^Б - \Delta\theta_0^Б. \tag{5}$$

Рассматривая (5) как уравнение относительно величины $\Delta\theta_0^Б$, находим расчетную поправку к ставке регионального налога на прибыль банка, при которой интегральный дисконтированный доход банка на планируемом интервале будет не меньше его альтернативного дохода I_0:

$$\Delta\theta_0^Б = \frac{I_0 - \widetilde{J}_0(\theta_0^Б)}{\widetilde{\widetilde{J}}_0}. \tag{6}$$

Если существует ограничение Δ_0, меньше которого региональная ставка налога на прибыль банка быть не может, то балансирующая процентная ставка налога на прибыль банка определяется из условия: $\theta_1^Б = \max\{(\theta_0^Б - \Delta\theta_0^Б), \Delta_0\}$.

Получая льготу в виде балансирующей ставки налоговых отчислений на прибыль, направляемых в региональный бюджет, банк с большей заинтересованностью будет относиться к вопросу своего вхождения в состав региональной финансово-промышленной корпоративной группы. Регион же в этом случае получит необходимые ему финансовые средства для своего социально-экономического развития, что в целом, можно рассматривать как повышение экономической стабильности региона и повышение экономической безопасности региональной деятельности.

Литература:

1. *Косачев Ю.В.* Экономико-математические модели эффективности финансово-промышленных структур. – М.: Логос, 2004.
2. *Косачев Ю.В.* Оптимальное управление инновационным процессом в рамках интегрированной структуры // Проблемы управления. – 2013. – № 1. – С. 32 – 39.
3. *Королев А.В., Косачев Ю.В., Румянцев В.П.* Основные задачи оптимального управления комплексом региональных финансово-промышленных структур//Сб. докл. междунар. конф. «Актуальные проблемы управления» / РГГУ. – 2014. – С. 355 – 358.

Авдеева З.К., Коврига С.В.

Анализ согласованности интересов активных субъектов социально-политической ситуации на модели причинно-следственных влияний

Аннотация: Рассмотрены возможности согласования интересов активных субъектов социально-политической ситуации с использованием когнитивных карт, включая этапы построения модели ситуации группой экспертов и анализа структурных свойств модели.

Ключевые слова: социально-политическая ситуация, политическая стабильность, принятие решений, заинтересованные стороны, когнитивная карта

Социально-политические ситуации (СПС), с которыми сталкиваются современные лица, принимающие решения, (ЛПР) характеризуются не только быстрой изменчивостью, взаимодействием многих междисциплинарных факторов, но также и наличием активных субъектов – заинтересованных сторон с различными интересами и пониманием ситуации. Кроме того, активные субъекты ситуации (АСС) имеют разный потенциал положительного или отрицательного влияния на развитие СПС.

Важнейшим условием политической стабильности в таких ситуациях является (1) достижение баланса интересов различных заинтересованных сторон (социальных групп и политических сил) в стране, (2) способность государства нейтрализовать негативные внутренние воздействия и воздействия извне, способные нарушить этот баланс.

В зарубежных публикациях активно используется категория «governance». Это уровень управления, направленный на оценку потребностей, условий и возможностей заинтересованных сторон в ситуации для определения сбалансированных согласованных целей, которые должны быть достигнуты; определение направлений их достижения и установление приоритетов; мониторинг эффективности и соответствия согласованным направлениям и целям [1]. В данной работе управление политической стабильностью рассматривается именно в таком аспекте.

В современной методологии принятия решений развиваются методы на основе когнитивных карт (КК). КК – это формализованная модель ситуации, отражающая знания индивидуального или коллективного субъекта о причинно-следственных влияниях между ее значимыми факторами. Спектр приложений КК простирается от концептуального моделирования, нацеленного на улучшение структуризации и понимания проблем путем построения слабо формализованной КК, до решения

практических задач анализа и моделирования динамики ситуаций. В последнем случае применяются формальные КК, в которых к элементам карты (факторам и связям) приписаны параметры и определены функции оценки изменения факторов; т. о. они допускают формальную обработку (Рис. 1) .

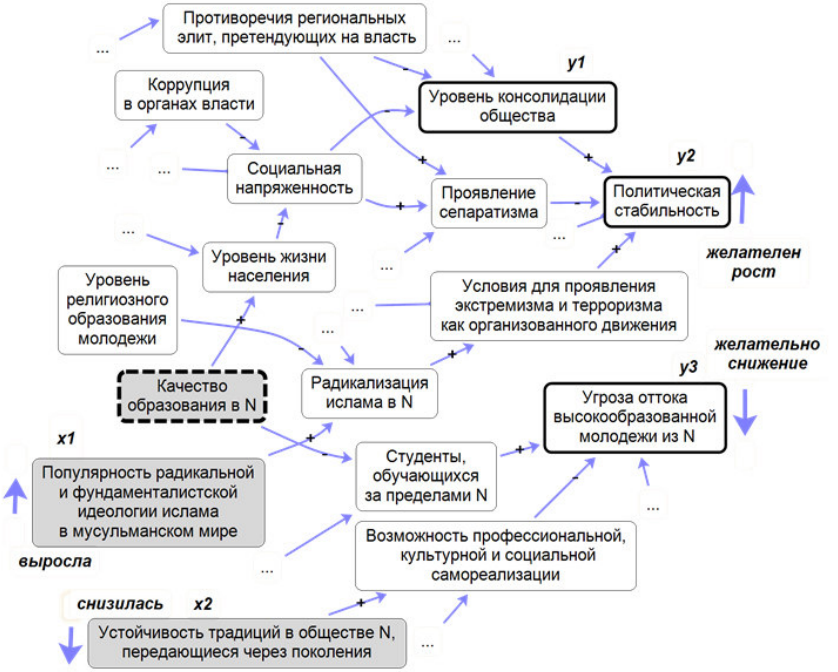


Рис. 1– Фрагмент знаковой КК (без весов влияний), отражающей СПС в одной из стран СНГ

В данной работе модель СПС представляется формальной КК, которая рассматривается как средство (1) обобщенного представления о СПС, (2) согласования интересов АСС и/или выявления возможных конфликтов интересов и путей их разрешения на основе анализа структурных свойств модели. В качестве АСС могут рассматриваться как персонифицированные субъекты ситуации, так и обезличенные субъекты, например, при анализе международных отношений в качестве субъектов рассматриваются целые страны с их государственными интересами, декларируемыми в доктринах и программных документах. В целях более полного представления о СПС к построению КК привлекаются

разнопрофильные эксперты. Здесь «полная» модель понимается как модель, достаточная для решения поставленной задачи с точки зрения привлеченных экспертов (и персонифицированных АСС, если последние непосредственно участвуют в построении КК). Соответственно, чем больше экспертов, различающихся по предметным областям, связанным с проблематикой исследуемой СПС, тем больше аспектов ситуации отражаются в модели. Неотъемлемой частью модели являются факторы, представляющие интересы выделенных АСС и их допустимые рычаги управления СПС, применяемые для достижения собственных интересов. Например, для анализа проблем международной стабильности, помимо специалистов в сфере международных отношений, необходимо привлечение экспертов военной сферы для учета факторов военно-политической обстановки, в значительной мере характеризующей общую международную обстановку.

Этап построения модели СПС. Для построения модели предлагается метод, сочетающий кластеризацию сходных мнений экспертов и уточнение и согласование их представлений с использованием ряда критериев улучшения качества коллективной КК для повышения объективности и работоспособности модели (применимости результатов ее использования при последующем принятии решений). Метод разработан с учетом существующих проблем в области построения коллективных КК [2,3].

Построение модели СПС должно проводиться при участии специалиста(ов) в области когнитивного моделирования, который модерирует этот процесс в целях (1) достижения приемлемого согласования представлений экспертов (здесь под «приемлемостью согласования» понимается такой его уровень, при котором возможно коллективное решение практической задачи без учета существующих различий в понимании ситуации разными участниками построения модели); (2) контроля над правильностью формализации первичных представлений в модель ситуации на языке формальной КК.

Пусть дано m индивидуальных знаковых КК, $\{K^l\}$, где m – количество экспертов. В знаковой карте задаются только знаки влияний: положительное (+) или отрицательное (–) влияние (рис. 1). (Наш практический опыт показывает, что для повышения обоснованности последующей оценки весов причинно-следственных влияний решающую роль играет спектр параметров качества знаковой карты, такой как понятность факторов, связей; упущенные или избыточные связи и т.д.).

Каждая K^l отражает представление l-го эксперта о СПС, включая основных АСС. При этом принято, что во всех $\{K^l\}$ АСС совпадают, и

область интересов каждого из них определена на одних и тех же факторах во всех картах.

Пусть K_l представлена квадратной матрицей $A^l = [a_{ij}^l]$, где $a_{ij}^l \in \{-1, 0, 1\}$ – знак влияния фактора-причины x_i^l на фактор-следствие x_j^l; из всех $\{K^l\}$ выделены общие факторы $X^{total} \subseteq X^l$ (т.е. факторы, представленные во всех или большинстве $\{K^l\}$). Общность факторов означает, что для их представления в картах используются одинаковые понятия и/или синонимичные, близкие по смыслу, понятия.

Множество $\{K^l\}$ интегрируются в коллективную КК, K^{col} (возможно, в нескольких $\{K_p^{col}\}$), основываясь на принципе близости экспертных представлений о СПС в контексте проблематики исследуемой ситуации. Для этого предлагается формальная процедура кластеризации карт, основанная на близости матриц $\{A^{l\_total}\}$, где каждая A^{l_total} – есть квадратная $n \times n$, где n – число общих факторов X^{total}. В качестве меры используется общий тип расстояния – «евклидово расстояние». Формируется один или несколько кластеров, каждый из которых включает в себя КК АСС со схожими представлениями о СПС (в рамках выделенных общих факторов). Далее в каждом кластере *p* формируется обобщенная карта K_p^{gen} на основе интеграции $\{A^{l\_total}\}$ с учетом представительности (по критерию большинства) соответствующих элементов $a_{ij}^{l\_total}$ в каждой A^{l_total} и знаков их влияния. Последующая процедура согласования $\{K_p^{gen}\}$ включает в себя определение существенных различий между ними, интеграцию их в общую карту K^{col} ситуации в случае слабых различий и анализ конфликтов в случае значительных различий. После завершения согласования карта K^{col} дополняется неучтенными факторами $\{X^l \setminus X^{total}\}$ из $\{K_l\}$ при наличии связей с факторами K^{col}. В общем случае, можно получить несколько $\{K_p^{col}\}$, что позволяет учитывать альтернативные взгляды на развитие СПС. Т. о. удается избежать «усреднения» (т.е. игнорирования различий) мнений экспертов, используемого в современных агрегирующих процедурах КК [3].

В части дальнейшего развития метода предполагается улучшение процедуры формальной кластеризации КК разной размерности в целях облегчения работы модератора, играющего значимую роль в обеспечении сходимости и результативности процесса построения коллективной карты.

Этап анализа модели СПС. В основе метода согласования интересов АСС лежит анализ структурных свойств модели СПС, представленной КК с весами влияний: (1) вычисление интегральных влияний одних факторов на другие факторы карты, включая идентификацию характера (благоприятного или отрицательного) этих влияний; (2) оценку этих влияний для выявления (i) противоречий между целевыми факторами из областей интересов АСС и (ii) нахождения факторов управлений, которые способствуют развитию СПС в интересах выбранных АСС, в том числе с учетом конфликта интересов. (Базовая постановка такой задачи и схема ее решения приведена в [4].)

Различия между нашим подходом и типичной практикой анализа структуры КК [5] состоит в следующем. Наш анализ учитывает динамические характеристики факторов ситуации и позволяет выявить возможности, скрытые в (часто сложной) структуре КК, чтобы выбрать вектор управляющих факторов, который потенциально эффективен в отношении достижения вектора целей. Однако метод применим в рамках следующих ограничений: (1) тип модели описывает стабильные ситуации, в которых есть устойчивые состояния по факторам; (2) рассматривается только параметрическое управление ситуацией без изменения структуры карты. В части дальнейшего развития предложенного подхода предполагается исследование возможности его распространения для модели ситуаций с более сложной динамикой.

Заключительные выводы. Все чаще появляются отечественные и зарубежные публикации, в которых обосновывается и демонстрируется перспективность применения КК в таких областях, как политика, геополитика, международные отношения (см., например, [6-8]). По нашему мнению, рассмотренные в данной статье возможности согласования интересов АСС расширяют инструментарий когнитивного моделирования для решения прикладных задач в сфере геополитики и международных отношений, где взаимодействие субъектов играет существенную роль в развитии ситуации.

Работа выполнена при частичной финансовой поддержке РФФИ (грант 18-07-01044а).

Литература:

1. *COBIT5:* A Business Framework for the Governance and Management of Enterprise IT. (2012). ISACA.
2. *Hodgkinson G.*, *Maule A.*, *Bown N.* Causal cognitive mapping in the organizational strategy field: a comparison of alternative elicitation procedures // Organizational Research Methods. – 2004. – Vol. 7, №1. – P. 3–26.

3. *Avdeeva Z., Kovriga S.* On approach to the agreement of diverse stakeholders' interests and goals in the governance // International Journal of Engineering and Technology (UAE). 2018. Vol. 7, № 2.28. P. 160-163.
4. *Avdeeva Z.K., Kovriga S.V.* On the approach to statement of control problems of the situation with many active stakeholders to support a dynamic goal setting // Proc. of the 11th IEEE International Conference on Application of Information and Communication Technologies (AICT2017). 2017. – Vol.2. – P. 222-227.
5. *Yoon B.S., Jetter A.J.* Comparative analysis for fuzzy cognitive mapping // Proc. of the Portland International Conference on Management of Engineering and Technology (PICMET2016), 2016, P. 1897-1908.
6. *Ormerod P., Riordan S.* New approach to the analysis of geo-political risk // Diplomacy & Statecraft. – 2004. – Vol. 15, Iss. 4. – P. 643-654.
7. *Shayji S., Kadhi N., Wang Z.* Fuzzy cognitive map theory for the political domain / / Proc. of the Federated Conference on Computer Science and Information Systems. – Szczecin, Poland, 2011. – P. 179-186.
8. *Абаев Л.Ч.* Об актуальных подходах к моделированию международных отношений // Проблемы национальной стратегии. – 2011. –№2(7). – С. 31–48.

Быстров В.В., Маслобоев А.В.

Проектный подход в управлении социально-экономической безопасностью региона

Аннотация: Работа посвящена развитию теоретических основ управления безопасностью сложных систем в части разработки методологии информационной поддержки принятия решений в сфере обеспечения безопасности региональных социально-экономических систем, а также в части создания формального аппарата и средств автоматизации управления в этой области. Рассматриваются вопросы применения проектного менеджмента и программно-целевого подхода в задачах управления региональной безопасностью.

Ключевые слова: проектный подход, информационная поддержка, управление, региональная безопасность, компьютерное моделирование

В настоящее время вопросам обеспечения безопасности в различных сферах на разных уровнях государственного управления уделяется особое внимание. Особенно остро проблемы безопасности проявляются на региональном уровне. Поэтому именно сегодня назрела объективная

необходимость в разработке и внедрении в области государственного управления средств поддержки принятия решений нового поколения, включая обучаемые нейронные сети, профессиональные социальные сети, мультиагентные и кибер-физические (виртуальные) системы. Однако, эта задача еще далеко от эффективного решения.

Успешное внедрение современных информационных систем и технологий, высокая степень автоматизации процессов принятия управленческих решений предоставляют новые возможности для повышения эффективности процессов управления безопасностью сложных социально-экономических объектов, к которым относятся региональные системы.

Современные средства информационной поддержки управления безопасностью социально-экономических систем зачастую оказываются функционально ограниченными и не всегда обеспечивают субъектов управления полной и аналитически обоснованной информацией о состоянии развития этих систем для принятия эффективных управленческих решений, особенно в условиях кризисных ситуаций в социально-экономической сфере. Очевидно, что устранение этих противоречий на практике представляет собой достаточно важную задачу и, в свою очередь, требует разработки единой и конструктивной теории, позволяющей с общих методологических позиций оценивать существующее положение дел в области управления безопасностью региональных социально-экономических систем (далее - региональной безопасностью). Трудностей добавляет отсутствие общей формализованной постановки проблемы управления региональной безопасностью и формального аппарата для системного решения этой проблемы. Эти ключевые факторы в совокупности обусловливают необходимость проработки широкого круга вопросов, связанных с моделированием данной предметной области и с автоматизацией синтеза гибких систем управления региональной безопасностью.

Работа посвящена развитию теоретических основ системного анализа, моделирования и автоматизации процессов управления региональной безопасностью. Исследованы системные связи, закономерности и тенденции, определяющие безопасность развития региональных социально-экономических систем.

Предложены новые формулировки терминов в сфере региональной безопасности, не противоречащие официально принятым и уточняющие содержание этой перспективной предметной области с помощью конкретных формализмов, что расширяет понятийный аппарат теории безопасности сложных систем и делает его более конструктивным.

В работе термин «региональная безопасность» определяется авторами как состояние защищенности региональной системы, при котором

действие внешних (глобальных) и внутренних (локальных) факторов не приводит к ухудшению или к невозможности ее функционирования и развития [2].

Основная идея работы заключается в рассмотрении мероприятия, тем или иным образом приводящего к изменению состояния региональной безопасности, как отдельного проекта в терминах проектного менеджмента.

Под проектом понимается ограниченное во времени целенаправленное изменение отдельной системы с установленными требованиями к качеству результатов, возможными рамками расхода средств и ресурсов и специфической организацией [1].

Проект в сфере обеспечения региональной безопасности – комплекс антикризисных мероприятий, проводимых субъектами регионального управления и заинтересованными лицами с целью получения определенных результатов требуемого качества, непосредственно или опосредованно влияющих на состояние социально-экономического развития региона с учетом ограничений на использование различного типа ресурсов (временных, финансовых, кадровых, материальных и др.). Цели определяются на основе анализа принятой стратегии социально-экономического развития региона и текущих проблем регионального развития.

Примерами проектов в сфере экономической безопасности исследуемого региона (Мурманской области) являются формирование эффективных инновационных структур, ориентированных на создание социально значимых объектов на территории Мурманской области, а также сети малых инновационных предприятий и научно-образовательных структур для поддержки устойчивого развития моногородов Севера России. Для обеспечения экологической и транспортной безопасности Северного морского пути такими проектами являются программы мероприятий по снижению рисков возникновения чрезвычайных ситуаций природного и техногенного характера, связанных с его активной эксплуатацией.

Существуют различные классификации проектов. Тип проекта определяет его свойства и характеристики, а также выбор методов принятия управленческих решений. В сфере обеспечения региональной безопасности преимущественно реализуются долгосрочные организационно сложные смешанные мегапроекты, а также модульные оперативные и стратегические программы управления региональным развитием.

Известны следующие методы и подходы для решения задач управления проектами:

1) Календарно-сетевое планирование и управления. В основе данного подхода лежит математический аппарат теории графов, позволяющий решать сложные оптимизационные задачи, используя методы дискретной математики.
2) Качественный подход к управлению проектами, близкий по своей методологии к менеджменту организаций и развиваемый, в основном, зарубежными учеными.
3) Количественный подход, основывающийся на анализе и синтезе математических моделей механизмов управления проектами и процедурах принятия управленческих решений. Данный подход оперирует комбинациями методов теории игр, исследования операций, имитационного моделирования, математической экономики, теории активных систем, а также программно-целевого и ситуационного планирования.

Позиционируя проводимое исследование в рамках приведенных подходов, можно сказать, что разрабатываемая информационная технология поддержки управления проектами в сфере обеспечения региональной безопасности использует комбинацию двух направлений – количественного и календарно-сетевого планирования и управления. При этом выбор математической модели того или иного типа определяется характеристиками решаемой задачи управления и заданными условиях для каждой конкретной ситуации.

Под системой информационной поддержки проектного управления региональной безопасностью понимается совокупность информационных технологий и средств, позволяющих неявно управлять ходом реализации мероприятий в сфере обеспечения безопасности региона. При этом основными задачами являются: 1) оценка текущего состояния региональной безопасности; 2) проведение анализа плана реализации или результатов выполнения проекта (мероприятия) в сфере региональной безопасностью с целью выявления потенциальных угроз; 3) выработка соответствующих рекомендаций ЛПР по реализации проекта или внесение корректировок в жизненный цикл проекта; 4) оценка последствий при реализации предлагаемого управляющего воздействия на состояние региональной безопасности за счет манипуляции планируемыми и реализуемыми проектами. Вместе с тем, такие системы ориентированы на снижение сложности и ресурсопотребления задач управления, а также на повышение качества принимаемых решений.

Предложены постановка и формализация общей задачи управления региональной безопасностью на основе матрицы безопасности региона и проектного подхода. Разработаны новые теоретико-множественные модели жизненного цикла управления региональной безопасностью в условиях кризисных ситуаций и системы управления безопасностью

региона. Эти концептуальные модели адаптированы и расширены на задачи обеспечения безопасности социально-экономических систем регионального уровня, а также отличаются полнотой формального описания объектов и задач управления безопасностью и связанных с ними информационных процессов. Модели имеют многоуровневую структуру и основаны на принципах классической теории управления и проектного менеджмента. В них используются формальное описание предметной области, аппарат теории управления проектами и формализованная схема управления безопасностью региона. Модели отражают специфику задач управления мероприятиями, оказывающими воздействие на состояние региональной безопасности. Предлагается каждое мероприятие рассматривать как отдельную совокупность проектов, что позволяет перевести исследование региональной безопасности в плоскость решения задач управления проектами.

Реализация созданных моделей позволяет осуществить автоматизированный синтез онтологических и имитационных моделей управления безопасностью и их последующее использование в составе интеллектуальных систем поддержки принятия решений по обеспечению региональной безопасности на базе ситуационных центров региона. Сценарный анализ и прогнозирование вариантов развития региональных кризисных ситуаций на основе моделей повышают информационную обеспеченность системы управления безопасностью региона и качество принимаемых управленческих решений. В модели могут быть встроены теоретические конструкции [3], что позволит также решать задачи координации в системах управления региональной безопасностью.

При реализации предлагаемых моделей необходимо учитывать, что появление новых проектов, как правило, зависит от состояния региональной безопасности, а цели проектов должны быть ориентированы на нейтрализацию потенциальных угроз и опасностей, а также на смягчение последствий возможных кризисных ситуаций в регионе.

Полученные результаты использованы при реализации «Стратегии развития Арктической зоны РФ и обеспечения национальной безопасности на период до 2020 года» на территории Мурманской области в части создания средств информационно-аналитической поддержки [4] для задач управления и принятия решений в сфере обеспечения региональной безопасности. Эти средства позволяют ЛПР получать в автоматизированном режиме агрегированную аналитическую информацию о возможных последствиях реализации того или иного регионального проекта еще на стадии планирования, а также оценивать и принимать решения в фазе оперативного управления проектом.

Работа выполнена при поддержке РФФИ (проекты 18-07-00167-а, 18-29-03022-мк).

Литература:
1. *Быстров В.В.* Применение проектного менеджмента в задачах управления региональной безопасностью: подход и формальный аппарат / *В.В. Быстров, А.В. Маслобоев, В.А. Путилов* // Надежность и качество сложных систем. – 2017. - №4. – С. 73-84.
2. *Маслобоев А.В.* Информационное измерение региональной безопасности в Арктике / *А.В. Маслобоев, В.А. Путилов*. - Апатиты: Изд-во КНЦ РАН, 2016. - 222 с.
3. *Маслобоев А.В.* Координация в многоуровневых сетецентрических системах управления региональной безопасностью: подход и формальная модель / *А.В. Маслобоев, В.А. Путилов, А.В. Сютин* // Научно-технический вестник информационных технологий, механики и оптики. - 2015. - Т.15. - №1. - С. 130-138.
4. *Маслобоев А.В.* Система поддержки принятия решений в условиях региональных кризисных ситуаций / *А.В. Маслобоев* // Информационные ресурсы России. - 2017. - №4(158). - С. 25-32.

III. Проблемы обеспечения информационной безопасности

Рожнов А.В.

Контрфактическое моделирование новых вызовов посткибератак посредством пертинентной обработки сверхбольших массивов данных и их визуализации

Аннотация: Представлено дальнейшее развитие прикладной разработки "Некоторые аспекты контрфактического моделирования новых вызовов посткибератак посредством пертинентной обработки сверхбольших массивов данных и их визуализации". Доклад основан на рабочих материалах предшествовавших депонированных работ расширенного авторского коллектива в ВИНИТИ РАН.

Ключевые слова: контрфактическое моделирование, посткибератаки, пертинентная обработка данных, сверхбольшие массивы данных, когнитивные искажения

Современный мир находится на грани кардинальных изменений многих ранее привычных представлений геополитики и её применимых организационных, финансовых и смежных информационно-логических "инструментов", научно-технических и технологических возможностей цивилизации ближайшего будущего, проявления угроз и появления целого ряда новых вызовов благополучного существования общества в связи с множеством взаимосвязанных причин от изменения климата и природных катаклизмов, до внезапной эскалации напряженности политико-экономических, социальных и иных всевозможных условий функционирования глобальных информационных сред и сервисов [1, 2].

В совокупности исследуемых направлений поиска искомых решений при парировании подобных сложноустранимых угроз следует обратить особое внимание на ёмкую проблемную область новых вызовов т.н. "посткибератак" на стыке смежных отраслей фундаментальной науки защиты информационной инфраструктуры и ликвидации последствий чрезвычайных ситуаций, весьма нетривиальный характер условий возникновения которых предопределяет высокий уровень значимости и научной новизны проводимых комплексных исследований элементов прорывных технологий обнаружения и своевременного устранения

уязвимостей гетерогенных информационных систем и сред в различных условиях обстановки. Представленные в таком инициативном проекте междисциплинарные вопросы, с учетом имеющегося задела, позволяют в ином ракурсе представлять предпосылки дальнейшего развития уже в среднесрочной перспективе показанной проблематики как в отдельных фундаментальных, так и в целом ряде производных прикладных работ (первоочередных задач выявления, локализации уязвимостей, др.) [1-5].

В целом проект соответствует направлению исследований в сфере информационных технологий цифровой экономики: новые методы исследования угроз, включая задачи выявления, локализации и защиты от них, в глобальных информационных системах поддержки цифровой экономики, разработка архитектурных решений по обеспечению информационной безопасности в гетерогенных информационных системах цифровой экономики, исследование системотехнических проблем информационной безопасности распределенных реестров данных. Также следует учитывать следующие дополнительные аспекты: контрфактическое моделирование, посткибератаки, пертинентная обработка данных, сверхбольшие массивы данных, когнитивные искажения и т.д. [5]. В разрезе ключевой научной проблематики таковой комплексной области новых вызовов посткибератак конечно превалируют интересы заблаговременного обнаружения уязвимостей глобальных информационных систем, которые направлены на решение актуальных и комплексных задач разработки элементов прорывных технологий и всесторонней теоретико-экспериментальной отработки их интеграционных компонентов посредством контрфактического моделирования среды функционирования в различных условиях обстановки ликвидации последствий чрезвычайных ситуаций, возникновения и внезапной эскалации напряженности, сбоев и аварий в работе, к примеру, энергетической инфраструктуры и обеспечивающих информационных сред и систем различного назначения [3-5].

Таким образом, в итоге системной интеграции и информационно-аналитического моделирования, научно-методического сопровождения гетерогенных информационных систем – предложены взаимоувязанные методы и модели контрфактического моделирования и анализа среды функционирования, отчасти доведенные точечно до экспериментальной отработки интеграционных компонентов внедряемых сервисов с бесспорным приоритетом выполнения требований импортозамещения.

Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 16-29-04326.

Литература:
1. *Богорадникова А.В., Оганджанян С.Б., Рожнов А.В.* и др. Некоторые аспекты контрфактического моделирования новых вызовов посткибератак посредством пертинентной обработки сверхбольших массивов данных и их визуализации. Часть I / Рос. технол. ун-т (МИРЭА). Депонированная рукопись № 69-В2018. ВИНИТИ РАН, 2018.
2. *Богорадникова А.В., Лобанов И.А., Гудов Г.Н.* и др. Некоторые аспекты контрфактического моделирования новых вызовов посткибератак посредством пертинентной обработки сверхбольших массивов данных и их визуализации. Часть II / Рос. технол. ун-т (МИРЭА). Депонированная рукопись № 70-В2018. ВИНИТИ РАН, 2018.
3. *Садовничий В.А., Васенин В.А.* Интеллектуальная система тематического исследования наукометрических данных: предпосылки создания и методология разработки. Часть 1 / Программная инженерия, изд-во Новые технологии (Москва), 2018, том 9, № 2. С. 51-58.
4. Интеллектуальная система тематического исследования научно-технической информации (ИСТИНА) / Садовничий В.А., Афонин С.А., Бахтин А.В., Бухонов В.Ю., Васенин В.А. и др. - М.: Изд-во Московского университета, 2014. - 262 с.
5. *Рожнов А.В.* Конвергенция технологий управления автономными системами в контексте развития интеграционных компонентов искусственного интеллекта // В сб.: Современные информационные технологии и ИТ-образование. Сб. научных трудов II Международной научной конференции и XII Международной научно-практической конференции. Под ред. В.А. Сухомлина. 2017. С. 20-31.

Курако Е.А., Орлов В.Л.

Организация защиты информации в системах, использующих сервис-браузеры

Аннотация: Рассмотрена задача организации защиты информационных систем, использующих сервер-браузеры. Показана возможность параллельной работы пользователя с несколькими системами при использовании одного сервис-браузера.

Ключевые слова: защита информации, информационная система, аутентификация, авторизация, сервис-браузер

Развитие информационных систем для различных направлений, начиная от малого бизнеса, включая крупные коммерческие решения и заканчивая государственными и международными структурами, в

настоящее время стало не просто фактом, но насущной необходимостью. И с изменением таких систем изменяются и клиентские места, предназначенные для операторов. Если 40 лет назад это были терминалы, взаимодействующие с мейнфреймами, то 30 лет назад – персональные компьютеры, реализующие в основном технологию «толстого» клиента. Дальше клиент становился все более тонким, то есть большую часть функций по обработке данных брал на себя сервер. На текущий момент в качестве клиента выступает обычно универсальный web-браузер, который выдает запросы на получение html-страниц от сервера и интерпретирует их, включая возможности выполнения скриптов, размещенных на страницах. Также перспективным решением представляется использование сервис-браузера [1,2], который работает не с html-страницами, а с объектами, возвращаемыми вызываемыми web-сервисами. Естественно, сервис-браузер ориентирован в основном на использование в информационных системах, и одной из отличительных его особенностей является встроенный механизм обеспечения безопасности.

Рассмотрим подробнее алгоритм развертывания прикладных систем сервис-браузером с использованием функций защиты.

Сервис-браузер в первую очередь проводит процесс аутентификации пользователя. Причем способы аутентификации могут быть различными (логин-пароль, тикеты, подписываемые электронной подписью, даже биометрические средства). Это зависит от конкретной реализации. Важно то, что аутентификация не зависит от выбора прикладной системы, то есть это именно единая и общая аутентификация пользователя. Если используется наиболее распространенный способ установления подлинности, такой как логин-пароль (а мы его рассмотрим в качестве примера), то разумеется, пароль не должен передаваться в открытом виде. В основном используют хеширование пароля с добавкой, обычно называемой «солью» [3]. После проверки пароля на сервере определяется идентификатор пользователя. Но тут нужно иметь в виду, что если аутентификация позволяет установить подлинность пользователя, то авторизация, которая проводится на сервере следом за аутентификацией, уже определяет полномочия пользователя для конкретной информационной системы. Поэтому между процедурами аутентификации и авторизации неизбежно вклинивается процедура определения информационной системы, с которой собирается работать пользователь. В простейшем случае идентификатор этой системы передается вместе с парой «логин-хеш соленого пароля».

Однако может возникнуть ситуация, когда пользователю необходимо поочередно обращаться к нескольким системам. При этом необязательно каждый раз вводить пароль. Достаточно указать, что он переходит на другую информационную систему и если в этой системе уже пройдена

процедура авторизации, то можно уже не запускать в этой системе начальный экран, а отображать то состояние системы, в котором она находилась ранее в данном сеансе связи.

Также интересен случай, когда мы имеем дело по существу с одной информационной системой, но разными базами данных. Примером такой системы является программный комплекс автоматизации филиалов какого-либо предприятия. В этом случае для всех филиалов программное обеспечение используется одно и те же, но базы данных (или фрагменты одной базы) – разные. Интересно, что и авторизация для этих систем также должна быть разной. Действительно, некий сотрудник может быть в одном филиале администратором, а в другой простым пользователем, которому разрешается выполнять только одну функцию, связанную, например, с получением какого-то подмножества статистических данных.

Возвращаясь к завершению процедуры авторизации, заметим, что сервис браузер в этот момент получает список модулей конкретной активной системы, который он отображает на экране. И затем дает возможность оператору запускать (активизировать) тот или иной из доступных ему прикладных модулей.

Каждый из прикладных модулей может вызывать прикладные web-сервисы, которые ему доступны, руководствуясь протоколом, определенным сервис-браузером.

Нужно заметить, что организация обращения к web-сервисам позволяет обеспечить передачу данных в открытом или закрытом виде. Для этого необходимо обеспечить лишь согласование канала передачи данных. Тогда на стороне сервера производится настройка web-сервера и прикладных сервисов на передачу сообщений, зашифрованных необходимыми алгоритмами шифрования. Следует учесть, что один и тот же сервис может работать в нескольких режимах, например, шифрование с помощью алгоритма AES, шифрование и подпись с помощью RSA или полностью открытый режим. При этом исходный код сервиса не требует изменений.

На стороне клиента, сервис-браузер позволяет подключать алгоритмы шифрования и подписи с помощью дополнительных модулей. А режим доступа настраивается для каждой прикладной системы или сервера. То есть при обращении прикладного модуля к прикладному сервису режим доступа невидим для модуля. Модуль знает, какой сервис надо вызвать, а обеспечение защиты возлагается на браузер.

Естественно, так как браузер взаимодействует напрямую с криптографическими драйверами, то для модулей предоставляется возможность использовать в своей работе электронную подпись (ЭП) и шифрование. Здесь примером может служить система электронного документооборота. Пользователь вставляет свой электронный брелок с

ключевой информацией и запускает сервис-браузер. Браузер определяет наличие ключевой информации и проводит аутентификацию пользователя, при этом, в зависимости от настроек, может затребовать дополнительно ПИН-код. После этого модуль работы с документами может подписывать созданные электронные документы ЭП пользователя и отправлять их в работу. Таким образом, документы, обрабатываемые в прикладной системе, имеют юридическую значимость, и ее можно интегрировать с информационными системами государственных органов. При этом затраты на разработку такой системы ниже благодаря решению криптографических задач с помощью сервис-браузера.

Практическая реализация сервис-браузера, обеспечивающего функционирование нескольких информационных системам, прошла успешную апробацию в режиме работы с двумя программными комплексами.

Литература:

1. *Курако Е.А., Орлов В.Л.* Сервис-браузеры для информационных систем / Программная инженерия. - Москва, 2017. – том 8, №9. - с. 413-421.
2. *Курако Е.А., Орлов В.Л.* Способ организации взаимодействия клиента с сервером приложений с использованием сервис-браузера: Патент на изобретение RU 2656735 C1; Зарегистрирован 06.06.2018. Заявлено 17.05.2017. Опубликовано: 06.06.2018 Бюллетень № 16.
3. *Козлов А.Д., Орлов В.Л.* Методы и средства обеспечения информационной безопасности распределенных корпоративных систем. М.: ИПУ РАН, 2017. – 156 с.

Людаговская М.А.

Концепция разработки многоуровневой интеллектуальной системы информационной безопасности на железнодорожном транспорте

Аннотация: Рассмотрена концепция построения многоуровневой интеллектуальной системы информационной безопасности, охарактеризованы ее структура и классы исходных данных.

Ключевые слова: интеллектуальные системы, средства и системы защиты, угроза безопасности информации, объект информатизации, информационная безопасность

Современные информационные системы ОАО РЖД содержат обширный перечень хранимой и необходимой для деятельности информации, которая может быть использована в целях совершения различных противоправных акций. Основным

средством эффективного управления ресурсами и направлениями производственно-технологической и административно-хозяйственной деятельности ЖТ является корпоративная АСУЖТ. Появление в АСУЖТ новых продуктов современных телекоммуникационных технологий влечет за собой появление новых видов угроз информационной безопасности, с которыми традиционные средства защиты информации (сети VPN, антивирусные средства, системы обнаружения атак, и пр.) справляются недостаточно эффективно. РЖД, являясь критической инфраструктурой, требует повышенного внимания к информационной безопасности, поэтому в систему защиты АСУЖТ необходимо внедрять интеллектуальные механизмы, которые делают эту систему многоуровневой интеллектуальной и наделяют принципиально новыми функциональными возможностями [1, 2].

В основу построения подобной системы может быть заложена обобщенная технология управления информацией и событиями безопасности SIEM (Security Information and Event Management), обладающая такими возможностями, как: гибридное онтологическое хранилище информации (репозиторий), логический вывод, межуровневая корелляция, моделирование поведения, визуальный анализ, анализ защищенности системы и трансформируемость. S IEM-системы способны обнаруживать угрозы безопасности не только на информационном уровне, но и на других уровнях защищаемой инфраструктуры и вырабатывать адекватные контрмеры в условиях поступления неполных и противоречивых данных [3].

В данной системе можно выделить три уровня:

1) уровень традиционных средств защиты (нижний);

2) уровень интеллектуальных сервисов сбора и хранения данных (средний);

3) уровень интеллектуальных сервисов анализа данных (высший) [4].

Нижний уровень системы содержит операционные системы рабочих станций, системы управления базами данных (СУБД), а также используемые в настоящее время в АСУЖТ, традиционные средства защиты информации, являющиеся источниками данных о событиях безопасности (событиях, способных привести к нарушению безопасности).

На среднем уровне осуществляется сбор, предварительная обработка и хранение информации о событиях безопасности. Для сбора данных используются два основных метода: «выталкивание» (источник сам посылает данные о событиях безопасности в систему) и «втягивание» (самостоятельное получение системой данных о событиях безопасности). Предварительная обработка информации включает в себя нормализацию,

фильтрацию, корреляцию, агрегацию и классификацию. Нормализация заключается в преобразовании собираемых данных к единому формату. В ходе фильтрации отбрасываются избыточные данные. Корреляция в процессе предобработки позволяет находить в поступающем потоке событий безопасности те, что являются критическими. Агрегация позволяет объединять события одного и того же вида. Классификация разделяет события на заранее выбранные классы. Предварительно обработанные данные помещаются на хранение в системный репозиторий. Для реализации системного репозитория очень важным моментом является то, какой вид модели представления данных поддерживает лежащая в его основе СУБД.

На верхнем системном уровне располагаются подсистемы, реализующие различные интеллектуальные сервисы анализа информации о безопасности, в том числе: сервисы анализа защищенности АСУЖТ и соединяющих их между собой СПД; сервисы моделирования атак на АСУЖТ и СПД; сервисы поддержки принятия решений; сервисы визуального анализа информации о безопасности [5].

Исходные данные для всех интеллектуальных сервисов анализа содержатся в гибридном онтологическом репозитории (GOR). В общем виде всех их можно разделить на следующие классы:

Sys — данные о защищаемой инфраструктуре (ее топологии, составе элементов, пользователях, ресурсах);

Events — прошедшие предобработку и находящиеся в репозитории на хранении данные о событиях безопасности;

Pattr — данные о шаблонах атак, инцидентах безопасности, и возможных контрмерах, которые формируются в ходе функционирования системы или загружаются из внешних баз данных;

Pol — данные о принятых в защищаемой инфраструктуре политиках безопасности [6].

Основная задача SIEM-системы – сбор и анализ информации, полученной от различных источников, таких как DLP-системы, IDS, маршрутизаторы, межсетевые экраны, АРМ пользователей, серверов. Однако, помимо регистрации и корреляционного анализа инцидентов, SIEM-система должна помогать фокусироваться на главных событиях, выявлять действия пользователей, программ и устройств, несущих реальную угрозу, отсеивать все несущественное и неприменимое. Эффективно решить эти задачи способна SIEM-система, понимающая работу сетевой инфраструктуры и содержащая в себе средства управления уязвимостями и моделирования, а также автоматизированные механизмы передачи в продукт экспертизы информационной безопасности и учета

новых опасностей. Такая SIEM-система способна выявлять широкий круг угроз, в том числе и атаки, распределенные во времени и не обнаруживаемые типовыми средствами защиты, выявляющиеся только через множество разрозненных некритичных событий, выстраиваемых в единую цепочку.

На этапе сбора информации для обобщенной SIEM-системы можно использовать возможности системы УРРАН (управление ресурсами, рисками и анализ надежности), ориентированной на унификацию, централизованное управление, оптимизацию затрат и оптимальное использование ресурсов на железнодорожном транспорте [7]. Кроме того, для решения ряда задач управления информационной безопасностью и создания АСУ для оценки состояния систем железнодорожного транспорта и их элементов можно использовать аппарат ТС-систем [8]. Преимуществом подхода к разработке методического обеспечения на основе ТС-систем является возможность представления исходных существенно нелинейных моделей в виде совокупности линейных моделей, аппроксимирующих исходную систему. Описание с помощью ТС-моделей базируется на правилах логического вывода и нечетких регуляторах. Преимущества ТС-моделирования систем связаны с тем, что возможен анализ качественных свойств изучаемых моделей не только в локальном, но и в глобальном смысле, а также возможна редукция базы правил без потери информации о модели;

Развитие концепции разработки многоуровневой интеллектуальной системы информационной безопасности на железнодорожном транспорте направлено на обеспечение безопасности и повышение уровня надежности работы интеллектуальных систем на всех уровнях АСУЖТ. Указанное развитие связано с перспективой развития интеллектуального управления движением поездов, предъявляющего высокие требования как к уровню безопасности автоматизированной системы автоведения поезда, так и к глубине анализа данных систем мониторинга.

Литература:

1. *Санькова Г.В., Одуденко Т.А*. Информационные технологии в перевозочном процессе. Хабаровск: Изд-во ДВГУПС, 2012.
2. Информационный бюллетень «Вестник АСУ «Экспресс–3», № 1 (3), Изд. ОАО "ВНИИЖТ", 2012. С. 5.
3. *Mille D.R., Harris Sh., Harper A.A., VanDyke S., Black Ch.* Security Information and Event Management (SIEM) Implementation. McGraw–Hill Companies, 2011.

4. *Котенко И.В., Саенко И.Б.* Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. Вып. 1(24). С. 21–40.
5. *Глухов А.П.* ОАО "РЖД": о приоритетах и перспективах // Информационная безопасность. 2007. № 2. С. 4–5.
6. *Котенко И.В., Саенко И.Б.* Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. Вып. 3(22). 2012. С. 84–100.
7. СТО РЖД 02.044–2011. Управление ресурсами, рисками и надежностью на этапах жизненного цикла (УРРАН).
8. *Tanaka K., Wang H.O.* Fuzzy control systems design and analysis: a linear matrix inequality approach. N.Y.: Wiley, 2001.

Козлов А.Д., Нога Н.Л.

Влияние субъективных факторов на безопасность сложных систем

Аннотация: Обсуждаются вопросы обеспечения безопасности сложных систем от внутренних угроз, исходящих, как от сотрудников организации, так и от сотрудников компаний, привлекаемых для проведения работ на правах аутсорсинга.

Ключевые слова: внутренние угрозы, субъективные факторы риска, благонадежность, облачные технологии, киберпреступления

Угроза информационной безопасности может быть реализована либо по техническим (отказ), природным (землетрясение, наводнение) причинам либо от воздействия человека. В первом случае такие факторы риска можно назвать объективными, а во втором – субъективные.

Бороться с объективными факторами можно путем повышения надежности, как отдельных элементов, так и системы в целом.

Чтобы успешно противостоять субъективным факторам, необходимо разобраться в их природе: откуда и почему могут исходить эти угрозы.

Основными побудительными мотивами являются: или навредить (нанести ущерб) атакуемой компании, или получить некую выгоду (прибыль) за счет реализации (продажи) похищенного информационного ресурса.

Ущерб можно нанести, проведя атаку на информационную систему и нарушив ее доступность, целостность, конфиденциальность или даже вывести из строя оборудование (например, вирус STUXNET вызвал в

Иране выход из строя центрифуг по обогащению урана [1]). Получить личную выгоду от атаки можно за счет реализации похищенных данных на внешнем рынке (средняя стоимость одной записи, содержащей персональные данные, на черном рынке составляет $1,5, а в 2016 году было похищено почти 1,1 миллиарда личных данных [1]), либо напрямую получив доступ, например, к финансовой информации. В любом случае выгода определяется ценностью информационного ресурса.

При этом ценность информационного ресурса для компании – держателя ресурса и для нарушителя может быть разной.

Для компании ценность ресурса определяется как:

$Ц_{рес} = З_{рес} + П_{пот}$,

где $Ц_{рес}$ – ценность ресурса, $З_{рес}$ - затраты на создание и содержание ресурса, $П_{пот}$ - потенциальная прибыль.

Для нарушителя ценность ресурса определяется размером получаемой выгоды от получения доступа к данному ресурсу.

В случае, когда эти ценности существенно отличаются, а затраты на защиту информационных ресурсов, как правило, не превышают потенциального ущерба, то нарушитель для реализации своей угрозы может потратить больше, чем компания для противодействия доступу.

Правда, если принять, что нарушителя интересует одна конкретная запись, а компания защищает весь массив, то в целом средства защиты и атаки становятся сопоставимы.

Самым критичным последствием для организаций, столкнувшихся с потерей данных, является возможная потеря бизнеса. После инцидента компании вынуждены предпринимать меры для сохранения доверия клиентов и уменьшения возможных убытков в долгосрочной перспективе. При этом соответствующий ущерб вычисляется следующим образом:

Ущерб = {Потери, возникшие в случае реализации угрозы} + {затраты, необходимые для восстановления исходного состояния системы}

В 2016 году средние затраты на восстановление одной скомпрометированной записи составили $158, а по оценкам специалистов к 2020 году составит $200-300 [1].

Существенно увеличивается доля мошенничества с полученными противоправным путем данными, что также увеличивает ущерб. По данным Infowatch [2] в 2017 году доля таких мошенничеств («квалифицированных утечек») в России составила 30% от общего числа утечек против 11% в 2016 году (в мире соответственно 11% против 7%).

По данным Infowatch [2] львиная доля утечек происходит по вине внутреннего нарушителя. В 2017 году в России по вине внутренних нарушителей произошло 76% утечек (в мире – 60%).

Тот же источник приводит распределение утечек по виновникам в России и мире (Таблица 1).

Таблица 1

Распределение утечек по виновникам

Виновник утечек	В России (%)	В мире (%)
Сотрудники	69,3	50,3
Внешние злоумышленники	21,3	41,7
Руководители	6,6	2,2
Подрядчики	2,2	2,0
Бывшие сотрудники	0,4	2,4
Системные администраторы	0,4	1,1

Что движет внутренним нарушителем? Основные причины: корысть и халатность. Побудительные корыстные и психологические мотивы нарушений такие же, как и у обычных преступников [3]. То есть киберпреступник – это преступник, имеющий соответствующие знания и квалификацию в сфере высоких технологий, позволяющие ему реализовывать свои преступные намерения и совершать противоправные действия именно в этой сфере.

Среди киберпреступников преобладает психотип «игрока», но, начиная совершать киберпреступления из «любви к чистому искусству», рано или поздно появятся корыстные мотивы. Но наибольшего эффекта хакер (либо другой внешний нарушитель) может добиться, обладая инсайдерской информацией, для чего он будет искать сообщников внутри организации.

Как видно из Таблицы 1 основные угрозы исходят от сотрудников, внешних злоумышленников, руководителей организации, а также подрядчиков. Именно они могут принести наибольший ущерб компании.

У сотрудников и руководителей разная мотивация. Если для рядовых сотрудников это просто корысть, то у руководителей преобладает утверждающий психотип, когда их возвышает мысль о владении и распоряжении определенной информацией [3]. А если руководитель приходит на «готовое» и не знает настоящей ее ценности, то он может разгласить важную информацию просто по халатности.

Введем в рассмотрение понятие благонадежности сотрудников организации. В толковом словаре В. Даля дается определение этого понятия, как надежность, прочность, твердость, основательность; несомненность, верность [4]. Будем полагать для облегчения расчетов, что значения благонадежности лежат на отрезке [0; 1]. Введем также в рассмотрение следующие градации благонадежности, приведенные в таблице 2.

Таблица 2

Уровень благонадежности	
Крайне низкий	[0; 0,3)
Низкий	[0,3; 0,5)
Средний	[0,5; 0,8)
Высокий	[0,8; 1]

В свою очередь благонадежность сотрудника (руководителя) зависит от его удовлетворенности материальным положением, работой (выполняемыми функциями, при этом творческая работа и работа с перспективой, как правило, дает большее удовлетворение, нежели повседневно повторяющаяся рутинная работа), заинтересованностью в конечном результате работы всего коллектива (а это зависит от продолжительности работы в организации (S_t – стаж), достижимости поставленных целей и задач).

При этом, понимая, что наибольшая угроза исходит из самой компании (инсайдерская угроза) или компаний - поставщиков внешних услуг, при использовании в процессе эксплуатации сложных систем аутсорсинга (облачные технологии, как частный случай такого аутсорсинга), то атмосфера излишней подозрительности, постоянный поиск потенциального нарушителя только добавляет нервозности в работе сотрудников и отрицательно влияет на конечный результат работы компании.

Чем больше стаж работы сотрудников в данной компании, меньше разброс зарплат $\Delta_з$, чем больше зависимость материального вознаграждения от конечного результата $K_з$ (% премии), а в случае руководства еще и ниже уровень доступа $K_д$ к информационным ресурсам компании, тем выше благонадежность сотрудников. Таким образом, благонадежность для простого *i*-го сотрудника

$$B_i' = B_i(S_t, \Delta_з, K_з) \tag{1}$$

а для *i*-го руководителя

$$B_i'' = B_i(S_t, \Delta_з, K_з, K_д). \tag{2}$$

Тогда средняя по организации благонадежность

$$M(B) = \overline{B} = \frac{1}{n_1}\sum_{i=1}^{n_1} B_i' + \frac{1}{n-n_1}\sum_{i=n_1+1}^{n} B_i'', \tag{3}$$

где n_1 – число простых сотрудников, а $n - n_1$ – число руководителей компании. Вычислив дисперсию благонадежности, используя среднее из (3), получаем отклонение значений благонадежности от среднего:

$$D(B) = M(B^2) - M^2(B). \quad (4)$$

Зависимость благонадежности и дисперсии показана на рис. 1. Таким образом, чем меньше дисперсия, тем выше благонадежность сотрудников и руководства.

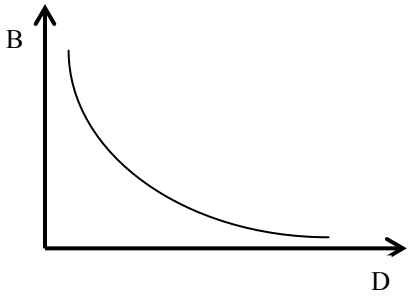


Рис. 1 – Зависимость благонадежности от дисперсии

Из (4) следует, что, чем меньше разброс в значениях благонадежности работников компании, тем ниже риски нарушения безопасности сложных систем предприятия по субъективным причинам.

Уменьшение дисперсии и увеличение благонадежности достигается за счет большей сплоченности коллектива, уменьшения текучести кадров и роста их профессионального уровня, увеличения зависимости размера материального поощрения от достигнутого результата каждым работником на определенном этапе.

Литература:

1. Кибер-риски в цифровом мире - Mains Insurance Brokers & Consultants 2017. [Электронный ресурс]. – Режим доступа: www.mainsgroup.ru. - (Дата обращения: 14.08.2017).
2. Утечки данных. Россия. 2017 год. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/report_ru2017. - (Дата обращения: 20.07.2017)
3. *Потапова Е.* Мотивация преступного поведения. Психология преступного поведения [Электронный ресурс]. – Режим доступа: http://fb.ru/article/306037/motivatsiya-prestupnogo-povedeniya-psihologiya-prestupnogo-povedeniya. - (Дата обращения: 04.09.2017)
4. *Даль В.И.* Толковый словарь живого великорусского языка" Т. 1-4. — М.: Русс. яз., 1989—1991.

Сиротюк В.О.

Разработка и реализация политики информационной безопасности организаций

Аннотация: Рассмотрены особенности разработки и внедрения правил, требований и норм политики информационной безопасности организаций на примере Евразийской патентной организации.

Ключевые слова: информационная безопасность, защита информации, конфиденциальность, целостность, доступность информации, политика информационной безопасности

Введение

Обеспечение высокого уровня безопасности информационных ресурсов, информационных технологий и инфраструктуры организаций является важной и актуальной задачей [1].

Основной стратегической целью организаций в области информационной безопасности (ИБ) является обеспечение конфиденциальности, целостности и доступности информационных ресурсов.

Для достижения поставленной цели руководство организации должно обеспечить разработку и внедрение в практику комплекса мер по поддержанию режима ИБ в организации. Задачей администрации при этом является выработка политики ИБ, содержащей набор общих формальных правил, которым должны подчиняться служащие организации и третьи лица, получившие доступ к информационным ресурсам, системам, технологиям и инфраструктуре организации [2].

Руководители структурных подразделений организаций должны отвечать за доведение положений политики ИБ до служащих, а специалисты ИТ - подразделения обеспечивать непрерывное и качественное функционирование информационных систем и технологий и отвечать за реализацию технических мер, необходимых для обеспечения необходимого уровня ИБ.

Реализация политики ИБ предусматривает принятие необходимых мер в целях защиты информационных ресурсов, информационных систем и инфраструктуры от случайного или преднамеренного изменения, раскрытия или уничтожения, обеспечения конфиденциальности, целостности и доступности информации, а также непрерывности технологических процессов автоматизированной обработки данных.

Разработка политики информационной безопасности

Рассмотрим правила, требования и нормы политики ИБ на примере разработки политики ИБ для Евразийской патентной организации (ЕАПО), выполняющей функции по приему и обработке заявок на изобретения, проведению патентного поиска и экспертизе заявок, выдаче патентов на изобретения и публикации заявок и патентов [2].

1. Правила доступа к информационным системам.

На рабочих местах служащих ЕАПО доступ к информационным ресурсам и системам ЕАПО должен быть обеспечен в рабочие дни с 8-00 до 19-30. Все работы выполняются служащими только на компьютерном оборудовании, закрепленном за сотрудниками.

Служащим может быть предоставлен удаленный доступ к информационным ресурсам организации, в соответствии с установленными для них правами в информационной системе. Служащим, работающим за пределами ЕАПО с использованием компьютера, не принадлежащего ЕАПО, запрещено копирование конфиденциальных данных на этот компьютер. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети ЕАПО, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

Любой вход в информационную систему должен осуществляться только с использованием уникального имени пользователя и пароля. Пользователям запрещается сообщать свой пароль или предоставлять свою учетную запись другим лицам.

Доступ к информационным ресурсам и системам, предназначенным для внешних пользователей, должен быть обеспечен круглосуточно. Правила доступа третьих лиц к информационным ресурсам и системам ЕАПО могут устанавливаться решениями распоряжениями руководства ЕАПО, условиями заключенных договоров и соглашений.

Доступ третьих лиц к внутренним информационным ресурсам и системам ЕАПО должен быть обусловлен только производственной необходимостью. Недопустимо предоставлять третьим лицам доступ к информационным ресурсам, системам и информационной инфраструктуре до тех пор, пока не установлены соответствующие мероприятия по управлению ИБ с учетом требований и норм политики ИБ ЕАПО.

2. Правила доступа к сети Интернет.

Доступ к сети Интернет регламентируется следующими основными правилами:

• запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит пропаганду расовой ненависти, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу религиозных

или политических убеждений, национального происхождения или недееспособности;

• служащие ЕАПО не должны использовать сеть Интернет для хранения конфиденциальной информации;

• служащим, имеющим учетные записи, предоставленные публичными провайдерами сети Интернет, не разрешается пользоваться ими на оборудовании, принадлежащем ЕАПО;

• служащие ЕАПО перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

• запрещается доступ в Интернет через сеть ЕАПО для всех лиц, не являющихся служащими ЕАПО, включая членов семей служащих.

Специалисты подразделения по обеспечению ИБ имеют право контролировать содержание всего потока информации, проходящего через канал связи к сети Интернет в обоих направлениях и вводить ограничения в соответствии со своими полномочиями, либо на основании распоряжений руководства ЕАПО или регламентирующих документов ЕАПО.

3. Защита информационной инфраструктуры.

Все компьютерное и коммуникационное оборудование и установленное на нем программное обеспечение должно использоваться исключительно в производственных целях.

Служащим ЕАПО запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят уполномоченные ИТ - специалисты.

Служащие ЕАПО должны принимать меры по обеспечению физической безопасности и сохранности компьютерного оборудования, закрепленного за ними, а также защите содержащейся на нем конфиденциальной информации.

Служащим запрещается устанавливать на компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности.

Все компьютеры должны быть оснащены средствами защиты от компьютерных вирусов и вредоносного программного обеспечения.

При разработке программного обеспечения сторонними организациями в техническое задание и в договор на разработку должны быть включены требования о соблюдении норм политики ИБ ЕАПО.

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на их пользователях.

Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения. При использовании

электронных носителей для хранения данных их следует периодически проверять на читаемость, как самих носителей, так и форматов данных в течение периода их хранения.

Только специалисты ИТ - подразделений на основании заявок руководителей подразделений могут создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

4. Правила пользования электронной почтой.

Содержание электронных сообщений должно соответствовать нормам деловой этики, принятым в организации. Электронные сообщения оформляются в соответствии с установленными в организации процедурами делопроизводства и подлежат такому же хранению, что и прочие средства письменных коммуникаций.

Использование служебных адресов электронной почты в личных целях не допускается.

Недопустимы следующие действия и случаи использования электронной почты:

• рассылка сообщений личного характера;

• рассылка рекламных материалов;

• подписка на рассылку, участие в дискуссиях и подобные услуги;

• поиск и чтение сообщений, направленных другим лицам;

•пересылка материалов, содержание которых является противозаконным.

Вложения, получаемые вместе с сообщениями, следует использовать с должной осторожностью.

5. Защита оборудования центра обработки данных (ЦОД).

Помещения ЦОД организации оборудуются системой кондиционирования, пожарной сигнализацией и системой оповещения о температурном режиме.

Доступ в помещения ЦОД разрешен только ответственным за их обслуживание специалистам ИТ - подразделений.

Доступ в помещения ЦОД посторонним лицам запрещен.

6. Сообщение об инцидентах ИБ, реагирование и отчетность.

Служащие обязаны сообщать подразделению по обеспечению ИБ об известных или подозреваемых ими нарушениях ИБ, а также ни при каких обстоятельствах не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

В свою очередь, ответственное за ИБ подразделение должно информировать служащих об известных способах или предполагаемых случаях нарушения ИБ. Контроль и учет сообщений об инцидентах для принятия соответствующих мер осуществляется в установленном порядке.

Если имеется подозрение или выявлено наличие вирусов или вредоносного программного обеспечения, то сразу после их обнаружения служащий обязан:

• проинформировать ответственное за ИБ подразделение;

• не пользоваться зараженным компьютером до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование компьютера специалистом по ИБ.

7. Обучение и повышение квалификации.

Служащих необходимо обучать процедурам безопасности и правильному использованию информационных систем, ресурсов и инфраструктуры с целью сведения к минимуму возможные риски ИБ.

Необходимо повышать квалификацию ИТ-специалистов в области ИБ с целью обеспечения высокого уровня безопасности организации.

Реализация политики информационной безопасности

Политика ИБ организации реализуется на основе подготовки и выпуска соответствующих распорядительных документов. В ЕАПО с этой целью разработаны следующие документы:

- нормативные документы в области ИБ в объеме, достаточном для обеспечения соответствия требованиям международного стандарта по ИБ ISO/IEC 27001:2013;

- уточненные с учетом требований и норм политики ИБ положения о структурных подразделениях и подразделения, ответственного за ИБ;

- инструкции пользователей по работе с информационными системами, ресурсами и технологиями;

- инструкции администраторов информационных систем;

- планы мероприятий по поддержанию работоспособности находящихся в эксплуатации автоматизированных информационных систем, включая планы проведения регламентных работ;

- планы восстановительных работ, направленных на ликвидацию последствий нарушений информационной безопасности и другие [3].

Нормативные правовые акты в области ИБ должны регулярно пересматриваться и развиваться с учетом новых требований к системе ИБ, выявленных уязвимых элементов, угроз и рисков ИБ.

С этой целью подразделение по обеспечению ИБ организует проведение аудита информационных систем, информационных ресурсов, информационной и обеспечивающей инфраструктуры, по результатам которого проводится пересмотр и развитие норм политики ИБ.

Заключение

В работе рассмотрены цели и задачи организаций в области ИБ в современных условиях, особенности разработки и внедрения политики ИБ

организаций. Рассмотрены правила, нормы и требования политики ИБ на примере ЕАПО, внедрение которых позволило повысить безопасность патентно-информационных ресурсов, информационной и обеспечивающей инфраструктуры патентной организации.

Литература:
1. Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. / *Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин* и др. - М.: Наука, 2006.
2. *Кульба В.В., Сиротюк В.О., Косяченко С.А.* Информационная безопасность патентных ведомств: теория и практика. – М.: ИПУ РАН, 2017. - 166 с.

Мистров Л.Е.

Об учете компетентности в задаче синтеза информационных систем безопасности

Аннотация: Предлагается подход к учету компетентности лиц, принимающих решение (ЛПР) в задаче синтеза предпочтительного варианта облика информационных систем безопасности (СБ) с учетом их априорной осведомленности о характеристиках составляющих его элементов (в первую очередь, подсистем).

Ключевые слова: информационная система безопасности, предпочтительный вариант, компетентность лиц, принимающих решения, априорная информационная осведомленность, энтропия, байесовский риск, апостериорная вероятность

1. Общие положения. Современные СБ характеризуются достаточно большим количеством параметров, наличием сложных зависимостей между ними, обусловливающих неопределенность в способах решения ими поставленных задач. Моделирование их функционирования на всех уровнях организационного построения представляет сложную и трудоемкую задачу, обусловливая для ее решения использование методов оптимизации для синтеза предпочтительного варианта построения.

В общем случае формирование СБ основывается на методе функционального синтеза решением задачи ее построения из m -го количества вариантов до уровня элементов. Его реализация осуществляется декомпозицией сформулированной в техническом задании (ТЗ) цели создания СБ на взаимосвязанную совокупность элементов с

установлением на уровнях соответствующего типа и функциональной принадлежности элементов. Основу выбора предпочтительного варианта СБ составляет компетентность ЛПР, от которой на этапах синтеза СБ в значительной мере зависят результаты выполнения требований ТЗ.

2. Постановка задачи. Основу синтеза СБ составляет обоснование ее облика как функции обликов ее элементов. При формировании СБ на этапе внешнесистемного синтеза существенные на этапе неполнота, неточность и размытость информации об ее облике и характеристиках элементов приводит к снижению информированности ЛПР о решаемых задачах СБ, условиях применения и ограничениях. Исследование компетентности ЛПР на этапе внутрисистемного синтеза для последующего уточнения СБ осуществляется в условиях вероятностной определенности информации, разрешимой при принятии соответствующих структуре СБ решений, например, на основе Байесовского подхода.

Пусть имеется j-ых. $j = 1,...,\ y_{ij}$ вариантов СБ, характеризуемых некоторым множеством $y_i \in D$ элементов. Каждый вариант y_i определяется множеством показателей эффективности СБ. Выбор варианта связан с определенным значением вектора критериев эффективности $U = (u_1(y_1), u_2(y_2),..., u_m(y_m))$ на множестве j-ых вариантов i-го типа элементов. Задача выбора СБ формулируется следующим образом.

Заданы: цель разработки (Z), условия (W) и ограничения (O) на построение СБ; облик j-го варианта i-го типа элементов $\{S_{ij}\}$; вектор выходных показателей качества элементов $\overline{Y} = (y_1, y_2,..., y_i,..., y_m)$

требуется для j-го варианта i-го типа элементов на S_{ij} множестве возможных вариантов облика СБ определить ее оптимальный вариант по экстремальному значению критерия эффективности в виде:

$$Q = \underset{Opt\, S_{ij}}{extr}\ U(Z, \overline{Y}, O, y_{ij}, S_{ij}, F_{ij}, W) \quad \forall y_i \in D, \tag{1}$$

при $D: D_1 \times D_2 \times ... D_m,\ A_i \le y_i \le B_i,\ i = \overline{1,m},\ f_\mu = (y_i) \le 0,\ \mu = 1,2,3,...$,

где $O_{Sij}\ \forall y \in D$ – метод оптимизации (оператор), реализующий правило выбора предпочтительного варианта СБ на $\{S_{ij}\}$ множестве возможных вариантов; y_{ij} – вариант СБ, характеризуемый $Y = (y_1,..., y_m)$ технико-экономических показателей качества i-го типа элементов и задающий параметрические ограничения на D область поиска решений, $y_i \in S_{ij}$; $U = (u_1(y_1), u_2(y_2),..., u_m(y_m))$ – вектор показателей эффективности (полезности) ИС; F_{ij} – информационная составляющая компетентности (ИСК) ЛПР, характеризующая его знания и умения при принятии решений относительно

j-го варианта i-го элемента СБ; A, B – параметрические ограничения на область поиска, представляющую множество вариантов решений; $f_{\text{ц}}$ – функциональные ограничения на D область поиска допустимых вариантов СБ.

3. Метод решения задачи. Основу синтеза СБ составляет: а) совокупность i-го типа элементов для генерирования вариантов СБ на $\{S_{ij}\}$ возможном множестве вариантов и б) методы поиска предпочтительного варианта по заданному критерию эффективности СБ.

В общем случае формирование СБ осуществляется направленным перебором $\{S_{ij}\}$ множества вариантов элементов на основе метода морфологического поиска. В соответствии с ним процесс синтеза j-го варианта СБ представляется цепочкой последовательных переходов $I_0 \to I_1 \to ... \to I_k \to ... \to I_{m-1} \to I_m$ содержательного преобразования информации. Он характеризует каждое состояние дерева решений $I_j = (S_{ij}, Q_j(F_{ij}))$ или j-е состояние процесса синтеза СБ, где S_{ij} – множество i-го типа элементов, идентифицированных в j-й точке процесса синтеза; Q_j – векторный критерий оптимизации выбора ЛПР предпочтительного варианта СБ; F_j – информационная характеристика компетентности ЛПР о данном состоянии процесса синтеза СБ.

Описание перехода $I_j \to I_i$ составляет основу синтеза СБ, который включает формализацию перехода $S_j \to S_i$, т.е. процессы генерирования вариантов и выбора среди них предпочтительного, что связано с представлением R_j пространства состояний СБ как функции ИСК F_{ij} ЛПР о j-ом варианте i-ых элементов.

Определим ряд понятий для формализации процесса синтеза СБ:

а) основное решение – представляет любой возможный вариант сгенерированного СБ, характеризуемый: перечнем i-ых элементов, включаемых в S_{ij} вариант СБ; точкой в p-мерном пространстве $\overline{Y} = (y_1, y_2, ..., y_p)$ выходных характеристик (ВХ) СБ; промежуточными решениями (ПР) $\{\overline{y}\}_{пр}$, которые представляются множеством точек в R^p пространстве состояний СБ; обобщенным решением $\{\overline{y}\}$ на множество всех возможных основных решений;

б) уровень принятия решений – характеризует степень информационной неопределённости сгенерированных вариантов СБ в отношении функциональной идентифицированности вариантов элементов.

Пусть для ПР неопределенность q-й компоненты y^q вектора $\overline{Y}$ относительно варианта i-го элемента выражается распределением $h^q(y^q)$. Полагается, что ЛПР имеет представление о каждом состоянии процесса синтеза СБ в виде F_{ij} ИСК, выражающейся функцией плотности вероятности $F_j = (f^1(\Theta^1), f^2(\Theta^2),..., f^q(\Theta^q),..., f^p(\Theta^p))$, где Θ^q – некоторый параметр распределения $h^q(y^q)$ относительно q-й компоненты, например, его среднее значение.

Переход от решения на i-ом уровне синтеза СБ к K-му решению на $(i+1)$-м уровне осуществляется на основе одноуровневого оператора O_{Sij}, формируемого математическими моделями оптимизации для получения j-го ПР или обобщенного решения на i-ом уровне элементов для: генерирования вариантов СБ с целью реализации K-го решения на $(i+1)$-ом уровне; оценки эффективности, т.е. определения результатов вычислений для различных вариантов элементов; выбора предпочтительного варианта решения, т.е. сравнения полученного варианта решения с другими вариантами того же $(i+1)$-го уровня.

Так как каждый оператор O_{Sij} связан непосредственно с конкретным i-ым типом элементов СБ, то предполагается, что ЛПР в состоянии его представить в виде некоторой функции правдоподобия $G_i = \{g_i^1(y^1 \mid \Theta^1), g_i^2(y^2 \mid \Theta^2),..., g_i^p(y^p \mid \Theta^p)\}$; $G_i^q = g_i^q(y^q \mid \Theta^q)$, определяющий степень правдоподобия (компетенции) ЛПР об информации данной выборки i-ых элементов.

Для организации процесса генерирования вариантов СБ или реализации перехода $S_j \to S_k$ используется информационно-эвристический подход [1] по упорядочению i-го типа элементов в целях конкретизации уровней иерархии в математических моделях принятия решений выбора, состоящий в усечении числа их вариантов на различных уровнях СБ на основе: фиксации вариантов элементов, изменение которых нежелательно вследствие их определяющей эффективности – это позволяет сформировать составляющую S^0 на верхнем уровне принятия решений; расположение элементов с незафиксированными вариантами по принципу убывания информационной значимости их влияния на достижение желаемых ВХ СБ, определяемых на основе вычисления энтропии сообщения $H(\Theta_i)$. Энтропия $H(\Theta_i)$ в предположении независимости ВХ i-ых элементов СБ вычисляется выражением:

$$H(\Theta_i) = \sum_{q=1}^{p} H_i^q, \text{ где } H(\Theta_i^q) = -\sum_{y}\sum_{\Theta} g_i(y^q \mid \Theta^q) \cdot \log g_i^q(y^q \mid \Theta^q). \qquad (2)$$

Пусть имеется N элементов СБ с незафиксированными j -ми вариантами решений. Тогда число уровней решений, различающихся степенью функциональной идентификации элементов в структуре СБ равно (N+1). Верхний (N+1)-й уровень соответствует представлению о СБ с фиксированными вариантами. Переход на N уровень осуществляется в результате подсоединения к фиксированному множеству на N уровне варианта элемента, информационная значимость влияния наибольшая. Каждый последующий уровень связан с функциональной идентификацией последующих элементов, проранжированных в соответствии с (2*)*.

Для каждого варианта решения на уровнях СБ формируется векторный критерий эффективности $Q = (u_1^j(y_1), u_2^j(y_2), ..., u_p^j(y_p))$, где в качестве $u_q^j(y_q)$ используется функция полезности, вычисляемая по формуле среднего Байесовского риска: $u_q = \sum_{y^q} p_{ij}^q \mu^q$, $q = \overline{1, p}$, где $p_{ij}(y^q)$ – вероятность получения y^q выходного результата при оценке эффективности j-го варианта на i-ом уровне СБ; $\mu^q(y^q)$ – степень полезности y^q выходного результата, определяемая Байесовским подходом.

Исходя из однородности f_j^q, как процесса приписывания не выявленному K -му решению той же информационной составляющей, что и на низшем уровне выявленному j-му решению, включающему K решение, ИСК ЛПР в процессе синтеза значение вероятности $p_{ij}(y^q)$ определяется в виде [1]: $p_{ij}^q(y^q) = \sum_{\Theta_q} g_i^q(y^q \mid f_j^q) f_j^q$.

Предположим, что в результате исследований получены решение K^* на $(i+1)$ -ом уровне и $\overline{Y}^*$ вектор ВХ СБ. Анализ ЛПР y^q результатов исследований по q-й компоненте вектора ВХ показывает, что его распределение по параметру $\Theta_{K^*}^q$ изменяется. Такое изменение определяется с помощью теоремы Байеса на основе функции правдоподобия для O_{Sij} оператора, который был применен для получения K^* решения.

Поскольку $f_j^q(\Theta^q) = f_{K^*}^q(\Theta^q)$, то можно записать:

$$f_j^{q^*}(\Theta^q \mid y^{q^*}) = \frac{f_j^{q^*}(\Theta^q) g_i^q(y^{q^*} \mid \Theta^q)}{p_{ij}^q(y^q)}, \qquad (3)$$

где $f_j^{q^*}(\Theta^q \mid y^{q^*})$ – апостериорное распределение ИСК ЛПР о q-й компоненте Θ параметра j-го варианта; $f_j^{q^*}(\Theta^q)$ – априорное распределение ИСК ЛПР о q-й компоненте Θ параметра j-го варианта решения.

Однако $\overline{Y}^*$ результат исследований не дает полной информации относительно всех решений в процессе синтеза СБ или не все априорные функции $F(\Theta)$ плотностей вероятности изменяются. В предположении, что информационные потоки при синтезе СБ строго "вертикальны", ЛПР пересмотр априорных вероятностей решений, включающих новое решение, осуществляется в соответствии с (3).

Для K^* решения q-я компонента ИСК F_{K^*} ЛПР равна:

$$f_{K^*}^{q^*}(\Theta^q \mid y^{q^*}) = f_j^{q^*}(\Theta^q \mid y^q), \quad q = \overline{1, p}.$$

ИСК ЛПР в K-й промежуточной точке синтеза СБ обусловлена предысторией процесса и не зависит от последовательности применения одноуровневых операторов O_{Sij}. Если решение было получено в результате последовательности из K этапов исследований, результаты которых представляют последовательность $H_j = (Y_1, Y_2, ..., Y_j)$, то апостериорное распределение ИСК ЛПР при синтезе предпочтительного варианта СБ после анализа j-го варианта, базирующееся на апостериорной вероятности выбора ЛПР j-го предпочтительного варианта СБ, вычисляется в виде:

$$f_j^{q^*(k)}(\Theta^q \mid H_{(k)}^q) = \frac{f^{q'}(\Theta^q)\prod_{m=1}^{j} g_{i(m)}^q(y_i^{q^*} \mid \Theta^q)}{\sum_{\Theta^q} f_j'^{q^*}(\Theta^q)\prod_{m=1}^{j} g_{i(m)}^q(y_i^{q^*} \mid \Theta^q)}.$$

Апостериорная вероятность выбора j-го варианта СБ отражает уровень компетентности ЛПР с учетом априорной его информированности о характеристиках составляющих элементов. Ее значение позволяет принимать решение об оптимальности предлагаемого ЛПР варианта СБ с вероятностью $f_j^{q^*(k)}(\Theta^q \mid H_{(k)}^q)$ на уровне уровня подсистем.

В заключение следует отметить, что метод может быть использован для решения задач синтеза облика СБ, требующих выбора ее предпочтительного варианта на множестве допустимых вариантов элементов с учетом компетентности ЛПР – специалистов синтеза.

Литература:
1. *Мальковская Л.И.* О процедуре эвристического синтеза технической системы на ранних этапах проектирования / Л.И. Мальковская, М.И. Ануфринчук. – М.: МВТУ им. Н.Э. Баумана, 1982.

Аникина Е.В.

Мониторинг информационной безопасности узлов гетерогенной сети на основе метода эффективного распределения сканеров

Аннотация: В работе рассматривается один из методов эффективного распределения ограниченного числа специализированных устройств (сканеров) для мониторинга информационной безопасности узлов гетерогенной сети.

Ключевые слова: гетерогенная сеть, мониторинг информационной безопасности, сканер безопасности, распределение ресурса, двудольный граф

Приоритетной целью государственной политики на современном этапе является ускоренный переход к цифровой экономике. Данный переход характеризуется интенсивным внедрением и использованием информационных технологий в сферах экономики и финансов, промышленности и энергетики, транспорта и связи, государственного и муниципального управления, обороны и безопасности, науки и культуры, образования и здравоохранения, и многих других. Однако, широкое использование информационных технологий немыслимо без повышенного внимания к проблемам их безопасности. И в первую очередь это относится к вопросам обеспечения информационной безопасности объектов *критической информационной инфраструктуры Российской Федерации* (далее – КИИ РФ) и КИИ РФ в целом. О том, что важность указанной проблемы отчетливо осознается, в том числе, на уровне Президента и Правительства Российской Федерации, говорит и недавно вступивший в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1].

В соответствии с [1] (статья 7) *категорирование* объекта КИИ РФ представляет собой установление соответствия объекта КИИ РФ критериям значимости, присвоение ему одной из категорий значимости и проверку сведений о результатах ее присвоения.

Категорирование объектов КИИ РФ осуществляется исходя из:

1) *социальной значимости*, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;

2) *политической значимости*, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;

3) *экономической значимости*, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам КИИ РФ и (или) бюджетам Российской Федерации;

4) *экологической значимости*, выражающейся в оценке уровня воздействия на окружающую среду;

5) значимости объекта КИИ РФ для *обеспечения обороны страны, безопасности государства и правопорядка*.

При этом устанавливаются три категории значимости объектов критической информационной инфраструктуры – первая, вторая и третья.

Для успешной реализации мероприятий по обеспечению безопасности объектов КИИ РФ и КИИ РФ в целом необходимо решение целого ряда сложных научно-технических задач, из которых задача мониторинга информационной безопасности КИИ РФ, в том числе, с помощью специализированных устройств, является одной из ключевых.

Именно решению задачи эффективного распределения ограниченного ресурса специализированных устройств (сканеров безопасности) для мониторинга информационной безопасности узлов гетерогенной сети, такой, как КИИ РФ или Интернет и будет посвящено дальнейшее содержание настоящей работы.

Необходимо отметить, что впервые близкая по постановке задача была рассмотрена в [2] (подробный анализ и библиографию см. там же), где рассматривалась проблема распределения ограниченного ресурса компьютерной системы, представленного некоторым количеством различных устройств между множеством пользователей, принадлежащих различным классам.

Ключевым отличием задачи, рассматриваемой в настоящей работе от задачи, представленной в [2], является переход от рассмотрения множества уникальных устройств к рассмотрению множества групп однотипных устройств, что представляет собой существенное обобщение и усложнение исходной задачи. Тем не менее, отдельные результаты, полученные в [2] будут использованы в данной работе.

Рассмотрим формальную постановку задачи.

Пусть имеется гетерогенная сеть, состоящая из узлов, относящихся к различным классам $\mathcal{K} = \{1, \dots, K\}$. Примерами таких сетей могут служить совокупность сетей, представляющих собой элементы КИИ РФ или Интернет. Обозначим X_k – количество узлов сети, относящихся к классу $k \in \mathcal{K}$ и $X = \sum_{k=1}^{K} X_k$ – общее количество узлов сети.

Положим, далее, что имеется некоторое количество специализированных устройств – сканеров для мониторинга информационной безопасности узлов сети (далее – сканер безопасности), также относящихся к различным классам $\mathcal{M} = \{1, \dots, M\}$. Обозначим Y_m – количество сканеров безопасности, относящихся к классу $m \in \mathcal{M}$ и $Y = \sum_{m=1}^{M} Y_m$– общее количество сканеров. Будем полагать, что сканеры безопасности различных классов обладают, в общем случае, различной эффективностью мониторинга информационной безопасности в отношении узлов сети, также относящихся к различным классам.

Вообще говоря, в качестве сканеров безопасности могут выступать не только специализированные устройства, но и программные агенты и даже эксперты и аудиторы информационной безопасности. Но, в рамках данной работы мы, будем предполагать, что сканерами безопасности будут являться именно специализированные устройства для мониторинга состояния узлов сети.

Будем считать, что эффективность (полезность) сканера безопасности класса $m \in \mathcal{M}$ является функцией от числа узлов, которые мониторит данный сканер: $\sigma_m(x)$, $m \in \mathcal{M}, x \in \mathbb{N}_0 = \{0, 1, 2, \dots\}$. В рамках данной работы, для простоты, будем полагать, что $\sigma_m(x)$ – вогнутая функция, которая не зависит от конкретных классов узлов, а определяется только общим числом узлов сети, мониторинг которых осуществляет данный сканер.

Обозначим $N_{m,k} \geq 0$ – максимальное число узлов класса $k \in \mathcal{K}$, которое может промониторить сканер безопасности класса $m \in \mathcal{M}$ и $N_m \geq 0$ – суммарное максимальное число узлов, которое может промониторить сканер безопасности класса $m \in \mathcal{M}$.

Необходимо отметить, что данное ограничение является вполне естественным, поскольку, с одной стороны, за конечный период времени любой сканер безопасности может проверить только ограниченное число узлов, а с другой, например, может оказаться, что сканер безопасности класса $m \in \mathcal{M}$ не может быть использован для мониторинга узлов класса $k \in \mathcal{K}$.

Таким образом, наша задача заключается в нахождении такого распределения узлов сети по сканерам безопасности, которое максимизирует суммарную эффективность (полезность) всех устройств пока удовлетворяются вышеприведенные ограничения.

Пусть $x_{m,k}^i$ – число узлов класса $k \in \mathcal{K}$, мониторинг которых осуществляет i-й сканер класса $m \in \mathcal{M}$, $i \in \{1, 2, \dots, Y_m\}$. Обозначим $x_m^i = \sum_{k=1}^{K} x_{m,k}^i$ – суммарное число узлов различных классов, мониторинг которых осуществляет i-й сканер класса $m \in \mathcal{M}$, $x_m = \sum_{i=1}^{Y_m} x_m^i$ – суммарное число узлов различных классов, мониторинг которых осуществляются сканерами класса $m \in \mathcal{M}$ и $z_k = \sum_{m=1}^{M} \sum_{i=1}^{Y_m} x_{m,k}^i$ – суммарное число узлов класса $k \in \mathcal{K}$, мониторинг которых осуществляется сканерами всех классов.

Тогда наша задача может быть формально записана следующим образом:

$$\sum_{m=1}^{M} \sum_{i=1}^{Y_m} \sigma_m(x_{m,k}^i) \rightarrow max \qquad \text{(Task)} \qquad (1)$$

при следующих ограничениях:

$x_{m,k}^i \in \{0, 1, \dots, N_{m,k}\}$,

$x_m^i \leq N_m$,

$z_k = X_k$,

$k \in \mathcal{K}$, $m \in \mathcal{M}$, $i \in \{1, 2, \dots, Y_m\}$.

При решении данной задачи в [3] был разработан базовый алгоритм на основе допустимого двудольного графа $G(\bar{X})$, реализующего все потенциальные распределения каждого узла сети по сканерам безопасности и допустимых назначений $\bar{X} = [x_{m,k}^i], T(\bar{X}, L), \bar{X}(j-1) = [x_{m,k}^i(j-1)]$.

Общий алгоритм решения задачи Task [3] представляет собой последовательное решение задач Task (j), при $j = 1, 2, \dots, X$, использующих базовый алгоритм [3]. Доказательство корректности работы алгоритма, а также основного результата настоящей статьи, являющегося обобщением Теоремы 1 из [2] представлено в [3].

Оценка вычислительной сложности алгоритма.

В работе [2] приводится оценка вычислительной сложности алгоритма, решающего задачу нахождения распределения ограниченного ресурса компьютерной системы, представленного некоторым количеством различных устройств между множеством пользователей, принадлежащих различным классам и имеющая вид: $O\ (M(LM + M^2 + LK))$, где M – число устройств, L – число пользователей и K – число классов пользователей.

Как уже говорилось выше, ключевым отличием задачи, рассматриваемой в данной работе, является переход от рассмотрения множества единичных устройств к рассмотрению множества групп однотипных устройств, что представляет собой существенное обобщение и усложнение исходной задачи. Тем не менее, поскольку, как и в [2]

решение задачи Task представляет собой последовательное решение задач Task (j), при $j = 1, 2, \dots, X$, то и в этом случае вычислительная сложность алгоритма решения задачи Task будет иметь вид: $O\ (Y(XY + Y^2 + XK))$, где Y – общее число сканеров безопасности, X – общее число узлов сети и K – число классов узлов.

Выводы

В работе была рассмотрена задача нахождения такого распределения узлов гетерогенной сети, относящихся к разным классам, по сканерам безопасности, также относящихся к разным классам, которое бы максимизировало суммарную эффективность (полезность) функционирования всех сканеров с учетом определенных для них ограничений. Был предложен общий алгоритм решения указанной задачи, доказана его корректность и проведена оценка его вычислительной сложности.

Необходимо отметить, что предложенный в данной работе метод эффективного распределения средств мониторинга информационной безопасности в рамках гетерогенной сети может быть успешно использован в рамках решения других задач. Например, при оценке безопасности КИИ РФ, в том числе, на основе метода вейвлет-анализа [4] или управления информационной безопасностью КИИ РФ на основе выявления ее аномальных состояний с использованием механизмов комплексной оценки [5] и кластерного анализа [6, 7].

Литература:

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Optimal a llocation o f multiple c lass r esources i n computer s ystems / A.N. Tantawi, G . T owsley, J . W olf // A CM S IGMETRICS P erformance Evaluation Review – 1988, May, Volume 16, Issue 1. P. 253-260.
3. Метод эффективного распределения сканеров для мониторинга информационной безопасности узлов гетерогенной сети/ А.О. Калашников, Е.В. Аникина // Информация и безопасность. – 2018. – Том 21. – № 4. – С. 455 – 464.
4. Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа / А.О. Калашников, Е.А. Сакрутина // Информация и безопасность. – 2017. – Том 20. – № 4(4). – С. 478 – 491.
5. Управление информационными рисками организационных систем: механизмы комплексного оценивания / А.О. Калашников // Информация и безопасность. – 2016. – № 3. – С. 315 – 322.

6. Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления ее аномальных состояний (часть 1) / А.О. Калашников, Е.В. Аникина // Информация и безопасность. – 2018. – Том 21. – № 2(4). – С. 145 – 154.
7. Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления ее аномальных состояний (часть 2) / А.О. Калашников, Е.В. Аникина // Информация и безопасность. – 2018. – Том 21. – № 2(4). – С.155 – 164.

Мирошник С.Н.

Построение верхней оценки межфайловой избыточности в БД реального времени

Аннотация: Настоящая работа является развитием результатов, описанных в [1], в которой приведены формулы для вычисления оценки внутрифайловой избыточности I_1 для одного файла и посвящена вычислению оценки для межфайловой избыточности в упрощённой постановке задачи.

Ключевые слова: база данных, межфайловая избыточность, файл, модуль, информационное поле

1. Введение

Рассматривается задача построения БД реального времени с минимальной избыточностью. Особенность такой БД состоит в том, что информация в БД обновляется с определенной частотой. Между обновлениями необходимо решить ряд задач, которые используют набор вычислительных модулей. Перед очередным обновлением информации все задачи должны быть решены. Отсюда достаточно жесткие требования к времени доступа модулей к информации в БД в реальном времени. Для выполнения этих требований необходимо минимизировать такую характеристику БД как ее избыточность. Проблема избыточности подробно исследована, что отражено в многочисленных публикациях. Понятие информационной избыточности используется в теории информации, и означает превышение количества информации над его информационной энтропией как мерой неопределенности информации [2, 3, 4, 5]. В БД, которая строится в данной работе, эта неопределенность, состоит в дублировании информации в БД.

2. Постановка задачи

Задан набор программных модулей $\{M\}_N$, которые используют информацию, содержащаяся в наборе полей $\{\phi\}_r$. Здесь N – количество

модулей, r – число полей. Все поля пронумерованы натуральным рядом чисел. Каждый из модулей M_i использует все поля своей записи длиной l_i, $i = 1,\ldots, N$. Записи не содержат неиспользуемые поля.

В работе [1], посвященной минимизации внутрифайловой избыточности, модули определенным образом объединяются в различные группы (файлы), причем каждый модуль содержится только в одном файле. Пусть построены файлы $F_1,\ldots, F_k$. В настоящей работе исследуется межфайловая избыточность. Эта избыточность образуется, когда файлы имеют общие поля. При работе БД в реальном времени поля каждого файла заполняются информацией отдельно, то есть общие поля файлов заполняются многократно. В этом проявляется межфайловая избыточность БД. В настоящей работе исследуется эта избыточность. Строится ее верхняя оценка при заданных числах N и r.

3. Вычисление верхней оценки межфайловой избыточности файлов $F_1,\ldots, F_k$

Воспользуемся гипотетической моделью, упрощающую исходную задачу и позволяющую построить верхнюю оценку межфайловой избыточности. Определим упорядоченную последовательность близких модулей. Понятие близких модулей используется во многих работах автора и означает сравнение совпадающих и несовпадающих полей модуля из некоторого набора близких модулей как целого. Будем считать, что все модули имеют одинаковую длину l, но пара последовательных модулей отличается одним полем. Таким образом строится весь набор близких модулей относительно одного модуля, который назначен опорным. Число таких модулей в одной группе легко вычисляется. Эти близкие модули вместе с опорным образуют группу. Таким образом, строятся все возможные группы близких модулей.

Теперь исходная задача преобразуется. Заданы модули $M_1,\ldots, M_N$ – одинаковой длины l. Длина модуля есть число используемых этим модулем информационных полей. Модули объединяются в группы $F_1,\ldots, F_k$ так, как описано в [1]. С учетом упорядоченности модулей и использованием понятия близости первую группу F_1 образуют модули $M_1,\ldots, M_n$ – первые n модулей из последовательности. Группу F_2 образуют следующие n модулей и т.д.

Все модули всех групп используют информацию из исходного набора полей $\phi_1,\ldots, \phi_r$, r – число полей. Число модулей в файлах есть $d = l-2$ (кроме опорного), причем $L= l + d$ – длина L каждого файла, где d – расширение полей опорного модуля.

Так как все модули отличаются только одним полем, то d есть число модулей в файле, кроме опорного. Здесь $n = l – 1$ – число модулей в файле. Заметим, что определенные таким образом группы имеют попарно общие

поля. В дальнейшем будет показано, что файлы через один не пересекаются.

3.1. Вычислим число общих полей на примере двух последовательных файлов F_1 и F_2. Для этого воспользуемся формулой, приведенной в [1]. В данном случае эта формула имеет вид:

$$I_2(F_1, F_2) = 2(l + d) - \tilde{r}\ .$$

Здесь $l+d$ – длина каждого из файлов F_1 и F_2. $\tilde{r}$ – сумма различных полей для F_1 и F_2. Заметим, что $I_2(F_1, F_2) < l$. Покажем это. Пусть $I_2 = l$. Но I_2 есть число общих полей для F_1 и F_2. Равенство означает, что существует модуль, принадлежащий обоим файлам. Отсюда: $I_2(F_1, F_2) = l-1$.

Вычислим $\tilde{r}$. Получаем:

$$\tilde{r} = 2(l + d) - (l - 1).$$

Но $d = l-2$, тогда $\tilde{r} = 3(l - 1)$.

Из выражения для I_2, следует, что файл F_2 увеличивает общую длину обоих файлов на $l-1$.

3.2. Вычислим $I_2(F_1,..., F_k)$.

Построены k одинаковых файлов $F_1,..., F_k$, каждый длиной $L = l+d$. Тогда

$$I_2(F_1,..., F_k) = \sum_{i=1}^{k} L_i - r_k, \text{ или}$$

$$I_2(F_1,..., F_k) = k(l + d) - r_k,$$

где r_k – число полей, которые используют файлы $F_1,\ldots, F_k$, $r_k \le r$, r – число заданных полей в исходной задаче, k – заданное число файлов. Вычислим r_k для k файлов.

Каждый файл увеличивает общую длину полей на $l-1$. Тогда: $r_k = (l+d)+(l-1)(k-1)$ или $r_k = (l-1)(k+1)$.

Теперь используемая оценка избыточности для $F_1,..., F_k$ при заданном числе файлов есть:

$$I_2(F_1,...,F_k) = (l-1)(k-1)$$

Далее рассмотрим исходную задачу, в которой число полей r задано. Оценим наибольшее число файлов, построенных в модели для r полей. Воспользуемся формулой для r_k. Тогда $k = \left[\frac{r_k}{l-1}\right] - 1$. Заменим в формуле r_k на r и $k = \left[\frac{r}{l-1}\right] - 1$. Заметим, что последний файл в списке может содержать меньшее число модулей.

Модули последнего файла используют поля числом $r - r_k$.

3.3. Рассмотрим более подробно расположение используемых группами $F_1,..., F_k$ полей. Покажем, что файлы $F_1,..., F_k$ имеют общие поля попарно,

т.е. F_t и F_{t+2} не имеют общих полей. В постановке задачи отмечено, что все поля пронумерованы, т.е. поле ϕ_t имеет номер t. Вычислим номера первых и последних полей каждого файла. Номера первого поля ϕ_t^1 файла F_t есть:

$\phi_t^1 = (t-1)(l-1)+1.$

Номер последнего поля ϕ_t^2 файла F_t есть:

$\phi_t^2 = (t+1)(l-1), \quad t = 1,...,k.$

Проверим неравенство: первое поле для F_{t+2} больше последнего поля для F_t. Получаем очевидное неравенство:

$(t+1)(l-1) < (t+1)(l-1)+1.$

В частности, отсюда следует вывод, что первое поле для F_{t+2} является следующим полем после последнего поля для F_t.

3.4. Покажем, при каких условиях объединение модулей в файлы уменьшает количество межфайловой избыточности для частного случая, когда r не задано, т.е. $N = k \cdot n$.

Пусть каждый модуль является отдельным файлом длиной l. Тогда

$I_2(M_1,..., M_N) = l \cdot N - r,$

где l – длина каждого модуля, N – число модулей, r – число полей, используемые этими модулями.

С другой стороны, пусть модули объединены в файлы $F_1,..., F_k$, так, как это описано в разделе 3. Межфайловая избыточность для $F_1,..., F_k$ есть

$I_2(F_1,...,F_k) = k(l+d)-r,$

где $l+d$ – длина каждого файла, $(d = l-2)$; k – число файлов.

Покажем, что $I_2(M_1,..., M_N) > I_2(F_1,..., F_k)$. Подставляя в неравенство формулы для $I_2(M_1,..., M_N)$ и $I_2(F_1,..., F_k)$ получаем:

$N \cdot l > k(l+d).$

По условию все файлы одинаковые и содержат равное количество модулей. Тогда $N = k \cdot n$, где n – число модулей в файле. Отсюда: $k \cdot n \cdot l > k2(l-1)$. Так как $n = d+1$, или $n = l-1$, тогда $l > 2$.

Вывод: объединение модулей по группам предпочтительнее, если каждый модуль использует больше двух полей.

4. Заключение

Таким образом, с помощью модели, упрощающей исходную задачу, построена верхняя оценка межфайловой избыточности файлов. Также на основе модели проведено некоторое исследование, отраженной в пунктах 1, 2, 3, 4, а именно:

Вычислено возможное число общих полей на примере двух файлов.

Вычислены общие поля для набора файлов и оценка межфайловая избыточность.

Показано, что файлы имеют общие поля только попарно.

Определено минимальное число используемых модулями полей, при котором объединение модулей в файлы лучше с точки зрения минимизации межфайловой избыточности.

Литература:
1. *Мирошник С.Н.* Алгоритмы построения базы данных с минимальной избыточностью информации для систем реального времени // Труды межд. конф. по исследованию операций ORM – 2016. – М.: ФИЦ ИУ РАН, 2016. – С. 51-52.
2. *Шеннон К.Э.* Работы по теории информации и кибернетике. – М.: ИЛ., 1963. – 829 с.
3. *Мартин Н., Ингленд Дж.* Математическая теория энтропии. – М.: Мир, 1988. – 251 с.
4. *Колмогоров А.Н.* Три подхода к определению понятия «количества информации». / Проблемы передачи информации. – 1965 – т. 1. – № 1. – С. 3–11.
5. *Jan Lindstream*. Real time database System. Solid and IBM Company: Italahdenkatn, Finland, March 25, 2008.

Сакрутина Е.А.

К вопросу оценки рискового потенциала значимых объектов критической информационной инфраструктуры

Аннотация: В работе рассматривается модель прогнозирования рискового потенциала для системы мониторинга угроз безопасности выхода технологического процесса на аварийные режимы на значимых объектах критической информационной инфраструктуры.

Ключевые слова: критическая информационная инфраструктура, значимый объект критической информационной инфраструктуры, оценка рискового потенциала

Приоритетной целью государственной политики на сегодняшний день является обеспечение информационной безопасности объектов критической информационной инфраструктуры Российской Федерации. В соответствии с действующим Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – ФЗ от 26.07.2017 № 187-ФЗ), введены такие понятия как: критическая информационная инфраструктура (далее – КИИ), объекты КИИ, субъекты КИИ, значимый объект КИИ (далее –

ЗОКИИ), безопасность КИИ. К ЗОКИИ относятся крупные гидротехнические сооружения, объекты атомной энергетики, вредные химические производства, нефтеперерабатывающие заводы, газопроводы, транспортные системы и т.п. Сбой в работе любого из объектов ЗОКИИ может отразится на здоровье, безопасности и благосостоянии граждан.

В соответствии с ФЗ от 26.07.2017 № 187-ФЗ будем полагать, что КИИ РФ состоит из объектов двух основных типов: ЗОКИИ и сетей электросвязи, используемые для организации взаимодействия таких объектов. Состояние ЗОКИИ может быть описано текущим уровнем информационной безопасности (далее – УИБ) и связанным с ним рисковым потенциалом (далее – РП). УИБ ЗОКИИ определяется текущим уровнем информационных угроз (далее – УИУ) и текущим уровнем защищенности (далее – УЗ) ЗОКИИ. В свою очередь, РП представляет собой прогнозную оценку последствий нарушения функционирования ЗОКИИ, при реализации компьютерных атак на ЗОКИИ и возникновении в результате этого компьютерных инцидентов. Оценка РП ЗОКИИ может быть представлена в многокритериальной (векторной) форме, учитывающей РП ЗОКИИ по отдельным направлениям, определенным ФЗ от 26.07.2017 № 187-ФЗ. На основании векторной оценки РП может быть построена интегральная оценка РП ЗОКИИ. При оценке РП ЗОКИИ следует отметить следующие особенности: во-первых, интегральный РП ЗОКИИ складывается из совокупности локальных РП ЗОКИИ, во-вторых, РП ЗОКИИ можно измерить лишь качественно (высокий, средний, низкий), в-третьих, оценка РП ЗОКИИ носит субъективный характер [1].

Воздействие компьютерных атак на информационно-технологическую инфраструктуру (далее – ИТИ) ЗОКИИ, приводящее к выходу ее технологических параметров за установленные нормативные пределы, может повлечь за собой реализацию нештатных ситуаций с тяжелыми и даже катастрофическими последствиями. Для успешной реализации мероприятий защиты ЗОКИИ необходимо решение ряда задач, из которых система мониторинга угроз безопасности является основной.

В последние годы, системные причины многих инцидентов на ЗОКИИ привели к существенному повышению интереса к процедурам идентификации и управления рисками [2], а также разработке и развитию проактивных моделей. Проактивные модели дают оценку РП выявленных факторов прежде чем произойдет инцидент и окажет влияние на функционирование ЗОКИИ.

Предположим, что модель ЗОКИИ состоит из трех взаимосвязанных уровней (Рис. 1). Подробнее см., например, [3].

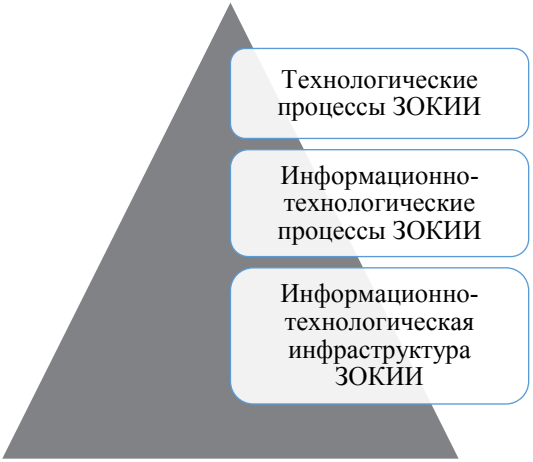


Рис. 1 – Уровни модели ЗОКИИ

Верхний уровень – уровень «технологических» (бизнес) процессов (далее – ТП) ЗОКИИ. Состояние ТП может быть описано текущим вектором значений параметров $X^{ТП}(t)=\{x_1^{ТП}(t),\ldots, x_N^{ТП}(t)\}$. Состояние ТП ЗОКИИ, в свою очередь, определяет текущий РП ЗОКИИ $R(t)=\{r_1(t),\ldots,r_p(t)\}$. Если значения вектора параметров не выходят за границы эксплуатационных пределов и установленных условий функционирования ЗОКИИ, то такое состояние ТП ЗОКИИ может считаться нормальным, а РП ЗОКИИ соответствует допустимому уровню. В противном случае, состояние ТП ЗОКИИ может считаться аварийным, а РП ЗОКИИ будет превышать допустимый уровень.

Средний уровень – уровень информационно-технологических процессов (далее – ИТП). Состояние ИТП также может быть описано вектором параметров $X^{ИТП}(t)=\{x_1^{ИТП}(t),\ldots,x_M^{ИТП}(t)\}$ (в общем случае отличным от вектора параметров ТП). Для обеспечения нахождение ТП в нормальном состоянии, значения вектора параметров ИТП также должны находиться в определенных диапазонах, которые будем считать диапазонами нормальных значений параметров ИТП.

Нижний уровень – уровень информационно-технологической инфраструктуры (далее – ИТИ) ЗОКИИ, обеспечивающий нормальное функционирование ИТП ЗОКИИ. Будем считать, что состояние ИТИ может быть описано вектором параметров $X^{ИТИ}(t)=\{x_1^{ИТИ}(t),\ldots,x_S^{ИТИ}(t)\}$ (в общем случае отличным от вектора параметров ТП и ИТП). Тогда, чтобы обеспечить нахождение ИТП в нормальном состоянии, значения вектора параметров ИТИ должны находиться в некоторых определенных

диапазонах, которые будем считать диапазонами нормальных значений параметров ИТИ. Если значения вектора параметров ИТИ находятся в пределах указанных выше диапазонов нормальных значений, то такое состояние ИТИ ЗОКИИ может считаться нормальным. Если значения вектора параметров ИТИ выходят за диапазоны нормальных значений, то такое состояние ИТИ ЗОКИИ может считаться аварийным. Следовательно, параметры вектора состояния ИТИ ЗОКИИ будем называть критическими переменными состояния.

Таким образом, можно считать, что существует определенная «функциональная» зависимость между состоянием ИТИ ЗОКИИ и РП ЗОКИИ. При построении модели ЗОКИИ представляется достаточным ограничиться построением параметрической модели ИТИ ЗОКИИ и некоторой регрессионной моделью, описывающей зависимость вектора РП от параметров ИТИ. Теоретические аспекты критических переменных состояния и их экстремальных значений нашли свое применение при описании ИТИ ЗОКИИ [3]. Примерами могут служить работы [1, 2, 4].

Предположим, что данные об оценках РП и критических переменных состояния ИТИ ЗОКИИ содержатся в некоторой пополняемой базе знаний (далее – БЗ), в которую заносятся данные о функционировании ИТИ ЗОКИИ. Пусть $x_1(t),\ldots,x_S(t)$ – параметры состояния ИТИ ЗОКИИ (включая критические переменные состояния), $X(t)$ – состояние ИТИ ЗОКИИ характеризующееся вектором параметров состояния ИТИ ЗОКИИ в момент времени t, $R(t)$ – РП состояния $X(t)$ ИТИ ЗОКИИ в момент времени t. Процесс обработки исторических данных в базе знаний сводится к ассоциативному поиску состояний ИТИ ЗОКИИ близких к текущему в базе знаний. Критерий близости между состояниями может быть представлен в виде расстояния в n-мерном пространстве.

В работах [5, 6] предложен подход к формированию поддержки принятия решения об управлении, основанный на динамическом моделировании процедуры ассоциативного поиска. Прогнозирование РП ИТИ ЗОКИИ заключается в качественной оценке локальных РП по прогнозу на основе ассоциативного поиска критических переменных состояния в части выхода за диапазоны нормальных значений.

Литература:

1. *Калашников А.О.* Управление информационными рисками организационных систем: механизмы комплексного оценивания / А.О. Калашников // Информация и безопасность. – 2016. – № 3. – С. 315-322.
2. *Sakrutina E.* Some Functions of the “Safety management system” in the Transportation Area Safety Assurance / E. Sakrutina // Proceedings of 2017 International Siberian Conference on Control and Communications (SIBCON) – 2017. – P. 1-5.

3. К вопросу о дискретизации критичных переменных состояния информационно-технологической инфраструктуры критически важного объекта / А.О. Калашников, Е.В. Ермилов, М.В. Бурса, Р.К. Бабаджанов, В.А. Кургузкин // Информация и безопасность – 2014. – Т. 17. № 4. – С. 536-547.
4. Методика управления информационными рисками атакуемых автоматизированных систем управления критически важных объектов / Е.В. Ермилов, А.О. Калашников // Информация и безопасность. – 2013. – Т. 16. № 3. – С. 379-382.
5. Идентификация систем на основе вейвлет-анализа / Е. А. Сакрутина, Н. Н. Бахтадзе // Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва) – 2014. М.: ИПУ РАН. С. 2868-2889.
6. Multi-agent Approach to Design of Multimodal Intelligent Immune System for Smart Grid / N.N. Bakhtadze, I.B. Yadykin, V.A.Lototsky, E. M. Maximov, E. A. Sakrutina // IFAC Proceedings Volumes – 2013. Vol. 46, № 9. P. 1164-1169.

Сомов С.К.

Обеспечение безопасности и производительности распределенных систем методами репликации массивов данных

Аннотация: В работе рассмотрен подход к решению задачи оптимального размещения реплик нескольких массивов данных в распределенной системе. В распределенной системе используются реплики нескольких массивов данных. Каналы связи распределенной системы ненадежны. Разные массивы могут иметь разное количество реплик. Критерий оптимизации задачи это минимум среднего времени ответа системы на запрос к репликам. Предложен эвристический алгоритм решения сформулированной задачи.

Ключевые слова: безопасность распределенных систем, репликация массивов данных, компьютерные сети

Эффективным методом повышения производительности и обеспечения высокого уровня безопасности распределенных систем обработки данных с ненадежными каналами связи является использование реплик массивов данных [1-3]. Оптимальное размещение в узлах распределенной системы нескольких реплик массива данных позволяет решить две основные задачи проектирования распределенных систем. Во-первых, наличие в сети нескольких узлов с идентичными данными реплик позволяет перенести

обработку запросов к реплике с одного узла сети на другой узел с такой же репликой в случае, если первый узел вышел из строя. Данная возможность позволяет повысить безопасность работы всей распределенной системы. Во-вторых, реплики массивов данных размещаются в узлах системы таким образом, чтобы максимально сократить расстояние от этих улов до узлов – источников запросов к репликам. Это приводит к увеличению производительности распределенной системы.

В статье рассматривается задача оптимального размещения реплик нескольких массивов данных в узлах распределенной системы обработки данных. Распределенная система функционирует на базе компьютерной сети с ненадежными каналами связи. В качестве критерия оптимизации задачи используется минимум среднего времени реакции системы на запросы к данным. Ограничениями задачи являются максимальная величина затрат на функционирование системы и ограничение на максимальное количество реплик, которые можно разместить в одном узле сети.

В узлах распределенной системы выполняется несколько прикладных процессов (задач) разных типов, которые инициируются пользователями системы. Каждая задача генерирует информационные запросы и/или запросы на модификацию массивов данных. Распределенная система функционирует на базе компьютерной сети, состоящей из N узлов. Топология сети представлена взвешенным графом $G = (X, \Gamma)$. Заданы длины дуг графа. В системе используется M $(m = \overline{1, M})$ массивов данных разного типа. Сеть передачи данных системы состоит из Φ $(\varphi = \overline{1, \Phi})$ каналов связи. Пропускная способность каждого -го канала связи равна C_φ единиц данных. Пусть $q_\varphi^* = 1 - \rho_\varphi^*, (\varphi = \overline{1, \Phi})$ это вероятность возникновения ошибки в φ-м канале. Успешность доставки сообщений подтверждается квитанций ACK (*ACKnowledgement*). Пусть t_{ACK} - время ожидания узлом-отправителем квитанции ACK о доставке сообщения. Частота решения задач в узлах системы задана матрицей $F^* = \left\| f_{nj}^* \right\|$ $(n = \overline{1, N};\ j = \overline{1, J})$, где f_{nj}^* это частота решения в n-м узле сети задачи j-го типа. Матрица $E^* = \left\| e^*{}_{jm} \right\|$, определяет частоту $e^*{}_{jm}$ – генерации задачей j-го типа информационных запросов к массиву m-го типа. Матрица $U^* = \left\| u^*{}_{jm} \right\|$ определяет частоту $u^*{}_{jm}$ генерации задачей j-го типа запросов на модификацию массива данных m-го типа. Время обработки каждого запроса в любом узле системы одинаково и равно T_{pr}.

Распределение реплик M массивов данных по узлам системы описывается элементами матрицы $A = \|a_{nm}\|$, в которой $a_{nm} \in \{0,1\}$, и $a_{nm} = 1$, если в n-м узле сети размещена реплика массива m-го типа. Определена матрица $SP = (sp_{nk})_{N \times N}$ кратчайших путей в графе G, где элемент sp_{nk} равен длине кратчайшего пути между узлами n и k [4].

Требуется разместить несколько реплик M массивов данных по узлам распределенной системы обработки данных таким образом, чтобы обеспечить минимальное значение функционала *F(A)*:

$$min\, F(A) = min(\tilde{T} + T_{pr} + \tilde{T}) \quad (1)$$

Здесь:

- $\tilde{T}$ - Среднее время передачи запроса в узел системы с репликой.
- T_{pr} – Среднее время обработки запроса.
- $\tilde{T}$ – Среднее время передачи ответа на запрос.

В задаче используются ограничения:

- на стоимость OP_{cost} функционирования системы (стоимость хранения реплик и обработки запросов в узлах сети, стоимость использования каналов связи системы):

$$OP_{cost} \le COST_{MAX} \quad (2)$$

- на максимальное RN_{MAX_n} количество реплик массивов, размещенных в отдельных узлах системы:

$$\sum_{m=1}^{M} a_{nm} \le RN_{MAX_n}, \quad n = \overline{1,N} \quad (3)$$

Сформулированная задача обладает большой вычислительной сложностью. Поэтому для ее решения предложен эвристический алгоритм, который описан ниже.

- Шаг 1. Подсчитывается частота fr_m запросов к каждому *m*-му массиву данных, которые генерируются в системе при решении задач пользователей во всех *N* узлах системы:

$$fr_m = \sum_{n=1}^{N} f_{nj}^{*} \left({v^*}_{jm} + {u^*}_{jm} \right);\ m = \overline{1,M}$$

- Шаг 2. Сортируются номера всех M массивов данных в порядке убывания соответствующих значений частот fr_m ($\mathrm{m} = \overline{1,\mathrm{M}}$).
- Шаг 3. Формируется вектор $VM = \langle vm_k \rangle, k = \overline{1,\mathrm{M}}$. Элемент vm_1 содержит номер массива, к которому генерируется наибольшее количество запросов. Элемент vm_M содержит номер массива данных, к которому генерируется наименьшее количество запросов.
- Шаг 4. Задается минимальное P_{min} и максимальное P_{max} количество узлов сети для размещения реплик каждого из M массивов данных.
- Шаг 5. В цикле по количеству p узлов с репликами, ($P_{min} \le p \le P_{max}$) выполняются шаги алгоритма с 6 по 11:
- Шаг 6. Поочередно в цикле выбираются номера vm_k ($k = \overline{1,\mathrm{M}}$) массивов данных из вектора VM.

Для каждого очередного *m*-го массива данных выполняются действия:

- Случайным образом из множества *X* узлов сети выбираются p узлов для распределения в них реплик *m*-го массива.
- Номера отобранных узлов образуют множество $X_p^m = \{x_{pi}^m \mid i = \overline{1,p}\}$. Элемент x_{pi}^m содержит номер *i*-го узла сети, в котором размещается одна из реплик *m*-го массива данных. Номера этих узлов заносятся в

множество X_m «протестированных» узлов. Остальные номера узлов множества X, не вошедшие в X_p^m, заносятся в множество $\bar{X}_m$ номеров «не протестированных» узлов. Т.е. $\bar{X}_m = \{X \backslash X_p^m\}$.

- Шаг 7. Присваивается значение A^{p*} тем элементам a_{nm}^p m-го столбца матрицы A^p, у которого номер n строки матрицы равен номеру x_{pi}^m узла сети с репликой.

Матрица $A^p = \|a_{nm}^p\|$ определяет распределение p реплик каждого из M массивов по узлам сети. Элемент $a_{nm}^p \in \{0,1\}$ матрицы равен *"1"*, если в узле n размещена реплика m-го массива.

- Шаг 8. Для матрицы $A^p = \|a_{nm}^p\|$ выполняются операции:
  - Подсчитывается значение функционала $F(A^p)$ в соответствии с (1).
  - Запоминаем полученное значение: $F_{min}^p = F(A^p)$
- Шаг 9. В цикле поочередно выбираются номера vm_k $(k = \overline{1, M})$ массивов данных из вектора VM.

  Для каждого очередного m-го массива данных выполняются действия:
  - Из множества $\bar{X}_m$ номеров «не протестированных» узлов случайным образом выбирается номер узла сети и запоминаем его в переменной x_i^{m*}.
  - Если «не протестированных» узлов больше нет, то возврат к шагу 9.
- Шаг 9.1. В цикле каждую вершину x_{pi}^m из множества $X_p^m = \{x_{pi}^m | i = \overline{1, p}\}$ заменяем на вершину x_i^{m*} .
  - Получаем новое множество X_p^{m*} в котором одна из вершин заменена на вершину x_i^{m*}.
  - Создаем копию матрицы A^p в виде матрицы A^{p*}.
  - Аналогично шагу 7 присваиваем значение «1» элементам a_{nm}^{p*} m-го столбца матрицы A^{p*} в соответствии со значениями элементов множества X_p^{m*}.
  - Подсчитываем значение функционала задачи $F(A^{p*})$ для матрицы A^{p*}.
  - Если $F(A^{p*}) \geq F_{min}^p$ то возврат к Шагу 9.1.
  - Проверяем выполнение ограничений задачи (2) и (3) для нового распределения реплик A^{p*}.
  - Если одно или оба ограничения нарушены, возвращаемся на Шаг 9.1.
  - Запоминаем новое значение функционала и новое распределение реплик:
  - $F_{min}^p = F(A^{p*})$, $A^p = A^{p*}$
  - Если цикл по вершинам множества X_p^m не завершен, то возвращаемся на Шаг 9.1.
  - Иначе возвращаемся на Шаг 9.
- Шаг 10. Если просмотрены не все массивы данных из вектора VM, возвращаемся на Шаг 6.

- Шаг 11. Если цикл по количеству p реплик не завершен $(p < P_{max})$, то возвращаемся на Шаг 5.
- Шаг 12. Поиск распределения реплик всех M массивов данных закончен.

Найдено близкое к оптимальному распределение реплик A^p. Найденное распределение обеспечивает значение среднего времени ответа системы на запрос, равное F_{min}^p.

Конец работы алгоритма.

Представленный алгоритм реализован в среде разработки MS Visual Studio на языке программирования C++. Используется в составе автоматизированного комплекса поддержки принятия решений в области обеспечения сохранности данных в распределенных системах.

Литература:

1. *Сомов С.К.* Репликация как инструмент повышения надежности функционирования распределенных систем/ Информационные технологии и вычислительные системы 2018, с.69-79.
2. *Микрин Е.А., Сомов С.К.* Обзор моделей и методов обеспечения сохранности данных в распределенных системах обработки данных/Информационные технологии и вычислительные системы, 4/2017. С. 5-28.
3. *Charron-Bost B., Pedone F., Schiper A.* (ed). Replication: T heory a nd Practice. (Lecture Notes i n C omputer S cience. v. 5959). - New Yo rk: Springer, 2010. — 290 p.
4. *Cormen T.H., et al.* Introduction to Algorithms, Third Edition. — The MIT Press, 2009. — 1313 p.

Асратян Р.Э.

Защита информационных запросов в распределенных системах на основе Синтаксиса криптографических сообщений (CMS)

Аннотация: Рассмотрены методы реализации сетевой Службы защищенных сообщений, предназначенной для реализации безопасной обработки информационных запросов в распределенных информационных системах. Отличительными особенностями службы являются тесная интеграция функций информационной защиты данных с функциями информационного взаимодействия в сети. Описаны особенности реализации службы на основе использования Синтаксиса защищенных сообщений (CMS) в Windows.

Ключевые слова: распределенные системы, Web-технологии, Интернет-технологии, информационное взаимодействие, информационная безопасность

Уже более десяти лет сетевая архитектура .NET и технология Web-сервисов [1] занимают ведущее положение в разработках распределенных информационных систем. Тем не менее, технология Web-сервисов не свободна от недостатков, которые зачастую создают трудности для разработчиков. Как следствие, в последние годы появилась тенденция поиска альтернативных решений. В качестве основных причин можно назвать:

- отсутствие в архитектуре .NET встроенных средств защиты и аутентификации сетевых сообщений,
- затрудненность отладки клиентских и сервисных компонент системы (и их взаимодействия) вне сетевой среды и Web-сервера.

В докладе рассматриваются принципы организации новой сетевой службы PMS (Protected Message Service), в разработке которой сделана попытка преодоления перечисленных выше недостатков. Суть подхода заключается в тесной интеграции функций сетевого информационного обмена с функциями защиты и аутентификации данных. Внешне эта интеграция проявляется в том, что отмеченные функции входят в набор методов главного класса службы – класса «Защищенное сообщение», отображающего электронный документ (информационный запрос или ответ), снабженный одной или несколькими удостоверяющими Электронными цифровыми подписями (ЭЦП). В отличие от технологии Web-сервисов описываемая служба опирается не на модель вызова методов удаленных объектов, а на модель обмена сообщениями. В данном случае это означает, что все сервисные обрабатывающие функции (методы) имеют одинаковую, жесткую спецификацию: они получают объект класса «Защищенное сообщение» в качестве параметра и возвращают объект того же класса. Эти обрабатывающие функции группируются в одну или несколько динамических библиотек, которые подключаются к серверу PMS в момент его запуска (каждая библиотека может рассматриваться как отдаленный аналог Web-сервиса в .NET), и становятся доступными для клиентских компонент. Web-технология (HTTP, HTTPS, SOAP, WSDL и т.п.), также как и Web-серверы вообще не используются [2,3].

Реализация PMS на основе криптосистемы «КриптоПро» версии 3.6 и проведенные лабораторные эксперименты показали достаточно высокое быстродействие новой службы, не уступающее, а в отдельных случаях превосходящее быстродействие Web-сервисов в одинаковых условиях [4]. Однако, при данном подходе возникает жесткая «привязанность» PMS к

определенной криптосистеме, что может создать неудобства для разработчиков распределенных систем.

В данной работе рассматривается новый подход к архитектурному построению PMS, основанный на применении стандарта Cryptographic Message Syntax (CMS) и его программной поддержки в среде Windows в качестве базисного средства реализации (рис. 1). Главное преимущество этого подхода заключается в том, что он позволяет PMS «унаследовать» способность гибкой настройки на использование любой криптосистемы, поддерживающей стандарт CMS, и, тем самым, устранить ту жесткую привязку к определенной криптосистеме, о которой говорилось выше.

Данный подход к реализации PMS основан на функциональном сходстве ее главного класса (PMSMessage) с главным классом CMS (SignedCMS): оба класса представляют контейнер для хранения произвольных данных, оснащенный необходимыми методами для формирования и проверки электронных подписей. Вместе с тем, CMS не содержит классов и методов для удаленной обработки данных в сети (аналогов класса PMSConnection или метода PMSMessage.Process). Фактически, описываемый подход можно рассматривать как создание своего рода «надстройки» над CMS, направленной на сетевую обработку данных.

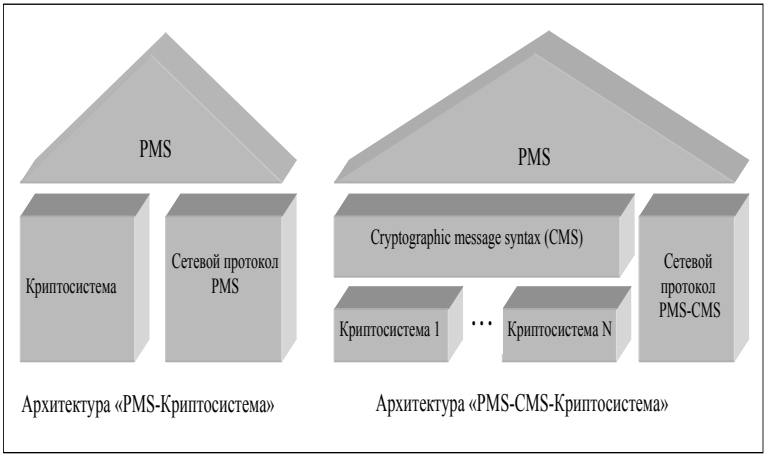


Рис. 1. – Архитектурные решения для реализации PMS

На рис. 2 проиллюстрировано соотношение основных классов и методов PMS и CMS, представляющее собой основу описываемого подхода. Стрелки обозначают прямой вызов одного метода другим. В

частности, метод AddSignatures класса PMSMessage выполняет вызов метода ComputeSignature класса SignedCMS для формирования каждой ЭЦП в защищенном сообщении, а метод Process опирается в своей работе на методы класса EnvelopedCMC для выполнения шифрования отправляемых в сеть данных и дешифрования данных, принятых из сети (методы Encrypt и Decrypt соответственно).

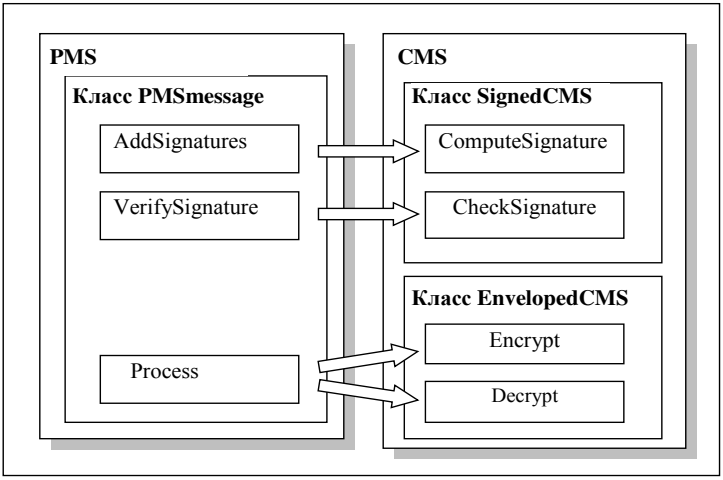


Рис. 2. – Основные классы и методы PMS и CMS

С целью сравнения быстродействия двух методов построения PMS (на основе архитектур «PMS-Криптосистема» и «PMS-CMS-Криптосистема») между собой, а также с быстродействием Web-сервисов в одинаковых условиях была проведена опытная реализация службы и ряд лабораторных экспериментов. Главное внимание уделялось вызовам сервисных функций с относительно малым (от нескольких миллисекунд до нескольких сотен миллисекунд) временем выполнения (при более длительной обработке разница между двумя технологиями практически нивелируется) с применением средств ЭЦП и шифрования сообщений на основе криптосистемы «КриптоПро» версии 3.6, соответствующей требованиям действующих в России ГОСТов в области криптографической защиты информации. В экспериментах с PMS использовались средства криптозащиты «КриптоПро», интегрированные в клиентскую библиотеку PmsBase.dll и сервер PMS или «напрямую» или посредством средств CMS. В экспериментах с Web-сервисами средства криптосистемы «КриптоПро» подключалась непосредственно к программе клиента и программе Web-сервиса. И серверы PMS с модельными библиотечными функциями и

Internet Information Server с модельными Web-сервисами были установлены на одном и том же четырехъядерном сервере приложений с тактовой частотой 2.4.ГГц в операционной среде Window 2003 Server, а в качестве клиентской рабочей станции использовался одноядерный компьютер с тактовой частотой 2.8 ГГц.

На рис. 3 показаны характерные результаты экспериментов с очень быстрой сервисной функцией, выполняющей простое перекодирование полученного строчного сообщения в верхний регистр и возврат результата клиенту, при длине сообщения в 2 Кбайт, 50 Кбайт и 100 Кбайт соответственно. На рисунке приведена диаграммы времен выполнения операции на сервере в реализации «PMS-КриптоПро» (черный столбик), в реализации «PMS-CMS-КриптоПро» (серый столбик) и с помощью Web-сервиса (белый столбик). В каждом режиме время выполнения вычислялось, как среднее значение для 100 последовательных вызовов сервисной функции.

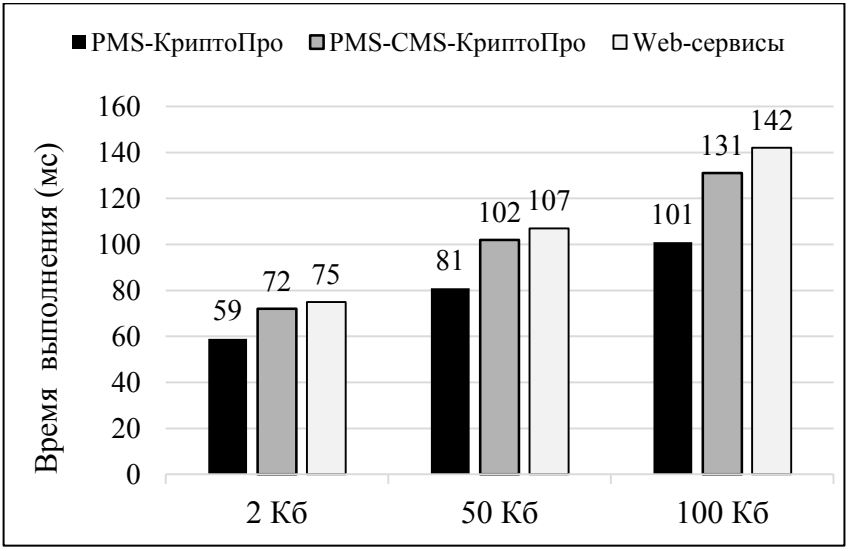


Рис. 3. – Оценки быстродействия двух реализаций PMS и Web-сервиса

В целом результаты экспериментов позволяют сформулировать следующие выводы.

- Реализация PMS на основе архитектуры «PMS-CMS-КриптоПро» в целом несколько уступает в быстродействии «прямой» реализации на основе архитектуры «PMS-КриптоПро», но в случае использования

относительно медленных сервисных функций (с временем выполнения более 0.5 секунды) разница становится пренебрежимо малой.

- Обе реализации PMS не уступают в быстродействии Web-сервисам.
- Применение средств криптозащиты в обеих реализациях PMS не разрушает положительного эффекта от многопоточной обработки запросов.
- Как и Web-сервисы, обе реализации PMS вполне позволяют поддерживать скорость обработки до нескольких и даже нескольких десятков запросов в секунду даже при использовании средств криптозащиты, что обычно бывает достаточным для большинства информационных систем.

Литература:

1. *Мак-Дональд М., Шпушта М.* Microsoft ASP.NET 3.5 с примерами на C# 2008 и Silverlight 2 для профессионалов. – М.: Вильямс. – 2009. – 1408 с.
2. *Хант К.* TCP/IP. Сетевое администрирование. – СПб.: Питер. –2007. – 816 с.
3. *Снейдер Й.* Эффективное программирование TCP/IP. Библиотека программиста. – СПб.: Символ-Плюс. – 2002. – 320 с.
4. *Асратян Р.*Э. Интернет-служба защищенной обработки информационных запросов в распределенных системах // Программная инженерия. – 2016. – № 11. – С. 490-497.

Мелихов А.А.

Разработка методики формирования стеганоконтейнеров на основе морфологической структуры предложений естественного языка

Аннотация: В статье рассматривается методика формирования стегоконтейнеров на основе свойств устойчивости морфологической структуры предложения к изменению низкоэнтропийных элементов, вводится классификация подобных элементов. В качестве примера рассматриваемого явления приводятся: изменение порядка слов при числительном, синонимичная замена единиц измерения, изменение типа артиклей.

Ключевые слова: стеганография; стегоконтейнер; лингвистическая стеганография; анализ естественного языка; морфологическая структура предложения

Потребность в защите конфиденциальности передаваемых по открытым каналам данных является актуальной для всех участников межсетевого взаимодействия. В гражданском сегменте средств защиты информации (СЗИ) широко применяются стеганографические методы, позволяющие скрывать сам факт передачи защищённой информации. Наиболее распространённые из них основаны на моделях и алгоритмах, жёстко привязывающих стегоконтейнер к формату файла, в который он встроен. Так, метод наименьшего значащего бита (LSB), эффективный при работе с кодируемыми без потерь изображениями, оказывается неэффективным при их сжатии, приводящем к разрушению контейнера. По этой же причине, упаковка сообщений в компактные графические, аудио и видеофайлы, равно как и в исполняемый двоичный код [1] требует разработки иных методов, основанных на выявлении скрытых закономерностей в характере самих данных, но не в форме их представления. Стоит отметить, что большая стегоёмкость мультимедиа связана с большими размерами самих файлов, поэтому на применение стегоконтейнеров может указывать передача нехарактерно больших файлов. Текстовое сообщение в данной роли обладает определённым преимуществом ввиду того, что подавляющее большинство информационных систем обмениваются текстовыми данными, как следствие, присутствие текста в общем потоке передаваемых данных не вызывает подозрений. Однако текстовые стегоконтейнеры обладают малой информационной ёмкостью, при этом также сильно зависят от формата кодирования и средств визуализации [2], что может порождать ситуации, когда стегоконтейнер может быть обнаружен в программе для просмотра текстовых файлов, который не поддерживает исходное форматирование и подменяет похожие по начертанию шрифты из-за отсутствия в системе оригинальных. В этом смысле, перспективным представляется развитие средств лингвистической стеганографии, обходящих указанные ограничения [3].

Целью настоящей работы является разработка метода формирования стегоконтейнеров на основе интралингвистических особенностей естественно-языкового текста, таких как устойчивость морфологической структуры предложения к сознательно вносимым в его состав изменениям [4]. Основные задачи исследования: 1) выявление в грамматической структуре элементов с минимальной энтропией (как с точки зрения семантики всего текста, так и по отношению к определению синтаксической структуры отдельного предложения); 2) определение степени толерантности алгоритма синтаксического разбора к внесению изменений в выявленные элементы и их классификация. Исходные данные представлены в виде текста на естественном языке (английский), а также формального описания его морфологической структуры, получаемое

посредством средств автоматизированного грамматического анализа – Stanford Parser[5]. В качестве исходной модели текста выступает разработанная ранее[6] модель представления предложения на естественном языке, учитывающая, с одной стороны, линейный характер письменного текста (порядок слов с частеречной разметкой) и иерархический характер грамматико-семантической структуры предложения с другой.

Практические результаты, полученные при разработке методики извлечения элементов, определяющих семантику текста[7], показали, что в процессе пошаговой свёртки пространства состояний, определяющего элементы предложения (лексемы с частями речи - токены) и иерархические связи между ними, грамматический анализатор обладает толерантностью к некоторым исходным свойствам текста. В случае с поисковой системой, данное свойство, применяется для определения важности отдельных токенов и их последовательностей. Фактически, правило свёртки формулируется следующим образом: «*если изменение порядка следования токенов и/или их грамматических характеристик влечёт изменение грамматико-семантической структуры предложения, то данные элементы являются высокоэнтропийными*». Если это правило обобщить не только на элементы, но и вообще на все свойства предложения (в т.ч. и структурные), то можно выявить те из них, изменение которых не приводит к формированию новой структуры. Такие элементы могут быть использованы для создания стегоконтейнера, а их информационная ёмкость будет определяться числом значений всех допустимых (не вызывающих структурных изменений) параметров. В таком случае, извлечение информации из такого состояния производится одним из двух способов: 1) если исходное (до внедрения сообщения) состояние параметра очевидно из контекста, то ключ для извлечения не требуется; 2) если исходное состояние неочевидно, то требуется ключ. Рассмотрим далее толерантность грамматического анализатора к языковым явлениям трёх типов: изменение порядка слов, прямая замена синонимичных элементов, модификация служебных частей речи.

К явлению первого типа относится перенос единиц измерения относительно базовой величины. В предложениях “Sam took out a **3$** million loan.” и “Sam took out a **3** million **$** loan.” иерархическая структура отношений подчинения и зависимости идентична [8], в иерархии фразовых структур изменился только порядок слов, т.е. с точки зрения грамматики зависимостей эти предложения идентичны, изменение кодируется как разница в конкретной фразовой структуре *при изменении порядка слов при числительном*. Во втором случае, *синонимичная замена единиц измерения*, как в предложении “Sam took out a **3** million **dollar** loan.”, равно как в “Sam took out a **dollar 3** million loan.” относительно вышеуказанных, приводит к

соответствующим последствиям. *Изменение типа артиклей* (третий случай) должно производиться с особой осторожностью: при сохранении грамматической структуры оно влияет на восприятие смысла предложения, а полное исключение приводит к серьёзным структурным изменениям. Данное обстоятельство объясняется тем, что число бинарных отношений универсальных зависимостей определяется как число токенов в предложении (верхний в иерархии токен связывается с виртуальным узловым элементом, что гарантирует связность элементов, каждый из которых теперь бывает в роли зависимого элемента [6]).

На основе предложенной ранее методики извлечения из предложения грамматически релевантных структур, разработана методика формирования стегоконтейнеров: определены элементы с минимальной энтропией, проведена их классификация. Результаты проведённого исследования позволяют сделать заключение о применимости разработанного метода, однако, ввиду малой информационной ёмкости стегоконтейнеров, требуется его доработка.

Литература:

1. *Нечта И.В.* Анализ устойчивости динамических водяных знаков // Безопасность информационных технологий. 2017. № 2. С. 72-81.
2. *Шутько Н. П.* Алгоритмы реализации методов текстовой стеганографии на основе модификации пространственно-геометрических и цветовых параметров текста // Труды БГТУ. Серия 6: Физико-математические науки и информатика. 2016. №6 (188). С.160-165
3. *Ефременко Н. В.* Лингвистическая стеганография // Вестник МГЛУ. 2011. №619. С.66-73
4. *Сокол Д.Т., Прокопов К.В., Довгаль В.М.* Методика стеганографии с использованием текстового контейнера на основе детерминированно-хаотических рядов // Auditorium. 2016. №4 (12). С.97-104.
5. *Ингерсолл Г.С., Мортон Т.С., Феррис Э.Л.* Обработка неструктурированных текстов. Поиск, организация и манипулирование. М.: ДМК Пресс, 2015.
6. *Мелихов А.А.* Применение дерева синтаксического разбора предложений для повышения релевантности результатов частотного анализа текста // Нейрокомпьютеры: разработка, применение. 2016. № 3. С. 39-46.
7. *Мелихов А.А., Смирнова О.С.* Методика автоматизированного формирования тезауруса на основе грамматически релевантных единиц // Образовательные ресурсы и технологии. 2016. № 4 (16). С. 41-51.

8. *Журавлева Н.Г., Мелихов А.А., Губин А.Н., Гудов Г.Н.* Синтаксический анализ и преобразование единиц измерения в предложениях естественного языка информационных ресурсов // Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта (CAD/CAM/PDM - 2015) Труды международной конференции. Под ред. А.В. Толока. 2015. С. 341-344.

Рыженко А.А.

Модель деструктора-полиморфа цифровой среды

Аннотация: Современной проблемой безопасности цифровой среды является появление новых деструктивных механизмов, разрушающих привычные понятия стабильной информационной среды. Приводится пример формализации поведения деструктора-полиморфа, как одной из самой сложной разновидностей.

Ключевые слова: информационное пространство, безопасность, полиморф, деструктор, модель

Современная товарно-денежная система отношений многих организаций произвольного уровня и профиля все чаще не может представлять целостность модели без цифровой составляющей. Как правило, данный фактор тесно связан, как с расширением рынка сбыта товаров и услуг, так и требованиям банковской системы-посредника и социальными отношениями между территориально удаленными контрагентами. Как следствие, проблема цифровой безопасности нарастает с каждым годом все больше. При этом также необходимо учесть, что существующие системы всесторонней безопасности уже не успевают за новыми веяниями саморазвивающихся систем деструкторов. Более того, явная тенденция к упрощению интерфейса взаимодействия между внутренними процесса информационной среды и непосредственными пользователями приводят все больше к непониманию «обратной стороны медали» цифровизации экономических отношений [1]. В результате, многие организации не только теряют денежные средства при транзакциях из-за непонимания архитектуры трансляции потоковых данных в сети Интернет, но и доверяют корпоративные данные, способные разрушить организацию в любой момент времени не зависимо от действий пользователя-владельца или пользователя-хозяина. Следует также напомнить, что в настоящее время практически не существует

нормативной документации, способной защитить человека от цифровой среды в случае хищения как юридической, так и личной информации.

Проведя анализ публикаций известных ресурсов Интернет, можно сделать вывод, что одним из самых опасных представителей цифровых деструкторов считается вирус-полиморф, обладающий примитивным интеллектом, но способным уклоняться от любых действующих современных антивирусных систем и прочих стенок-защит. Так же необходимо учесть, что определение полиморфа как вируса не дает полного представления о возможностях, следовательно, далее описание представлено только в ключе деструктора цифровой среды.

Многолетние исследования независимых специалистов результатов деятельности существующих представителей деструкторов-полиморфов позволили систематизировать типовые действия, выявить закономерности [2]. В результате получена трёхуровневая модель «черного ящика», позволяющая определить возможные действия при внедрении, распространении и заражении действующей системы (рис. 1).

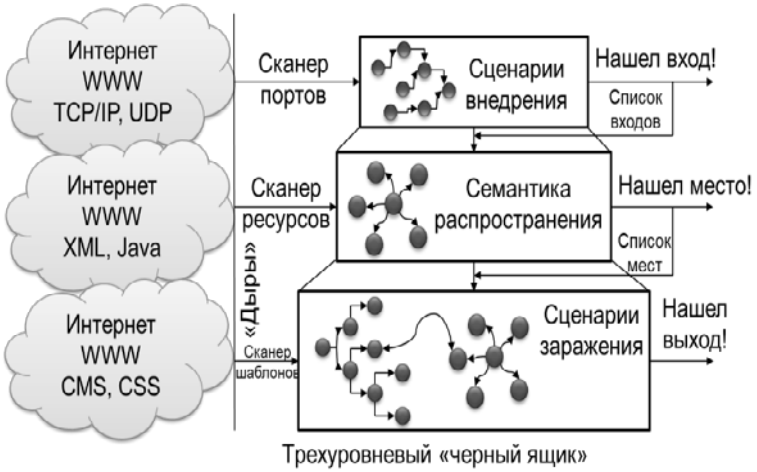


Рис. 1 – Модель диструктора «Полиморф»

Вариативной составляющей типового деструктора является автономность головы и хвоста каждого полиморфного наследника [3]. В результате, обобщая деятельность каждого представителя, получена следующая последовательность действий:

на первом этапе голова деструктора ищет возможные пути внедрения в действующую систему, используется сканер входных шлюзов (портов) на основе горизонтального сценарного дерева синтеза. Таблицы доступных

входов не существует, каждый атакуется при обнаружении, возможны повторы и дубликаты;

на втором этапе – сканер ресурсов позволяет строить семантическое дерево открытости ресурсов для распространения, при этом деструктор отделяет хвост для адаптации к каждому выявленному ресурсу (рис. 2). Как правило, переходные состояния между узловыми точками концентрации не превышают двух, что позволяет распространяться достаточно быстро, а также не вызывать подозрения у контролирующих и блокирующих систем;

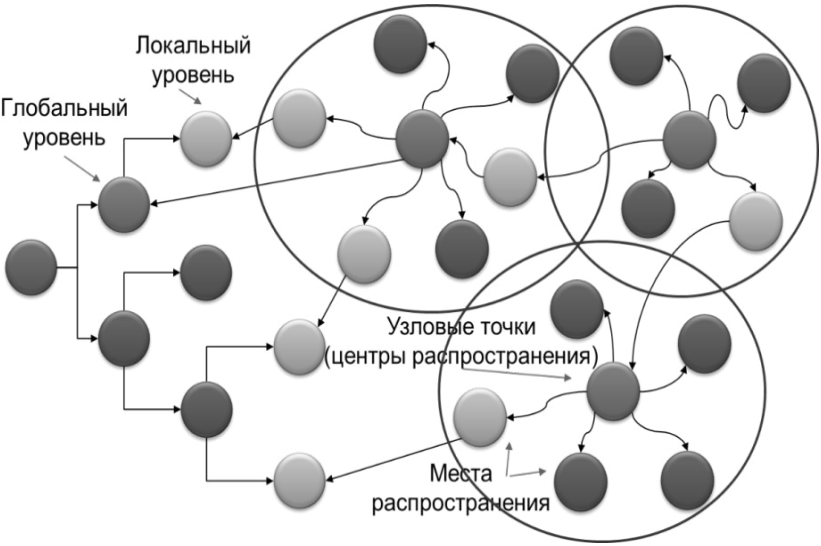


Рис. 2 – Семантическая сеть с локализацией узлов

на третьем – хвост определяет сценарий заражения с использованием горизонтального дерева анализа, формирует новую голову, атакует ресурс, размножается, порождает наследника (рис. 3). Каждый последующий автономный элемент независим, не имеет связи с родителем, но полностью дублирует действия. Процесс адаптации и обнаружения прочих наследников также независим, возможные коллизии недопустимы, т.к. голова содержит основной функционал взаимодействий по аналогии с протоколом TCP\IP.

В результате, представленную последовательность процессов можно описать в виде кубической системы ($И^3$), где три источника порождают все возможные состояния поведения деструктора (рис. 4).

Рис. 3 – Сценарный механизм с автономными элементами

Представленная модель системы полностью дублирует организаторскую деятельность конкурирующих организаций реальной экономической системы с использованием третьих лиц для совершения деструктивных действий (поглощения соперников). Как правило, в данных условиях, обычные средства противодействия не позволяют защитить действующие системы, так как явных нарушений со стороны нет. Цифровая среда существенно усугубляет данную проблему, так как также не известны внутренние операции и промежуточные состояния системы и потоковой информации. В результате, использование стандартных программных и аппаратных систем не позволит внести готовых решений данной проблемы.

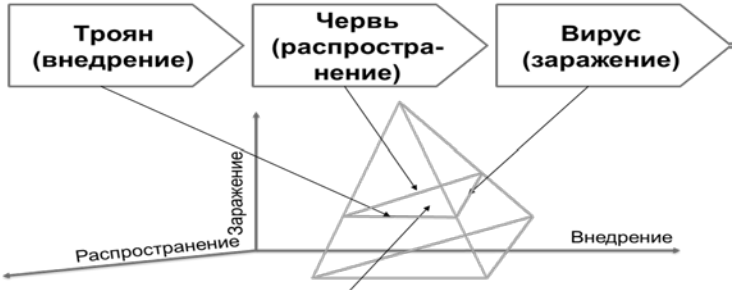


Рис. 4 – Система размножения деструктора в форме $И^3$

Как вариант выхода предлагается использовать цифровую среду-архитектор, позволяющую использовать фасетную систему организации данных, работающих по принципу невмешательства в основные процессы

жизненного цикла. Основные положения использования данной архитектуры представлены в работах [4, 5].

Литература:
1. Цифровизация экономики. – режим доступа: http://bit.samag.ru/uart/more/67 (Дата обращения: 16.10.2018 г.).
2. Виды компьютерных вирусов. – режим доступа: https://sites.google.com/site/virusyantivirusyinfo/vidy-komputernyh-virusov (Дата обращения: 16.10.2018 г.).
3. Деструктор. – режим доступа: https://www.yandex.ru/search/?text=%D0%B4%D0%B5%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D0%BE%D1%80%20-%20%D1%8D%D1%82%D0%BE&lr=213&clid=2186621 (Дата обращения: 16.10.2018 г.).
4. *Топольский Н.Г., Рыженко А.А.* Модель единого информационного пространства поддержки управления государственной метакорпорацией МЧС России / Проблемы управления безопасностью сложных систем: Труды XXIV Международной конференции, Москва, декабрь 2016 г. / Под ред. Н.И. Архиповой, В.В. Кульбы. М.: РГГУ, 2016. – С. 17-21.
5. *Рыженко А.А.* Проектирование алгебраической формы распределенной базы правил системы с автономными элементами / Седьмая Международная конференция «Системный анализ и информационные технологии» САИТ – 2017 (13-18 июня 2017 г., г. Светлогорск, Россия): Труды конференции. – С. 324-328.

Алексейчук А.Е.

Технология анализа защищенности информационной системы

Аннотация: Рассматриваются современные инновационные методы и инструментальные средства анализа степени защищенности информационных систем и различного рода риски, связанные с их применением на практике. Предложена формальная модель с полным перекрытием, включая взаимодействие области угроз, защищаемой области и системы защиты. Суть деятельности по управлению рисками состоит в том, чтобы оценить их размер, выработать меры по уменьшению размера и создать механизм контроля того, что остаточные риски не выходят за приемлемые ограничения.

Ключевые слова: информационная безопасность, социальные сети, инновационные технологии, социальные проблемы, интернет-риски

Методологические аспекты анализа

В процессе создания архитектуры и компонентов информационной системы необходимо обращать внимание на проблему обеспечения безопасности как всей системы так и отдельных ее частей. Необходимо обеспечить такую систему инструментальными средствами мониторинга и анализа таких взаимно пересекающихся видов работ, как реализация ИС и аттестация, аудит и обследование безопасности ИС.

Формальное описания системы защиты традиционно считается моделью системы защиты с полным перекрытием, в которой рассматривается взаимодействие "области угроз", "защищаемой области" и "системы защиты", что выглядит в виде трех множеств:

$T = \{t_i\}$ - множество угроз безопасности,

$O = \{o_j\}$ - множество объектов (ресурсов) защищенной системы,

$M = \{m_k\}$ - множество механизмов безопасности АС.

Элементы этих множеств находятся между собой в определенных отношениях, собственно и описывающих систему защиты. Для описания системы защиты обычно используется графовая модель. Множество отношений угроза-объект образует двухдольный граф {T, O}. Цель защиты состоит в том, чтобы перекрыть все возможные ребра в графе. Это достигается введением третьего набора M; в результате получается трехдольный граф {T, M, O}.

Развитие модели предполагает введение еще двух элементов.

V - набор уязвимых мест, определяемый подмножеством декартова произведения $\{T \times O\} : v_r = <t_i, o_j>$. Под уязвимостью системы защиты понимают возможность осуществления угрозы T в отношении объекта O. (На практике под уязвимостью системы защиты обычно понимают, те свойства системы, которые либо способствуют успешному осуществлению угрозы, либо могут быть использованы злоумышленником для ее осуществления).

Определим B как набор барьеров, определяемый декартовым произведением $\{V \times M\}: b_l=<t_i, o_j, m_k>$, представляющим собой пути осуществления угроз безопасности, перекрытые средствами защиты. В результате получаем систему, состоящую из пяти элементов: <T, O, M, V, B>, описывающую систему защиты с учетом наличия уязвимостей

Для системы с полным перекрытием для любой уязвимости имеется устраняющий ее барьер. Иными словами, в подобной системе защиты для всех возможных угроз безопасности существуют механизмы защиты, препятствующие осуществлению этих угроз. Данное условие является первым фактором, определяющим защищенность ИС, второй фактор - "прочность" и надежность механизмов защиты.

В идеале каждый механизм защиты должен исключать соответствующий путь реализации угрозы. В действительности же

механизмы защиты обеспечивают лишь определенную степень сопротивляемости угрозам безопасности. Поэтому в качестве характеристик элемента набора барьеров $b_l=<t_i,o_j,m_k>$ может рассматриваться набор $<P_l, L_l, R_l>$, где P_l - вероятность появления угрозы, L_l - величина ущерба при удачном осуществлении угрозы в отношении защищаемых объектов (уровень серьезности угрозы), а R_l - степень сопротивляемости механизма защиты m_k, характеризующаяся вероятностью его преодоления.

Надежность барьера $b_l=<t_i,o_j,m_k>$ характеризуется величиной остаточного риска $Risk_l$, связанного с возможностью осуществления угрозы t_i в отношении объекта информационной системы o_j при использовании механизма защиты m_k. Эта величина определяется по формуле:

$Risk_l = P_k \times L_k \times (1 - R_k)$.

Для нахождения примерной величины защищенности S можно использовать следующую простую формулу: $S = 1/Risk_0$, где $Risk_0$ является суммой всех остаточных рисков, $(0 < [P_k, L_k] < 1)$, $(0 \le R_k < 1)$.

Суммарная величина остаточных рисков характеризует приблизительную совокупную уязвимость системы защиты, а защищенность определяется как величина, обратная уязвимости. При отсутствии в системе барьеров b_k, "перекрывающих" выявленные уязвимости, степень сопротивляемости механизма защиты R_k принимается равной нулю.

На практике получение точных значений приведенных характеристик барьеров затруднено, поскольку понятия угрозы, ущерба и сопротивляемости механизма защиты трудно формализовать. Так, оценку ущерба в результате несанкционированного доступа к информации политического и военного характера точно определить вообще невозможно, а определение вероятности осуществления угрозы не может базироваться на статистическом анализе. Построение моделей системы защиты и анализ их свойств составляют предмет "теории безопасных систем", еще только оформляющейся в качестве самостоятельного направления.

Вместе с тем для защиты информации экономического характера, допускающей оценку ущерба, разработаны стоимостные методы оценки эффективности средств защиты. Для этих методов набор характеристик барьера дополняет величина C_l затраты на построение средства защиты барьера b_l. В этом случае выбор оптимального набора средств защиты связан с минимизацией суммарных затрат $W = \{w_l\}$, состоящих из затрат $C=\{c_l\}$ на создание средств защиты и возможных затрат в результате успешного осуществления угроз $N = \{n_l\}$.

Формальные подходы к решению задачи оценки защищенности из-за трудностей, связанных с формализацией, широкого практического распространения не получили. Значительно более действенным является использование неформальных классификационных подходов. Для этого применяют категорирование: нарушителей (по целям, квалификации и доступным вычислительным ресурсам); информации (по уровням критичности и конфиденциальности); средств защиты (по функциональности и гарантированности реализуемых возможностей), эффективности и рентабельности средств защиты и т. п.

Анализ и управление рисками при осуществлении политики ИБ

Одним из важнейших аспектов реализации политики ИБ является анализ угроз, оценка их достоверности и тяжести вероятных последствий. Риск появляется там, где есть угрозы. Суть деятельности по управлению рисками состоит в том, чтобы оценить их размер, выработать меры по уменьшению и создать механизм контроля того, что остаточные риски не выходят за приемлемые ограничения. Таким образом, управление рисками включает в себя два вида деятельности: оценку рисков и выбор эффективных и экономичных защитных и регулирующих механизмов.

Процесс управления рисками можно подразделить на следующие этапы:

- идентификация активов и ценности ресурсов, нуждающихся в защите;
- выбор анализируемых объектов и степени детальности их рассмотрения;
- анализ угроз и их последствий, определение слабостей в защите;
- классификация рисков, выбор методологии оценки рисков и проведение оценки;
- выбор, реализация и проверка защитных мер;
- оценка остаточного риска.

Политика ИБ включает разработку стратегии управления рисками разных классов. После проведения анализа угроз, их возможных последствий и идентификации риска возможно несколько подходов к управлению: уменьшение риска, уклонение от риска, изменение характера риска, принятие риска.

Многие риски могут быть существенно уменьшены путем использования весьма простых и недорогих контрмер. Например, грамотное управление паролями снижает риск несанкционированного доступа. От некоторых классов рисков можно уклониться - вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов. Если не удается уклониться от риска или эффективно его уменьшить, можно принять некоторые меры страховки. Примеры: оборудование может быть застраховано от пожара и стихийных бедствий,

можно заключить договоры с поставщиками программно-аппаратных и телекоммуникационных средств на их техническое сопровождение и компенсацию ущерба, вызванного нештатными ситуациями из-за брака в поставленном оборудовании. Некоторые риски не могут быть уменьшены до малой величины, однако после реализации стандартного набора контрмер их можно принять, постоянно контролируя остаточную величину риска.

При идентификации активов и информационных ресурсов - тех ценностей, которые нужно защитить, - следует учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, в том числе текущий рейтинг и репутацию компании. Тем не менее одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее использования.

Выбор анализируемых объектов и степень детальности их рассмотрения - следующий шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру, для крупной - следует сосредоточиться на наиболее важных сервисах. Если важных сервисов много, то выбираются те из них, риски для которых заведомо велики или неизвестны. Если информационной основой организации является локальная сеть, то в число аппаратных объектов следует включить компьютеры, периферийные устройства, внешние интерфейсы, кабельное хозяйство и активное сетевое оборудование. К программным объектам следует отнести операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, программы управления сетью и отдельными подсистемами. Важно зафиксировать, в каких узлах сети хранится программное обеспечение, где и как используется. Третьим видом информационных объектов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, а также способы доступа к ним. Все это важно для оценки рисков и последствий нарушений информационной безопасности.

Оценка рисков производится на основе накопленных исходных данных и оценки степени определенности угроз. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на величину предполагаемого ущерба. Если для вероятности осуществления угрозы и величины предполагаемого ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и

четвертый - к среднему, два последних - к высокому. По этой шкале можно оценивать приемлемость рисков.

Понятия "оценка рисков" (Risk Assessment) и "управление рисками" (Risk Management) появились сравнительно недавно, но эти дисциплины стали неотъемлемой составляющей деятельности в области обеспечения непрерывности бизнеса (Business Continuity) и информационной безопасности (Information Security). Подготовлено и активно используются более десятка различных стандартов и спецификаций, детально регламентирующих процедуры управления информационными рисками, среди которых наибольшую известность приобрели международные спецификации и стандарты ISO 15408: 1999 ("Common C riteria f or Information T echnology Security E valuation"), I SO 17799: 2002 ("Code o f Practice f or I nformation S ecurity Management"), S CIP, N IST, S AS 7 8/94, COBIT и др.

При выполнении полного анализа рисков приходится решать ряд сложных проблем – как определить ценность ресурсов, как составить полный список угроз ИБ и оценить их параметры, как правильно выбрать контрмеры и оценить их эффективность и приемлемые расходы и т. д. Для их решения существуют специально разработанные инструментальные средства, построенные с использованием структурных методов системного анализа и проектирования (SADT - Structure Analysis and Design Technique). На практике такие методики управления рисками позволяют:

- создавать модели информационных активов компании с точки зрения безопасности;
- классифицировать и оценивать ценности активов;
- составлять списки наиболее значимых угроз и уязвимостей безопасности;
- ранжировать угрозы и уязвимости безопасности;
- обосновывать средства и меры контроля рисков;
- оценивать эффективность/стоимость различных вариантов защиты;
- формализовать и автоматизировать процедуры оценивания и управления рисками.

Применение соответствующих программных средств позволяет уменьшить трудоемкость проведения анализа рисков и выбора контрмер. В настоящее время разработано более десятка программных продуктов для анализа и управления рисками базового уровня безопасности. Примером такого достаточно простого средства является программный пакет BSS (Baseline Security Survey, UK). Программные продукты более высокого класса: CRAMM (компания Insight Consulting Limited, UK), RiskWatch, COBRA, Buddy System. Наиболее популярный из них - CRAMM (Complex Risk Analysis and Managment Method), реализующий метод анализа и контроля рисков. Метод и продукт разработаны по заказу Центрального

агентства по компьютерам и телекоммуникациям (CCTA - Central Computer and Telecommunication Agency) Великобритании. Существенным достоинством метода является возможность проведения детального исследования в сжатые сроки с полным документированием результатов.

В основе метода CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для больших, так и для мелких организаций, как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (Profiles). Для коммерческих организаций имеется Коммерческий профиль (Commercial Profile), для правительственных организаций - Правительственный (Government Profile). Правительственный вариант профиля, также позволяет проводить аудит на соответствие требованиям американского стандарта TCSEC ("Оранжевая книга"). Судя по числу ссылок в Internet, этот метод является, одним из самых распространенных методов анализа и контроля рисков.

Литература:

1. *Кульба В.В., Сиротюк В.О., Косяченко С.А.* Информационная безопасность патентных ведомств: теория и практика. М.: ИПУ РАН, 2017. – 166 с.
2. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Информационное управление в условиях глобализации. М.: ИПУ РАН, 2017. – 130 с.
3. *Кульба В.В., Алексейчук А.Е.* Новые подходы к управлению социально-экономическими процессами в стране / Материалы Международной научной конференции "Актуальные проблемы управления" (Москва, 2015). М.: Издательский Центр РГГУ, 2015. С. 208-217.

Муромцев В.В., Муромцева А.В.

Информационная безопасность в условиях виртуализации инструментов управления

Аннотация: Рассматриваются проблемы, возникающие в условиях виртуализации инструментов управления, и сопутствующие им угрозы информационной безопасности.

Ключевые слова: информационные технологии, безопасность, инструменты управления, виртуализация

Сегодня информационные технологии широко используются в процессе управления, и всё в большей степени они уходят в виртуальное пространство. В результате меняется структура организации и технологии принятия управленческих решений. Это отражается не только на отдельных организациях, но и на государстве в целом.

В июле 2017 года правительство Российской Федерации утвердила программу «Цифровая экономика Российской Федерации» [1].

Государственное управление в соответствии с программой предполагает использовать новые цифровые технологии, основанные на технологиях «электронного правительства». Виртуализация пространства управления уже сегодня достигла довольно высокого уровня. В связи с этим, возросла актуальность обеспечения информационной безопасности в данном пространстве.

Традиционно большое внимание в РФ уделяется вопросам обеспечения информационной безопасности объектов газоснабжения, энергоснабжения и ядерных объектов. Сегодня в этих отраслях произошли серьёзные изменения в системах управления. Всё больше процессов реализуется с помощью автоматизированных систем, использующих виртуальные инструменты управления.

Для формирования информационного обеспечения систем организационного управления, как правило, используется целый ряд информационных систем. Это, например, системы создания и верификации документов, системы электронного документооборота, коммуникационные средства, базы и банки данных, мультимедийные средства, активно развивающиеся в сторону виртуальных представлений информации, справочно-правовые системы, системы Интернет и Интранет, системы интеллектуальной поддержки принятия решений, системы информационно-аналитической обработки информации и многое другое [2].

Современная интегрированная система менеджмента (СМ) организации включает нескольких систем менеджмента, это: система менеджмента качества (СМК), система экологического менеджмента (СЭМ), система управления охраной труда (СУОТ) и система менеджмента информационной безопасности (СМИБ). Каждая из этих систем является важным и взаимозависимым элементом общего менеджмента организации [3] и способствует изменению структуры и технологий управления, которые всё в большей степени используют виртуальные инструменты, обеспечение безопасности которых требует внимания и дополнительных усилий.

За три последних года количество преступлений в цифровой среде возросло на 75 процентов [1], что говорит о необходимости совершенствования систем информационной безопасности не только в

рамках государственных систем управления, отраслей промышленности, объектов и компаний, а также в частных организациях.

Сейчас, в рамках цифровой среды, можно говорить о следующих угрозах, влияющих на управление организацией:

- обеспечение прав людей в цифровом мире, которая выливается сразу в несколько факторов: идентификация и соотнесении человека с его цифровым образом, сохранность цифровых данных пользователя;
- обеспечение доверия граждан к цифровой среде, что влияет на вовлечённость людей различные цифровые технологии;
- обеспечение организационных прав в цифровом мире, состоящих в неприкосновенности частной жизни сотрудников организации при использовании информационных технологий;
- угрозы личности, бизнесу и государству, связанные с тенденциями к построению сложных иерархических информационно-телекоммуникационных систем, широко использующие виртуальные коммуникации (облачные хранилища данных, разнородные технологии связи и другие);
- наращивание возможностей внешнего информационно-технического воздействия на информационную инфраструктуру;
- рост масштабов компьютерной преступности, в том числе международной;
- отставание от ведущих иностранных государств в развитии конкурентоспособных информационных технологий [1,4].

Эти факторы влияют как на работников организации, так и на потребителей, что препятствует развитию электронного бизнеса и экономике страны. Кроме того, те технические средства (сервера и др.), на которых базируются информационные технологии обмена, хранения, передачи часто принадлежат иностранным государствам и частным лицам, что формирует дополнительные угрозы информационной безопасности в виртуальной сфере.

Однако, говоря о глобальных угрозах невозможно не остановиться на фактах безграмотности большого числа пользователей, на что и обращается внимание в программе. Согласно проведённым исследованиям на 100 человек только 3% знают, как защитить свой документ, созданный в программе MSWord. О возможности скрытия папок среди обычных пользователей и того меньше. Большинство из них даже не задумывались о защите своих документов. В этих условиях формирование элементарной информационной культуры пользователей является важной задачей, решение которой обеспечит на нижнем уровне определённый уровень информационной безопасности.

Таким образом, обеспечение информационной безопасности виртуальных инструментов управления представляет собой в связи с переходом процессов управления в виртуальное пространство важную общегосударственную задачу, решение которой во многом зависит от успешной реализации программы «Цифровая экономика РФ».

Литература:

1. Распоряжение правительства Российской Федерации от 28 июля 2017 года № 1632-р «Программа “Цифровая экономика Российской Федерации”».
2. Информационный менеджмент // Н.И. Архипова, В.В. Кульба, С.А. Косяченко, А.Б. Шелков. - М.: Экономика, 2013.
3. Муромцев В.В., Можаев О.А., Муромцева А.В., Совершенствование системы управления безопасностью организации на основе современных стандартов менеджмента. Проблемы управления безопасностью сложных систем: Труды XXV Международной научной конференции. Москва, декабрь 2017 г./ Под ред. Н.И. Архиповой, В.В. Кульбы - М.: РГГУ, 2017. С 603-609.
4. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".
5. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы".

IV. Экологическая и техногенная безопасность

Raikov A.N.

Emergency medicine diagnostics based on strong and collective artificial intelligence technologies

Abstract: Contingency emergencies are characterized by the presence of wounded and/or dead, wounded need medical assistance with the fast determination of the optimal approach. Medical conversations that are conducted for determining patient diagnoses in these conditions can give erroneous recommendations. The errors grow if recommendations are created in a networked condition, when the doctors do not hear and see each other. To improve the medical advice services it is advisable to apply strong (general) and collective artificial intelligence technologies, including cognitive modeling and a genetic algorithm. An important issue of application artificial intelligence technologies in advice conversations is transforming the divergent conversation's process to convergent conversations that ensures the achievement of the consent of the doctors regarding the diagnosis for a short time. It can lead to a holistic plan for improvement of the patient's health.

Keywords: artificial intelligence, convergent conversations, emergency medicine, medical assistance, medical conversations.

The digital evolution in medical practice and artificial intelligence (AI) has made networked advice conversations (meetings) and doctors' group expert procedures an increasingly important part of doctors' practice and medical assistance. For the conditions of catastrophes, such procedures become especially relevant, since professional specialists are far from the scene of the incident.

Contingency emergencies are characterized by the following features:

- the presence of wounded and/or dead;
- wounded need medical assistance with the fast determination of the optimal approach;
- the possibility of significant destruction, contamination of the area, damage to toxic substances of people;
- multi-departmental and distributed decision making;
- a sharp lack of time and, possibly, funds;
- consideration of explicit and implicit elements of exposure is required;

- the need for holistic and rapid modeling in the presence of non-causal (unreasonable) factors.

In these conditions fairly brief conversations between distributed doctors must lead to the right decisions under complex and latent information about a patient. But although increased attention is being paid to networked medical advice meetings, most doctors would say that these networked procedures are not as effective as an advice meeting that takes place in one room and all the doctors are able to see each other.

Difficulties in networked procedures in medicine are caused by the absence of a special technology that would makes sure the convergence of the consultation process towards agreement on the patient's diagnosis. These difficulties could be overcome if health professionals were equipped with special technology that supports the conversation's convergence in analyzing the information about the patient and achieve successful practice of treatment.

To ensure the convergence process the convergent conversations technology could be recommended. As known it is useful for strategic planning applications [1]. It is obvious that it can raise the mutual doctors' trust in networked conditions. This technology has also to accelerate in finding the idea for the cure with subsequent confirmation during the convergent conversation.

The convergence technology is difficult because complex scientific components have to be applied and used. For example, the problem of the consistency of the questions in discussion has to be solved. It is important to choose the right initial phase of the conversation, to define techniques for achieving in-depth discussion, decision-making and summation.

Emotions play a big part in the conversation; they give new meanings to words and can divert the discussion towards. And what is important, emotions cannot be formalized, verbally presented. The strong feelings in the meeting can help to bring out helpful ideas. Emotions supplement words with the cognitive (thought, meditation) semantics, which are much more powerful than the denotative semantics that are formed by formalized elements: things, images, verbal descriptions. On the other hand, emotions can have a negative influence.

The traditional semantic representations of cognitive models have the denotative character. This is, first of all, a combination of words, terms, factors, their mutual influences, and, after that, their mathematical description in various spaces. The limitation of denotative semantics is using a finite dictionary, determined by the number of word forms.

The classic decision-support systems that are based on knowledge management systems focus on logical and symbolic information, etc. Different types of goals may be desired, for example: traditional or unusual goals. Usual goals are extrapolated from experience. They can be achieved with traditional

Medical Expert Systems [2]. Most of the evaluations of those systems are based on a paradigm related to pattern recognition, and clustering methods: accuracy, predictive, positive and negative values. They use expert systems' values as a standard. For example, three main stages of expert evaluation could be considered:

- Define correct diagnosis, input–output requirements, and clinical context;
- Test the prototype on a proper sample and compare it with relevant previous results;
- Experts compare the doctors' performance in real situations.

This is a classical deductive approach to the health recovery of the patient. But for achieving an unusual goal and getting perhaps more effective and nonstandard results than have been achieved previously, the convergent approach is suggested

But now non-deterministic and ill-defined problems have to be solved in a networked environment. It is necessary to:

- Increase the level of participants' understanding;
- Consider hidden fluctuations in the data chaos;
- Use big data analysis technologies;
- Take into account electronic message content;
- Consider cognitive and denotative semantic interpretations;
- Ensure sustainable and purposeful process;
- Ensure convergence of the process.

The non-formalized aspect of words' interpretations is very important. The doctors should predict what the patient wants when things go wrong. Patients would be well served if presentations of medical error followed this outline.

The main scientific components of convergent technology for supporting networked medical advice conversations are as follows: strong artificial intelligence, inverse problem solving method, control thermodynamics, theory of category, cognitive and quantum semantics, cognitive modeling in non-metric spaces.

If health professionals take part in conversations they have to apply different paradigms of AI: classical AI with direct problem solving and general (strong) AI with inverse problem solving.

The traditional AI uses logical, ontological, and so on formalized methods. But in strong AI non-formalized factors begin to influence the process very strongly. These have to be considered in order to make the discourse holistic.

The Tychonoff theorem [3] for inverse problem solving on topological spaces and the control thermodynamic laws were applied to ensure a holistic discourse and stable purposefulness of the conversation process. The use of the mentioned approaches for decision-making support is demonstrated on Fig. 1.

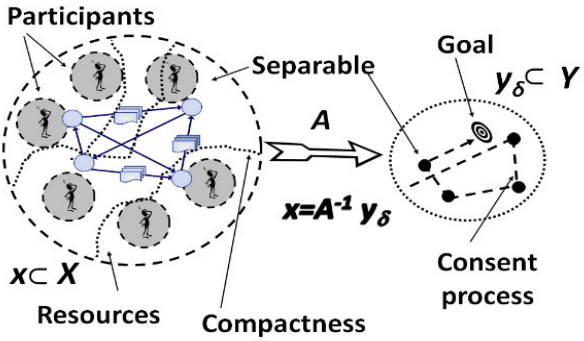


Fig. 1. Invers problem solving

As a result, the following rules make the process sustainable and purposeful:

- Separate goals, resources and actions;
- Goals should be arranged in hierarchical levels;
- The various resources should be separated into a finite number of parts;
- Control all aspects of the problem's solution, connections between goals and resources;
- Never underestimate small factors, etc.

The networked conditions of organizing collective medical conversations make it necessary to change the methodological basis, especially in the theory of AI. It is necessary to develop a General AI approach. GAI is considered to be a future AI system that will be capable to realize a wide range of human cognitive capabilities, collective unconscious phenomenon and emotional potential of human being.

There is a large gap between AI and GAI. In the structure of GAI it is necessary to consider such aspects as:

- Imitation of human brain behavior with non-classical methods, such as quantum and optical calculations;
- Supplementing the work of the human brain, which is influenced by the physical fields?
- Joint interpretation of formalized and non-formalized (cognitive) semantics;
- Collective cognitive AI.

The development of General AI requires an assembling of interdisciplinary methods and technologies from: philosophy, psychology, neurophysiology, law, quantum physics, mathematics, convergent management, cognitive modeling, category theory, inverse problems solving, and neural technologies, synthesis of materials, cosmology and so on.

Within the framework of an expert session and a strategic discussion were held with the goal of collectively formulating a strategy for the development of the health system of the region. Networked medical conversations for determining patient diagnoses are the next step of proposed technology application.

This work is partly funded by: Russian Science Foundation, grant No. 17-18-01326 "Development of socio-humanitarian technologies for distributed situational centres system in Russia based on self-developing polysubject environments methodology"

Литература:

1. *Raikov A.N., and Panfilov S.A.* Convergent decision support system with genetic algorithms and cognitive simulation, Proc. of the IFAC Conference on Manufacturing Modelling, Management and Control, MIM'2013, Saint Petersburg, Russia, June 19-21, 2013, pp. 1142-1147
2. Expert Systems and Decision Support in Medicine, Proc. 33rd Annual Meeting of the GMDS. EFMI Special Topic Meeting. Peter L. Reichertz Memorial Conference. Otto Rienhoff, Ursula Piccolo, Berthold Schneider (Eds.), Hanover, Sept. 1988, 2012.
3. *C.K. Wong.* Covering properties of fuzzy topological spaces. Journal of Mathematical Analysis and Application, 1973, vol. 43, pp. 697-704.

Кусакина Ю.Н.

О технологической безопасности России на примере титановой отрасли

Аннотация: В работе рассмотрены проблемы технологической безопасности в контексте развития титановой отрасли. С учетом различных аспектов применения титана и его сплавов выявлены компоненты технологического фактора обеспечения национальной безопасности. Установлена взаимосвязь технологической безопасности с экономической, энергетической и экологической безопасностью, а также обороноспособностью страны

Ключевые слова: технологическая безопасность, национальная безопасность, титановая отрасль, конкурентоспособность, производство

В современных условиях проблема обеспечения национальной безопасности является чрезвычайно актуальной. Как отмечено в указе Президента РФ от 31 декабря 2015 года №683 «О Стратегии национальной безопасности Российской Федерации», национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности» [1]. Одной из стратегических целей обеспечения национальной безопасности в области науки, технологий и образования определено развитие системы научных, проектных и научно-технологических организаций, способной обеспечить модернизацию национальной экономики, реализацию конкурентных преимуществ Российской Федерации, оборону страны, государственную и общественную безопасность, а также формирование научно-технических заделов на перспективу. Для ее выполнения заявлена необходимость повышения уровня технологической безопасности. В данной работе будет проанализировано, каким образом развитие титановой отрасли может повлиять на отдельные вышеупомянутые виды безопасности, и отразится на национальной безопасности в целом, в основном через технологические факторы и рассмотрена проблема технологической безопасности. Технологическая безопасность в масштабах государства базируется на возможности обеспечить конкурентоспособность, трактуемую в [1] как формирование явных по отношению к другим государствам преимуществ в научно-технологической области и, как следствие, в социальной, культурной, образовательной и экономической областях. Титановая отрасль России в структуре национального промышленного производства, представляет сложный набор составляющих, определяющих трансформацию титанового сырья и изделий из титана на всех этапах их жизненного цикла продукции. Эту отрасль составляют горнодобывающие предприятия, и предприятий цветной металлургии, научно-производственные структуры, предприятий обрабатывающих изделия из титана. Господствовавшая долгое время парадигма экономической интеграции в мировую глобальную экономику привела к проблемам в ряде производств, составлявших ранее как основу социально-экономического развития страны, так и отдельных отраслей, что нанесло серьезный урон производственной, технологической сфере обеспечения национальной безопасности. В работе [2] отмечено негативное влияние распада титановой отрасли как высокоорганизованного содружества

специализированных заводов, Всесоюзного института легких сплавов (ВИЛС) и Всесоюзного института авиационных материалов (ВИАМ). Возрождение этих производств и переформатирование их на выпуск качественно иной, конкурентоспособной, продукции должно сопровождаться рядом обеспечительных мер технологического плана, к которым как раз и относится развитие титановой отрасли. В этом аспекте титановая отрасль должна рассматриваться как один из ключевых технологических факторов обеспечения национальной безопасности. Положительные тренды технологического развития титановой отрасли в период с начала 2000-годов по настоящее время проявились, прежде всего, в образовании и развитии территориально-производственного объединения – корпорации ВСМПО-АВИСМА, завоевании им устойчивого положения на мировом рынке титана и активизации работ по реконструкции и модернизации производства, увеличения в производстве доли изделий глубокой переработки. Технологическими факторами, связанными с различными видами национальной безопасности, являются факторы, оказывающие влияние на производственную сферу и обороноспособность страны. Производственная сфера является базисом и фактором обеспечения не только экономической безопасности, но и экологической, энергетической, транспортной и других видов безопасности. Рассмотрим влияния технологического фактора национальной безопасности на обеспечение национальной безопасности на примере титановой отрасли. Неспособность промышленности страны производить конкурентоспособные на внутреннем и мировом рынке изделия, соответствующие современному уровню развития науки и техники, приводит к потере экономической независимости и обороноспособности, таким образом, проблема обеспечения технологической безопасности тесно связана с различными видами национальной безопасности. Связь технологической безопасности с экономической безопасностью страны обеспечивается возможностью выпуска конкурентоспособной на отечественном и мировом рынке продукции. Конкурентоспособность современной продукции во многом определяется свойствами материалов, из которых она произведена, а значит и возможностями производить и обрабатывать эти материалы. Титан является материалом, сочетающим в себе комплекс уникальных свойств, обеспечивающих конкурентоспособность продукции в самых разных отраслях народного хозяйства. Титановые сплавы находят применение при создании конкурентоспособной высокотехнологичной продукции для самых различных отраслей - авиационной и космической, судостроительной, автомобилестроительной, а также химической,

металлургической промышленности и медицины. Титановые сплавы могут быть использованы для создания изделий, эксплуатирующихся в условиях криогенных температур, до температуры жидкого водорода. В кораблестроении титановые сплавы находят применение благодаря сочетанию высокой коррозионной стойкости, немагнитности и высокой удельной прочности. В автомобилестроении перспективы использования титановых сплавов обусловлены возможностью повышения мощности автомобильных двигателей за счет снижения массы деталей без потери прочности. При изготовлении морских буровых установок использование титановых труб обеспечивает 23-кратную экономию по массе, в сравнении со стальными трубами, а долговечность труб возрастает в 10 раз [3]. Благодаря коррозионной стойкости применяются титановые сплавы и в металлургии, нефтехимической и химической промышленности для изготовления различных видов оборудования. Новейшее поколение авиалайнеров, например, Boeing787 имеет массу титановых деталей, превышающую 20%. В современных авиационных газотурбинных двигателях доля титановых деталей приближается к отметке 40%, при этом в компрессоре она может составлять почти 90% (приводятся усредненные показатели). Основным партнером Boeing стала российская Корпорации ВСМПО-АВИСМА. По некоторым оценкам ВСМПО-АВИСМА обеспечивает до 40% потребностей в авиационном титане Boeing, 60% потребностей EADS (Airbus) и 100% — Embraer [4]. Аддитивные технологии – яркий пример нетрадиционного подхода к использованию титановых сплавов. Развитие аддитивного производства в России требует создания оборудования для выпуска порошкового сырья и оборудования для трехмерной печати, тем более что рынок по данному сектору будет только расти. Мировой рынок только 3D-принтеров растет на десятки процентов в год и в ближайшее время составит по объему десятки миллиардов долларов США. Ориентация на закупку зарубежного оборудования в этой связи может быть определяющим фактором отставания в технологическом развитии в производстве сложных деталей из титановых сплавов. Технологическая безопасность, обеспечивающая возможность применения титановых сплавов при создании авиационной, ракетной, морской и сухопутной военной техники определяет вклад титановой отрасли в обороноспособность страны. В военно-морской промышленности из него изготавливаются, например, глушители для дизельных двигателей подводных лодок и другие изделия. Задача снижения массы танковой техники на 30% при сохранении прочности его брони также решается применением титановых сплавов. Титановая броня обеспечивает не только лучшую броневую защиту и большую

маневренность, но и снижение радиационного и теплового излучения, что снижает вероятность обнаружения боевых машин оптико-электронными средствами разведки. Вклад в такой компонент национальной безопасности как энергетическая безопасность страны вносит технологический фактор, связанный с производством титановых сплавов для атомной промышленности. Титановые сплавы находят широкое применение в атомной промышленности благодаря тому, что обеспечивают гарантированный ресурс работы на период до 60 лет, что сопоставимо с ресурсом работы ядерного реактора, из них изготавливают конденсаторы и рабочие лопатки паровых турбин, теплообменное оборудование. Основным поставщиком тонкостенных сварных труб для этих объектов является ОАО «Корпорация ВСМПО-АВИСМА» [5]. Кроме того, современные титановые сплавы в малой степени подвержены радиационному охрупчиванию, в них полностью отсутствует радиационно-стимулированная ползучесть и опасность вторичного излучения, быстро снимается наведенная активность [6]. Обеспечение экологической безопасности с технологической безопасностью связано с проблемой увеличения импорта конечной продукции титановых сплавов и применением современного производственного оборудования. Прогнозирование действия фактора технологической безопасности показывает, что уже в скором времени потребности отечественных производителей и совместных предприятий с участием заинтересованных в развитии с Россией не только экономического, но и военно-политического партнерства стран могут существенно возрасти. В связи с этим возникнут определенные проблемы, как относительно производства первичного сырья титановой отрасли, так и для первичного обеспечения товарной продукцией указанных предприятий. Санкционные меры, введенные против России рядом стран, неспособны разрушить отечественную экономику и ее отдельные отрасли, а лишь могут придать им импульс развития, вследствие ограничения поставок с запада высокотехнологичной продукции и некоторых видов сырья и материалов.

Литература:

1. О Стратегии научно-технологического развития Российской Федерации, Указ Президента РФ от 01 декабря 2016 года №6422.
2. *Ежов А.О.* Периодизация становления и развития титановой промышленности России: историография проблемы // Вестник ТГУ, т.20, вып. 11(151), 2015, с. 86-92.
3. *Ильин А.А., Колачев Б.А., Полькин И.С.* Титановые сплавы. Состав, структура, свойства. Справочник. – М.: ВИЛС-МАТИ, 2009.

4. URL: https://topwar.ru/128253-titДanovyy-udar-po-amerike-sem-raz-otmerili-odin-raz-ne-otrezhut.html Титановый удар по Америке: семь раз отмерили, один раз не отрежут? / Военное обозрение [Электронный ресурс]. - (Дата обращения: 20.10.2018).
5. https://www.lkmportal.com/articles/titan-i-titanovye-splavy-dlya-razlichnyh-otrasley-promyshlennosti [Электронный ресурс]. - (Дата обращения: 20.10.2018).
6. http://www.crism-prometey.ru/about/activities/titanium-alloys.aspx [Электронный ресурс]. - (Дата обращения: 20.10.2018).

Широкий А.А.

Групповой подход в системах ситуационной поддержки

Аннотация: Задачи управления крупномасштабными организационными системами предполагают анализ множества факторов различной природы. Для их решения необходимо привлекать множество экспертов в различных предметных областях и координировать их деятельность. Таким образом, возникает необходимость применения технологий коллективного (или группового) выбора, основанных на процедурах согласования индивидуальных предпочтений участников коллективного органа принятия решений (КОПР). В работе формально поставлена задача согласования предпочтений и сделан вывод об эффективности применения группового подхода в автоматизированных системах ситуационной поддержки.

Ключевые слова: автоматизированные системы управления, системы ситуационной поддержки, групповой подход, согласование предпочтений, КОПР

Введение

Задачи управления крупномасштабными организационными системами предполагают анализ множества факторов различной природы. Поиск решения осложняется тем, что факторы могут относиться к совершенно разным предметным областям. Такая ситуация весьма характерна для задач междисциплинарного характера, в частности, управления стратегическим сдерживанием. Для её решения необходимо привлекать множество экспертов в различных предметных областях и координировать их деятельность для определения целей, выявления и анализа существенных взаимосвязей между ними и средствами их достижения,

формирования критериев эффективности, набора ключевых индикаторов, оценки альтернатив и, в итоге, принятия управленческих решений.

Таким образом, возникает необходимость применения технологий коллективного (или группового) выбора, основанных на процедурах согласования индивидуальных предпочтений участников коллективного органа принятия решений (КОПР) [1, 2, 4, 5]. Хорошо известно, что качество сложных решений, принятых коллективом, в среднем выше, чем у решений, принимаемых отдельным лицом. Это можно объяснить невозможностью для отдельного лица, принимающего решения, обработать весь объём необходимых данных за приемлемое время. Поэтому решения, найденные группой не просто рациональны, но формируются именно благодаря тому, что вся группа участвовала в их выработке. В связи с этим весьма актуальной является задача создания условий для наиболее полного взаимодействия участников групп и различных групп между собой, для чего и применяется групповой подход.

При этом, однако возникает проблема согласования мнений. Эффективным способом её решения является проведение совещаний, в ходе которых участники КОПР выступают в роли экспертов, оценивающих эффективность возможных альтернативных решений и убеждающих других участников поддержать их мнение. Результатом такого конструктивного обсуждения формируется единое мнение, отражающему компромисс между участниками КОПР.

Постановка задачи группового предпочтения

Запишем для группового КОПР задачу принятия решения:

$$\langle S_0,\ T,\ R \mid S,\ A,\ L,\ Y,\ F(p), Y^* \rangle, \qquad (1)$$

где

S_0 – проблемная ситуация;

T – время для принятия решения;

R – ресурсы, затрачиваемые для принятия и реализации решения;

S – множество альтернативных ситуаций;

$A = (A_1, \ldots, A_k)$– множество целей;

$L = (L_1, \ldots, Y_l)$– множество ограничений;

$Y = (Y_1, \ldots, Y_m)$ – множество альтернативных вариантов решения;

Y^* – оптимальное решение;

$F(p)$ – функция группового предпочтения;

$p = (p_1, \ldots, p_d)$ – вектор индивидуальных предпочтений участников КОПР;

d – количество членов группы.

Задача группового предпочтения формулируется следующим образом.

Пусть предложен набор альтернатив $Y = (Y_1, ..., Y_m)$ для решения некоторой проблемной ситуации. Имеется КОПР из d участников. Каждый участник выбирает решения из набора в соответствии со своими индивидуальными предпочтениями. Назовём вектор $p = (p_1, ..., p_d)$ групповой оценкой решений. Нам необходимо сформировать единое групповое предпочтение $F = F(p_1, ..., p_d)$. Для этого индивидуальные предпочтения должны быть согласованы на основе некоторого критерия – принципа диктатора, большинства голосов или Парето.

Назовём коалицией группу участников КОПР с совпадающими целями. Обозначим множество коалиций как $V = (V_1, V_2, ..., V_s)$, где s – число коалиций. При $s = d$ число участников совпадает с числом коалиций, т. е. цели всех участников различны. При $s = 1$ коалиция единственна, включает всех участников КОПР и имеет единую цель. При количественной оценке предпочтений одно решение предпочитается в коалиции другому, если у всех участников коалиции одинаковое предпочтение. При этом последнее является взвешенной суммой предпочтений участников коалиции:

$$p_{V_j} = \sum_{i \in V_j} k_i p_{ij}. \qquad (2)$$

Здесь k_i – весовые коэффициенты индивидуального предпочтения p_{ij} i-го участника в j-й коалиции. Таким образом, каждой коалиции поставлена в соответствие её функция предпочтения, а в целом множество коалиций в КОПР характеризуется вектором $p = (p_{V_1}, ..., p_{V_s})$.

Обозначим n_{V_j} число участников коалиции V_j, причём $n_{V_1} + n_{V_2} + ... + n_{V_{j_s}} = d$. Групповое предпочтение будем определять в соответствии с одним из трёх принципов – принципа большинства, принципа диктатора и принципа Парето.

В первом случае групповое предпочтение соответствует предпочтению коалиции с числом участников, превышающим заданный порог:

$$F(p_{V_1}, p_{V_2}, ..., p_{V_s}) - p_{V_j}, \ n_{V_j} > \frac{B^d}{2}, \ B \in [1, 2] \qquad (3)$$

где p_{V_j} – функция предпочтения коалиции с числом участников n_{V_j}; B – задающий порог голосов коэффициент. При этом значение $B = 1$ соответствует простому большинству, $B = 4/3$ – квалифицированному большинству с порогом, равным 2/3, а $B = 2$ – абсолютному большинству.

При применении принципа диктатора мы должны принять предпочтение одного из участников в качестве группового предпочтения. Тогда функция группового предпочтения примет вид:

$$F(p_1, p_2, ..., p_d) = p_K, \quad (4)$$

где p_K – функция предпочтения диктатора. Следует отметить, что в этом случае применение понятия КОПР становится бессмысленным, поскольку групповое предпочтение соответствует индивидуальному.

Принцип Парето предполагает, что группа может улучшать свои решения без нанесения ущерба каждому участнику в отдельности, поэтому его следует использовать при сильной связи всех участников КОПР, выражающейся в общности целей. Формально решение Y^* называется оптимальным по Парето, если не существует другого решения, строго лучшего, чем Y^* для всех участников КОПР вместе [3], т. е.

$$[p_1(Y^*), ..., p_d(Y^*)] \geq [p_1(Y_j), ..., p_d(Y_j)] \ \forall j : Y_j \neq Y^*. \quad (5)$$

Согласно этому принципу решение Y_i следует предпочесть решению Y_j, если вектор значений функции индивидуального предпочтения участника КОПР для решения Y_i не хуже, чем для Y_j. Следовательно, $Y_i \geq Y_j$, если

$$[p_1(Y_i), ..., p_d(Y_i)] \geq [p_1(Y_j), ..., p_d(Y_j)]. \quad (6)$$

Это соотношение выполняется тогда, когда все участники группы оценили решение Y_i не хуже решения Y_j и как минимум один участник высказался за строгое предпочтение решения Y_i по сравнению с Y_j, т. е.

$$p_s(Y_i) \geq p_s(Y_j),\ p_k(Y_i) > p_k(Y_j),\ s \neq k,\ s = 1, 2, ..., d. \quad (7)$$

Сравнение всех решений по векторам значений функций предпочтения позволяет определить множество эффективных решений, которое называется множеством Парето.

Заключение

Эффективность автоматизированных систем ситуационной поддержки группового принятия решений оценивается по показателям, характеризующим качество и эффективность, во-первых, самих принятых решений, а во-вторых – процесса их принятия (поведения системы). Степень участия членов группы в решении проблемы и их персональный вклад в это решение является одним из показателей качества проведения совещания участников КОПР. Автоматизированные системы поддержки процесса группового принятия решений обеспечивают не только более полное участие всех членов группы в процессе принятия решений, но и позволяют более чем вдвое сократить требуемое для принятия решений время.

Литература:

1. *Евланов Л. Г.* Теория и практика принятия решений. – М.: Экономика, 1994. – 176 с.

2. *Драккер П. Ф.* Управление, нацеленное на результаты. – М.: Технологическая школа бизнеса, 1994. – 191 с.
3. *Подиновский В. В.*, *Ногин В. Д.* Парето-оптимальные решения многокритериальных задач. – М.: Физматлит, 2007. – 256 с.
4. *Шульц В. Л.*, *Кульба В. В.*, *Шелков А. Б.*, *Чернов И. В.*, *Богатырева Л. В.* Анализ методов группового управления развитием арктической зоны российской федерации // Тренды и управление. – № 4, 2017. – С. 35–51.
5. *Эддоус М.*, *Стенсфилд Р.* Методы принятия решений. – М.: Аудит, ЮНИТИ, 1997. – 587 с.

Косяченко С.А., Богатырева Л.В.

Некоторые исторические аспекты стратегического сдерживания

Аннотация: Рассматривается вопрос стратегического сдерживания в исторической ретроспективе.

Ключевые слова: стратегическое сдерживание, ядерное оружие, силовое и несиловое давление

Ключевую роль в трансформации взглядов на механизмы реализации сдерживания сыграл научно-технический прогресс. Появление ядерного оружия в значительной степени обогатило арсенал национальных средств сдерживания, позволив вести речь об устрашении оппонента на совершенно иных уровнях информационного взаимодействия. Развитие средств поражения позволило в составе инструментов сдерживания с условной самостоятельностью рассматривать т.н. силовые инструменты.

Для теории сдерживания характерно несколько парадигм, проявившихся на различных этапах ее становления [1].

1) Парадигма «стратагемного» сдерживания в неядерном мире (до 1940-х годов). В целом основной характеристикой знаний о сдерживании в этот период выступает их структура в форме набора их тактических и психологических приемов, используемых в конкретных случаях древними полководцами, в основе которых лежит идея воздействовать на восприятие противника таким образом, чтобы удержать его от нежелательных поступков. Понятие «сдерживание» до середины XX в. не имело конкретного политического наполнения, теоретического обоснования, само сдерживание не рассматривалось как основа официальных военно-политических установок государства.

2) Парадигма «ядерного» сдерживания (1945 - конец 1980-х годов). Характерными для начального периода формирования этой парадигмы являются ее основания, выраженные в форме доктрин или концепций (концепция всеобщей ядерной войны, концепция ограниченной ядерной войны, концепция взаимного гарантированного уничтожения).

Д. Кеннан является признанным автором доктрины сдерживания, которую он сформулировал и анонимно опубликовал, опираясь на свои идеи, изложенные в «Международном положении России после окончания войны с Германией» (1945 г.) и секретной телеграмме, отправленной госдепартаменту в феврале 1946 г. Согласно Кенанну, в основе «политики сдерживания» должен лежать ментальный фактор, значение которого прежде игнорировалось. В современных геополитических моделях он приобрел решающую роль: противоборство перешло в область идей и ценностей. Кеннан объяснял природу оппозиционности внешней политики СССР в отношении западных держав изначальным свойством коммунистического мировоззрения и советской системы - враждебностью к внешнему миру. Ее смысл состоит в том, чтобы противодействовать «русским при помощи всегда имеющейся в наличии противостоящей силы в любой точке, где проявляются признаки покушения на интересы мирного и стабильного мира».

Проблема сдерживания разрабатывалась американскими военными, политиками и учеными. В СССР понятие сдерживание не использовалось. Практика военного дела и внешняя политика подходили к оценке текущей ситуации с точки зрения классового подхода, т.е. заставляли адекватно отвечать на вопросы военного и политического противостояния.

Основной тенденцией военных стратегов стало осмысление двух военно-технических сдвигов. В 1953 г. появилось термоядерное оружие, а также в середине 1950-х гг. были созданы ракеты-носители ядерного оружия, что позволило доставлять ядерные боезаряды к цели с высокой гарантией. Возникла техническая возможность выбирать масштаб и набор целей в применении ядерного оружия в ходе военных действий, соразмерно стратегической обстановке.

Одновременно во второй половине 1950-х гг. произошла революция в средствах доставки - были созданы баллистические ракеты стратегического назначения и ядерные силы превратились в «триады». Это позволило перейти к стратегии «гибкого реагирования», поскольку авиационные «монады» были оптимальны лишь для «массированного возмездия». Следующим по важности фактором следует считать усовершенствование точности доставки - создание разделяющихся головных частей индивидуального наведения на рубеже 1970-х гг. На этой технологической базе была создана концепция «ограниченных ядерных ударов», по сути - дальнейшее развитие «гибкого реагирования».

Сдерживание может быть эффективным только до тех пор, пока политическая цена действий или бездействия остается ниже прогнозируемых издержек. Соответственно, чем выше прогнозируемый ущерб от войны, тем более весомые политические требования могут быть реализованы без непосредственного применения силы, исключительно через сдерживание.

Вместе с тем политическая цель имеет свою цену не только для того, против кого она выдвинута, но и для того, кто ее выдвигает. Сдерживание по самой своей природе взаимно и обусловлено военными возможностями каждой из сторон, какими бы различными они ни были. При этом сдерживающий эффект военного потенциала более слабой стороны проявляется в корректировке тех политических целей, которые выдвигает более сильная сторона в ходе противостояния.

В силу этого политические цели, реализуемые через политику сдерживания, неизбежно оказываются соразмерны со всей системой национальных приоритетов сдерживающей стороны и той ценой, которую она готова платить в случае, если сдерживание не сработает и противник предпочтет варианты силового ответа. Таким образом, сдерживание - прежде всего, политико-психологический феномен, для которого характерно сложное сочетание прямых и обратных связей [2, 3].

Ситуация «взаимного гарантированного уничтожения» (ВГУ) была постулирована Р. Макнамарой в конце 1960-х гг. Именно она стала базой для кодификации ядерного сдерживания в договорах об ограничении стратегических вооружений. В рамках негласного кодекса поведения СССР и США согласились признать ситуацию ВГУ, которая ограничивала свободу действий каждой из сторон. Теоретически такое положение сохраняется до сих пор [4].

Гарантируя стратегическую стабильность, ситуация взаимного гарантированного уничтожения существенно связывает ядерным державам руки в мировой политике. Поэтому, начиная с середины 1970-х гг., непрерывно ведется поиск выхода из этой ситуации, что составляет основное содержание третьей волны развития теории ядерного сдерживания.

3) Парадигма стратегического сдерживания и стратегической стабильности (2000 - настоящее время). Смена парадигмы сдерживания на рубеже XXI в. во многом связана с процессом появления новых инструментов как силового, так и несилового давления (принуждения одних государств другими). Стало заметным продолжающееся смещение в сторону более востребованных теорий сдерживания с помощью обычных вооружений, а также применения сдерживания скорее к региональным, а не глобальным системам безопасности. С началом XXI в. стали предприниматься более активные попытки проецирования теории

сдерживания на новые вызовы и угрозы безопасности, в том числе нетрадиционного характера.

В настоящий момент развертываются новые высокоточные средства поражения в неядерном оснащении, способные решать стратегические задачи «проецирования силы» на любые регионы мира. В связи с этим вопросы дальнейшего развития теоретических основ стратегического сдерживания сохраняют свою актуальность.

Литература:

1. *Печатнов Ю.А.* Ретроспективный анализ эволюции концепций сдерживания // Вооружение и экономика, 2010. № 1 (9). С. 11-18.
2. *Савельев А.Г.* Стратегическая стабильность и ядерное сдерживание: уроки истории // Вестник МГУ. Сер.25. Международные отношения и мировая политика. 2015 №3. С. 57-84.
3. *Веселов В.А.* Ядерный фактор в мировой политике: структура и содержание // Вестник МГУ. Сер.25. Международные отношения и мировая политика. 2010 №1. С. 68-90.
4. *Колтунов В.С.* Стратегические ядерные силы США и России - состав, ядерные доктрины и программы развития. Текст лекции В.С. Колтунова, состоявшейся 1 октября 2003 г. в МФТИ для слушателей курса «Режим нераспространения и сокращения оружия массового поражения и национальная безопасность» [Электронный ресурс]. - http://www.armscontrol.ru/course/lectures03b/vsk031001.htm (Дата обращения: 22.08.2018)

Еременко В.А., Манаенкова Н.И.

Влияние пороговой нелинейности на безопасность системы взаимодействия волна – ионосфера

Аннотация: Рассмотрена задача нелинейного распространения радиоволн. Исследованы условия существования солитонов, - сосредоточенных решений соответствующих волновых уравнений, для Керровской и для пороговой нелинейности. В случае пороговой нелинейности взаимодействие отдельных солитонов может приводить к их слиянию в уединенную волну большой мощности.

Ключевые слова: распространение радиоволн, нелинейные волны, пороговая нелинейность, взаимодействие солитонов

Нелинейные эффекты при распространении радиоволн в ионосфере проявляются уже для радиоволн относительно небольшой интенсивности. Так как длина свободного пробега электронов в плазме значительна, электрон успевает получить от поля заметную энергию за время одного пробега. В результате электроны плазмы сильно «разогреваются» в электрическом поле. Диэлектрическая проницаемость плазмы становится зависящей от электрического поля волны. Нелинейные эффекты могут проявляться как самовоздействие волны и как взаимодействие волн между собой. Теоретические оценки эффектов разогрева ионосферной плазмы мощным радиоизлучением появились достаточно давно [1,2]. Экспериментальные подтверждения взаимодействия мощного коротковолнового излучения с ионосферной плазмой при наклонном распространении [3,4] активизировали дальнейшее развитие теории этого взаимодействия [5,6].

Наиболее часто используемая модель нелинейности, - так называемая Керровская нелинейность, где нелинейное возмущение диэлектрической проницаемости пропорционально квадрату модуля амплитуды волны. Это предположение позволяет описывать основные эффекты, возникающие при нелинейном взаимодействии излучения со средой распространения. Однако этот подход имеет определенные ограничения. Очевидно, что нелинейные эффекты не возникают, пока мощность волнового поля недостаточна. Но, как только величина амплитуды волны преодолевает некоторое пороговое значение, происходит «пробой» среды и возникает нелинейная зависимость диэлектрической проницаемости от амплитуды волнового поля.

Рассмотрим типичную картину распространения радиоволн в ближайшем околоземном пространстве. В области фокусировки лучей интенсивность сигнала увеличивается значительно, следовательно, возможно нелинейное взаимодействие радиоволны с ионосферой [5,6].

Чтобы описать волновое поле в этой малой области, воспользуемся уравнением Гельмгольца для амплитуды волнового поля

$$\Delta u + k^2 \cdot \varepsilon \cdot u = 0 ,$$

где k - волновое число и ε - диэлектрическая проницаемость.

При высокой интенсивности излученного сигнала диэлектрическая проницаемость становится зависимой от амплитуды излученной волны и тогда для описания распространения радиоволн потребуется решать нелинейную задачу.

Будем рассматривать распространение узкого коротковолнового пучка. Построим решение уравнения Гельмгольца, сосредоточенное в малой окрестности лучевой траектории. В этой окрестности введем ортогональную систему координат: x - длина дуги траектории; y -

расстояние вдоль направления, ортогонального лучу. Представим комплексную функцию u в виде: $u = v \cdot \exp(ik\psi)$, где v и ψ - действительные функции, и перейдя к безразмерным переменным $\xi = kx$, $\eta = ky$, получим в главном приближении типичную задачу нелинейного распространения радиоволн [7].

$\frac{d^2v}{d\eta^2} = q^2 v - (1 + \varepsilon_n(v^2))v$, где $q = \frac{d\psi}{d\xi}$ - безразмерное волновое число, $\varepsilon = 1 + \varepsilon_n(v^2)$. Первый интеграл этого уравнения имеет вид $\left(\frac{dv}{d\eta}\right)^2 - \lambda^2 v^2 + F(v^2) = E, \quad E - const$, $F(v^2) = \int_0^{v^2} \varepsilon_n(t)dt$, $\lambda^2 = q^2 - 1$. Это уравнение при $E = 0$ предполагает существование сосредоточенных волн, при условии, что уравнение $F(t) - \lambda^2 t = 0$ имеет корни $t = 0$ и $t = t_0 > 0$ [7].

Рассмотрим далее модель распространения волны в условиях пороговой нелинейности, считая, что нелинейные эффекты возникает только для волн, интенсивность которых превышает некоторое пороговое значение. Нелинейное возмущение диэлектрической проницаемости в этом случае может быть представлено формулой:

$\varepsilon_n(v^2) = \alpha v^2 \cdot \theta(v^2 - A^2)$,

где $\theta(x)$ - функция Хэвисайда, $\theta(x) = \begin{cases} 1 & \text{ïðè } x \geq 0 \\ 0 & \text{ïðè } x < 0 \end{cases}$,

A - пороговое значение. В этом случае функция $F(v^2)$ имеет вид

$$F(v^2) = \int_0^{v^2} \varepsilon_n(t)dt = \frac{\alpha}{2}(v^4 - A^4) \cdot \theta(v^2 - A^2)$$

Нетрудно видеть, что и в этом случае уравнение $F(t) - \lambda^2 t = 0$ имеет простые корни $t = 0$ и $t = t_0 > 0$, что гарантирует существование сосредоточенного решения.

Сосредоточенное решение в среде с пороговой нелинейностью очень напоминает обычный солитон, но пучок – более узкий в центре и имеет «длинные хвосты». Примеры пучков с одинаковой энергией для различных уровней порога (A^2=0, линия 1; A^2=0,6, линия 2; A^2=0,9, линия 3) приведены на рис.1.

При малых значениях порога A^2 максимум пучка чуть превышает максимум стандартного Керровского солитона. При уровне порога превышающем 0,8 амплитуда начинает уменьшаться.

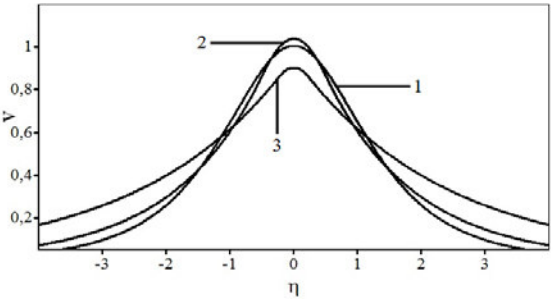


Рис. 1 – Вид солитонов в среде с пороговой нелинейностью

Пример взаимодействия уединенных волн в среде с пороговой нелинейностью приведен на рис. 2. (Керровские солитоны - линия 1; “пороговые” солитоны с порогом A^2 =0,6 - линия 2).

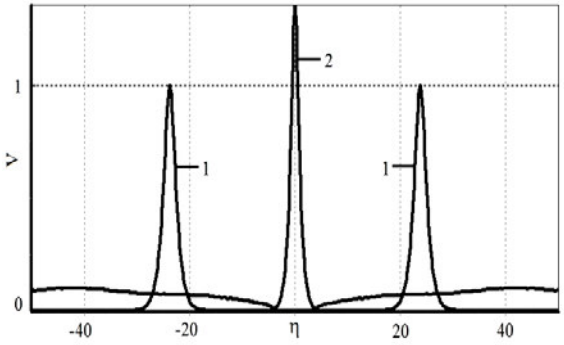


Рис. 2 – Взаимодействие солитонов в среде с пороговой нелинейностью

Взаимодействие таких пучков может значительно отличаться от взаимодействия Керровских солитонов, восстанавливающих свою форму после столкновения. Как видно из рисунка, в отличие от “стандартных” солитонов, разошедшихся после взаимодействия, “нестандартные” солитоны слиплись в единый конгломерат повышенной интенсивности. Таким образом, распространение мощного радиоизлучения в ионосфере в

условиях пороговой нелинейности может привести к изменениям среды распространения сигнала, небезопасным для систем радиосвязи, навигации, радиолокации.

Литература:
1. *Гинзбург В.Л., Гуревич А.В.* Нелинейные явления в плазме, происходящие в переменном электромагнитном поле. // Успехи физических наук. 1960. Т.70. С.201-246.
2. *Farley D.T.* Artificial heating of the electrons in the F-region of the ionosphere. //Journal of Geophysical Research. 1963. V.68. P.401-413.
3. *Бочкарев Г.С., Ким В.Ю., Лобачевский Л.А., Лянной Б.Е., Мигулин В.В., Сергеенко О.С., Черкашин Ю.Н.* Взаимодействие декаметровых радиоволн на частотах вблизи МПЧ F2 при наклонном распространении. //Геомагнетизм и Аэрономия. 1979. Т.19. С.830-833.
4. *Bochkarev G.S., Eremenko V.A., Lobachevcky L.A., Ljannoy B.E., Migulin V.V., Cherkashin Yu.N.* Non-linear in teraction o f decameter r adio waves at close frequencies on oblique propagation. //Journal of Atmospheric and Terrestrial Physics. 1982. V.44. № 12. P.1137-1141.
5. *Бочкарев Г.С., Еременко В.А., Лобачевский Л.А., Лянной Б.Е., Мигулин В.В., Черкашин Ю.Н.* Моделирование воздействия мощной волны на ионосферу при наклонном падении. //Геомагнетизм и Аэрономия. 1980. Т.20. С.848-853.
6. *Molotkov I.A., Cherkashin Yu.N.* S ome nonlinear ef fects o f wave b eams propagation in th e io nosphere.// Journal o f A tmospheric an d T errestrial Physics. 1994. V. 56. № 11. P. 1477-1481.
7. *Еременко В.А., Манаенкова Н.И.* Влияние типа нелинейности на существование сосредоточенных волн. // Успехи современной радиоэлектроники. 2017. №6. С.49-54.

Товмасян Т.А.

Анализ характеристик рисков ЧС в Армении

Аннотация: В работе представлен анализ чрезвычайных ситуаций, которые наиболее вероятны на территории Армении. Для реализованных ЧС проведен анализ среднегодового экономический ущерба. Определены характерные режимы сейсмичности в регионе, которые проявляются в ступенчатости сейсмической активности либо ее периодичности. Проанализированы циклы сейсмической активизации.

Ключевые слова: транспортные и промышленные аварии**,** меридиональное укорочение, степень сейсмичности. сейсмические события, очаги землетрясений, геохимические пробы

Армения является одной из наиболее подверженных бедствиям стран, среди своих соседей по южному Кавказу. Страна уязвима в отношении бедствий, вызываемых как природными угрозами, включая землетрясения, засухи, наводнения, оползни, лавины, грязевые потоки, сильные ветры, снежные бури, заморозки и град, так и техногенными, включая транспортные и промышленные аварии. Наиболее серьёзную угрозу в Армении представляют землетрясения. Согласно GSHAP (GSHAP, 1998г.) Армения расположена в зоне, характеризующейся умеренной до высокой степенью сейсмической опасности.

События с вероятностью возникновения в 0,5% в год в среднем происходят раз в 200 лет и, как правило, соответствуют по своим характеристикам катастрофическим событиям. События с вероятностью возникновения в 5 и 20 процентов в среднем возникают каждые 20 и 5 лет соответственно.

Анализ данных о бедствиях (1987-2008гг.) показывает, что хотя в количественном отношении землетрясений за этот период произошло меньше чем наводнений, землетрясения нанесли стране непропорционально большой ущерб. В результате наиболее разрушительного землетрясения, произошедшего 7 декабря 1988г. в Спитаке с магнитудой 6,9, погибло 25 000 и пострадало 1,6 млн человек. Прямой экономический ущерб по оценкам составил 14,2 млрд долларов. При Ноемберянском землетрясении в июле 1997г. число пострадавших составило 15 000 человек, а нанесённый экономический ущерб был оценен в 33,33 млн. долларов. Также серьёзную угрозу в Армении представляют засухи. Если взять события, произошедшие за последние несколько лет количество пострадавших от засухи в 2000г. составило 297 тыс. человек, а экономический ущерб равнялся 100 млн. долларов. Также серьёзную угрозу представляют наводнения. В результате одного единственного наводнения в июне 1997г. пострадало 7 000 человек, а нанесённый ущерб составил 8 млн. долларов. По данным за указанный период, никакие бедствия, связанные с оползнями, в Армении зафиксированы не были. Однако одна третья часть территории Армении подвержена угрозе оползней. За последние пять лет в результате оползней без жилья остались более 2 000 семей: в среднем по 400 семей в год. В апреле 2004г. в результате резкого понижения температуры на 15ºС на обширных площадях пострадали сельскохозяйственные посевы. Армении пришлось столкнуться и с многочисленными техногенными бедствиями. Имеются данные о трех крупных транспортных и одной производственной аварии, а

также двух несчастных случаях. Согласно отчетам, в результате этих аварий погибло 119 и пострадало 810 человек. Однако данных об экономическом ущербе нет. Страна также подвержена угрозе химического заражения, ввиду наличия химических заводов и трубопроводов для транспортировки химических продуктов, а также возможной опасности радиоактивного заражения – ввиду наличия атомной электростанции в Метсаморе. Международное агентство по ядерной энергии (МАГАТЭ) считает, что эта АЭС представляет опасность из-за своего конструктивного исполнения и расположения в сейсмоопасном районе (Анагности, 2008г.).

Характеристики риска, индикаторы уязвимости, такие как количество произошедших бедствий, погибших, пострадавшего населения и размер экономического ущерба, были соотнесены с типами угроз и распределены по пятилетним интервалам, охватывающим двадцатилетний период с 1988 по 2007гг. Из показаний соотношений между количеством погибших, пострадавших, объёмом экономического ущерба и каждым типом угрозы сделаны анализы по распределению по временным показателям и распределённые по пятилетним периодам. Данные показали, что из всех угроз землетрясения стали причиной наибольшего числа погибших (25 000), наибольшего числа пострадавших (1,66 млн) и нанесли самый серьёзный экономический ущерб (14,2 млрд долларов), несмотря на низкую частоту (два события за указанный период). Период с 1988 по 1992гг. был наименее благоприятным с точки зрения количества погибших (25 038), количества пострадавших (1,64 млн.) и объёма экономического ущерба (14,2 млрд долларов). Самая высокая частота повторяемости отмечается в отношении наводнений и транспортных аварий (0,15 в год). Уровень смертности является самым высоким в результате землетрясений (1,250). Индекс относительной уязвимости (погибшие/ год/млн.) был самым высоким в отношении землетрясений (417). На втором месте следуют транспортные аварии (1,37).

Преобладающий фактор риска в Армении связан с землетрясениями, среднегодовой экономический ущерб в результате которых составляет 680 млн. долларов. Далее с большим отставанием следуют засухи (СГУ 6 млн. дол.) и наводнения (0.7 млн дол.) (Рис. 3а). Ущерб от всех угроз с периодом повторяемости в 20 лет составляет 3,94 млрд. долларов (43% ВВП), тогда как ущерб от событий с периодом повторяемости в 200 лет равняется 12,16 млрд долларов (132,5% ВВП). Следует отметить, что приведённый выше анализ является "необъективным" ввиду землетрясения, произошедшего в Спитаке в декабре 1988г.

Ввиду большого количества и импульсного характера проявления землетрясений их изучение можно проводить статистическими методами, принятыми в математике для подобных исследований. Произведём

исследование периодичности сейсмических событий в регионе на основании временных гистограмм. Поминутное распределение частоты встречаемости землетрясений региона в окне длительностью в одни сутки показывает статистически неслучайную привязанность сейсмических событий к полудню по местному времени. Выявлена полуденная приуроченность сейсмических событий, в то же время прослеживается небольшая их активизация, приуроченная к полуночи. Минимальные значения наблюдаются при значениях, соответствующих 180 и 900 минутам, что соответствует 3 часам утра и 3 часам дня местного времени. Эта выявленная особенность суточной периодичности сейсмичности региона не может быть случайной, так как основана на большой и статистически значимой выборке. Подобная 12- и 24-часовая квазипериодичность сейсмичности в приведенном каталоге может быть важной составляющей тех низкочастотных природных процессов, которые ответственны за процесс зарождения и эволюции очагов сильных землетрясений. Следует также отметить, что 12- часовой период цикличности, по-видимому, составляет самую высокочастотную часть спектра среди относительно низкочастотных циклических природных процессов, отмеченных в регионе. Половина всех сейсмических событий региона приходится на промежуток времени от 9 до 15 часов по Гринвичскому времени. Эти данные полностью подтверждают сделанное на данных по Армении наблюдение приуроченности землетрясений к полудню местного времени и подчеркивают важность постоянства суточной привязанности времени отбора геохимических проб.

Для более детального анализа распределения сейсмических событий и их зависимости от суточного времени необходимо проследить поминутное суточное распределение землетрясений, в связи с точной привязкой к координатной сетке в зависимости от восточной долготы реального положения Солнца в зените. Это необходимо потому, что реальный полдень и часовой полдень в связи с часовой разбивкой могут существенно различаться. Так, к примеру, когда часовая стрелка находится на 12:00 по полудни, то считается, что Солнце находится в зените на всём пространстве от Черного до Каспийского морей. Однако истинное положение зенита Солнца может быть в любой точке этого промежутка и должно быть уточнено для каждого сильного события. Интересно, отметить, что разрушительное Спитакское землетрясение в декабре 1988 года произошло в близкое к полудню местное время 11 часов 41 мин. Более подробный анализ проведенный для этого землетрясения, показал, что данное событие произошло в момент, когда Солнце по отношению к эпицентральной точке находилось в 55 минутах до своего истинного зенита, а Луна 40 минут как прошла точку своего апогея. Фактически само землетрясение произошло по времени в точке, когда воздействие комбинированных гравитационных сил Луны и Солнца достигло

максимума. Это обстоятельство показывает важность учета комбинированного влияния не только солнечного, но и лунного (лунные сидерические сутки) периода на цикличность сейсмических событий.

Таким образом, изучение сейсмического режима Армении и сопредельных областей за последние 40 лет показывает наличие двоякого характера сейсмичности. С одной стороны это выявленный характер ступенчатости сейсмического режима, маркируемый сильными сейсмическими событиями, с другой - его периодический характер. Активизация сейсмичности имеет несколько периодов длительностью в 12 часов, одни сутки, а также 14 и 28 суток. Выявленные особенности сейсмического режима необходимо учитывать при проектировании режима опроса сетей по изучению процессов возникновения сильных землетрясений в регионе. Наличие периодичности сейсмического режима может стать важным также при обработке и интерпретации данных, собранных с мониторинговых сетей, ведущих продолжительные наблюдения. Более глубокое изучение комплексного проявления ступенчатого и волнового характера сейсмичности в регионе поможет лучше понять природу и механизм возникновения, как сильных землетрясений, так и их предвестников.

Литература:

1. Armenia C ountry P aper - Land P olicy - Prepared f or t he S outh Caucasus Regional Land P olicy C onference, T ibilisi, F ebruary 2 4-26 2003; Communities Finance Officers Association (CFOA) 2003, Yerevan.
2. *Muradyan A.* The land consolidation pilot project in Armenia: preparation of a national strategy and experiences in the field. Real Property Valuation and Monitoring Department, http://www.fao.org/fileadmin/user_upload/Europe/documents/Events_2007/Lan d2007/Armenia.pdf. (Дата обращения: 15.11.2018).
3. *Igumnov V., Stepanian Z., Kazarian A.* On t he mechanism o f t he geochemical precursors to earthquake. "Abstract on International Conference on Continental Collision zone: earthquake and earthquake hazard reduction". Yerevan, Armenia, 1993, p.17.
4. *Kazarian A., Igumnov V.* Some as pects o f ear thquake p rediction b y geochemical methods", "Abstract o n I nternational C onference o n Continental Collision z one: earthquake a nd e arthquake hazard r eduction". Yerevan, Armenia, 1993, p.46.
5. *Джрбашян Р.Т., Казарян Г.А., Карапетян С.Г., Меликсетян Х.Б., Мнацаканян А.Х., Ширинян К.Г.* Мезокайнозойский базальтовый вулканизм северо-восточной части Армянского нагорья. Изв. НАН Армении, сер. Науки о Земле, Ереван, 1996, 1-3, с.19-32.

V. Методы моделирования и принятия решений при управлении безопасностью сложных систем

Райков А.Н.

Стратегическое совещание с применением экспертных процедур и когнитивного моделирования для повышения качества показателей в системах обеспечения безопасности

Аннотация: В условиях обострения международной обстановки, введения экономических санкций растет актуальность повышения качества систем обеспечения безопасности (национальной, экономической и др.). При этом особое внимание уделяется росту качества исходных данных, показателей, на основе которых осуществляется целеполагание и принимаются решение. Наиболее сложно обеспечить качество неколичественной информации, формируемой экспертным путем. Здесь могут помочь специальным образом организованные стратегические совещания, включающие сетевые экспертные процедуры, когнитивное и эволюционное моделирование, определение согласованности экспертных оценок. Имеется практическая апробация подхода.

Ключевые слова: системы безопасности, стратегические совещания, качественные показатели, обратные задачи, экспертные процедуры

Качество функционирования систем обеспечения безопасности (национальной, экономической, информационной и др.), например, системы распределённых ситуационных центров [1], в значительной степени определяется достоверностью имеющихся исходных данных. Обычно под контролируемые показатели формируются соответствующие методики сбора и обработки данных. Обычно данные опираются на статистику. Однако различные нюансы ситуации, учет новых угроз и рисков, случайным образом выявленных факторов может потребовать быстрого принятия решений по формированию новых исходных данных, ранее не предусмотренных методиками.

При этом в повышении качества исходных данных особо нуждаются качественные факторы, полученные, например, экспертным путем. Вместе с тем, даже данные (показатели), формируемые по сложным методикам на основе официальной статистической информации, нуждаются в качественной верификации, проверке. Это может быть осуществлено путем, например:

Проведение стратегического совещания, на котором в групповом экспертном процессе и в контексте поставленных целей (национальных целей, обеспечения национальной безопасности, обеспечения экономической безопасности и др.) участники совещания (далее, команда), ответственные за решение проблем, приходят к согласию относительно факторов (показателей) и отношений между ними, характеризующих детальные аспекты этих проблем.

Для повышения объективности и достоверности экспертных оценок требуется верификация (проверка) создаваемых экспертами модели, на правильность, адекватность модели реальной действительности через их отображение на иные пространства (автоматизированное «дообучение» или построение модели).

Стратегическое совещание проводится по строго определенной методике [2]. При решении оперативных вопросов оно может носить сетевой характер, то есть проводиться в территориально распределенной среде с подключением удаленных экспертов.

Сетевое совещание проводится под непосредственным председательством Руководителя коллектива (с согласованной выработкой целей, формулированием проблем, построением путей действий) и ведется когнитологом (модератором), владеющим специальными методами. Методики проведения сетевых стратегических совещаний выстраивается на основе использования специальных методов, например:

- стратегического совещания с подключением экспертных процедур и познавательного (когнитивного) моделирования, обеспечивающего стратегический прогноз по нескольким качественным факторам;
- эволюционных вычислений, помогающих решать обратную задачу и обеспечивающих учет множества «теневых» факторов и мнений экспертов;
- решения некорректных задач в топологических пространствах [3], теории катастроф, фундаментальной термодинамики и конвергентного управления;
- латентного синтеза решений, использующего, помимо контекста экспертных сообщений, данные о трафиках электронных сообщений при взаимодействии экспертов;

– социологических исследований, проведения фокус-групп и глубинных интервью;
– статистического моделирования и прогноза (стандартные методы);
– определения согласованности экспертных оценок;
– определения на основе моделирования поправочных стратегических коэффициентов для уточнения статистического прогноза и др.

Остановимся подробней на основных из перечисленных пунктах. Так, типовой порядок модерации *стратегического совещания* включает следующие этапы:
– Предварительное формирование дерева целей решения проблемы с поддержкой метода анализа иерархий;
– Выявление внешних факторов, характеризующих ситуацию (SWOT-анализ);
– Выявление факторов, характеризующих внутренние возможности команды;
– Формирование приоритетного перечня проблем, препятствующих достижению целей;
– Формирование перечня перспектив (направлений) действий;
– Оценка приоритетов перспектив (направлений) и влияния различных факторов на развитие ситуации;
– Оценка различных сценариев действий, ответы на вопросы, типа «Что делать?»;
– Подготовка рекомендаций.

В процессе проведения совещания формируется приоритетный перечень проблем, препятствующих достижению целей. Для этого заполняется Матрица «Окно возможностей». Строки и столбцы этой матрицы соответствуют внутренним и внешним факторам. На пересечении строки и столбца ставится экспертная оценка важности сочетания соответствующих факторов для решения проблемы. Например, если некий фактор угрозы значим для сильной стороны команды, то оценка значимости такого сочетания будет высокой. Используется десятичная шкала от -1 до 1.

Такой анализ позволяет, исходя из состояния внешней среды, определить, насколько существенны сильные стороны и слабы слабые, а также насколько важны угрозы и возможности для роста эффективности управления.

Эволюционные вычисления. Наиболее сложный вопрос, на который должно ответить совещание, «Что надо сделать, чтобы…..?». При поиске ответа на этот вопрос (обратная задача) можно использовать метод эволюционных вычислений генетического алгоритма (Рис. 1). С его

помощью можно быстро определить оптимальное соотношение управляющих факторов, создающих необходимую синергию действий.

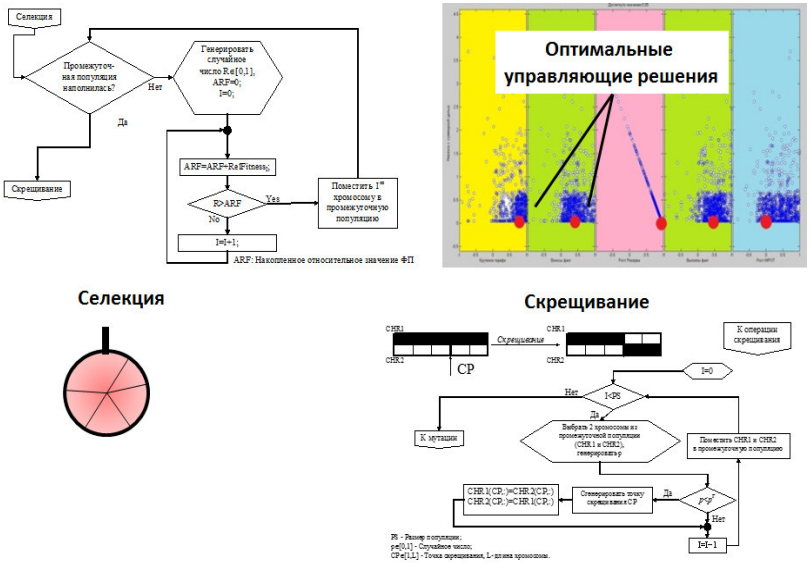


Рис. 1 – Генетический алгоритм решения обратной задачи на когнитивном графе

Верификация данных, полученных экспертным путем, может быть проведена с применением метода анализа больших данных, то есть путем отображения элементов имитационной модели на релевантные массивы больших данных. При этом предполагается, что сначала строится когнитивная модель, а затем она верифицируется на больших данных.

В разработанном подходе алгоритм проверки наличия связи между двумя факторами имитационной модели предусматривает несколько вариантов решения:

– «Связь присутствует с высокой вероятностью» – найден релевантный документ или несколько документов, в которых есть ключевые слова обоих факторов;
– «Связь присутствует с низкой вероятностью» – не найден релевантный документ или несколько документов;
– «Связь отсутствует» – для каждого фактора найдены непересекающиеся совокупности релевантных документов, либо вообще не найдены релевантные документы.

При таком подходе:

– В позитивном направлении трансформируется когнитивная модель и качество исходных данных;
– Повышается качество и оперативность получения искомого результата на основе моделирования;
– Улучшается качество самих данных (очистка данных).

Методы верификации имитационной модели с применением больших данных могут совершенствоваться и далее, вплоть до доведения процесса до автоматизации построения имитационной модели на основе анализа больших данных с применением средств искусственного интеллекта, нейросетевых технологий (когнитивный подход).

Результат реализации нового подхода к поддержке принятия решений и повышения качества экспертных данных на основе совмещения методов когнитивного моделирования и анализа Больших Данных прошел практическую, а также теоретическую и практическую апробацию на реальных примерах при разработке серии отраслевых и социально-экономических стратегий [4].

Согласованность экспертных оценок. При построении алгоритмов для ускорения согласованности группового экспертного знания в системах поддержки решений наблюдаются следующие ограничения: неполнота; нечеткость; неопределенность; противоречивость.

Все эти моменты являются неотъемлемыми признаками знаний, получаемых от экспертов. После проведения очередной итерации опроса группы экспертов осуществляется обработка результатов. Целью обработки является получение обобщенных данных, приоритетных оценок и новой информации, содержащейся в скрытой и явной форме в экспертных оценках. На основе результатов обработки формируется решение проблемы.

Для определения согласованности экспертных оценок при построении взвешенного дерева целей вычисляются компоненты собственного вектора как средние геометрические по строке. После нахождения компоненты собственного вектора нормируются, что дает вектор приоритетов или весов сравниваемых объектов. После проведения парных сравнений соподчиненных целей и получения данных по собственному значению и собственному вектору можно определить согласованность. Для этого, используя отклонение максимального собственного числа от размерности матрицы, рассчитывается величина, называемая индексом согласованности. Полученное значение сравнивается с соответствующим индексом, полученным для матрицы, построенной случайным образом. Приемлемым является отношение согласованности не более 10%.

При формировании алгоритма оценки экспертного согласия могут быть использованы существующие способы оценки согласованности мнений экспертов. При этом определяется степень согласованности мнений экспертов и составляется рейтинг экспертов. Ранжирование представляет

собой процедуру упорядочения экспертируемых объектов по важности. На основе своих знаний и опыта каждый эксперт располагает объекты в порядке предпочтения, руководствуясь одним или несколькими выбранными критериями сравнения. Возможным методом проверки согласованности является определение согласованности ранжировок с помощью коэффициента ранговой конкордации Кендалла.

Имеется апробация приведенного подхода применительно к созданию системы обеспечения безопасности критически важных объектов, а также к социально-экономической сфере.

Работа выполнена при поддержке РНФ, проект № 17-18-01326

Литература:

1. *Зацаринный А.А., Ильин Н.И., Колин К.К., Лепский В.Е., Малинецкий Г.Г., Новиков Д.А., Райков А.Н., Сильвестров С.Н., Славин Б.Б.* Ситуационные центры развития в полисубъектной среде //Проблемы управления. 2017. № 5. – С. 31-42
2. *Губанов Д.А., Коргин Н.А., Новиков Д.А., Райков А.Н.* Сетевая экспертиза. 2-е изд. / Под ред. чл.-к. РАН Д.А. Новикова, проф. А.Н. Райкова. М.: Эгвес, 2011. – 166 с
3. *Иванов В.К.* Некорректные задач в топологических пространствах // Сибирский математический журнал. Т. X, № 5, 1969. С. 1065 -1074
4. *Raikov A.N., Avdeeva Z., Ermakov A.* Big D ata R efining o n t he B ase o f Cognitive M odeling. P roceedings o f t he 1s t I FAC C onference on C yber-Physical&Human-Systems, Florianopolis, B razil. 7 -9 D ecember, 2016. pp. 147-152.

Коврига С.В.

Общие подходы и методы анализа и прогнозирования военно-политической обстановки

Аннотация: Рассмотрены общие подходы и методы к анализу, моделированию и прогнозированию военно-политической обстановки (ВПО) в контексте решаемых практических задач оценки ВПО. Выделены ряд проблем, ограничивающих их применение с учетом фактических потребностей в средствах поддержки экспертно-аналитической деятельности в военной сфере и сфере международных отношений, и направления их разрешения.

Ключевые слова: безопасность, стратегическая стабильность, военно-политическая обстановка, стратегическое планирование, модели и методы анализа и прогнозирования

Формирование благоприятных условий для реализации национальных интересов, устойчивого развития РФ на долгосрочную перспективу осуществляется путем обеспечения стратегической стабильности (СС). СС рассматривают в качестве военно-политического аспекта безопасности, связанного с балансом военных сил в рамках определенной системы безопасности (международной, региональной и т.д.). Она выступает как качественная характеристика всей системы международных отношений. В широком смысле СС – это общая характеристика состояния международных отношений, определяемая наличием или отсутствием серьезных дестабилизирующих факторов не только военного-политического характера, но и связанных с экономическими и другими кризисами, эпидемиями, катастрофами, серьезными террористическими актами и т. п. Поэтому оценка ВПО является базовым условием обеспечения национальной безопасности страны [1]. В общем виде, ВПО выступает как срез внутренней политической обстановки в государстве (его части) и внешней МО в каком-либо регионе или в мире в целом. ВПО – это состояние мировой военно-политической системы в определенный период времени, характеризуемое составом субъектов военной политики, их состоянием и особенностями военно-политических отношений между ними. ВПО оценивается совокупностью результатов действий одних субъектов военно-политических отношений в отношении других [2].

Оценка ВПО осуществляется по разным направлениям, определяющим широкий спектр целевых задач анализа и прогнозирования ВПО. Среди них можно выделить наиболее распространенные: (1) оценка военно-политического потенциала мировых держав, баланса сил субъектов ВПО; (2) анализ и прогнозирование международных конфликтов и кризисов; (3) анализ переговорных процессов; (4) прогнозирование тенденций развития ВПО по различным срезам; (5) мониторинг и анализ существующих и прогноз будущих опасностей и угроз. Особая роль при решении целевых задач принадлежит прогнозным заключениям, которые по своему смыслу остаются вероятностными, но существенно повышают определенность целеполагания при принятии решений. [1]

Краткое описание основных подходов и методов. Для исследования военно-политических процессов и международных конфликтов используются общенаучные методы познания [2, 3]:

эвристические: наблюдение, описание, изучение источников и др.;

теоретические: анализ, синтез, экстраполяция, интерполяция, индукция, дедукция и др.;

специальные: метод экспертных оценок, математические методы – методы теории вероятностей, математического моделирования, теории игр, теории принятия решений, статистические методы и др.

Эвристический метод прогнозирования основан на использовании предсказаний (прогнозов) специалистов в данной области знаний. Необходимым условием формирования качественного прогноза и оценки процессов является наличие большого объема знаний и опыта, который формируется в повседневной деятельности и заключается в прогнозировании будущего результата реализации процесса, сравнения его с результатами, получаемыми на практике, и корректировки с учетом субъективных особенностей восприятия исследуемого процесса. Поэтому для проведения эвристического прогнозирования ВПО привлекаются наиболее подготовленные в данной области специалисты с большим опытом [3]. Несмотря на развитие математических методов прогнозирования, эвристическое прогнозирование сохраняет свое значение в тех случаях, когда формализация прогнозируемых процессов затруднена или практически невозможна, нет возможности получения в полном объеме исходной информации для прогнозирования. Одним из наиболее отработанных и приемлемых для практического решения задач военно-политического прогноза и оценки обстановки является метод экспертных оценок.

Теория игр является еще одним популярным научным направлением, применяемым при оценке ВПО и международных отношений. Математический аппарат теории игр позволяет принимать решения в условиях неопределенности [1]. Игровое моделирование позволяет в явном виде оценить, как влияет на развитие конфликта деятельность всех участников событий по реализации ими собственных целей, что значительно повышает адекватность и надёжность получаемых результатов. При этом во многих случаях оцениваются не только альтернативные стратегии поведения сторон, участвующих в конфликте, но и последствия применения этих стратегий, что позволяет предлагать варианты возможных сценариев развития конфликтов и кризисов и выявлять среди них наиболее вероятный [4]. Современное развитие теории игр породило новые методы, применение которых целесообразно при анализе и прогнозировании кризисов и конфликтов: методы (1) рефлексивных игр, (2) теоретико-драматического анализа конфликтов и (3) игрового моделирования с переменными векторами приоритетов сторон. Они снимают ряд ограничений методов классической теории игр, что расширяет спектр решаемых прикладных задач анализа и прогнозирования конфликтов и кризисов в международных отношениях. Среди основных сфер, в которых используется теоретико-игровой подход, следует выделить проблемы нераспространения ядерного оружия и

ядерного сдерживания, введения экономических санкций и мировой торговли, анализ различных международных конфликтов и их влияния на внутреннюю политику государств, анализ переговорных процессов [4].

Статистические методы базируются на развитых научных методах теории вероятностей и математической статистики, методах обработки результатов измерений. Они широко применяются в научной и практической деятельности в различных областях экономики, техники, военного дела, социологии и в других сферах. Использование данных методов предполагает сбор и анализ данных о прогнозируемом процессе. Имея данные об изменении характеристик процесса во времени, можно отследить закономерности и спрогнозировать результат в будущем, проверять правильность выдвигаемых гипотез. Именно данная группа методов чаще всего подразумевается под количественным анализом в зарубежной международно-политической науке [5]. Основные недостатки заключаются, во-первых, в необходимости наличия большого количества точных данных за длительный период времени по анализируемому процессу. Во-вторых, математическая статистика критикуется сторонниками системного подхода за проверку отдельных переменных, вырванных из контекста [5]. Наконец, такой подход не позволяет предсказать результат, который не встречался ранее [3].

Методы моделирования процессов. Прогнозирование на основе данных методов включает: выбор и обоснование модели, расчет (определение) на модели характеристик прогнозируемого процесса для времени прогнозирования и анализ, и оценку точности результатов. Основным допущением при прогнозировании на основе моделирования процессов является предположение о неизменности модели, принятой на интервале наблюдения, т.е. предполагается, что прогнозируемый процесс развивается в настоящем и будет развиваться в будущем. К числу распространённых методов относится метод анализа системной динамики, предназначенной для изучения то, как внутренние контуры обратной связи в структуре системы создают ее поведение. Для достижения наилучшего понимания системы во времени используется компьютерное имитационное моделирование [3].

Компьютерные модели, позволяющие анализировать общие параметры международной ситуации, можно разделить на несколько категорий, связанных с определением фоновых моментов развития ВПО в ее различных измерениях [1]. К наиболее простым компьютерным моделям по международной проблематике относятся международные системы антикризисного реагирования. К более сложным системам компьютерного моделирования, связанным уже с интерпретацией сравнительно отдаленных во времени первичных данных, относятся системы анализа и прогнозирования. По объекту моделирования компьютерные модели

международных отношений можно подразделить на (1) модели международных конфликтов; (2) модели принятия решений в кризисных ситуациях; (3) модели баланса сил и мирового развития.

Модели международных конфликтов основаны на гипотезе о цикличности развития социальных процессов, а также на свойственной человеческой природе автоматической реакции (рефлексы) на внешние раздражители. На первом этапе создается обширная база данных по конфликтам, формализованная по определенному шаблону (критериям). Посредством использования метода ассоциаций, любой современный конфликт сравнивается с уже имевшими место из базы данных, при этом несущественные (шумовые) признаки отличий опускаются. На основе анализа схожих конфликтов делаются выводы о возможных сценариях развития ситуации в ходе текущего кризиса. Помимо моделей анализа конфликтов существует целый ряд моделей принятия решений в конфликтных ситуациях, имитирующих процесс принятия решений с учетом внутреннего состояния ЛПР в период международного кризиса, а также целого ряда других событий, влияющих на процесс принятия решений. Модели баланса сил и мирового развития основаны на многокритериальном анализе военной, политической или экономической мощи государств на международной арене.

Выводы. При долгосрочном прогнозировании и планировании решающее значение играет адекватный выбор методов прогноза количественных и качественных показателей и критериев, влияющих на развитие ВПО. К настоящему времени существует множество разнообразных подходов и методов, однако ни один из них не может быть назван бесспорным и абсолютно достоверным.

Основные проблемы применения современных подходов и методов анализа и прогнозирования развития ВПО связаны

- с возрастающим разнообразием и сложностью целевых задач анализа и прогнозирования развития ВПО и международных конфликтов;
- с потребностью оценки как отдельных срезов ВПО, так и комплексной оценки ВПО, характеризующейся ростом многообразия политических и военно-политических, экономических и социальных отношений внутри отдельных государств и между ними;
- со сложностью описания военно-политического процесса в требуемой нотации и несоответствием большинства методов современным требованиям (постоянно растущему объему обрабатываемой информации), т.к. в большинстве из них трудоемкость использования пропорциональна объему анализируемых данных;
- с динамичностью ВПО, неопределенностью, обусловливающей непредсказуемость и нестабильный характер развития ВПО.

Характер факторов неопределенности исключает возможность формирования однозначного прогноза развития ВПО. Данное обстоятельство превращает факторы неопределенности в особую категорию военного планирования. Одна из рекомендаций компании RAND, относительно учета неопределенности при стратегическом планировании состоит в необходимости ее преобразования в пространство возможностей или пространство сценариев [2], что требует разработки соответствующих методов прогнозирования.

Взаимодополняющие направления возможного разрешения обозначенных проблем состоят в следующем. Первое направление – это использование комбинации количественных и качественных методов, которая в итоге может повысить точность прогноза, а иногда является единственным способом выполнения поставленной целевой задачи дать наиболее точный результат [1,3]. При этом математические модели не заменяют и не могут заменить экспертных оценок. Они являются лишь вспомогательным инструментом, помогающим экспертам прийти к тому или иному выводу и сделать правильные рекомендации для военно-политического руководства страны [1].

Второе направление связано с дальнейшим совершенствованием моделей и методов анализа и прогнозирования ВПО. При этом специалисты в области международных отношений отмечают потребность в комплексной оценки ВПО на базе «полной» (комплексной) модели МО и ВПО [1, 2]. В рамках совершенствования методов оценки ВПО целесообразно развитие комплексной методологии прогнозирования ВПО и МО для формирования различных сценариев обеспечения СС. В качестве основы для ее создания предлагается методология сценарного анализа и прогнозирования развития сложных систем различной природы, разработанная в ФГБУН Институте проблем управления им. В.А. Трапезникова РАН [6].

Литература:

1. Некоторые аспекты анализа военно-политической обстановки: монография / под ред. А. И. Подберезкина, К. П. Боришполец. – М.: МГИМО–Университет, 2014.
2. *Подберезкин А.И. и др*. Стратегическое прогнозирование и планирование внешней и оборонной политики. Том 1. – М.: МГИМО–Университет, 2015.
3. *Моисеев М.А.*, *Терехов В.П*. Исследование методов прогнозирования международных конфликтов / Научный журнал, 2016. – №6(7).
4. *Абаев Л.Ч*. Об актуальных подходах к моделированию международных отношений / Проблемы национальной стратегии, 2011. – № 2(7). – С. 31-48.

5. *Дегтерев Д.* Количественные методы в международных исследованиях / Международные процессы, 2015. – Том 13, № 2. – С. 35-54.
6. *Шульц В.Л., Кульба В.В. и др.* Сценарный анализ в управлении геополитическим информационным противоборством. – М.: Наука, 2015.

Баранов Л.А., Логинова Л.Н.

Моделирование сложных транспортных систем для обеспечения безопасности движения

Аннотация: В статье приведены требования по составу подмоделей, которые должны являться неотъемлемой частью модели транспортной системы, обеспечивающей управление движением поездов на линии метрополитена в чрезвычайных ситуациях. Рассматриваются так же требования к модели, реализующей обучения оперативного персонала транспортной системы.

Ключевые слова: безопасность, движение поездов, метрополитен, моделирование, требования к модели, обучение, чрезвычайные ситуации

Современное общество характеризуется цифровизацией всех сфер жизнеобеспечения. Одной из главных функций цифровизации является повышение обеспечения безопасности на разных уровнях сложных транспортных систем, к которым непосредственно относится метрополитен. Для решения таких задач, как разработка, проектирование и эксплуатация технических средств управления движением поездов на метрополитене при обеспечении заданного уровня безопасности целесообразно использовать имитационное моделирование, так как аналитическое вычисление критериев качества функционирования транспортных систем на фоне существующей в них многомерности вызывает определенные затруднения [1].

Основными достоинствами методов имитационного моделирования для исследования сложных систем считаются [1]:

• возможность изучения функционирования системы в любых условиях, в том числе, когда имитируются аварийные ситуации;

• значительное сокращение времени испытаний по сравнению с натурным экспериментом;

• возможность изменения структуры и параметров моделируемой системы без существенных затрат на реализацию.

При разработке модели, которая обеспечивает выполнение требований обеспечения заданного уровня безопасности такой транспортной системы, как линия метрополитена, необходимо учитывать следующие подмодели[2]:

- подмодель движения поездов;
- подмодель интервального регулирования;
- подмодель управления стрелками и сигналами;
- подмодель маршрутно-релейной централизации;
- подмодель автоматических режимов;
- подмодель построения планового графика движения поездов;
- подмодель задания, корректировки и контроля начальных условий;
- подмодель задания возмущающих воздействий.

Вышеперечисленные подмодели обеспечивают реализацию линии метрополитена в виде цифровой модели для решения разного рода задач повышения безопасности управления движением поездов.

Для проведения имитационного моделирования управления движением поездов на линии метрополитена в чрезвычайных ситуациях модель должна быть дополнена такими подмоделями как:

- подмодель задания типовых неисправностей на линии метрополитена,
- подмодель контроля действий оперативного персонала в чрезвычайных ситуациях,
- подмодель хранения результатов управления движением поездов, т.е. подмодель ведения архива,
- подмодель сравнения полученного исполненного графика движения с архивными соответствующими графиками движения поездов для проведения подробного анализа реализованного управления.

Для повышения качества управления, и как следствие для повышения безопасности движения поездов на линии метрополитена, необходимо не только проводить проверку умений оперативного персонала принимать правильные решения в условиях чрезвычайных ситуаций, но так же постоянно проверять квалификацию работников метрополитена, которая определяется действиями, которые они предпринимают как при нормальной работе линии, так и при возникновении сбоя [5]. Порядок действий в нормальных условиях повторяется, поэтому в основном не вызывает затруднений. Если же происходит чрезвычайная ситуация на линии, то диспетчер должен предпринять меры, чтобы привести ситуацию в нормальное состояние. Важно так же обучать новых сотрудников для обеспечения резерва кадрового состава.

Для обучения оперативного персонала модель транспортной системы должна содержать все вышеперечисленные подмодели, а так же:

- подмодель управления линией для возможности осуществления диалога между моделью и диспетчером,
- подмодель анализа действий поездного диспетчера для проведения автоматизированного анализа всех предпринятых действий,
- подмодель сбора и хранения информации о процессе проверки знаний для сохранения всех действий, предпринятых диспетчером при управлении линией, для последующего анализа,
- подмодель автоматического расчета таких показателей качества, как количество несвоевременных действий, соотношение правильных команд к общему числу команд, время выполнения сценария, и др.

На кафедре «Управление и защита информации» Российского университета транспорта (МИИТ) накоплен значительный опыт создания, внедрения и эксплуатации различных цифровых моделей транспортных объектов:

- модель линии метрополитена, которая используется для определения оптимального управления движения поездов всей линии метрополитена [2],
- модель системы автоматизированной проверки знаний поездных диспетчеров метрополитена, используемая как для периодического контроля знаний, так и для постоянного обучения [4],
- модель движения поезда, которая позволяет находить оптимальные траектории движения поездов[6] и др.

Вышеперечисленные модели прошли адаптацию и проверены на адекватность с помощью проведенных многочисленных опытов. Модели соответствуют заданным требованиям и выполняют задачи, поставленные перед ними. Например, опыт использования модели линии метрополитена дал положительные результаты при анализе и синтезе алгоритмов централизованного управления движением поездов на линии метрополитена[2, 3]. Работа с системой автоматизированной проверки знаний поездных диспетчеров метрополитена показала целесообразность проведения обучения оперативных работников. Анализ и рекомендации, полученные в результате использования автоматизированной системы проверки знаний поездных диспетчеров, эффективно повышают уровень знаний и умений оперативных работников метрополитена[4, 5]. Модель движения поезда, позволяющая находить оптимальные траектории движения поездов, предоставляет траектории движения поезда на линии метрополитена, при этом уменьшая расход электроэнергии на тягу поездов [6].

Литература:
1. *Л.А. Баранов, Е.П. Балакина* Перспективы использования многофункциональных моделей// Мир транспорт. – 2012. - №2. – С. 70-74.
2. *Баранов Л.А., Балакина Е.П., Воробьева Л.Н.* Связь ограничений на управление с состоянием системы в централизованных системах автоведения поездов// Сборник тезисов докладов третьей международной конференции «Системы безопасности на транспорте». - Чехия, Пшибрам, 2007.
3. *Lyudmila Loginova, Leonid Baranov, Ekaterina Balakina, Pavel Vorobiev* "Automatic Train Control Algorithms with Regulation Restrictions Adaptive to System State Changes","International Journal of Engineering Research & Science", ISSN 2395-6992, vol.2, issue 4, pp.85-96, 2016.
4. *Логинова Л.Н.* Внедрение автоматизированной системы проверки знаний поездных диспетчеров линии метрополитена// Труды Межрегиональной научно-практической конференции «Модернизация процессов перевозок, систем автоматизации и телекоммуникаций на транспорте» – Хабаровск: Изд-во ДВГУПС, 2010.-216 с.
5. *Логинова Л.Н.* Роль системы автоматизированной проверки знаний поездных диспетчеров линии метрополитена в повышении качества обучения//НТТ−Наука и техника транспорта. – 2011. – №1.
6. *Баранов Л.А. Максимов В.М.* Повышение энергоэффективности управления движением поездов метрополитена // Электротехника. – 2018. – № 9. С. 45 – 48.

Мавлянкариев Б.А., Хатамов Б.Б., Пен А.Ю., Талибджанов И.Р.

Системная интеграция этапов жизненного цикла технической системы - как инновационный ресурс её эффективного применения

Аннотация: Освещен опыт выбора направления инновационной деятельности на примере декомпозиции жизненного цикла технической системы.

Ключевые слова: системная интеграция, инновационный подход, этап, жизненный цикл, эффективность

К сожалению, динамика кризисных ситуаций в мире, связанных с гибелью людей, в последнее время растет и становится неотъемлемой частью нашей повседневной хроники. В этих условиях все чаще стали

говорить о новых, инновационных подходах к решению возникших проблем. Ученые и специалисты, при анализе деятельности службы пожарной безопасности, обосновывает подобную логику следующим:

1. наметилась явная диспропорция между ростом всевозможных рисков обществу и методами (средствами) их предупреждения (ликвидации);

2. расширение производства, развитие общества и соответственно, стоимость их противопожарной защиты, требует комплексного повышения эффективности применяемых методов и средств обеспечения безопасности;

3. служба пожарной безопасности связана с риском здоровью и спасением пострадавших людей, что обязывает принятие кардинальных решений.

В настоящей статье освещается опыт выбора направления инновационной деятельности службы пожарной безопасности, и соответственно выбору, определения инновационных подходов способствующих совершенствованию отдельных этапов данного направления. Понимание термина инновационного подхода, предполагает знание его корня-инновации. В последние годы термин - **"инновация"** получил широкое распространение [1].

Если быть лаконичным, инновации - это создание и внедрение нововведений, существенное изменение в любой области науки, техники, общественного развития, направленное на достижение положительного эффекта.

Инновационный процесс является управляемым и имеет свой жизненный цикл. В связи с неопределённостью конечных результатов каждого из его этапов инновационный процесс характеризуется повышенным уровнем риска. Недоверие к новым техническим, и особенно организационно-управленческим, идеям часто является существенным сдерживающим фактором при разработке и внедрении нововведений в деятельность службы пожарной безопасности. Основные проблемы инновационного процесса представлены на рис. 1 .

Служба пожарной безопасности имеет много примеров нереализованных инновационных возможностей. Отдельные из них представлены на рис. 2 [1].

Нововведения затрагивают все сферы человеческой деятельности: технические, экономические, социальные, организационные, управленческие, образовательные и другие.

Учитывая профиль Института пожарной безопасности рассмотрим объявленную проблему – повышение эффективности технической системы.

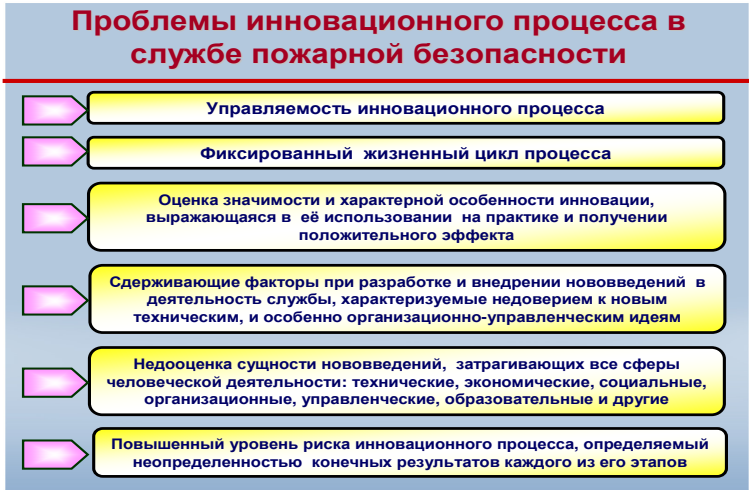


Рис.1 – Основные проблемы инновационного процесса

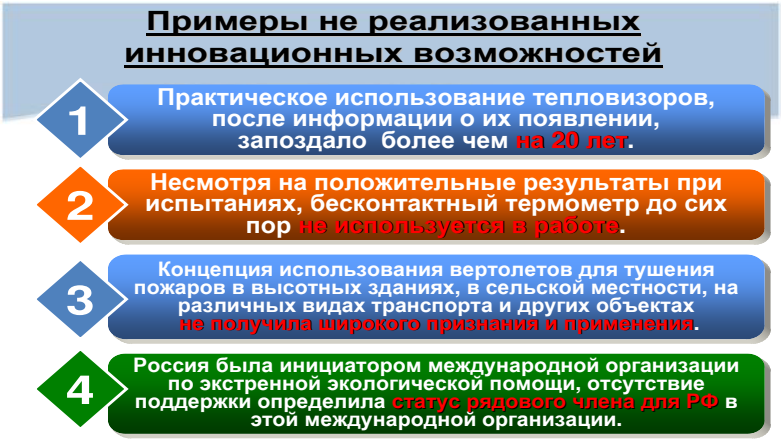


Рис.2 – Нереализованные инновационные возможности

Предлагается декомпозиция технической системы по этапам её жизненного цикла, включающей «разработку-комплектацию-внедрение-эксплуатацию».

Для лучшего уяснения сути проблемы и основных этапов её решения обратимся к вспомогательному примеру. Фирма «Боинг», при реализации

своей продукции-самолетов, ориентируется на наличие в покупаемой стране, или в ближайшем от неё регионе соответствующего сервисного центра обслуживания данного типа летательных систем.

Этот сервисный центр, обычно, является завершающим этапом обозначенного выше полного жизненного цикла для отдельного самолета. «Боинг», благодаря системно объединенному- интегрированному решению всех задач, связанных с этапами создания, комплектации, внедрения и обслуживания самолетов, имеет заслуженный коммерческий успех и стабильную эффективность деятельности во всех подразделениях.

Благодаря объявленному инновационному, системно интегрированному подходу, мы предлагаем решение всех этапов жизненного цикла технической системы, от его создания до практического использования [2]. Ниже представлена структура основных этапов синтеза и применения многофункциональной пожарной спецтехники (рис. 3).

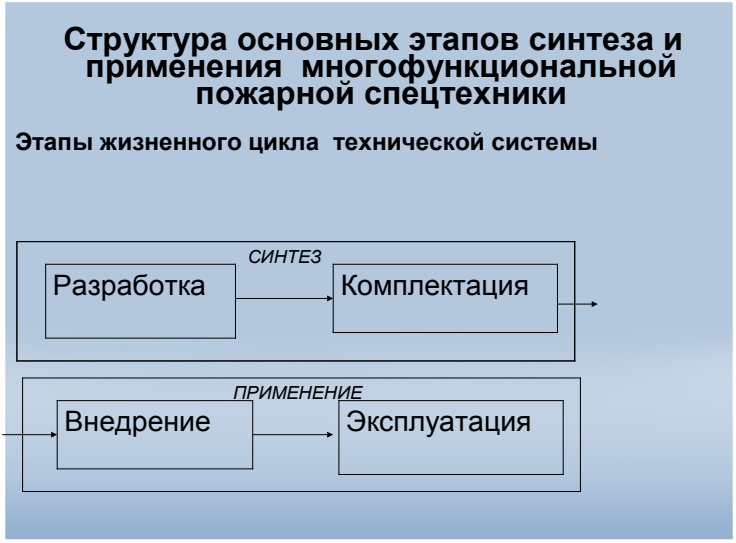


Рис.3 – Структурная декомпозиция жизненного цикла технической системы

Результаты использования данного подхода реализованы в виде конструктивных и методологических решений:

Конструктивные:

1.разработка способа и устройства многофункционального действия по дистанционной доставки огнетушащих, спасательных средств;

2.многофункциональное устройство хранения тушащего вещества, обнаружения, тушения, сигнализации о пожаре, а также отключения от питания.

Методологические:

Создание методологических основ для системно интегрированного анализа и использования технической системы.

Применяя предлагаемый подход нами были исследованы научно обоснованное создание и рациональные практические рекомендации по использованию вышеобозначенных многофункциональных технических систем пожарной безопасности сложных объектов. Инновационный процесс характеризуется эффективностью, зависящей от многих факторов (рис. 4).

Рис.4 – Влияние факторов на инновационный процесс в системе безопасности

Главной особенностью любого нововведения (инновации) является его использование на практике и получение положительного эффекта.

Будучи образовательным учреждением, мы должны формировать чувствительность к нововведениям, заботиться о воспитании молодого

поколения «зараженного» идеями инновации. Эта работа определяется обозначенными выше направлениями [3].

Здесь, учитывая специфику задач вузов силового блока, следует особо подчеркнуть о необходимости всемерного расширения кооперации с учеными со смежных вузов. Это можно реализовать на всех этапах инновационного процесса. Последний включает следующие этапы: фундаментальные и прикладные исследования, маркетинговые исследования, опытно-конструкторские работы, производство, практическое использование. Разрывы между этапами приводят к резкому снижению эффективности всего инновационного процесса. Например, в середине прошлого века НИР, ОКР и производство пожарной техники в СССР было распределено между организациями трёх министерств. Наверное, поэтому и качество выпускаемых в тот период пожарных автомобилей не могло быть высоким [1].

Следует также учесть, что процесс разработки нового, внедрения нововведений, как показывает опыт, требует планомерной работы на всех этапах обучения. Он, обычно, активизируется в период подготовки диссертационного исследования, так как ускоряется «созревание» специалиста, приобретается опыт масштабного, логико-системного видения вопроса и, нестандартного его решения.

И наконец, в целях повышения инновационного потенциала организации (это показатель, который характеризует готовность и способность исследователей, разработчиков и особенно руководителей организации к осуществлению процессов нововведений), следует поощрять кооперацию ученых, специалистов специализированных фирм, путём создания научных лабораторий, учебно-научных комплексов вузов, филиалов кафедр в научных учреждениях, в специализированных фирмах.

Подводя итог образовательному сегменту поставленной задачи можно обозначить следующие направления и пути формирования инновационной культуры в институте пожарной безопасности [2]:

1.Изучение зарубежного опыта;

2.Организация учебных курсов для различных категорий слушателей /магистры, высшие курсы руководящих работников ГСПБ РУз, руководители объектов экономики;

3.Разработка учебно-методической продукции;

4.Подготовка диссертаций, с примерами инновационных идей и их воплощения.

Каждый период развития общества ставит свои, приоритетные задачи. Подготовка кадров всегда определялась как сложная её составляющая с особыми требованиями к воспитателю. Сегодня необходимо привлечь молодежь к исследовательскому творчеству, научить инновационному

«чутью», желанию качественно улучшить выполняемые функции и изготавливаемую продукцию.

Это, несомненно, сложный процесс, требующий от руководителей и наставников, помимо знаний, определенного спектра качеств человеческого измерения, и конечно же личностного примера.

Литература:

1. *Семиков В.Л.* Управление инновационной деятельностью в системе ВУЗов противопожарного профиля// Матер.XXII межд. НТК «Системы безопасности СБ-2013» М., 2013. С.292-296.
2. *Мавлянкариев Б.А*, *Хатамов Б.Б.* Повышение эффективности пожарно-технического вооружения на многофункциональной основе //Материалы 6-ой НПК ”Пожаротушение: проблемы, технологии, инновации”. М., 2018. С. 343-345.
3. *Козлачков В.И.* Проблемы подготовки специалистов государственного пожарного надзора к деятельности в условиях информационных перегрузок и высокой динамики информационных процессов// Матер.XXII межд. НТК «Системы безопасности СБ-2013». М., 2013. С. 296-297.

Карпов В.В., Бочкарев А.П.

Применение методологии IDEF0 для построения функциональной модели деятельности центра управления кризисными ситуациями

Аннотация: В статье рассматриваются вопросы построения функциональной модели деятельности центра управления кризисными ситуациями с использованием методологии IDEF0.

Ключевые слова: центр управления кризисными ситуациями, функциональная модель, методология IDEF0, информационные и расчетно-аналитические задачи

Анализ деятельности центров управления кризисными ситуациями (далее – центров управления) органов государственной власти Российской Федерации показывает, что выполняемые ими функциональные задачи можно разделить на две основные группы:

- информационные;
- расчетно-аналитические.

Информационные задачи обеспечивают процессы сбора и обобщения данных обстановки, их формализацию, хранение и распределение заинтересованным лицам.

Расчетно-аналитические задачи обеспечивают процессы поддержки принятия решений: идентификацию кризисных ситуаций; выработку вариантов решений по применению сил и средств; моделирование и прогнозирование развития обстановки [2].

В общем виде деятельность центра управления можно представить в виде контекстной диаграммы, состоящей из следующих модулей (рис.1):

информационного – набор входных данных (донесений, справок, оперативных сводок и др.) свидетельствующий о возникновении кризисной ситуации;

- *нормативно-правового* – совокупность нормативно-правовых актов регламентирующих деятельность центра управления (в виде приказов, распоряжений регламентов и др.);
- *организационно-технического* – инструмент для преобразования входной информации в конкретные предложения по разрешению кризисной ситуации;
- *модуля информационной поддержки принятия решений* – практический результат решения информационных и расчетно-аналитических задач, в виде предложений по разрешению кризисной ситуации.

Рис. 1 – Контекстная диаграмма деятельности центра управления

Следуя методологии IDEF0, декомпозируем деятельность центра управления, представив ее в виде набора функциональных блоков, каждый из которых представляет собой совокупность процессов [3]:

- сбор данных обстановки из всех доступных источников;

– актуализация баз данных по основным направлениям деятельности центра управления;
– обобщение данных обстановки для решения информационных и расчетно-аналитических задач;
– решение информационных и расчетно-аналитических задач;
– экспертно-аналитическая оценка данных обстановки;
– оценка результатов решения расчетно-аналитических задач;
– подготовка предложений руководству на основе мнений экспертов-аналитиков и результатов решения задач.

В ходе проведенных исследований была разработана функциональная модель деятельности центра управления состоящая из следующих элементов (рис 2.).

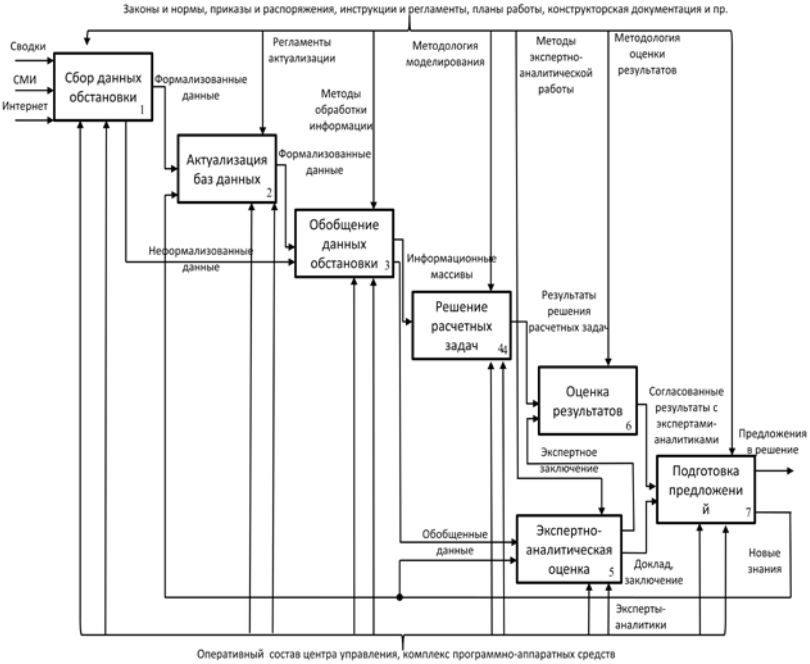


Рис. 2 – Схема функциональной модели деятельности центра управления

Функциональный блок *«Сбор данных обстановки»* отражает процессы сбора данных от разнородных источников первичной информации, представления данных в виде удобном для принятия управленческих решений. Если центр управления является высшим звеном в

иерархической системе, состоящей из подобных ему центров, то решаемые им задачи должны опираться на агрегированную информацию, а сбор и обмен данными между ними осуществляться на основе соответствующих регламентов информационного взаимодействия.

Функциональный блок *«Актуализация баз данных»* представляет собой процессы формирования и периодического обновления (актуализации) баз данных, в соответствии с нормативно-правовыми документами. Уточнение данных производится по мере необходимости, что позволяет обеспечить их требуемую достоверность и полноту.

Функциональный блок *«Обобщение данных обстановки»* - совокупность процессов преобразования данных в специальный вид для решения информационных и расчетно-аналитических задач. Результатом работы являются структурированные информационные массивы, которые используются, в качестве исходных данных для расчетно-аналитических задач.

Функциональный блок *«Решение расчетно-аналитических задач»* отражает соответствующие процессы по оценке и моделированию развития обстановки, расчету сил и средств, анализу их возможностей, технической оснащенности. Данный блок предусматривает решение расчетных задач с использованием графических документов, а также хранение результатов в базе данных для их дальнейшего применения.

Функциональный блок *«Экспертно-аналитическая оценка данных обстановки»* представляет собой процессы, связанные с применением методов аналитической обработки информации в интересах поддержки принятия решений. В результате формируются различные сценарии развития обстановки и аналитические отчеты, используемые как самостоятельно, так и в качестве обоснования при подготовке предложений руководству[1].

Функциональный блок *«Оценка результатов решения информационно-расчетных и информационно-аналитических задач»* является одним из ключевых элементов в деятельности центра управления. На этом этапе происходит обобщение результатов решения расчетных задач и деятельности специалистов экспертно-аналитических подразделений, осуществляется оценка сходимости результатов совместной работы.

Функциональный блок *«Подготовка предложений руководству»* состоит из процессов по формированию различных вариантов предложений руководству и отбору одного из них для последующего утверждения.

К основным достоинствам представленной функциональной модели можно отнести:

– возможность агрегирования и детализации информационных потоков с целью выявления «слабых мест» (дублирование информации,

однотипность выполнения задач структурными подразделениями и др.) и принятия решений по оптимизации организационной структуры центра управления;
- высокий потенциал визуализации функциональных процессов, позволяющий выработать системное представление о деятельности центра управления;
- простота реконфигурации, позволяющая оперативно адаптировать алгоритм работы и распределение функций между структурными подразделениями центра управления в кризисных ситуациях.

Литература:

1. *Курносов Ю.В.* Аналитика как интеллектуальное оружие / *Ю. Курносов* – Москва: РУСАКИ, 2012. – 613 с.
2. Методы построения и технологии функционирования ситуационных центров. / Сборник статей под редакцией доктора технических наук *А.А. Зацаринного* – М.: ИПИ РАН, 2011. – 258 с.
3. Сборник материалов научного семинара «Актуальные проблемы теории и практики военного управления» - М.: ВАГШ ВС РФ, 2017. – 145 с.

Плотников Н.И.

Социально-политический портрет авиатерроризма

Аннотация: Представлены основные проблемы авиатерроризма в мировой гражданской авиации. Выполнен краткий обзор авиатерроризма XX-го века и на рубеже тысячелетий. Составлен социально-политический портрет авиатерроризма.

Ключевые слова: терроризм, авиатерроризм (hijacking), безопасность, гражданская авиация

Содержание проблемы. Многочисленные исследования феномена терроризма и нарастание глобальных угроз показывает геополитические мультикультурные, религиозные, экономические источники и причины его проявления. Все новые резонансные акты терроризма выставляют проблему в абсолютный глобальный приоритет. Сложность международного, правового, политического кооперативного противодействия терроризму представляет проблему как почти неразрешимую. Проблема характеризуется нечеткостью понятийных описаний и предметной идентификации терроризма, разногласиями определений терроризма в разных странах.

Более полувека в мировой практике противодействия терроризму для обнаружения угроз используется концепция сплошного сканирования потоков и скоплений людей, багажа и грузов. Данная концепция основана (1) на постоянном отслеживании всего потока (2) техническими устройствами (3) за счет внимания сотрудников служб безопасности в зрительном просмотре мониторов и при непосредственном контакте с объектами. Потоки и скопления не бывают постоянными, сплошными и бесструктурными, технические устройства настроены на известные из возможных угроз, имеют пределы технической разрешимости, человеческое внимание непостоянно и подвергается утомлению. Любая изощренная выдумка террористов, такие, как пластиковые ножи для разрезания бумаги или провоз пластида под одеждой смертников приводит к новым резонансным терактам.

Предметная нечеткость терроризма затрудняет статистический учет, анализ и планирование превентивных мер. Операционные меры защиты, называемые превентивными или предупредительными, являются контрольной функцией в слабоструктурированном пространстве. Нормативная и регулирующая деятельность защиты от терроризма имеет преобладающий реагирующий характер. После терактов организуются «повышенные» меры безопасности временным увеличением количества сотрудников, усилением внимания – в рамках тех же принятых методов и технологий распознавания угроз. Спустя некоторое время все постепенно возвращается в прежний режим. Комплекс безопасности требует огромных расходов, новых методов и технологий защиты. Совокупность проблем состоит в: а) неадекватности идентификации предмета терроризма, б) несостоятельности метода наблюдения слабоструктурированным сплошным сканированием угроз, в) реагирующем характере стратегий противодействия терроризму.

Незаконное вмешательство (НВ) в деятельность гражданской авиации (ГА) остается уязвимой областью воздушного транспорта и мирового сообщества. Акты незаконного вмешательства (АНВ) вызывают огромный общественный резонанс, нарушают международное право, государственный суверенитет и обостряют международные отношения. Неопределенность событий АНВ обязывает увеличение непредсказуемого инвестирования безопасности транспорта. Наряду с глобальным содержанием разрешения проблем существуют подходы и ведутся поиски локальных решений. Наиболее известны и упоминаются методы и практика противодействия терроризму и создания комплексов защищенности в странах, где воздействия террористических актов происходит постоянно и десятилетиями, наиболее часто ссылаются на опыт в Израиле. Таким образом, разрешение проблемы глобального и локального противодействия терроризму возможны как объединением

международных усилий, так и путем оригинальной инициативы подходов и разработки методов и механизмов обеспечения защищенности от террористических воздействий, актов незаконного вмешательства. Именно второй из указанных подходов разрешения проблемы террористических воздействий определяет цель настоящей работы.

Предмет терроризма. Исследования природы и источников насилия и агрессии в поведении человека обнаруживают множество каких угодно причин: шум, загрязнение среды обитания, телевидение, нестабильность социумов. Неполнота знаний особенно заметна, если учесть, что: а) не обнаруживается зависимость агрессии во времени: акт насилия может быть регулярным, периодическим и разовым в жизни индивида; б) насилие чаще не совпадает и никак не связано с приемом алкоголя, наркотиков и других подобных веществ, которые являются традиционными виновниками неадекватного поведения; в) агрессия может появляться на фоне абсолютного психического здоровья. Важность исследования терроризма в том, что феномен агрессии и насилия может проявляться совершенно непредсказуемым образом с глобальными последствиями и потрясениями.

Явление терроризма рассматривают как способ воздействия на общество посредством устрашения. Термин «терроризм» (terror) означает ужас, страх. Понятие терроризма содержит использование насилия и угрозы уничтожения против людей, групп и государств для исполнения личных целей. Терроризм относят к международным преступлениям, опасным в глобальном масштабе и требующим международных усилий противодействия [1, 2]. Отличие терроризма от других видов насилия заключается в следующем: это всегда организованное, специально подготовленное насилие; это нагнетание максимального страха и неопределенности исхода для людей; все – потенциальные жертвы, терроризм имеет виртуальные мишени для нападения на кого угодно, где угодно, когда угодно, в любых, наименее защищенных местах и наименее защищенных людей.

Обзор авиатерроризма. Термин авиатерроризм (hijacking) означает угон, похищение ВС, воздушное пиратство, воздушный бандитизм. Уязвимость гражданской авиации как объект и мишень авиатерроризма исторически оказалась предопределённой. Угон ВС представляет минимальную опасность для преступника и большую угрозу жизни пассажиров и экипажа. Захват и угон расценивается преступником как одно из результативных средств достижения задуманной цели при использовании минимальных сил и средств. Захват и угон может осуществить небольшая группа. Преступление совершается индивидуально, независимо от того, является ли его исполнитель одиночкой или соучастником преступной группы. Действующие

группировки преступников считают захват ВС наиболее легким и дешевым способом приобретения популярности, освобождения, отбывающих освобождение наказание террористов, получение выкупа. Немаловажное значение для них имеет побег в государство, предоставляющее им убежище. В случае катастрофы большинство пассажиров погибает, террорист остается анонимным лицом. ВС представляет значительную ценность, которой трудно поступиться. Последствия от терактов в авиации очень тяжелые.

Внутренний авиатерроризм. Обзор выполнен на содержании **с**ерии цикла «Расследование авиакатастроф» телеканала National Geografic Channel. Введение террориста в роли служащего воздушного транспорта вызвано тем, что в этой роли террорист обладает наибольшими возможностями организовать доставки угрозы и совершить теракт во многих пространствах. Известно, кто совершил нападение 11 сентября 2001 года – террористы с профессиональной летной подготовкой. В данном случае роли служебная и пассажирская смешиваются, что представляет собой дополнительную задачу защиты.

Авиакатастрофа А320 под Динь-ле-Беном 24 марта 2015 года между городами Динь-ле-Бен и Барселоннет (Франция). Авиалайнер Airbus A320-211 авиакомпании Germanwings выполнял пассажирский рейс 4U9525 по маршруту Барселона - Дюссельдорф, а на его борту находились 144 пассажира и 6 членов экипажа. Но через 30 минут после взлёта самолёт внезапно перешёл в быстрое снижение и ещё через 10 минут врезался в горный склон в Прованских Альпах и полностью разрушился. Все находившиеся на его борту 150 человек погибли. Официальной причиной катастрофы - самоубийство пилота.

Авиакатастрофа Boeing 737 под Палембангом 19 декабря 1997 года. Авиалайнер Boeing 737-36N авиакомпании SilkAir выполнял рейс MI 185 по маршруту Тангеранг—Сингапур, но через 35 минут после взлёта, находясь на крейсерской высоте (10668 метров), по неустановленным причинам перевернулся, перешёл в практически вертикальное пикирование и рухнул в реку Муси в окрестностях Палембанга. Погибли все находившиеся на его борту 104 человека - 97 пассажиров и 7 членов экипажа. Одна из ключевых версий причин катастрофы - самоубийство пилота.

Попытка захвата DC-10 над Мемфисом, авиапроисшествие, произошедшее 7 апреля 1994 года, в ходе которого пассажир Оборн Кэллоуэй пытался захватить грузовой самолёт McDonnell Douglas DC-10-30F авиакомпании FedEx, совершавший рейс FDX705 по маршруту Мемфис—Сан-Хосе, убить всех трёх членов экипажа и покончить с собой, имитировав авиакатастрофу. Его целями были одновременно и месть авиакомпании за увольнение и получение страховки в размере $ 2 500 000.

Авиакатастрофа под Пасо-Роблесом 7 декабря 1987 года. Авиалайнер BAe 146 -200A авиакомпании Pacific Southwest Airlines (PSA)совершал рейс PSA 1771 по маршруту Лос-Анджелес—Сан-Франциско, но через 14 минут после взлёта один из пассажиров застрелил 2 пассажиров и 3 членов экипажа и направил лайнер в пикирование. Самолёт рухнул на землю, все находившиеся на его борту 43 человека (38 пассажиров и 5 членов экипажа) погибли.

Таран жилого дома самолётом Ан-2. Авиакатастрофа 26 сентября 1976 года в Новосибирске в результате преднамеренного столкновения самолёта Ан-2 с пятиэтажным жилым домом. Ранним утром 26 сентября 1976 года пилот Западно-Сибирского Управления гражданской авиации Владимир Серков (дата рождения 25 июля 1953 года) произвёл самовольный взлёт на самолёте Ан-2 (регистрационный номер СССР-79868) без пассажиров с одной из рулёжных дорожек аэропорта «Новосибирск-Северный». Некоторое время покружив над городом на предельно малой высоте, в 8 часов 20 минут утра пилот направил свой самолёт в пятиэтажный жилой дом, находящийся по адресу Степная ул., 43/1. В результате самолёт столкнулся с фасадом дома между третьим и четвёртым этажами в районе лестничной клетки, пробив в стене дыру около 2 метров в диаметре. Сам лётчик при столкновении погиб. Хотя бóльшая часть конструкции самолёта после столкновения осталась вне здания и упала на землю, в доме возник пожар ввиду того, что авиационный бензин выплеснулся внутрь здания и загорелся. Несмотря на то, что спасение людей из объятого огнём подъезда было быстро организовано вначале оказавшимися поблизости жителями города, а затем и прибывшими на место происшествия пожарными, в результате удара, от ожогов, неудачных прыжков из окон и с балконов погибло 5 человек (включая инициатора катастрофы) и пострадало 11 жильцов (4 человека получили тяжёлые повреждения, 5 - средней тяжести и 2 -лёгкие). Автор настоящей публикации работал пилотом в Новосибирском авиапредприятии и в этот день выполнял полеты на ИЛ-14. Между рейсами узнал о происшествии. Ранее встречал этого пилота. Причиной установили психические расстройства, связанные с шизофренией.

Анализ статистических глобальных наблюдений АНВ

Параметры	Обобщение
Количество актов	Наибольшее количество АНВ произошло на американских континентах. Количество АНВ имеет неопределенный характер без связи пиков с другими с событиями.

Параметры	Обобщение
Количество попыток и захватов	Из трех актов на одну попытку приходится два захвата. Вероятность захвата равна 0,71.
Количество погибших и раненых	Соотношение количества раненых и погибших, а также числа погибших к общему количеству жертв, имеет случайный характер и не связано с общим количеством АНВ. Соотношение количества раненых и погибших примерно равно.
Количество актов и жертв	На один акт приходится около шести жертв: погибших и раненых.
Количество завершенных и незавершенных актов	Состоявшиеся захваты могли быть завершенными или не завершенными по какой-либо причине. Завершенных АНВ примерно половина от общего количества актов.
Причины актов	Наибольшая доля - 63% АНВ приходится на политические причины. Существенные доли причин: вымогательства – 9,9% и освобождение заключенных – 6,2%.
Социальный состав участников	Мужчины, женщины, сопровождающие дети: преобладающее большинство актов совершают мужчины 91,3%. Доля женщин составляет 5,2%, акты в сопровождение детей 3,6%.
Дни недели актов	Значительная доля АНВ происходит в среду 21,1% и в пятницу 17,3%.

Политическая международная трансформация, распад стран, реструктурирование политических, военных блоков и альянсов, открытие и закрытие границ сопровождается обострением терроризма. Совершенно очевидно, в последней трети XX-го века и на рубеже тысячелетий произошла эскалация терроризма и демонстрация еще большей неопределенности и непредсказуемости феномена. Выполненный статистический обзор авиатерроризма может быть дополнен учетом актов насилия последнего десятилетия, начиная с теракта 11 сентября 2001 года в США. Следует признать, что сложившиеся параметры наблюдений и анализ статистических данных составляет умеренные возможности для выработки нормативных решений. Однако данные представляет собой приемлемую полноту и точность, на основании которых могут составляться стратегии и технологии защиты. Основной вывод настоящей работы заключается в необходимости ревизии существующей теории и практики защиты от АНВ и разработка новой методологии наблюдения предметной области.

Социально-политический потрет авиатерроризма. На основании исследования, выполненного в работе [3] составлен исторический социально-политического портрета терроризма XX века:

«Группа латиноамериканцев, совершивших угон самолета по политическим мотивам, завершившийся контртеррористической операцией, гибелью и ранением пассажиров, экипажа и террористов».

Обобщенный портрет современного терроризма представляет собой глобальную социальную группу организованного террора против огромного множества сфер деятельности объектов насилия. Количество актов терроризма имеет случайный характер, не определяемый со стороны объектов насилия. Акты насилия имеют значительную вероятность завершенного результата с числом жертв на один-два порядка превышающих число террористов. Терроризм распространяется по геополитическим причинам в странах с контрастным социальным неравенством. Соответственно и глобальные стратегии могут формироваться двух видов: а) противодействие и защита от терроризма; б) устранение причин терроризма.

Выводы. Концепция защиты от события АНВ является нормативное содержание, структурированными определениями понятий опасности и угроз. Практическая цель: а) кардинальное изменение организационных и технических меры защиты, которые четко определяют каналы доставки и пространства проникновения угроз в контур защиты, б) удовлетворение общественных потребностей в авиаперевозках, поставщиков услуг - авиакомпаний, аэропортов и служб безопасности в активных мерах защищенности и снижении рисков чрезвычайных событий АНВ, в) сохранение жизней, имущества и снижение стоимости защиты общественных объектов и воздушных судов за счет паретооптимизации структуры комплекса антитеррористической защиты.

Литература:

1. *Карпец И.И.* Преступления международного характера / И.И. Карпец. - М.: Юрид. лит., 1979. - 264 с.
2. Международный терроризм: политический анализ рисков и стратегий обеспечения безопасности: в 3 т. / Оводенко А.А. – СПб: 2008: Т. 1: Глобализация и риски безопасности: тенденции научного анализа. – 493 с. Т. 2: Модели и стратегии управления рисками международного терроризма. – 451 с. Т. 3: Международный терроризм: Библиография. Документы. Материалы социологических исследований. – 480 с.
3. *Плотников Н.И.* Ресурсы безопасности транспортных комплексов. Монография. – Новосибирск: ЗАО ИПЦ «АвиаМенеджер», 2013. – 286 с.
   Скачать: http://aviam.org/images/sampledata/book/pilot_resources.pdf.

Морозов Д.В.

Особенности математического обеспечения работы алгоритма повышения надежности функционирования системы управления

Аннотация: Разработан оптимальный алгоритм повышения надежности функционирования системы управления беспилотным летательным аппаратом. Алгоритм позволяет, при обнаружении отказа в контрольно-проверочной аппаратуре, произвести анализ принадлежности отказа функциональной части и реализовать соответствующие решения. Решение продолжить выполнение целевой задачи системой управления беспилотного летательного аппарата, сопровождается оптимальной глубиной самоконтроля контрольно-проверочной аппаратуры. Выбор очередной элементарной самопроверки производится на основании методики определения риска потерь. В качестве потерь используется вероятностный показатель достоверности контроля (вероятность ложного забракования). Методика решения задачи основана на использовании комбинированного метода ветвей и границ.

Ключевые слова: контролируемая область элементов, подозреваемая на отказ область элементов, самоконтроль, система управления, беспилотный летательный аппарат.

Обобщенная блок-схема (часть) оптимального алгоритма повышения надежности функционирования системы управления беспилотным летательным аппаратом (СУ БЛА) приведена на рис. 1.

При проведении рабочей программы полета (или самоконтроле КПА) по одной из ЭП (допустим π_γ) получен результат "не норма". В этом случае фиксируется ее номер γ и заносится в *мас.* А**.**

На основании анализа результатов логического суммирования в блоках 12, 13, 14, 15, 16 принимаются следующие решения:

1. Если $\Sigma = 01$, d_3^{01} (решение №1. Прекратить проверки и забраковать КПА);

2. Если $\Sigma = 10$, d_n^{10} (решение 2. Продолжить локализацию отказа) или d_3^{10} (решение 3. Прекратить локализацию отказа и продолжить выполнение СУ БЛА программы полета по измененному алгоритму).

3. Если $\Sigma = 11$, решение 2.

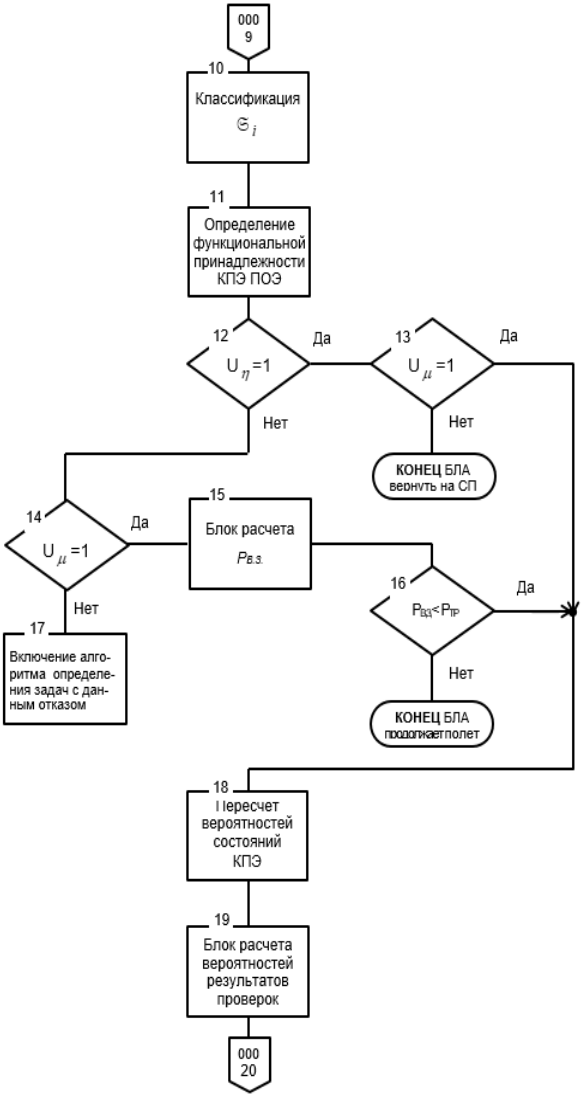


Рис. 1 – Обобщенная блок-схема (часть) алгоритма повышения надежности функционирования СУ БЛА

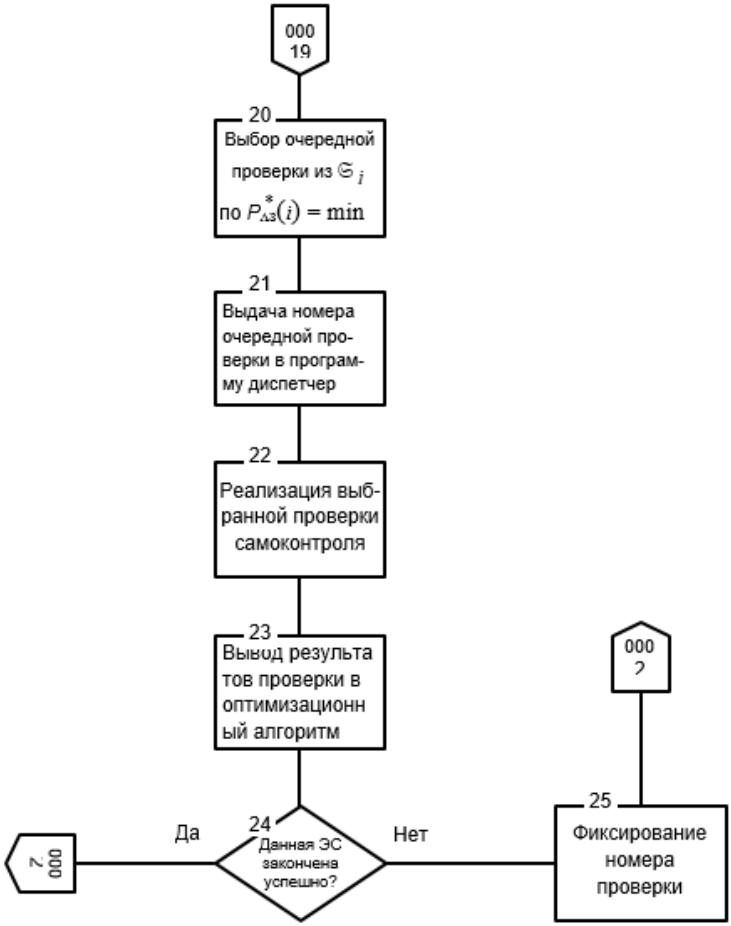


Рис.1 – Обобщенная блок-схема алгоритма повышения надежности функционирования СУ БЛА (окончание)

В блоке 15 производится вычисление $P_{B.3}$, на основании формулы Байеса, которая имеет вид [2]

$$P(И / Г) = \frac{P_O P_{АПП} R_{АПП}}{R_{АПП}(P_O P_{АПП} + P^{к}_{O} P^{к}_{АПП}(1 - P^{нк}_{O} P^{нк}_{АПП}))}, \quad (1)$$

где $R_{АПП}$ - вероятность безотказной работы аппаратуры самоконтроля части *АПП* КПА; P_O - вероятность безотказной работы БА СУ; $P_{АПП}$ - вероятность безотказной работы аппаратуры части *АПП* КПА; $P_O^{к}$, $P_O^{нк}$ - вероятность безотказной работы контролируемой и неконтролируемой части БА СУ, соответственно; $P_{АПП}^{к}$, $P_{АПП}^{нк}$ – вероятность безотказной работы функциональной части *АПП* КПА, подвергаемая и не подвергаемая самоконтролю. В блоке 18 производится перерасчет вероятностей состояний КПЭ $\{b_j\} \in \mathfrak{C}_\gamma^{t_o}$. При проведении самоконтроля КПА имеем следующие гипотезы о состоянии множества $\mathscr{B}$ КПЭ КПА, которые являются группой несовместных событий: Γ_0 - в $\mathfrak{A}_\gamma$ ЭС нет отказов; Γ_i, $i=\overline{1,N}$ - отказ только в $\{b_i\}$, $i=\overline{1,N}$ КПА. В результате проведения π_γ зафиксирован отказ – событие C_γ. Однако оно может иметь место и при других гипотезах ($\Gamma_{r,i}$ – отказ принадлежит b_i и b_r КПЭ КПА, например). В этом случае полную вероятность события C_γ целесообразно выразить через вероятность противоположного события $\overline{C_\gamma}$ – отказ не зафиксирован в π_γ. Для переоценки вероятностей гипотез о состоянии КПЭ КПА, составляющих $\mathfrak{A}_\gamma$, с учетом C_γ, используем формулу Байеса

$$P(\Gamma_i/C_\gamma) = \frac{P(\Gamma_i)\,P(C_\gamma/\Gamma_i)}{P(C_\gamma)}, \qquad (2)$$

где $P(C_\gamma/\Gamma_i)$ – условная вероятность получения результата – отказ в π_γ, при условии, что отказ в $\{\bar{b}_i\} \in$ КПА. Если $\{\bar{b}_i\} \in \mathfrak{C}_\gamma$, то в рамках принятых допущений $P(C_\gamma/\Gamma_i)=1$, и в противном случае $P(C_\gamma/\Gamma_i)=0$. Подставляя полученные выражения в формулу (2), после соответствующих преобразований, получим

$$P(\Gamma_i/C_\gamma) = \frac{\frac{1}{P_i}-1}{\frac{1}{P_\gamma}-R_\gamma}, \qquad (3)$$

где P_γ – вероятность отсутствия отказа в КПЭ покрывающих $\mathfrak{A}_\gamma$. Выражение (3) для вычисления апостериорной вероятности $P(\Gamma_i/C_\gamma)$ удобно для алгоритмизации процесса вычисления. Для результатов проведения ЭС "норма" формула (3) имеет вид

$$P(\Gamma_i/C_\gamma) = \frac{\frac{1}{P_i}-1}{P_\gamma\ R_\gamma}. \qquad (4)$$

Алгоритм расчета аналогичен как и для результата "не норма".

Работа блока 19 основана на методике определения риска потерь в решении задач повышения надежности функционирования СУ БЛА [3]. Причем она позволяет не только рассчитать составляющие выражения $P^*_{\Lambda.З.}(i)$ для всех ЭС составляющих $\mathfrak{S}^{t_o}_\gamma$, но и спрогнозировать процесс изменения C^{t_i} ,S^{t_i} на следующем шаге локализации отказа. Анализ аналогичен работе алгоритма блока 11: рассчитываем значения $P^*_{\Lambda.Ç.}(i)$ для ЭС с признаком Σ=10 и с признаком Σ=11. Таким образом, на основании прогнозирования изменения состава ПОЭ и ОПП производится расчет $P^*_{\Lambda.Ç.}(i)$, $i=\overline{\gamma+1,\mathcal{M}}$, т.е. всех ЭС, составляющих начальную ОПП, и по минимальной $P^*_{\Lambda.З.}(i)$ принимается решение $d^{\varphi i}_n$ – о том, что следующей будет реализована i -ая ЭС. После реализации i -ой ЭС, на основании полученного результата ("норма", "не норма"), производится уточнение ПОЭ. По результатам реализации i -ой ЭС заносим ее номер в *мас.* **А** или *мас*. **В** . Анализ $\mathfrak{C}^{t1}_i$, $\mathfrak{S}^{t1}_i$ определяет области $\mathfrak{G}^{\varphi}_n$, $\mathfrak{G}_\psi$. При попадании в область $\mathfrak{G}^{\varphi}_n$ ход работы алгоритма локализации отказа в КПА аналогичен выше описанному. Все расчеты на t_1 шаге локализации производятся для i-ой ЭС. Алгоритм будет работать до тех пор, пока составляющие наблюдаемых процессов изменения $\mathfrak{C}^{t_i}_j$ и $\mathfrak{S}^{t_i}_j$ не попадут в область $\mathfrak{G}_\psi$ и по ним будет принято решение $d^{01}_З$ или $d^{10}_З$. При получении решения $d^{01}_З$, количество шагов и последовательность выбора и реализация ЭС из ОПП определяют оптимальную стратегию самоконтроля. Количество КПЭ, содержащееся в ПОЭ, определяет глубину самоконтроля в КПА.

Выводы

На каждом цикле выполнения алгоритма наблюдаемыми областями являются ПОЭ и ОПП. В качестве потерь принимается вероятность ложного забракования КПА по выполняемой ЭС, выбираемой из области ОПП ЭС, покрывающую подозреваемую на отказ область комбинаторных подмножеств элементов. Применение алгоритма позволяет решить задачу определения оптимальной глубины локализации отказов, с учетом пересечения элементарных самопроверок и применить гибкий алгоритм функционирования системы управления беспилотным летательным аппаратом в полете, для выполнения конечной задачи целевого применения.

Литература:

1. *Морозов Д.В*. Методика повышения надежности функционирования системы управления летательного аппарата// V Международная научно-практическая конференция ITS Forum-Kazan «Современные проблемы безопасности жизнедеятельности: интеллектуальные транспортные системы и ситуационные центры». 27–28 февраля 2018 г. – С.123–138.
2. *Морозов Д.В.* Повышение надежности функционирования системы управления беспилотного летательного аппарата в полете Вестник Казанского государственного технического университета им. А.Н. Туполева, 2017. № 3(89). – С.112–118.
3. *Морозов Д.В.* Методика определения потерь в решении задач повышения надежности функционирования системы управления беспилотного летательного аппарата в полете//Труды Международного симпозиума надежность и качество (Пенза, 21–31 мая 2018 г.). – 2018. – т. 1. – С.139–144.

Орёл Е.Н.

Минимизация рисков при управлении динамической системой в условиях конфликта и конкуренции

Аннотация: Для двух соперничающих динамических систем (фирм или объектов) рассматривается возможность численного построения цены динамической игры. Руководствуясь этой ценой, система может принимать решения с практически минимальным риском.

Ключевые слова: динамические игры, стратегии, риски, ячейки, элементарные траектории

В задачах динамической оптимизации будущее системы не всегда зависит только от принятого решения. Весьма часто имеется соперничающая сторона, которая стремится свести на нет усилия системы. С теоретической точки зрения возникает динамическая игра двух лиц [1,2]. Оптимальные стратегии партнёров определяются ценой (значением) игры. Эту цену даже в сравнительно простых динамических играх найти невозможно. Здесь будет рассмотрен численный подход, который в известных дифференциальных играх проявил себя достаточно успешно. В основе подхода лежит разбиение пространства состояний на ячейки (классы) [3,4].

Поведение соперников в достаточно общем случае определяется векторными дифференциальными уравнениями

$$\frac{dx_i(t)}{dt} = f_i(x_i(t), u_i(t), t), \;\; i = 1,2. \qquad (1)$$

Пусть Y – пространство состояний, X_i - фазовое пространство для i -го партнёра, U_i - множество допустимых управлений i-го игрока. Каждой паре

$(x_1 \in X_1, \;\; x_2 \in X_2)$

соответствует вектор состояния

$y = h(x_1, x_2) \in Y.$

Так, если рассматривается плоское движение с ограниченной кривизной обоих соперников, то

$X_i = R^2 \times I, \;\; i = 1,2, \;\; Y = R \times I^2,$

где I – единичная окружность. Игра заканчивается на терминальном множестве $\Theta \subset Y$. Выигрыш второго игрока, равно как и потери первого, составляют

$$J = \int_0^T L(x_1(t), x_2(t), u_1(t), u_2(t), t)\, dt,$$

где 0 и T - соответственно моменты начала и окончания игры, $L > 0$ - функция Лагранжа.

Выбирая управление, каждый партнёр имеет возможность использовать текущее состояние игры $y(t) = h(x_1(t), x_2(t))$. Стратегией i -го игрока называется функция $u_i = s_i(y)$, определённая на множестве Y и принимающая значения в множестве U_i. В теории игр определяются минимаксные и максиминные стратегии, а также цена игры. Всё это в задачах динамической оптимизации – теоретические конструкции, которые аналитически построить невозможно, за исключением весьма частных случаев. Необходимо переходить к дискретным структурам. Но если перейти от фазовых координат к точечной решётке, то возникнет неразрешимая проблема движения по точкам, поскольку многократно придётся решать уравнения (1) для двух точек фазового пространства.

В [1,2] предложен общий подход для решения задач оптимального управления, основанный на разбиении пространства состояний на конечное число множеств, называемых *ячейками*, или *классами*. На множестве классов за каждого игрока строится функция Беллмана. Ясно, что она имеет конечное число значений. Получается, что все точки ячейки имеют одно и то же значение функции Беллмана. Эти значения для всех ячеек формируются на первом этапе.

В настоящей работе показывается, как этот подход можно использовать в динамических играх. Для этого в простом варианте надо задать элементарный промежуток времени Δt и в множествах U_i выбрать конечные подмножества, так что управления должны быть кусочно постоянными функциями. Можем с самого начала считать, что U_i конечны. Теперь следует определить элементарные траектории как решения уравнения (1) при постоянных управлениях на промежутке времени Δt.

Начальные значения функций Беллмана B_i задаём, исходя из принципа априорного оптимизма. Значит, в начальный момент функция Беллмана для первого игрока тождественно равна нулю $B_1(y) \equiv 0$, а для второго игрока она задаётся формулой

$$B_2(y) = \begin{cases} 0, & \text{если } y \in \Theta, \\ M, & \text{если } y \in Y \backslash \Theta. \end{cases}$$

где M - достаточно большое положительное число.

Теперь с помощью подхода, напоминающего имитационное моделирование, многократно случайным образом выбираем «начальные» фазовые точки $\left(x_1^{(0)}, x_2^{(0)}\right)$. В этих точках (точнее, в соответствующих классах состояний $\bar{h}\left(x_1^{(0)}, x_2^{(0)}\right)$) корректируются значения функций Беллмана $B_i\left(x_1^{(0)}, x_2^{(0)}\right)$.

Из точки $x_1^{(0)}$ выходит конечное число элементарных траекторий. Для каждой такой траектории γ_1 перебираем все элементарные траектории, выходящие из точки $x_2^{(0)}$. Обозначим

$$l_{\gamma_1} = \max_{\gamma_2}[J + B_1].$$

Здесь максимум берётся по всем элементарным траекториям, выходящим из $x_2^{(0)}$. Первым слагаемым является значение функционала J вдоль траекторий (γ_1, γ_2). Второе слагаемое – текущее значение функции Беллмана B_1 в конечном состоянии пары траекторий (γ_1, γ_2).

Далее вычисляем

$$l = \min_{\gamma_1} l_{\gamma_1}.$$

Минимум берётся по всем траекториям γ_1, выходящим из текущей точки. Коррекция функции B_1 в текущей ячейке производится по формуле

$$B_1\left(x_1^{(0)}, x_2^{(0)}\right) :=\propto B_1\left(x_1^{(0)}, x_2^{(0)}\right) + (1-\propto)l,$$

где $\propto \in (0,1)$. Аналогично корректируется значение $B_2\left(x_1^{(0)}, x_2^{(0)}\right)$, только вместо минимакса берётся максимин. Чем больше генерируется случайных точек, тем точнее будет результат и меньше будет риска для каждого из соперников. Предложенная процедура решает задачу для каждого из них. Им нет смысла уклоняться от той стратегии, которая определяется найденными приближёнными значениями функций Беллмана.

После формирования функции B_i-й игрок можно переходить к управлению реальным процессом. При таком управлении отклонения от оптимальных стратегий партнёров будут минимальными, а их риски - незначительными.

Предложенный подход был проверен на известных задачах преследования. Во всех случаях результаты были достаточно убедительными. На рис. 1 приведены две партии игры преследования на плоскости при постоянных скоростях $v_1 > v_2$ и ограниченной кривизне траекторий.

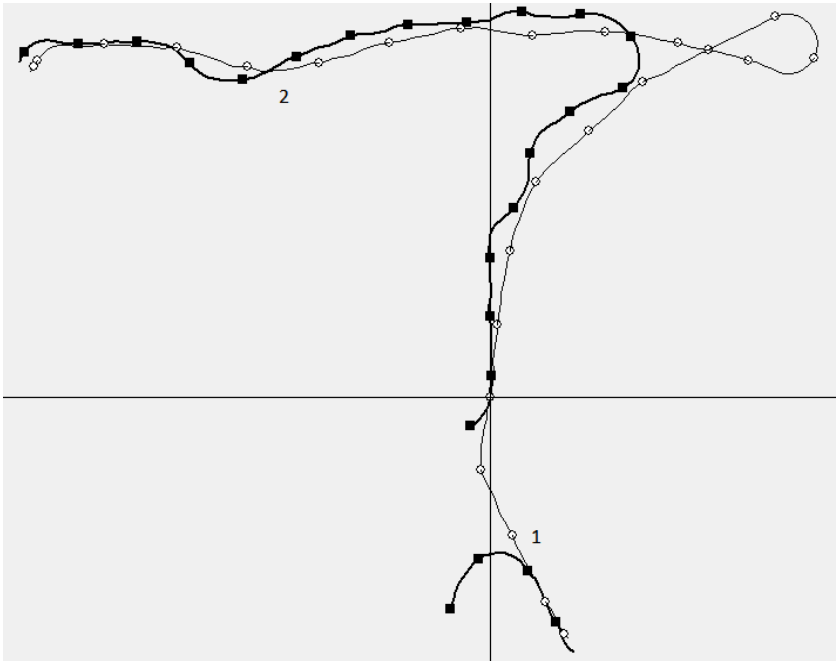


Рис. 1 – Две партии игры преследования
при ограничениях на кривизну

Рисунок построен программой Borland Delphi, поэтому необходимы пояснения. Как всегда, числовые оси пересекаются в начале координат O. Траектории преследующего (первого игрока) обозначены тонкой линией. Для наглядности все они начинаются в точке O.

Начальное направление движения первого игрока выбирается случайным образом. Начальные координаты и начальное направление движения второго игрока выбирались генератором случайных чисел. Его траектории обозначены жирной линией. Через равные промежутки времени на траекториях поставлены вехи – пустые круги и полные квадраты, благодаря чему можно видеть, где находились противники в любой момент времени.

В партии номер 1 начальное направление движения преследователя было чуть меньше двухсот семидесяти градусов. Второй игрок в начальный момент находился в третьей четверти и был направлен примерно в начало координат. Чтобы не столкнуться с первым игроком, он вынужден был развернуться, в результате чего первый игрок зашёл ему «в хвост». Встреча состоялась, так как первый игрок обладает большей скоростью.

В партии номер 2 в начальный момент первый игрок имел направление чуть меньше девяноста градусов, а второй игрок находился в третьей четверти и имел направление около сорока пяти градусов по отношению к оси Ox. Пользуясь этим положением, второй игрок зашёл «в хвост» первому игроку. Благодаря большей скорости первый игрок развернулся (в районе правого верхнего угла рисунка) и оказался сзади второго, после чего легко догнал его. Упомянутый разворот происходил по минимально возможному радиусу.

В реальных динамических играх отсутствуют препятствия для разбиения пространства состояний на ячейки и выбора элементарных траекторий. Благодаря этому можно будет строить стратегии минимального риска.

Литература:

1. *Айзекс Р.* Дифференциальные игры. - М.: Мир, 1967. 480 с.
2. *Петросян Л.А., Зенкевич Н.А., Семина Е.А.* Теория игр. - М., Высшая школа, Книжный дом “Университет”, 1998. 304 с.
3. *Орёл Е.Н.* Метод решения задач оптимального управления // Доклады Академии Наук. – т. 306, 1989, № 6.
4. *Орёл Е.Н.* Алгоритмы поиска квазиоптимального управления, использующие разбиение пространства состояний // Ж. вычисл. матем. и матем. физ. – т. 29, 1990, № 9.

Гучук В.В.

Вопросы применения технологии упреждающей критериальной адаптации для мониторинга и управления сложными системами

Аннотация: Повышению эффективности работы механизмов предотвращения и локализации нештатных и аварийных ситуаций может способствовать использование технологии упреждающей критериальной адаптации – ситуационно-контекстной перестройки системы управления, осуществляемой по определенным принципам и направленной на обслуживание режима выхода из наиболее вероятного негативного развития управляемого процесса. Такая технология необходима для систем с быстротекущими процессами, в которых время между явным проявлением скатывания процесса управления в нештатный режим и началом неуправляемого развития аварии бывает настолько ничтожно малым, что сложившуюся ситуацию уже невозможно исправить никаким образом, в том числе из-за загруженности системы аварийной защиты отработкой алгоритмов не самых актуальных на данный момент.

Ключевые слова: критерий, адаптация, динамические параметры, нештатная ситуация, интерактивный режим, аварийная защита

Для повышения эффективности работы механизмов предотвращения и локализации нештатных и аварийных ситуаций представляется целесообразным использовать технологию упреждающей критериальной адаптации (ТУКА), предложенную в [1] - ситуационно-контекстную настройку системы управления, осуществляемую по определенным принципам и направленную на обслуживание режима выхода из наиболее вероятного негативного развития управляемого процесса. Такая технология необходима для систем с быстротекущими процессами, в которых время между явным проявлением скатывания процесса управления в нештатный режим и началом неуправляемого развития аварии бывает настолько ничтожно малым, что сложившуюся ситуацию уже невозможно исправить никаким образом, в том числе из-за загруженности системы аварийной защиты отработкой алгоритмов не самых актуальных на данный момент. Использование ТУКА - это попытка подойти наиболее подготовлено к возникающим ситуациям в управляемом объекте. Конечно, эта цель ставится во многих разрабатываемых системах мониторинга и управления. Речь идет о более пристальном внимании к этой проблеме и о попытке повысить статус разработки инструментария именно в плане упреждающей стратегии.

В арсенале технологии: - попытка максимально объективизировать актуализацию необходимых алгоритмов выхода из возможной нештатной ситуации, что требует дополнительной обработки данных в реальном и часто “жестком” времени; - освобождение системы прерываний от обработки поступающих данных, не актуальных для возникающей ситуации; - корректировка пороговых значений определенных контрольных параметров для более раннего определения самого факта разладки в контексте текущей ситуации; - сопоставительный анализ возможных последствий отклонения тех или иных параметров от нормативных значений с учетом достоверности имеющейся информации. Возможный эффект от использования упреждающей критериальной адаптации на примере работы алгоритма предотвращения развития нештатной ситуации иллюстрирует рис. 1.

Упреждающая критериальная адаптация:

- позволяет выстроить адекватную для текущей ситуации систему приоритетов и ранжиров параметров и показателей, что исключает запуск неактуальных алгоритмов, могущих заблокировать на определенное время ΔT (рис. 1) включение нужного алгоритма (важнейший фактор для работы сложно-технических изделий в условиях жесткого временного лимита);

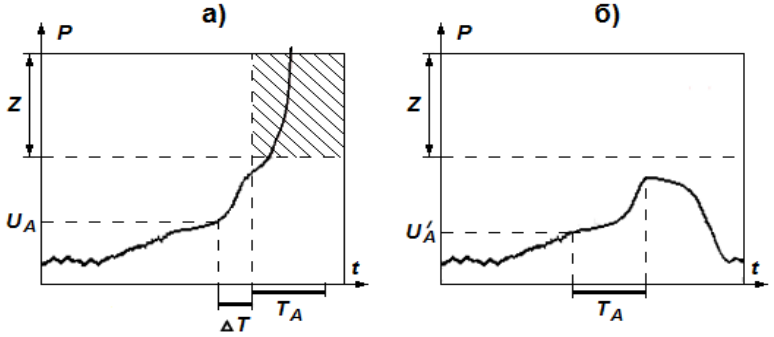


Рис. 1 – Работа алгоритма предотвращения развития нештатной ситуации: а) без использования ТУКА (реальная авария сложного научно-технического изделия) и б) с ее использованием (гипотетическая кривая, построенная по апостериори найденным признакам скатывания в нештатную ситуацию)

На рисунке:

P - значение контролируемого параметра;

Z - зона неуправляемого развития нештатной ситуации;

U_A - порог срабатывания алгоритма;

T_A - время, необходимое для отработки алгоритма;

ΔT - время ожидания отработки других, уже запущенных алгоритмов;

U'_A - скорректированный порог срабатывания алгоритма.

- настраивает уровни прерывания, пороги и условия срабатывания алгоритма предотвращения неблагоприятного развития нештатной ситуации, что позволяет осуществить более ранний запуск алгоритма и тем самым кардинально повысить его эффективность;

-одновременно, за счет настройки уровней прерывания, порогов и условий срабатывания алгоритма, порождает и комплементарный эффект – уменьшение вероятности ложного срабатывания алгоритма, что дает возможность корректной эксплуатации дорогостоящего объекта управления;

- дополняется ситуационно-контекстной визуализацией, которая дает максимально возможное представление о состоянии управляемой системы в каждый конкретный момент, и в то же время позволяет человеку-оператору адекватно воспринимать представленную информацию и принимать осознанные и эффективные действия;

- может включать визуальную поддержку человека-оператора при осуществлении им логического анализа текущей ситуации (см. выше).

Понижение порога срабатывания – это один из возможных вариантов подстройки системы диагностики и прогнозирования к текущей ситуации. В зависимости от конкретного объекта такая процедура может быть и не допустимой, или для ее реализации не будет достаточных знаний о процессах в объекте. В общем случае понижение порога срабатывания может дополняться или замещаться другими процедурами. Достаточно прозрачным, для определенного режима эксплуатации, может быть решение объединить ряд параметров в группу, и определять достоверно начало движения к выходу из штатной ситуации по одинаковой почти неявной динамике всех или большинства параметров этой группы. Понижение порога в определенном смысле может быть чисто символическим понятием. В простейшем случае можно сузить коридор допустимых значений параметров, характеризующих уровень вибраций или шумов [2].

Основная сложность реализации ТУКА состоит в необходимости обеспечения достоверного прогнозирования развития управленческой ситуации, и в определении момента перестройки системы управления. Конечно, есть тривиальные решения, когда объект управления переходит из одного режима работы в другой – это и является сигналом к перестройке. Также ясно, что необходимо использовать наиболее эффективные алгоритмы прогнозирования. Как показывает практика [3], такие алгоритмы достаточно просто разработать для моделирования предупреждения возникновения неуправляемой нештатной ситуации по данным уже произошедшей аварии, но эти алгоритмы нельзя распространить на более широкий класс задач. Это обусловлено наличием неопределенностей и неполного представления о свойствах новых научно-

технических объектов. Они, как правило, являются уникальными образцами. Отсутствует достаточная статистика, и имеются лишь приближенные модели процессов, протекающих в этих объектах. Отсюда желательно самообучение и самонастройка алгоритмов диагностики и прогнозирования с непременным участием экспертов (в том числе из состава разработчиков). Необходимо обезопасить эксплуатацию с самого начала, еще до получения содержательного материала для совершенствования алгоритмов.

Вопросам предотвращения и локализации нештатных и аварийных ситуаций уделяется пристальное внимание при разработке систем мониторинга и управления [4]. Представляется целесообразным дополнять арсенал повышения эффективности создаваемого инструментария за счет использования наиболее корректных методов превентивной адаптации.

Литература:

1. *Безгубова Ю.К., Гучук В.В.* Технология упреждающей критериальной адаптации в мониторинге и управлении сложными научно-техническими объектами / Материалы 7-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2013, Москва). М.: ИПУ РАН, 2013. Т.2. С. 420-423.
2. *Guchuk V.* Applied aspects of the organization of an interactive mode for increasing the security of functioning of control systems of complicated objects // European Science. 2018, № 1. – P. 18-21.
3. *Guchuk V.* Development of information exchange of software and hardware tools of system of test of difficult scientific-technical objects / Proceedings of the 10th International Conference "Management of Large-Scale System Development" (MLSD). M.: IEEE Explore Digital Library, 2017. С. 1-5.
4. *Бигус Г.Ф., Даниев Ю.Ф., Быстрова Н..А, Галкин Д.И.* Диагностика технических устройств. – М.: МГТУ им. Н.Э. Баумана, 2014. – 615с.

Прошина О.М.

Моделирование системы обеспечения пожарной безопасности образовательного комплекса

Аннотация: Предлагается рассмотреть применение современных компьютерных средств с использованием соответственного программного обеспечения для образовательных комплексов, что позволит максимально эффективно проводить профилактику пожаров, выполнять их локализацию и тушение.

Ключевые слова: моделирование; пожарная безопасность; система обеспечения пожарной безопасности; образовательные комплексы

Современные технические средства обеспечения безопасности образовательных комплексов на сегодняшний день предполагают расширенную охранную и защитную функцию, однако, возникла другая проблема – порядок взаимодействия должностных лиц при пожарах и чрезвычайных ситуациях на территории комплексов [1].

Проблема возникла в связи с тем, что предварительно практически не были подготовлены необходимые документы по формированию основ организации систем безопасности для нового типа объектов. При возникновении ЧС или пожара на территории комплексов порядок взаимодействия внутренних и привлекаемых специальных служб действуют «по старинке», что уже является нарушением. При этом действующие лица вынуждены в обязательном порядке ждать решения ответственных администраторов комплексов. В связи с возникшей проблемой предлагается разработать модель управления системой обеспечения пожарной безопасности и взаимодействия ответственных лиц при пожаре и ЧС, применимые к образовательным комплексам (рис.1) [2].

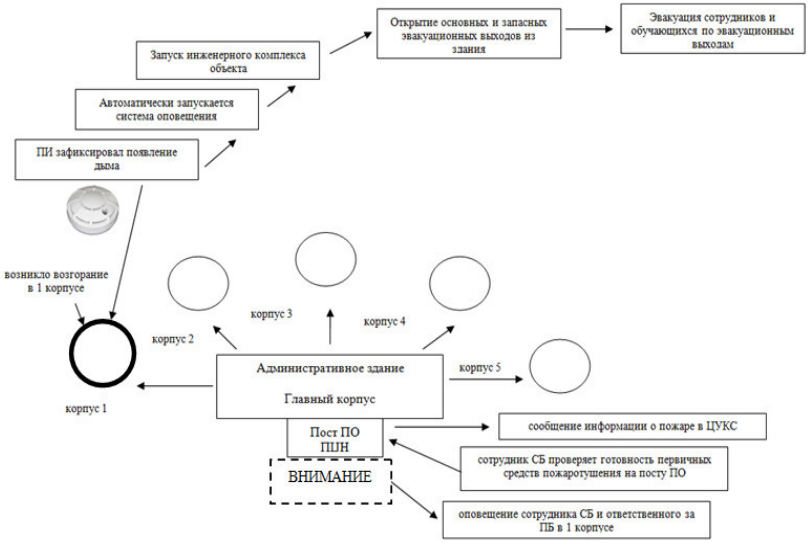


Рис. 1 – Порядок управления системой обеспечения пожарной безопасности и взаимодействие ответственных лиц при пожаре

С целью моделирования развития чрезвычайных ситуаций в образовательном комплексе необходимо рассмотреть различные сценарии

развития чрезвычайных ситуаций на объекте защиты, так как на каждом этапе управления действия персонала могут отличаться от действий того же персонала при других факторах развития чрезвычайных ситуаций. Необходимо отметить, что системы обеспечения пожарной безопасности также будут выполнять свои функции по-разному, в зависимости от сценария развития чрезвычайных ситуаций на объекте.

Так, например, в случае задымления в помещении в подвальной части здания система отработает по сценарию «ВНИМАНИЕ» и «ПОЖАР» с запуском системы управления инженерным комплексом объекта. Запуск системы оповещения и эвакуации людей при пожаре позволит оперативно эвакуировать обучающихся, а система дымоудаления, установленная в подвальных помещениях, поможет оперативно удалить продукты горения и облегчит доступ пожарных подразделений к месту возникновения пожара, его локализации и тушения [3].

В то же время при развитии пожара по другому сценарию, а именно, возгорание на одном из этажей, произойдет запуск инженерного комплекса объекта, запуск системы оповещения и эвакуации людей при пожаре, также произойдет открытие фрамуг дымоудаления. Данный факт говорит о том, что в зависимости от места возникновения чрезвычайных ситуаций, инженерный комплекс объекта осуществляет управление инженерными системами по запрограммированному сценарию управления, производит запуск нужных сопутствующих инженерных систем, а также посредством системы оповещения людей о пожаре в автоматическом режиме выдает команды на управление личным персоналом с целью эвакуации персонала по безопасным путям эвакуации. С точки зрения моделирования развития чрезвычайных ситуаций на объекте, возможны различные сценарии развития опасных ситуаций. В качестве первичных факторов пожара может быть дым, открытое горение, утечка ЛВЖ, и при каждом из сценариев личный персонал, администрация и инженерный комплекс объекта должны работать слаженно, как единое целое, придерживаясь единым целям, минимизации человеческих жертв, минимизации потерь имущества на местах.

Необходимо осуществить оценку наихудшего сценария развития пожара с помощью моделирования. Во время данной оценки анализируются системы оповещения о пожаре, сигнализации и тушения, противопожарные средства и оборудование. Кроме того, выполняется анализ вида и количества горючих материалов, число людей и их вероятное место расположения, значимость самого объекта (материальная и социальная).

В развитии пожара в помещениях можно выделить три стадии:

1. Начальная стадия. Интервал: от возникновения локального неконтролируемого очага возгорания до полного охвата помещения огнем.

Особенности: невысокая средняя температура среды в помещении; внутри и вокруг зоны горения температура достаточно высока.

2. Полное развитие пожара. Особенности: горят горючие вещества и материалы; интенсивность тепловыделения от горящих объектов максимальная.

3. Затухание пожара. Особенности: снижение интенсивности процессов горения путем выгорания горючих материалов или воздействия средств тушения.

Необходимо обратить внимание, что безопасная эвакуация людей может происходить лишь на первой стадии пожара. Но и данная стадия несет в себе множество опасностей, а именно: пламя с возможностью возгорания, высокий уровень температуры, выделение токсичных веществ, снижение процента содержания кислорода в воздухе.

Для прогнозирования опасных факторов пожара можно использовать 3 эффективных и утвержденных модели: интегральная, зонная, полевая.

Интегральная модель предполагает выполнение прогноза усредненных значений параметров состояния среды в помещении на любой момент развития пожара. Этот вариант расчетов применяется в отношении зданий с простой конфигурацией и множеством небольших помещений. Он эффективен при работе с объектами, размеры комнат в которых соизмеримы (линейные отклонения не превышают 5-кратного значения). Кроме того, его используют для построения сценария с наиболее масштабными последствиями.

Зонная модель - выполняется прогноз размеров характерных пространственных зон, возникающих при пожаре в помещении. Данная методика позволяет моделировать ситуации для объектов с простой планировкой и незначительными отклонениями в размерах комнат. Она даст точные результаты, если очаг возгорания окажется значительно меньше объема одного помещения. Актуален алгоритм и при проработке сценария для сооружений с различным положением рабочих зон (наклонные ниши, антресоли и прочее).

Полевая модель предполагает выполнение прогноза пространственно-временного распределения температур и скоростей газовой среды в помещении, концентраций компонентов среды, давлений и плотностей для любой точки помещения. Этот алгоритм разработан специально для многофункциональных зданий со сложной планировкой. Полевой метод актуален при создании моделей для уникальных объектов, зданий неправильной геометрии. Этот вариант используется при формировании сценария развития пожара на территории подземных стоянок, тоннелей и прочих сооружений [4].

Разрабатывая вышеописанные алгоритмы, можно получить объективные данные. Моделирование дает возможность:

– определить наиболее опасные зоны (требуется при разработке СТУ, формировании схем, планов и прочего);
– выделить недостатки систем защиты от огня, тушения возгораний, эвакуации людей;
– оценить достаточность мероприятий по пожарной безопасности;
– выявить ранее не исследованные опасные факторы;
– проверить эффективность дополнительных средств защиты.

По итогам составляют отчет с полным описанием ситуаций и прогнозами. Особое внимание уделяется последствиям пожаров, а также рискам возникновения человеческих жертв. Приоритетом в создании моделей является максимальная достоверность.

Наиболее простые способы моделирования возможного пожара носят название вербальных. Они включают в себя описание возгорания, изменения температуры в помещении, появлении продуктов горения, аккумуляции тепла конструктивными элементами и оборудованием, в результате чего происходит деструкция сгораемых частей.

Ввиду распространения огня происходит его расширение на другие площади и объекты. Поэтому для ликвидации пожара необходимо одновременно принимать все средства для его локализации при обеспечении одновременной эвакуации материально-технических ценностей. Для этого одновременно применяют методические и практические способы изучения пожара, базирующиеся на основе физико-математических наук, механики, материаловедения и пр.

В настоящее время разработаны программные комплексы, позволяющие создавать и разрабатывать сложные многофакторные модели пожаров в полевом режиме. Всего известно более 150 моделей развития пожара, включающих процессы тепломассопереноса, возгораемости веществ и строительно-конструктивных элементов. Поэтому разработка данных моделей должна включать в себя особенности эвакуации людей и животных в чрезвычайных ситуациях, создания приборов с повышенной пожаробезопасностью. Для обеспечения пожарной безопасности зданий, людей, технологических процессов следует предусмотреть использование современных средств пожарной защиты в программном комплексе.

Таким образом, моделирование пожара является важным инструментом практической части ввиду определения возможных сценариев развития возгорания. Применение современных компьютерных средств с использованием соответственного программного обеспечения для образовательных комплексов позволяет максимально эффективно проводить профилактику пожаров, выполнять их локализацию и тушение.

Литература:
1. *Прошина О.М.* Проблемы обеспечения пожарной безопасности образовательных комплексов мегаполисов // Материалы 26-й междунар. научн.-техн. конф. «Системы безопасности - 2017». – М.: Академия ГПС МЧС России, 2017. – С. 419-421.
2. *Прошина О.М., Рыженко, А.А.* Пожарная безопасность образовательных комплексов мегаполисов // Сборник материалов XII Международной научно-практической конференции, посвященный Году гражданской обороны. – Иваново: ФГБОУ ВО Ивановская пожарно-спасательная академия ГПС МЧС России, 2017. – С. 154-155.
3. *Прошина О.М.* Проблема взаимодействия внутренних и привлекаемых специальных служб при пожарах и чрезвычайных ситуациях в образовательных комплексах // Материалы VII Международной научно-практической конференции молодых ученых и специалистов «Проблемы техносферной безопасности - 2018». – М.: Академия ГПС МЧС России, 2018. – С. 40-44.
4. *Серебренников Д.С., Охроменко, А.С.* Математическое моделирование как инструмент анализа пожарной опасности конструкций, зданий и сооружений // Молодой ученый. — 2010. — №12. Т.1. — С. 33-35.

Акатьев С.В., Куранцов В.В., Назаркин А.С., Еремин М.С., Кормилицин А.И.

Применение волновой теории ударной безопасности для моделирования напряженного состояния (несущей способности) технических объектов с помощью комплекса программ Мусаева В.К.

Аннотация: Приводится информация о применении численного моделирования для определения волн напряжений в деформируемых объектах различной формы. Применяется волновая теория ударной безопасности. Для решения поставленной задачи применяется метод конечных элементов в перемещениях. Рассмотрены некоторые задачи при ударных нагрузках и воздействиях.

Ключевые слова: детерминированное моделирование, волновая теория ударной безопасности, ударные воздействия, волновая теория, динамическая теория упругости, напряженное состояние, численный метод, алгоритм, комплекс программ Мусаева В.К.

Информация о моделировании нестационарных волн напряжений в деформируемых телах сложной формы приведена в следующих работах [1–5] .

Некоторая информация о верификации рассматриваемого численного метода, алгоритма и комплекса программ приведена в следующей работе [1].

Применение численного моделирования в задачах безопасности сложных объектов при ударных воздействиях рассмотрено в следующих работах [2–5].

Решена задача о воздействии упругой ударной волны на фундамент машин без полости [2]. Исследуемая расчетная область имеет 14320 узловых точек. Решается система уравнений из 57280 неизвестных. Получены напряжения в точках на поверхности упругой полуплоскости около фундамента машин без полости (рис. 1).

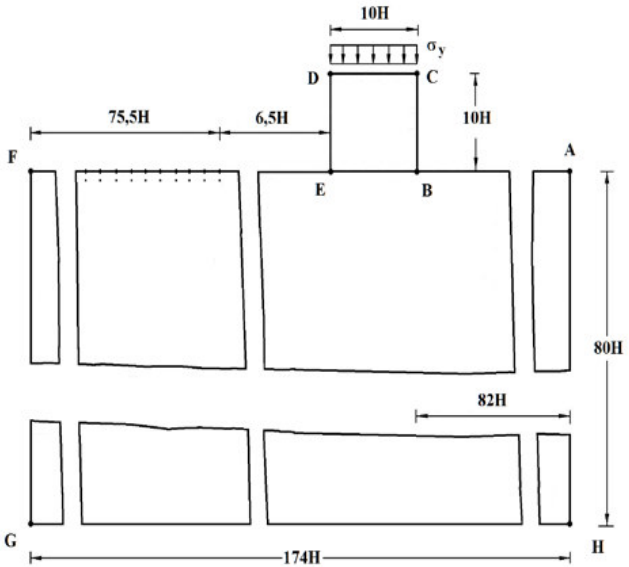


Рис. 1 –Постановка задачи о воздействии упругой ударной волны на фундамент машин без полости [2]

Решена задача о воздействии воздушной ударной волны на консоль (соотношение ширины к высоте консоли – один к десяти) с упругой полуплоскостью [3]. Исследуемая расчетная область имеет 4008004 узловых точек. Решается система уравнений из 16032016 неизвестных (рис. 2).

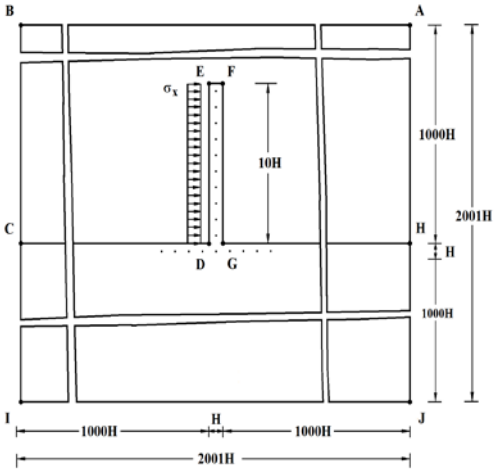


Рис. 2 – Постановка задачи о воздействии воздушной ударной волны на консоль с упругой полуплоскостью
(соотношение ширины к высоте консоли – один к десяти) [3]

Решена задача о распространении нестационарных упругих волн в пластинке (воздействие – сосредоточенное; соотношение толщины пластинки к длине волны воздействия – один к двум). Исследуемая расчетная область имеет 22011 узловых точек. Решается система уравнений из 88044 неизвестных.

Решена задача о распространении нестационарных упругих волн в пластинке (воздействие – сосредоточенное; соотношение толщины пластинки к длине волны воздействия – один к одному). Исследуемая расчетная область имеет 42021 узловую точку. Решается система уравнений из 168084 неизвестных.

Решена задача о распространении нестационарных упругих волн в пластинке (воздействие – сосредоточенное; соотношение толщины пластинки к длине волны воздействия – полтора к одному). Исследуемая расчетная область имеет 62031 узловую точку. Решается система уравнений из 248124 неизвестных.

Решена задача об ударном аварийном выбросе нефти в сложной системе, которая состоит из разных деформируемых сред (водной, нефтяной и твердой), а так же из твердого деформируемого саркофага (соотношение высоты к ширине два к семи) (рис. 3) [4]. Исследуемая расчетная область имеет 4014010 узловых точек. Решается система уравнений из 16056040 неизвестных.

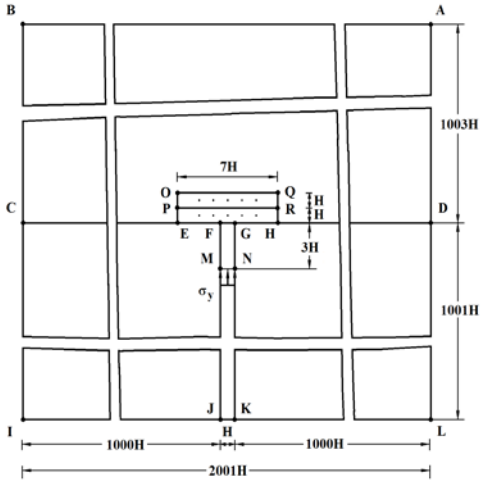


Рис. 3 – Постановка задачи об ударном аварийном выбросе нефти в сложной деформируемой системе с саркофагом (плита: соотношение высоты к ширине два к семи) [4]

Решена задача об ударе самолета на систему сооружение-фундамент-основание (Архангельская атомная станция) (H = 69,9 м) (рис. 4) [5]. Исследуемая расчетная область имеет 1096 узловых точек. Решается система уравнений из 4384 неизвестных. Получены контурные напряжения в защитной оболочке реакторного отделения атомной станции.

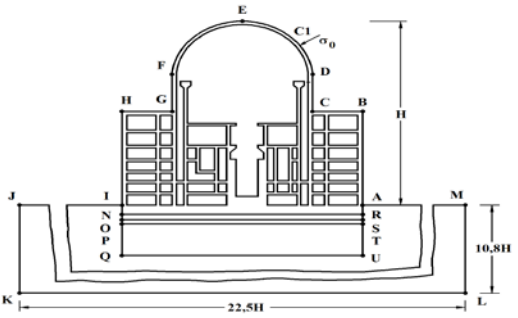


Рис. 4 – Постановка задачи для Архангельской атомной станции [5]

Авторы выражают благодарность Мусаеву В.К. за оказанную помощь и внимание к работе.

Литература:
1. *Musayev V.K.* Estimation of accuracy of the results of numerical simulation of unsteady wave of the stress in deformable objects of complex shape // International Journal for Computational Civil and Structural Engineering. – 2015. – Volume 11, Issue 1. – P. 135–146.
2. *Мусаев В.К.* Численное моделирование динамических напряжений в фундаменте машин с основанием (полуплоскость) при воздействии нестационарной упругой ударной волны // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 3–2. – С. 232–236.
3. *Мусаев В.К.* Моделирование нестационарных волн напряжений в задаче о воздействии воздушной ударной волны на консоль (соотношение ширины к высоте один к десяти) с упругой полуплоскостью // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 3–1. – С. 38–42.
4. *Мусаев В.К.* Численное моделирование саркофага (соотношение ширины к высоте семь к одному, двум и трем) в водной среде для уменьшения ударного воздействия (выброса) нефти из скважины // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 11–3. – С. 408–413.
5. *Musayev V.K.* Numerical simulation of non-stationary elastic contour stresses in the shell of the reactor compartment of the nuclear power station with the foundation and basis (half-plane) at impact of aircraft // International Journal for Computational Civil and Structural Engineering. – 2016. – Volume 12, Issue 4. – P. 116–126.

Дикова Е.В., Шиянов М.И., Кулагина Н.В., Зимин А.М., Куранцов О.В.

Применение волновой теории сейсмической безопасности для моделирования несущей способности уникальных объектов с помощью численного метода, алгоритма и комплекса программ Мусаева В.К.

Аннотация: Приводится некоторая информация о численном моделировании волн напряжений в различных деформируемых объектах. Применяется волновая теория сейсмической безопасности. Для решения задач используется численный метод, алгоритм и комплекс программ Мусаева В.К. Программный комплекс позволяют решать задачи при нестационарных воздействиях на объекты сложной формы при волновых сейсмических воздействиях.

Ключевые слова: численное моделирование, волновая теория сейсмической безопасности, сейсмическое воздействие, численный метод Мусаева В.К., функция Хевисайда, фундаментальное воздействие, изгибные волны

В работах [1–5] приведена информация о моделировании нестационарных волн напряжений в деформируемых телах сложной формы.

Некоторая информация о физической достоверности и математической точности рассматриваемого численного метода, алгоритма и комплекса программ приведена в следующей работе [2, 5].

Рассматривается задача о воздействии плоской продольной упругой волны в виде функции Хевисайда на свободное круглое отверстие. Исследуемая расчетная область имеет 1536 узловых точек. Контур круглого отверстия аппроксимирован 28 узловыми точками.

Рассматривается задача о воздействии плоской продольной упругой волны в виде функции Хевисайда на подкрепленное круглое отверстие. Исследуемая расчетная область имеет 1536 узловых точек. Внутренний контур подкрепления аппроксимирован 28 узловыми точками. По толщине подкрепление аппроксимировано двумя узловыми точками.

Рассматривается задача о воздействии плоской продольной упругой волны на Курпсайскую плотину с основанием [2]. Сейсмическое воздействие моделируется в виде функции Хевисайда. Исследуемая расчетная область имеет 953 узловых точек. Курпсайская плотина аппроксимирована 224 узловыми точками. Курпсайская плотина моделируется с упругим основанием без заполненного водохранилища. Упругое контурное напряжение на гранях Курпсайской плотины является почти зеркальным отражением одна другой, то есть антисимметричным. Курпсайская плотина при сейсмическом воздействии работает как стержень переменного сечения, то есть если на одной грани растягивающие напряжения, то на другой сжимающие напряжения. На контурах Курпсайской плотины при сейсмическом воздействии в основном преобладают изгибные волны (рис. 1).

Рассматривается задача о воздействии плоской продольной упругой волны на плотину Койна с основанием [1, 3]. Сейсмическое воздействие моделируется в виде функции Хевисайда. Исследуемая расчетная область имеет 522 узловые точки. Плотина Койна моделируется с упругим основанием без заполненного водохранилища.

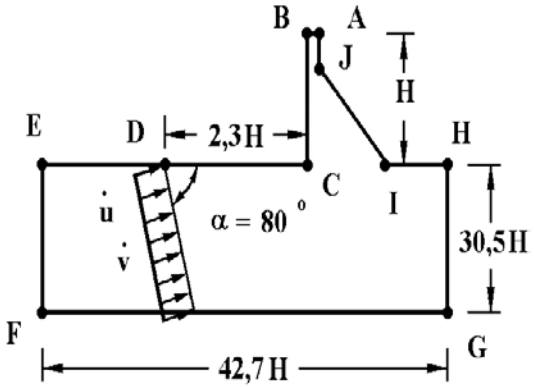


Рис. 1 – Постановка задачи для системы сооружение-основание (Курпсайская плотина) [2]

Упругое контурное напряжение на гранях плотины Койна является почти зеркальным отражением одна другой, то есть антисимметричным. Плотина Койна при сейсмическом воздействии работает как стержень переменного сечения, то есть если на одной грани растягивающие напряжения, то на другой сжимающие напряжения. На контурах плотины Койна при сейсмическом воздействии в основном преобладают изгибные волны (рис. 2).

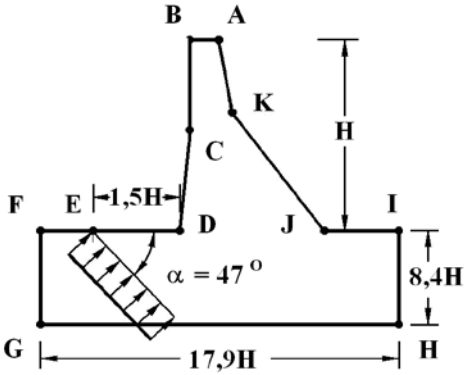


Рис. 2 – Постановка задачи для системы сооружение-основание (плотина Койна) [1, 3]

Решена задача о воздействии плоской продольной сейсмической волны на упругую полуплоскость с полостью (соотношение ширины к высоте один к пяти, десяти и пятнадцати) (рис. 3) [4]. Решается система уравнений из 8016008 неизвестных. Рассматриваются некоторые точки в окрестности полости на свободной поверхности упругой полуплоскости.

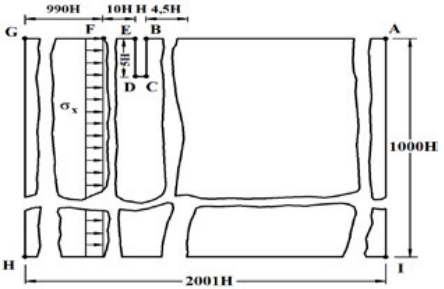


Рис. 3. –Постановка задачи о воздействии плоской продольной сейсмической волны на упругую полуплоскость с полостью (соотношение ширины к высоте один к пяти) [4]

Авторы выражают благодарность Мусаеву В.К. за оказанную помощь и внимание к работе.

Литература:

1. *Мусаев В.К.* Определение упругих напряжений в плотине Койна с основанием с помощью волновой теории сейсмической безопасности // Успехи современного естествознания. – 2014. – № 12–3. – С. 235–240.
2. *Musayev V.K.* Mathematical modeling of seismic nonstationary elastic waves stresses in Krpsai dam with base (half-plane) // International Journal for Computational Civil and Structural Engineering. – 2016. – Volume 12, Issue 3. – P. 73–83.
3. *Musayev V.K.* Numerical simulation of non-stationary seismic stresses in elastic waves dam Koyna with base (half-plane) // International Journal for Computational Civil and Structural Engineering. – 2016. – Volume 12, Issue 3. – P. 84–94.
4. *Мусаев В.К.* Применение нестационарной волновой теории сейсмической безопасности к моделированию напряжений в упругой полуплоскости с вертикальной полостью (соотношение ширины к высоте один к двенадцати) // Новые технологии науки, техники, педагогики высшей школы: материалы Международной научно-практической конференции «Наука – Общество – Технологии – 2017». – М.: Московский политех, 2017. – С. 246–252.

5. *Мусаев В.К.* Сопоставление численного метода с результатами динамической фотоупругости при решении задачи о воздействии плоской продольной волны на свободное круглое отверстие // Высшая школа. Новые технологии науки, техники, педагогики: материалы Всероссийской научно-практической конференции «Наука – Общество – Технологии – 2018». – М.: Московский политех, 2018. – С. 303–313.

Мусаев В.К.

Моделирование безопасности по несущей способности плотины Койна (Индия) с основанием в виде полуплоскости при нестационарном переходном процессе

Аннотация: Рассматриваются вопросы численного моделирования сейсмической безопасности плотины Койна (Индия) с основанием в виде полуплоскости при нестационарных волновых воздействиях. Упругое контурное напряжение на гранях консоли является почти зеркальным отражением одна другой, то есть антисимметричным.
В плотине преобладают изгибные волны.

Ключевые слова: вычислительная механика, контурные напряжения, волновая теория сейсмической безопасности, сейсмическое воздействие, функция Хевисайда, фундаментальное воздействие, плотина Койна, контурное напряжение, изгибные волны

Рассматривается задача о воздействии плоской продольной упругой волны на плотину Койна с основанием (рис. 1). Начальные условия приняты нулевыми.

Некоторые вопросы в области моделирования нестационарных динамических задач с помощью применяемого метода, алгоритма и комплекса программ рассмотрены в следующих работах [3–5].

На основе метода конечных элементов в перемещениях разработаны алгоритм и комплекс программ для решения линейных плоских двумерных задач, которые позволяют решать задачи при нестационарных волновых воздействиях на сложные системы.

В работах [3–4] приведена информация о физической достоверности и математической точности моделирования нестационарных волн напряжений в деформируемых телах с помощью рассматриваемого численного метода, алгоритма и комплекса программ.

Расчеты проводились при следующих единицах измерения: килограмм-сила (кгс); сантиметр (см); секунда (с). Для перехода в другие единицы

измерения были приняты следующие допущения: 1 кгс/см^2 ≈ 0,1 МПа; 1 кгс с^2/см^4 ≈ 10^9 кг/м^3.

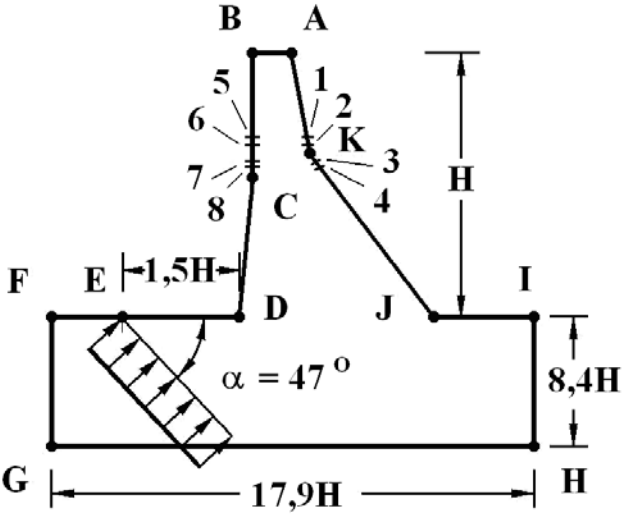


Рис. 1 – Постановка задачи для системы сооружение-основание (плотина Койна)

В сечении на расстоянии 1,5H (рис. 1) при $0 \le n \le 26$ ($n = t/\Delta t$) скорости упругих перемещений $\dot{u}$ и $\dot{v}$ изменяются линейно от 0 до $\dot{u} = P\sin\alpha$ и $\dot{v} = P\cos\alpha$, а при $n > 26$ $\dot{u} = P\sin\alpha$ и $\dot{v} = P\cos\alpha$ ($P = \sigma_0/(\rho C_P)$, $\sigma_0 = 0{,}1$ МПа (1 кгс/см^2)). Контур плотины IJKABCDEF (кроме точки E) предполагается свободным от нагрузок при $t > 0$. Граничные условия для контура FGHI при $t > 0$ $u = v = \dot{u} = \dot{v} = 0$. Отраженные волны от контура FGHI не доходят до исследуемых точек при $0 \le n \le 900$.

Расчеты проведены при следующих исходных данных: H=103 м; $\Delta t = 0{,}104 \cdot 10^{-2}$ с; $E = 0{,}36 \cdot 10^4$ МПа ($0{,}36 \cdot 10^5$ кгс/см^2); $\nu = 0{,}36$; $\rho = 0{,}122 \cdot 10^4$ кг/м^3 ($0{,}122 \cdot 10^{-5}$ кгс с^2/см^4); C_p = 1841 м/с.

Исследуемая расчетная область имеет 522 узловые точки. Решается система уравнений из 2088 неизвестных.

На рис. 2–5 показано изменение контурных напряжений $\bar{\sigma}_k$ в плотине Койна в точках 1–8 во времени $t/\Delta t$.

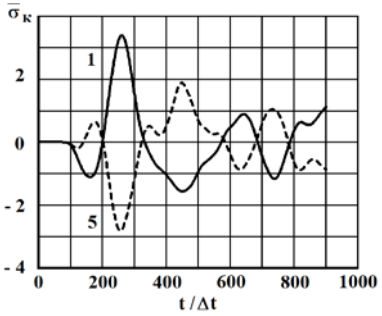


Рис. 2 – Изменение упругого контурного напряжения $\overline{\sigma}_k$ в точках 1 и 5 на контуре плотины Койна во времени $t/\Delta t$

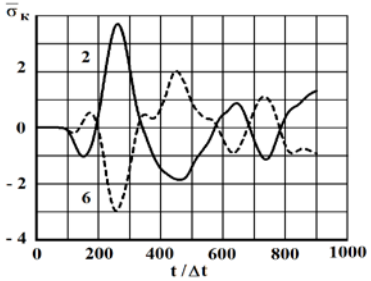


Рис. 3 Изменение упругого контурного напряжения $\overline{\sigma}_k$ в точках 2 и 6 на контуре плотины Койна во времени $t/\Delta t$

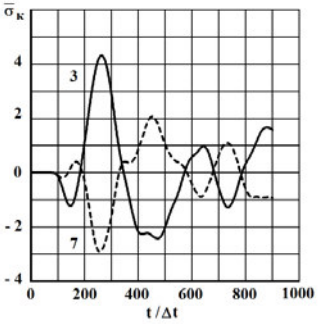


Рис. 4 – Изменение упругого контурного напряжения $\overline{\sigma}_k$ в точках 3 и 7 на контуре плотины Койна во времени $t/\Delta t$

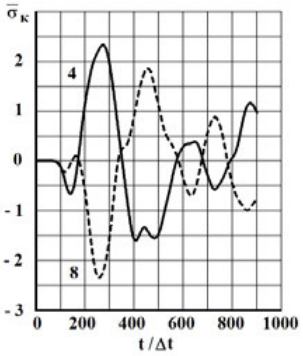


Рис. 5 – Изменение упругого контурного напряжения $\bar{\sigma}_k$ в точках 4 и 8 на контуре плотины Койна во времени $t/\Delta t$

Изменение нестационарных изгибных волн для упругого контурного напряжения $\bar{\sigma}_k$ приведены в следующих точках рассматриваемого объекта А1 (–) и А5 (--) (рис. 2), А2 (–) и А6 (--) (рис. 3), А3 (–) и А7 (--) (рис. 4), А4 (–) и А8 (--) (рис. 5).

В связи с большой глубиной расположения предполагаемых гипоцентров землетрясения плотины Койна [2] будем предполагать, что плотина подвергается воздействию плоской продольной упругой волны типа функции Хевисайда σ_0 [1].

Максимальное растягивающее упругое контурное напряжение при сейсмическом воздействии определяем по следующим формулам

$$\sigma_k = \sigma_k^d + \sigma_k^c, \quad (1)$$

$$\sigma_k^d = \sigma_c \bar{\sigma}_k, \quad (2)$$

$$\sigma_k^c = \gamma h, \quad (3)$$

$$\sigma_c = \frac{\ddot{u}}{2\pi g} \gamma C_p T, \quad (4)$$

где: σ_k – максимальное растягивающее упругое контурное напряжение на контуре плотины при сейсмическом воздействии σ_c; $\bar{\sigma}_k$ – максимальное растягивающее контурное напряжение в точке 3; σ_c – максимальное напряжение в сейсмическом воздействии; $\frac{\ddot{u}}{g}$ – относительное максимальное ускорение, соответствующее баллу землетрясения; γ - объемный вес массива; C_p – скорость распространения

продольной волны в массиве; T – преобладающий период сейсмических колебаний; $\overline{\sigma}_k^d$ – максимальное растягивающее контурное напряжение при нестационарном волновом сейсмическом воздействии в точке 3; $\overline{\sigma}_k^c$ – максимальное напряжение от собственного веса в точке 3; h – вертикальное расстояние от верха плотины до рассматриваемой точки 3.

Таким образом, окончательно получим: σ_c = 1 МПа (10 кгс/см^2) максимальное растягивающее контурное напряжение на контуре плотины в точке 3 при сейсмическом воздействии; $\overline{\sigma}_k$ = 4, 1; σ_k^d = 4,1 МПа (41 кгс/см^2); σ_k^c =-0,436 МПа (-4,36 кгс/см^2); σ_k = 3,664 МПа (36,64 кгс/см^2).

Сравнивая полученное значение максимального растягивающего упругого контурного напряжения σ_k с пределом прочности бетона плотины на растяжение (σ_p =2,45 МПа (24,5 кгс/см^2)) [2] видим, что величины нестационарного волнового напряжения вполне достаточно для создания зарегистрированных после землетрясения разрушений в виде сквозных трещин в окрестности точки 3 (рис. 4).

Литература:

1. *Напетваридзе Ш.Г.* Сейсмостойкость гидротехнических сооружений. – М.: Госстройиздат, 1959. – 216 с.
2. *Chopra A., Chakrabarti P.* Analysis of earthquake performance of Koyna dam // Bulletin of the indian society of earthquake technology. – 1972. – V. 9, № 2. – P. 49–60.
3. *Мусаев В.К.* Численное моделирование динамического напряженного состояния сооружений уравнениями двумерной теории упругости и пластичности. Автореферат диссертации на соискание ученой степени доктора технических наук по специальности 01.02.04. – М.: Совинтервод, 1993. – 46 с.
4. *Musayev V.K.* Mathematical modeling of seismic nonstationary elastic waves stresses in Kurpsai dam with a base (half-plane) // International Journal for Computational Civil and Structural Engineering. – 2016. – Volume 12, Issue 3. – P. 73–83.
5. *Musayev V.K.* Numerical simulation of non-stationary seismic stresses in elastic waves dam Koyna with base (half-plane) // International Journal for Computational Civil and Structural Engineering. – 2016. – Volume 12, Issue 3. – P. 84–94.

Сиротский А.А.

Измеримые критериальные методы оценки состояния информационной безопасности объектов информатизации в непрерывных управленческих процессах

Аннотация: Рассматривается принцип оценки состояния информационной защищенности организаций на основе построения системы измеримых критериальных показателей, которые могут быть положены в основу выработки управленческих решений в системе управления информационной безопасностью компании.

Ключевые слова: информационная безопасность, угрозы, риски, система, управление, критериальные показатели, метрики.

Перед менеджером по информационной безопасности (ИБ) фирм и предприятий встают проблемы не только соответствия требованиям нормативной документации и регуляторов, но и требованиям бизнеса. Как говорят некоторые руководители служб ИБ – «мы служим бизнесу». Для этого как минимум необходимо выстроить процессы защиты информации, соорганизовав и синхронизировав их между службой ИБ и другими службами в компании. Здесь также следует отметить, что проблема может осложняться еще и тем, что не во всех коммерческих компаниях имеется служба информационной безопасности как самостоятельная организационная структура. Во многих небольших организациях функции службы ИБ сконцентрированы в службе информационных технологий (ИТ).

На рис. 1 приведен перечень служб, которые, в том или ином виде существуют в любой средней и крупной организации, а также показана общая модель процессного взаимодействия между ними.

Следует также заметить, что фактические и нормативные требования по ИБ могут в общем случае различаться. При этом нормативные требования должны быть выполнены безусловно.

Задачами менеджера по ИБ в рамках создания и сопровождения системы управления информационной безопасностью (СУИБ) являются: организация межпроцессного взаимодействия между службами; выработка и внедрение процессов управления ИБ; создание системы отчётности перед регуляторами; контроль изменений в бизнес-процессах; выявление и оценка угроз и рисков ИБ; управление рисками; реагирование на инциденты ИБ; контроль выполнимости требований по ИБ; оценка эффективности СУИБ [1].

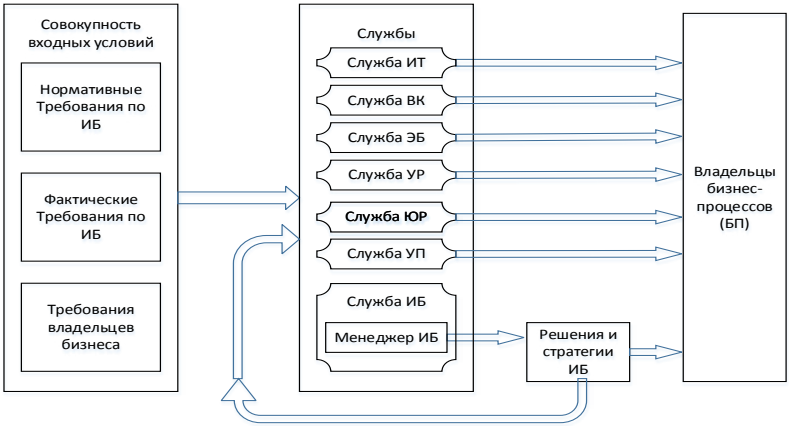


Рис. 1 – Процессное взаимодействие между службами в коммерческих компаниях и учреждениях: Служба ИТ – служба информационных технологий; Служба ВК – служба внутреннего контроля; Служба ЭБ – служба экономической безопасности; Служба УР – служба управления рисками; Служба ЮР – юридическая служба; Служба УП – служба управления персоналом

Реализация процесса управления информационной безопасностью в стремлении соответствовать системе стандартов ГОСТ/ISO 27xxx, требует налаживания цикла Деминга (рис. 2), представляющего собой модель непрерывного улучшения процессов PDCA (Plan - Do - Check - Act) [2, 3, 4].

Рис. 2 – Цикл Деминга в СУИБ

При этом связь между основными участниками процесса СУИБ, влияющими факторами и управляющими воздействиями имеет общий вид, показанный на рис. 3.

Исходя из того, что главная задача управления ИБ – это управление рисками и инцидентами, менеджер ИБ решает все задачи в контексте движения от состояния «как есть» к состоянию «как нужно» [5].

В настоящее время для оценки качества процессов наибольшую популярность зарекомендовали системы, основанные на построении набора критериальных исчислимых показателей, которые чаще всего называются метриками. Метрика – технически или процедурно измеряемая величина, характеризующая объект управления. В этом определении видно два важных момента. Первый – метрика может измеряться как технически, так и процедурно, второй – метрика должна характеризовать объект управления, она должна нести полезную информацию об объекте. Стоит заметить, что в зарубежной литературе в последнее время чаще используется термин «измерение», это подчёркивает, что применяются только количественные метрики. Метрики ИБ – это средства, предназначенные для содействия принятию решений по управлению системой защиты информации.

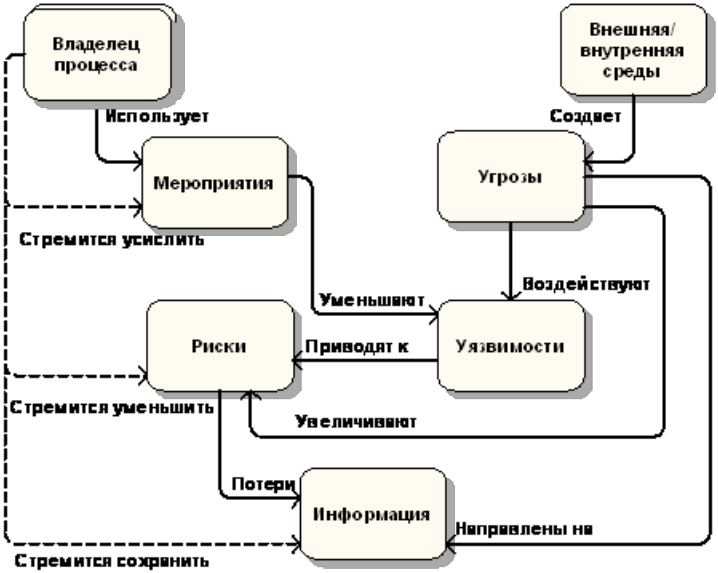


Рис. 3 – Модель связей в СУИБ

Набор метрик ИБ должен быть основан на целях и задачах, которые должен выполнять объект. Такие цели и задачи нужно указывать при разработке СУИБ, как для СУИБ в целом, так и для её элементов. Как правило, цели и задачи СУИБ и её элементов уже указаны в нормативных документах каждой организации и являются частью политики ИБ предприятия. Метрики ИБ должны давать количественную информацию для сравнения, применять математические методы для анализа и отслеживать изменения, используя одни и те же точки отсчёта.

Примером метрики ИБ может быть «количество учётных записей уволенных сотрудников, не удаленных из системы» или «количество сообщений антивируса о выявленном вредоносном ПО при сканировании за отчётный период». Посмотрев на значения этих метрик, менеджер по ИБ может принять решение об ужесточении политики контроля за учётными записями или о смене антивируса.

Можно выделить 3 типа метрик:

1. Метрики выполнения. Такие метрики отражают степень выполнения программ и политик ИБ.

2. Метрики эффективности. Такие метрики используются для контроля правильной реализации процессов и программ. Они позволяют оценить степень достижения ожидаемых результатов.

3. Метрики воздействия. Такие метрики предназначены, чтобы определить воздействие программы ИБ на главную цель организации. Эти метрики индивидуальны для каждой организации.

Таким образом, метрики как исчислимые показатели, способны дать реальное представление о состоянии ИБ и эффективности применяемых в компании мер защиты, а также стать основой для выработки управленческих решений по совершенствованию СУИБ в непрерывном цикле Дёминга. Данный подход находит высокую востребованность при управлении информационной безопасностью в непрерывных динамичных бизнес-процессах с высокой степенью информатизации, в частности, в дистанционном банковском обслуживании [6].

Литература:

1. *Сиротский А.А.* Современные технологии ведения бизнеса и управления предприятиями / Современные проблемы информационной безопасности и программной инженерии. Сборник избранных статей научно-методологического семинара кафедры информационной безопасности и программной инженерии. М.: Издательство «Спутник+», 2012. – С. 19-26.

2. *Сиротский А.А.* Об инновационных подходах, средствах и методах эффективного управления предприятием // Человеческий капитал, 2011. – №11 (35). – С. 64-66.
3. Сиротский А.А. Технологии конкурентоспособного управления предприятиями машиностроения // Техника машиностроения, 2012. – №4 (84). – С. 33-37.
4. *Сиротский А.А.* Технологии конкурентоспособного управления предприятиями машиностроения // Ученые записки Российского государственного социального университета, 2013. Т. 2. – №5 (120). – С. 177-181.
5. *Сиротский А.А.* Научный подход в управлении бизнесом / Преподавание информационных технологий в Российской Федерации. Материалы Десятой открытой Всероссийской конференции. М.: ФГБОУ ВПО «МГУ им. М.В. Ломоносова», 2012. – С. 438-446.
6. *Сиротский А.А.* Пути повышения защищённости от несанкционированного доступа в системах дистанционного банковского обслуживания / Современные проблемы информационной безопасности и программной инженерии. Сборник избранных статей научного семинара №1(6) кафедры информационной безопасности и программной инженерии. М.: ООО «Сам полиграфист», 2014. – С. 6-13.

Сорокин Л.А.

Модель информационно-аналитической поддержки управления безопасностью на основе анализа и синтеза состояний объектов управления

Аннотация: рассматривается модель, позволяющая с учетом состояния пассивных и активных компонент выбирать управляющие воздействия при рациональном использовании ресурсов и обоснованном прогнозировании вариантов развития угроз.

Ключевые слова: моделирование, системы безопасности, анализ, синтез, информационно-аналитическая поддержка управления

Актуальность материала обусловлена имеющимся на настоящий момент противоречием между потребностью в повышении эффективности управления безопасностью и сложившимся теоретико-методологическими подходами, на практике не обеспечивающие достаточную защищенность людей. Указанное противоречие обуславливает необходимость уточнение

существующих и формирование новых моделей и алгоритмов информационно-аналитической поддержки управления безопасностью.

На основе научных работ [1-2] предложена модель информационно-аналитической поддержки управления безопасностью, которая в отличие от существующих, позволяет для произвольных объектов описать управление безопасностью с учетом параметров технических систем безопасности и индивидуальных особенностей сотрудников службы безопасности.

Общая схема модели поддержки управления безопасностью представлена на рис. 1. Основными элементами схемы являются: модели оценки вероятности обнаружения дестабилизаций, прогнозирования вариантов распределения угроз, координации сотрудников службы безопасности, а также модели регистрации и обработки информации в технической системе безопасности и системе информационно-аналитической поддержки управления (далее – СИАПУ).

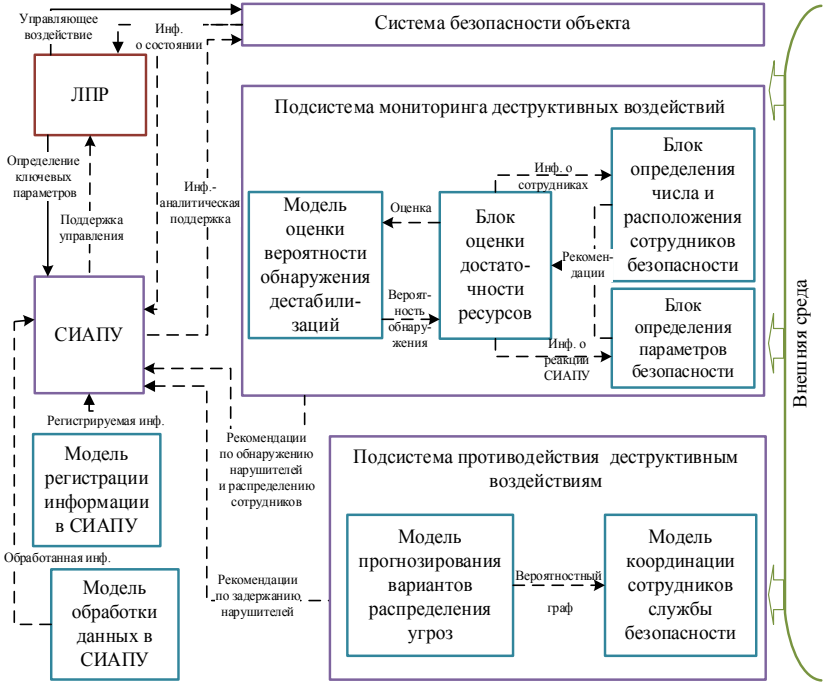


Рис. 1 – Схема модели поддержки управления безопасностью

Таким образом, объект управления описывается уравнением вида $\Theta(t) = \Phi[Y(t), U(t), X(t), t] \in Y$ (рис. 2).

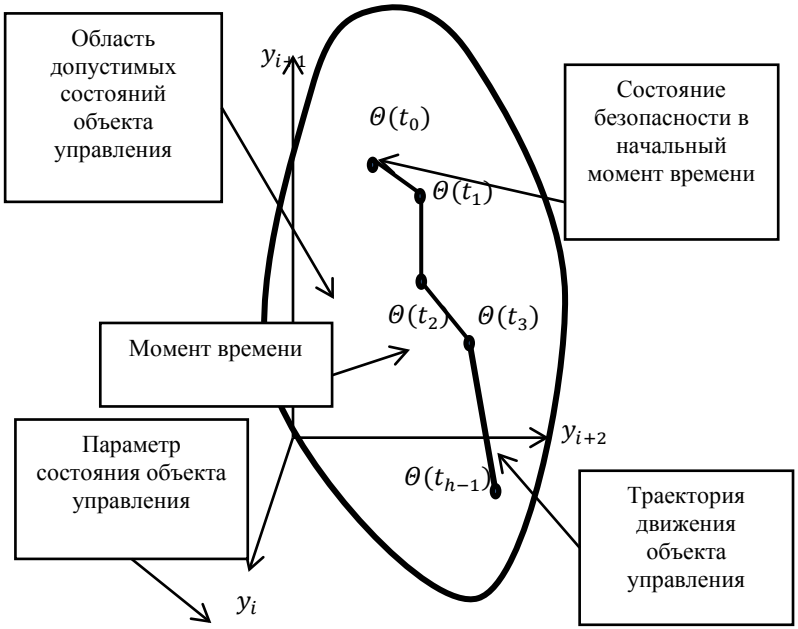


Рис. 2 – Фазовое пространство управления

В работе используется подход, в котором состояние безопасности описывается $y \in Y$, где Y – множество возможных состояний объекта управления. Значение y зависит как от управляющих $u \in U$, так и деструктивных воздействий $x \in X$. Множество состояний объекта управления (Y) является декартовым произведением множеств состояния пассивных (Y_1) и активных (Y_2) компонент: $Y = Y_1 \times Y_2$.

Под состоянием активной составляющей объекта управления (Y_1) подразумеваются состояние сотрудников службы безопасности, которые обладают собственными целями, интересами и свободой выбора состояния. Состояние пассивной составляющей (Y_2) представляется значением параметров технической системы безопасности. Особенностью данной компоненты является отсутствие свободы выбора состояния и детерминированность.

Взаимодействие пассивных и активных компонент моделируется в Римановом пространстве с использованием свертки (1): θ_1 – функции реагирования сотрудников службы безопасности (2) и θ_2 – функции реагирования технической системы безопасности.

$$\theta_1(t) * \theta_2(t) = \int_0^t \theta_1(\tau) \cdot \theta_2(t-\tau) d\tau \quad (1)$$

$$\theta_1 = a_0 \cdot {y'_1}^{l_0}(t) \cdot \ldots \cdot {y'_n}^{v_0}(t) + \cdots + a_{h-1} \cdot {y'_1}^{l_{h-1}}(t) \cdot \ldots {y'_n}^{v_{h-1}}(t) \quad (2)$$

где ${y'_1}^{l_i}(t) \ldots {y'_n}^{v_i}$– показатели эффективности сотрудника ($i \in \{1 \ldots h\}$), h – количество измерений, $a_1, \ldots, a_{h-1}$ – коэффициенты регрессии. На основе регрессионного анализа лицо принимающее решение может оказывать обоснованные управляющие воздействия, которые позволят повысить эффективность обеспечения безопасности.

Таким образом, предложена модель информационно-аналитической поддержки управления безопасностью. Модель позволяет органу управления в комплексе и автономно анализировать влияние параметров пассивных и активных компонент системы безопасности на защищенность людей в местах массового пребывания.

Литература:

1. *Бутузов С.Ю., Сорокин Л.А.* Методика обеспечения безопасности в местах массового пребывания людей / Технологии техносферной безопасности. – 2017. – Вып. 2 (72). – 0,34 п.л. – Режим доступа: http://ipb.mos.ru/ttb.(Дата обращения: 15.11.2018).
2. *Сорокин Л.А*. Информационно-аналитическая поддержка управления безопасностью в местах массового пребывания людей / Автореф. дис. на соиск. учен. степ. канд. техн. наук (05.13.10); Академия ГПС МЧС России. – Москва, 2017.

Агаев Р.П., Никифоров С.В.

О собственном проекторе лапласовских матриц орграфов коммуникаций многоагентных систем второго порядка и модели регуляризации этих систем

Аннотация: В работе описано условие достижения консенсуса в многоагентных системах второго порядка с несвязным орграфом коммуникаций. Были обобщены некоторые ранее полученные результаты. В частности, модели регуляризации для многоагентных систем первого порядка были применены для многоагентных систем второго порядка.

Ключевые слова: многоагентные системы, консенсус, собственный проектор, лапласовская матрица орграфа, регуляризация

Многоагентные системы с информационной связью широко применяются в различных областях теории управления и принятия решений. Такие системы описываются ориентированным орграфом, а условия достижения согласия – консенсуса – характеризуются спектральным свойством соответствующей лапласовской матрицы. В частности, для моделей первого порядка консенсус достигается тогда и только тогда, когда орграф коммуникаций содержит остовное исходящее дерево.

Для модели второго порядка $\dot{\xi}_i = \zeta_i,\ \dot{\zeta}_i = u_i$, где
$u_i = -\sum_{j=1} a_{ij}\left[\left(\xi_i - \xi_j\right) + \gamma\left(\zeta_i - \zeta_j\right)\right]$,
протокол согласия имеет следующее представление:

$$\begin{bmatrix}\dot{\xi}(t)\\ \dot{\zeta}(t)\end{bmatrix} = \begin{bmatrix}0_{n\times n} & I_n\\ -L & -\gamma L\end{bmatrix}\begin{bmatrix}\xi(t)\\ \zeta(t)\end{bmatrix}. \quad (1)$$

Рассмотренная модель впервые была изучена в работах [1,2]. В таких системах единственность нулевого собственного значения лапласовской матрицы является необходимым, но не достаточным условием для консенсуса. При определенном ограничении на параметр γ, входящий в систему, консенсус также определяется единственным нормированным левым собственным вектором лапласовской матрицы. Здесь мы изучим более общий случай, когда ограничение на параметр γ удовлетворяет определенному условию, но кратность нулевого собственного значения лапласовской матрицы больше единицы.

Для такого случая поведение системы однозначно описывается собственным проектором лапласовской матрицы орграфа коммуникации. Если для γ выполняется следующее условие из [3],

$$\gamma^2 > \max_{\mu_i \neq 0} \frac{1}{\mathrm{Re}(\mu_i)} \cdot \frac{\mathrm{Im}^2(\mu_i)}{\mathrm{Im}^2(\mu_i)+\mathrm{Re}^2(\mu_i)}, \quad (2)$$

а кратность нулевого собственного значения матрицы L равна m, то для достаточно большего значения t и $\delta \to 0$ асимптотическое поведение системы (1) будет иметь следующее представление:

$$\begin{bmatrix}\xi(t)\\ \zeta(t)\end{bmatrix} = \begin{bmatrix}1 & t\\ 0 & 1\end{bmatrix} \otimes L^{\vdash}\begin{bmatrix}\xi(0)\\ \zeta(0)\end{bmatrix}, \quad (3)$$

где $L^{\vdash}$ - идемпотентная матрица, являющаяся собственным проектором лапласовской матрицы.

На самом деле формула (3) обобщает многие результаты, ранее полученные в [1, 4]. В частности, если система имеет первый порядок, а орграф коммуникаций содержит остовное дерево, то из (3) получается

$\xi(t) = L^{\vdash}\xi(0)$.

В случае достижения консенсуса при любом векторе начальных значений все строки матрицы $L^{\vdash}$ одинаковы (столбцы данной стохастической матрицы пропорциональны).

Для многоагентной системы второго порядка при достижении консенсуса формула (3) полностью описывает линии развития характеристик отдельных агентов.

Однако если ноль не является простым собственным значением в многоагентной системе второго порядка, то консенсус достигается не для каждого вектора начальных характеристик. В этом случае возникает необходимость в регуляризации протокола консенсуса.

Для систем первого порядка в работе [5] было предложено несколько протоколов регуляризации. Важно отметить, что, несмотря на различные способы регуляризации, согласно этим протоколам, в конечном итоге консенсус определяется произведением $EL^{\vdash}$, где E – стохастическая матрица с одинаковыми элементами. Цель этих протоколов - регуляризировать модель таким образом, чтобы при любом векторе начальных мнений, в системе был достигнут консенсус. В настоящей работе один из таких протоколов мы применим для многоагентной системы второго порядка и для достаточно большого значения времени *t* выведем выражение для асимптотического консенсуса. Согласно предложенному протоколу к исходному орграфу зависимостей добавляется полный простой граф с весами δ, а консенсус определяется пределом, при значении δ, стремящемся к нулю. В [5] такой протокол был назван протоколом с фоновыми связями. Применив описанный метод регуляризации к многоагентным системам второго порядка мы получим следующий протокол регуляризации:

$$\begin{bmatrix}\dot{\xi}(t)\\ \dot{\zeta}(t)\end{bmatrix} = \begin{bmatrix}\mathbf{0_{n\times n}} & I_n\\ -(L+\delta K) & -\gamma(L+\delta K)\end{bmatrix}\begin{bmatrix}\xi(t)\\ \zeta(t)\end{bmatrix}. \quad (4)$$

Утверждение 1. (Основной результат). Если для γ выполняется условие (2), а кратность нулевого собственного значения матрицы *L* равна *m*, то для достаточно большего значения *t* и $\delta \to 0$ асимптотическое поведение системы (4) будет иметь следующее представление:

$$\begin{bmatrix}\xi(t)\\ \zeta(t)\end{bmatrix} = \begin{bmatrix}1 & t\\ 0 & 1\end{bmatrix} \otimes EL^{\vdash}\begin{bmatrix}\xi(0)\\ \zeta(0)\end{bmatrix}. \quad (5)$$

Выражение (5) обобщает некоторые результаты, полученные ранее в [1,4,5].

Другие протоколы регуляризации, приведенные в [5] также можно использовать в многоагентных системах второго порядка и можно доказать, что «усреднение» характеристик, так или иначе, определяется

произведением стохастической матрицы E и собственного проектора лапласовской матрицы.

В отличие от ранее предложенных методов регуляризации, использованные методы не подвергают изменению векторы начальных характеристик, а требуется лишь добавления или слабых фоновых связей или же «скрытого агента», т.е. вершины орграфа, одинаково влияющего на других агентов.

Отметим, что собственный проектор лапласовской матрицы позволяет «предугадать» поведение системы в зависимости от вектора начальных значений. Например, переопределяя эти значения в зависимости собственного проектора, всегда можно достичь консенсуса. В качестве примера, можно рассмотреть собственный проектор второго ранга с линейно независимыми строками (0,5; 0,5; 0; 0) (0; 0; 0,25; 0,75). Заметим, что для некоторых векторов начальных характеристик консенсус не достигается, но для заранее выбранных векторов, удовлетворяющих определенному условию, консенсус достигается.

Литература:

1. *Ren W., Atkins E.* Distributed m ulti-vehicle co ordinated co ntrol v ia l ocal information e xchange / / I nternational J ournal o f R obust a nd N onlinear Control. —2007. —V. 17. —No. —10-11. P. 1002—1033.
2. *Olfati-Saber R.* Flocking for multi-agent dynamic systems: Algorithms and theory //IEEE Transactions on automatic control. —2006. —V. —51. —No. 3. —P. 401—420.
3. *Liu H., Xie G., Wang L.* Necessary a nd s ufficient c onditions for s olving consensus pr oblems o f doubl e-integrator d ynamics via sampled c ontrol //International Journal of Robust and Nonlinear Control. —2010. —V.20. —No. 15. —P. 1706—1722.
4. *Chebotarev P., Agaev R.* The F orest C onsensus T heorem / / IE EE Transactions on Automatic Control. —2014. —V. 59. —No. 9. —P. 2475—2479.
5. *Агаев Р.П., Чеботарев П.Ю.* Модели латентного консенсуса // Автоматика и телемеханика. —2018. —№ 1. —С. 106—107.

Косяченко С.А., Богатырева Л.В.

К проблеме использования сценарного подхода в стратегическом сдерживании

Аннотация: Рассматриваются общие подходы использования сценарного анализа в стратегическом сдерживании.

Ключевые слова: стратегическое сдерживание, сценарный анализ, методология

Сдерживание войн и локальных конфликтов в современном мире предполагает предупреждение и нейтрализацию угрозы военного вторжения, основывающееся на способности вооруженных сил нанести неприемлемый ущерб агрессору. В Российской Федерации сдерживание от угроз региональной и крупномасштабной войны возлагается на стратегические ядерные силы, потенциал которых поддерживается на минимально достаточном уровне. Стратегическое сдерживание как элемент безопасности в Российской Федерации формируется и поддерживается с целью обеспечения безопасности страны и поддержания ее обороноспособности. Методы обеспечения безопасности делятся на военные и невоенные. Военные - наличие вооруженных сил, способных отразить ядерную и неядерную агрессию, невоенные - пропаганда, психологические, информационные операции, экономические и финансовые.

Эквивалентом стратегического сдерживания для США является стратегическая стабильность, она призвана решать адекватные стратегическому сдерживанию задачи: политические, дипломатические, информационные, военные и т.п.

Новым подходом к проблеме стратегического сдерживания является использование методологии формирования сценариев развития сложных слабо формализуемых организационных систем (ОС), которая позволяет проводить исследования их поведения при различных стратегических управленческих воздействиях. На основе выделения и формализации основных компонентов сценария рассматриваются операции в сценарных пространствах, которые позволяют синтезировать сценарий с заданными свойствами. Построение математических моделей и методов моделирования, анализ и синтез сценариев развития организационных систем, совокупность которых имеет важное значение в развитии нового перспективного направления в теории и практике стратегического сдерживания.

Разработанный подход позволяет с необходимой степенью адекватности описывать процесс развития организационных систем на разных уровнях детализации, учитывать динамику и дискретный характер изменения различных ее элементов, формализовывать ресурсные, технологические, логические и другие ограничения и решать на единой методологической основе широкий класс задач стратегического управления развитием ОС различного типа и назначения. Принципиальной новизной предлагаемого подхода является возможность прогнозировать поведение моделируемых объектов путем формирования спектра сценариев их развития, в том числе наиболее вероятных. Анализ спектра

сценариев позволяет оценивать эффективность и согласованность множества управленческих решений, распределенных во времени и пространстве, при выборе и реализации комплексных программ развития, т.е. в случаях, когда экспериментирование на реальных объектах практически невозможно, экономически нецелесообразно и опасно в социальном плане.

В рамках данного подхода могут быть разработаны модели и методы выбора оптимального сценария из заданного множества альтернативных сценариев. Поставленная задача сводится к задаче выбора оптимального сценария по векторному критерию оптимизации. Могут быть использованы различные методы решения поставленной задачи: свертка частных критериев в единый интегральный критерий, согласование частных критериев для определения оптимального сценария; применение операций сценарного исчисления для формирования оптимального сценария.

Могут использоваться многошаговые процедуры формирования оптимальных сценариев развития ОС при заданной модели ее структуры, заключающиеся в выборе оптимальной стратегии формирования последовательности экспертно-значимых событий в условиях неопределенности с учетом пространственных характеристик и свойств формируемых сценариев.

Перспективно применение разработанной методологии анализа и синтеза сценариев развития ОС на основе использования модифицированной модели операторных ориентированных графов, т.е. возможна разработка методов автоматической генерации и моделирования сценариев развития ОС с использованием указанной модели. Могут быть предложены постановки и проведено решение задач синтеза оптимальных сценариев развития организационных систем на операторном ориентированном графе по заданным критериям устойчивости и безопасности ОС.

Разработанный методологический подход, системный аппарат сценарного исследования, методы и средства моделирования позволяют существенно повысить эффективность анализа, изучения предыстории, текущего и предполагаемого развития процессов в СО различного назначения, а в ряде случаев пересмотреть сложившиеся представления о принципах и закономерностях стратегического сдерживания.

Необходимость разработки актуальных новых научных направлений в гражданской и военной областях обусловлена тем, что устойчивое развитие и безопасность государства предполагают его способность противостоять враждебным, деструктивным силам политического, природного, техногенного и социального характера, нейтрализовать их. Она означает защищенность суверенитета государства; его социальных и

национальных групп - их статуса, функциональных ролей, самобытности; общества - его материальных и духовных ценностей; государства - его территориальной целостности, суверенитета, конституционного строя. Все эти уровни взаимосвязаны, а приоритеты здесь носят ситуационный характер и могут меняться в зависимости от обстоятельств.

Отметим: если прежняя классическая прогностика в основном отслеживала тенденции, то новая, постклассическая, требует не только формировать, но и предвосхищать альтернативы развития ОС на основе следующих методологических принципов:

- принцип неопределенности будущего, который соответствует новой научной картине мира, связанной с критикой классического детерминизма и исследованием стохастических процессов;
- учет бифуркации - раздвоения течения тех или иных процессов, достигших определенной критической величины, после которой однозначная зависимость между прошлым и будущим состояниями и системами теряется;
- принцип дискретности пространства - времени, означающий, что в точках бифуркации образуются предпосылки качественно новых состояний, дающих качественно иное будущее.
- анализ альтернативных сценариев развития ОС при принятии стратегических решений при различных начальных условиях и ограничениях.

Таким образом, стратегическое прогнозирование развития ОС должно являться процедурой открытия качественно новых состояний современного взаимосвязанного мира в целом, связанных с деятельностью местной, региональной, государственной и глобальной власти. Оно должно вооружить политические элиты страны, принимающие решения, новым знанием, необходимым для построения управленческих сценариев бескризисного поступательного развития России.

Необходимо отметить важное методологическое различие между краткосрочным и долгосрочным глобальным прогнозированием. В первом случае более применимы процедуры экстраполяции, анализ сложившегося соотношения сил и стартовых условий. При долгосрочном прогнозировании развития ОС вступают в действие принципиально иные процедуры. Здесь важнейшее значение имеют такие понятия как качественный прогноз, относительная временная дискретность, реактивность, альтернативность, открытое будущее, политическая воля и др.

Как правило, для ОС существует несколько вариантов или сценариев развития в условиях активных внешних воздействий. Каждый из них является прогнозом поведения системы во времени, и выделить среди них один, наиболее вероятный, возможно далеко не всегда. Однако можно

анализировать исходы или результаты каждого сценария, соответствующего определенной программе мероприятий, оценивая возможные потери по критериям эффективности функционирования системы.

Литература:
1. *Шульц В.Л., Кульба В.В., Кононов Д.А., Косяченко С.А., Шелков А.Б., Чернов И.В.* Модели и методы анализа и синтеза сценариев развития социально-экономических систем. В 2-х книгах. - М.: Наука, 2012. - Кн.1 - 304 с. Кн. 2 - 358 с.

Фуругян М.Г.

Распределение ресурсов в многопроцессорной АСУ реального времени с нефиксированными параметрами

Аннотация: Решается задача составления допустимого расписания без прерываний и переключений в многопроцессорной АСУ реального времени для случая, когда работы имеют общий директивный интервал, а длительности их выполнения линейно зависят от объема выделенных им дополнительных ресурсов. Разработан алгоритм решения задачи, который является псевдополиномиальным при фиксированном числе процессоров.

Ключевые слова: многопроцессорная АСУ реального времени, директивный интервал, допустимое расписание без прерываний, распределение ресурсов.

1. Введение

Одна из основных задач, возникающих при разработке математического и программного обеспечения многопроцессорных АСУ реального времени и связанных с безопасностью испытаний и эксплуатации сложных технических объектов, заключается в поиске алгоритмов построения допустимого расписания, показывающего, когда и какому программному модулю следует выделять те или иные вычислительные ресурсы. Такие задачи возникают при испытаниях самолетов, проектировании ядерных реакторов, конвейерных линий, разработке систем экологического и экономического мониторинга, в других областях деятельности человека.

В случае, когда прерывания и переключения с одного процессора на другой не допускаются, такие задачи, как правило, являются NP-трудными и все известные в настоящее время точные алгоритмы их решения

являются переборными, а точных полиномиальных (эффективных) алгоритмов не известно. Поэтому актуальным является вопрос о поиске псевдополиномиальных алгоритмов.

Задачи нахождения допустимых расписаний без прерываний и переключений и без дополнительного ресурса широко освещены в литературе. Отметим, например, такие методы их решения, как метод ветвей и границ [1], муравьиные алгоритмы [2], вероятностные алгоритмы [3], генетические алгоритмы [4], различные эвристические алгоритмы [5], алгоритмы агрегирования [6]. Задачи с дополнительным ресурсом ранее рассматривались для составления расписаний с прерываниями и переключениями.

В настоящей статье рассматривается задача составления многопроцессорного расписания без прерываний и переключений для случая, когда задан общий для всех работ директивный интервал. Кроме того, предполагается, что помимо процессоров, имеется несколько типов дополнительных ресурсов, а длительности выполнения работ линейно зависят от количества выделенных им этих ресурсов. Для случая, когда процессоры идентичные и их число фиксировано, предлагается псевдополиномиальный алгоритм построения допустимого расписания.

2. Постановка задачи

Рассматривается вычислительная система реального времени, состоящая из m идентичных процессоров, и множество работ $A = \{1,...,n\}$, подлежащее выполнению. При выполнении работ не допускаются прерывания и переключения с одного процессора на другой. В фиксированный момент времени каждый процессор может выполнять не более одной работы, а каждая работа может выполняться не более чем одним процессором. Для всех работ $i \in A$ задан общий директивный интервал $[0;T]$, в котором они могут выполняться, т.е. каждая работа должна быть завершена не позднее момента времени T. Помимо процессоров в системе имеется K типов дополнительных ресурсов невозобновляемого типа. Суммарное количество k-го типа этого ресурса составляет R_k, $k = 1,...,K$. Если работе i выделено r_{ik} единиц дополнительного ресурса k-го типа, $i \in N;\ \ k = 1,...,K$, то ее длительность составляет

$$t_i = d_i - \sum_{k=1}^{K} a_{ik} r_{ik}\ , \qquad (1)$$

где

$$r_{ik} \in [0,\ \bar{r}_{ik}],\ \bar{r}_{ik} \le R_k,\ \ i \in A,\quad k = 1,...,K\ , \qquad (2)$$

$$\sum_{i \in N} r_{ik} \le R_k, \quad i \in A, \tag{3}$$

a_{ik}, d_i, $\bar{r}_{ik}$ – заданные величины, $a_{ik} \ge 0$, $0 < d_i \le T$, $\bar{r}_{ik} > 0$, d_i – длительность выполнения работы i в случае, если ей дополнительных ресурсов не выделено, $a_{ik}, d_i, r_{ik}, \bar{r}_{ik} \in Z$, Z – множество целых чисел, $d_i - \sum_{k=1}^{K} a_{ik} \bar{r}_{ik} > 0$. Таким образом, $t_i \in [d_i - \sum_{k=1}^{K} a_{ik} r_{ik};\ d_i]$ при всех $i \in A$, причем $t_i \in N$, N – множество натуральных чисел.

Требуется найти такое распределение ресурсов r_{ik}^0, $i \in N$; $k = 1,...,K$, удовлетворяющее ограничениям (2), (3), при котором существует допустимое расписание (т.е. такое расписание, когда каждая работа полностью выполняется на одном процессоре без прерываний и переключений в директивном интервале $[0, T]$), или установить, что такого распределения ресурсов не существует.

Под расписанием выполнения работ будем понимать разбиение множества A на m непересекающихся подмножеств

$$A_1, A_2, ..., A_m \quad (A = \bigcup_{j=1}^{m} A_j;\ A_{j_1} \bigcap A_{j_2} = \varnothing \text{ при } j_1 \ne j_2).$$

Работы из множества A_j приписываются процессору j и выполняются на нем одна за другой в произвольном порядке.

Как известно, данная задача является *NP*-трудной даже при отсутствии дополнительных ресурсов и фиксированном m, а при произвольном m – *NP*-трудной в сильном смысле.

3. Алгоритм решения задачи

Для работы $i \in A$ определим U_i как множество всех векторов распределения ресурсов $X = \{r_{i1}, r_{i2}, ..., r_{iK}\}$, удовлетворяющих условиям (2), (3), а V_i – множество всех различных значений t_i, вычисленных по формуле (1) для каждого такого вектора из U_i. Для определенности будем полагать, что $V_i = \{v_{i1}, v_{i2}, ..., v_{ih_i}\}$, а число векторов в U_i также равно h_i. Действительно, число элементов в множестве U_i не меньше числа элементов в V_i. Если же для некоторого значения v_{ip}, $1 \le p \le h_i$, существует несколько векторов X, то оставим любой один из них, а

остальные исключим из множества U_i. Пусть $H = \max_{i \in N} h_i$. Из постановки задачи следует, что $v_{ih} \in N$ при всех $i \in A$, $h = 1,...,h_i$ Будем строить допустимое расписание с помощью точек m-мерного куба E^m с ребром T, имеющих целочисленные координаты. Множество этих точек разбивается на n уровней (возможно, пересекающихся). Каждая точка уровня l, $1 \le l \le n$, соответствует одному из всех возможных вариантов распределения дополнительных ресурсов между работами $i = 1,...,l$, $l \le n$, и вариантов распределения этих работ по процессорам при заданном директивном сроке T. Кроме того, точке уровня l приписывается номер уровня (т.е. l) и матрица $\|r_{ik}\|$, $i = 1,...,l$, $k = 1,...,K$, распределения дополнительных ресурсов между работами $i = 1,...,l$, где r_{ik} удовлетворяют условиям (2), (3). Точка $(c_1, c_2,..., c_m)$ уровня $l-1$, $l \le n$, куба E^m и соответствующая ей матрица распределения ресурсов $\|r_{ik}\|$, $i = 1,...,l$, $k = 1,...,K$, связаны не более чем с mh_l точками уровня l, которым соответствуют векторы загруженности процессоров $(c_1 + t_l, c_2,..., c_m)$, $(c_1, c_2 + t_l,..., c_m)$, $(c_1, c_2,..., c_m + t_l)$ и матрица распределения ресурсов $\|r_{ik}\|$, $i = 1,...,l$, $k = 1,...,K$, удовлетворяющие соотношениям (2), (3). Здесь $t_l = d_l - \sum_{k=1}^{K} a_{lk} r_{l2} \in V_l$, $(r_{l1}, r_{l2}, ..., r_{lK}) \in U_l$.

Если хотя бы одна компонента m-мерного вектора загруженности процессоров превышает величину T, то соответствующая точка куба E^m исключается из дальнейшего рассмотрения. Допустимое расписание в поставленной задаче существует в том случае, когда хотя бы одна точка n-го уровня содержится в кубе E^m. Для построения допустимого расписания разработана специальная процедура.

Вычислительная сложность алгоритма составляет $O(mHT^m)$ операций с m-мерными векторами и матрицами размером $l \times K$, $l = 1,...,n$. Выполнение одной такой операции с m-мерным вектором загруженности процессоров заключается в вычислении величины $t_l = d_l - \sum_{k=1}^{K} a_{lk} r_{lk}$ по формуле (1) и сложении ее с одной из компонент вектора. А выполнение одной операции с матрицей распределения дополнительных ресурсов заключается в добавлении к ней строки $(r_{l1}, r_{l2}, ..., r_{lK})$. Поскольку $t_l \le T$, $r_{lk} \le R_k$ при всех $l \in A$, то при фиксированном m предложенный алгоритм является псевдополиномиальным.

Литература:
1. *Алексеев О.Г.* Комплексное применение методов дискретной оптимизации. — М.: Наука, 1987.
2. *Штовба С.Д.* Муравьиные алгоритмы // ExponentaPro. Математика в приложениях. — 2003. — № 4. — С. 70—75.
3. *Raghavan R.* Probabilistic Construction of Deterministic Algorithms: Approximating Packing Integer Programs / / J. Computer and System Sciences. — 1988. — V. 37. — P. 130-143.
4. *Костенко В.А., Смелянский Р.Л., Трекин А.Г.* Синтез структур вычислительных систем реального времени с использованием генетических алгоритмов // Программирование. — 2000. — № 5. — С. 63-72.
5. *Brucker P.* Scheduling Algorithms. Heidelberg: Springer, 2001.
6. *Красовский Д.В., Фуругян М.Г.* Алгоритмы решения минимаксной задачи составления расписания // Изв. РАН. ТиСУ. — 2008. — Т.47. — №5. — С. 732-736.

Алексейчук А.Е., Грузман В.А.

Методы и инструментальные средства бизнес-анализа в управлении

Аннотация: В статье рассматриваются перспективы развития информационно-аналитических систем на основе технологий бизнес-аналитики. Показаны возможности прогнозного моделирования для повышения операционной эффективности управления предприятиями и организациями в условиях цифровой эры.

Ключевые слова: бизнес-аналитика; методы и инструменты прогнозной аналитики; система бизнес-интеллекта; модель, управляемая данными; мониторинг результативности бизнес-аналитических методов в управлении

Глобальное информационное пространство сегодня стремительно меняется, что отражается и на не менее глубоких преобразованиях в экономике, общественной жизни, в государственном и муниципальном управлении. О наступлении эры цифровых технологий в управлении заговорили не только экономисты, менеджмент и специалисты по IT технологиям, но и политики разного уровня управления.

Рынок информационных услуг при работе с данными большого объема (Big data) растет ежегодно на треть и к 2018 году составит $41,5 млрд. Общий объем цифровой информации увеличится примерно в 10 раз к 2020 году. Объем данных в облачном сегменте *(**облачное** хранилище данных*

(англ. cloud storage) — модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной.) в 2018 году будет доведен до 50%. Для коммерческих предприятий и организаций социальной сферы внедрение цифровых технологий не только повысит эффективность их работы, но и значительно поменяет организационную и функциональную структуру и методы управления в этих организациях.

Компьютерная аналитика - основа цифровых технологий в экономике и социальной жизни

Переход на цифровые технологии в управлении потребует широкого внедрения информационно-аналитических методов и инструментальных средств поддержки процессов принятия решений. Современные предприятия и организации при решении задач планирования и мониторинга своей деятельности используют приложения в которых заложены OLTP (Online Transaction Processing — обработка транзакций в реальном времени) и OLAP (англ. online analytical processing, аналитическая обработка в реальном времени) технологии. Самой широко распространенной системой в классе OLTP-систем является современная ERP-система. К классу OLAP-систем можно отнести приложения бизнес-интеллекта BI (Business Intelligence), равно как и системы CPM (Corporate performance management) управления корпоративной результативностью.

Применение прогнозной аналитики (Predictive analytics) дополняет и усиливает возможности **BI-**технологий и CPM-систем при прогнозировании будущего. Прогнозная аналитика использует разные инструменты интеллектуального анализа данных, статистические пакеты, средства моделирования, машинного обучения и искусственного интеллекта для анализа исходных данных, прогнозирования предстоящих событий. Модели прогнозной аналитики ориентированы на связи между большим числом факторов для прогноза риска с заданным множеством исходных условий.

Инструментальные средства интеллектуального анализа данных (Data mining, Text mining, Web mining, Social mining) с использованием методов статистического анализа позволяют бизнес-пользователям проектировать интеллектуальные системы прогнозирования, прояснять связи между структурированными и неструктурированными данными. Источниками структурированных данных, к примеру, являются все справочные базы данных, информационные транзакционные системы и иные данные, имеющие жесткую структуру. Неструктурированные (или слабоструктурированные) данные – это информация, которую нам привнесла цифровая экономика. Эти данные не могут иметь определенной

структуры, поскольку она не упорядочена в установленном порядке. Примером таких данных могут быть текстовые данные социальных медиа-контентов.

Из крупных, мирового уровня, аналитических компаний чаще всего ссылаются на IDC и Gartner. Специалисты этих компаний утверждают, что со временем мировой рынок бизнес-анализа будет продвигаться через освоение продвинутой аналитики (advanced analytics), в том числе прогнозного анализа, построение симуляторов и вариативных моделей. Предложенные компанией ***Forrester research*** подходы к внедрению инструментов прогнозной аналитики подразумевают непрерывный цикл обработки данных, превращающих их в знания, что хорошо согласуется с требованиями цифровой экономики.

Главной проблемой в прогнозной аналитике является нахождение параметров или сущностей, влияющих на прогнозируемое событие. При проведении прогнозного анализа требуется четко следовать такой последовательности действий:

- постановка цели, выборка данных из разных источников, ввод данных,
- построение прогнозной модели, тестирование модели,
- экспериментальное и рабочее внедрение модели,
- постоянный контроль результатов эксплуатации модели.

Вместе с требованием обеспечить качество прогнозной информации для «Цифрового предприятия» становится все более значимым обеспечение скорости ее получения. В скором времени «Цифровая» аналитическая система, работающая с большими данными, должна будет не только иметь в себе интеллектуальные модели, управляемые данными (data driven model), но также работать в режиме реального времени (Real time system).

Инструментальные средства позволяют создавать модели, используя при этом транзакционные данные. Такие модели работают как в пакетном режиме, так и в режиме реального времени на потоковых данных. Информация, получаемая при функционировании моделей, может быть применена на этапе итоговой оптимизации с тем, чтобы можно было сравнивать результаты, полученные другими моделями, и создавать множества самых эффективных. Модули прогнозного моделирования можно строить непрерывно, сравнивая их с реальными процессами и оптимизируя их для получения качественных результатов.

Как примеры проведения прогнозного анализа, хотелось бы упомянуть: директ–маркетинг; оценка эффективности компаний-толкачей; таргетирование рекламы; поиск схем мошенничества; моделирование политических событий; создание моделей ранней диагностики в медицине и многое другое.

Одним из главных условий качественного проведения прогнозного моделирования многоуровневых систем является установление баланса между количественными и качественными характеристиками в таких системах. Такая задача сложна, поскольку такие системы являются слабоструктурированными, и получить нужную добавочную информацию можно только с участием человека. И это не зависит от того, присутствует ли в прогнозной модели дополнительная информация от эксперта (группы экспертов) или ее получают от других людей (целевой группы привлеченных респондентов), но все же эти данные являются субъективными. Вот почему при моделировании сложных социально-экономических систем часто используется не только математические методы, но и комплексы когнитивных сетей, модели, создаваемые с использованием теории нечетких игр, нечетких множеств, нечеткой логики, нейронные сети, когнитивные карты, эволюционные алгоритмы и др.

К когнитивным методам анализа, которые широко используются в интеллектуальных системах поддержки принятия решений, также следует отнести:

- когнитивные карты (образ знакомого пространственного окружения); знаковые графы;
- сетевые модели; графы причин и следствий; каузальные сети; байесовские сети; сети доверия; аналитические сети Саати.

Сегодня на рынке можно встретить десятки программно-инструментальных средств для прогнозного анализа – как системы открытого доступа (Open source: Orange, Python, R, RapidMiner, и др.), так и коммерческие системы прогнозного анализа (TIBCO, Mathematica, MATLAB, STATISTICA и др.). [1]. В особую группу можно выделить аналитические приложения, входящие в промышленные корпоративные системы лидирующих поставщиков (Oracle Data Mining (ODM), SAS Enterprise Miner, IBM SPSS Statistics and IBM SPSS Modeler, и др.). Важно отметить, что прогнозная аналитика как когнитивная система предлагается на рынке не только в виде лицензионного программного обеспечения, но и в облачном виде на основе технологии SaaS (Software as a Service) [2].

Сценарный подход к анализу обстановки, выработке управленческих решений и прогнозу последствий их реализации

В России для реализации функций в рамках прогнозной аналитики в течение многих лет использовались методы сценарного подхода для исследования состояния сложных систем, выработки эффективных управляющих решений в рассматриваемой предметной области, а также прогноза последствий этих решений и возможных угроз [3,4].

При принятии управленческих решений в сложных системах необходимо учитывать различные факторы при оценке обстановки: политические, военные, экономические, социальные и т.п. Не всегда их можно измерить количественно. При оценке ситуации используются знания экспертов в различных областях, которые необходимо свести в единую согласованную модель. Часто эти знания носят качественный характер, что ограничивает возможность формирования и использования точных моделей объекта управления или обстановки.

Кроме того, традиционные методы моделирования основаны на наличии полной информации о сложной системе, ее окружении и их взаимодействии. Однако реально данные необходимой степени полноты и точности собрать практически невозможно, особенно в условиях быстро меняющейся обстановки. В этих условиях единственным эффективным средством поддержки принимаемых решений и прогноза их последствий является использование сценарного подхода. Сценарий развития системы или обстановки является необходимым промежуточным звеном между этапами целеполагания и формирования, а также реализации конкретных управленческих решений, направленных на достижение поставленных целей.

Для описания объекта моделирования используется понятие фактора. *Фактор* – это любой семантически определенный в исследуемой предметной области и количественно измеряемый параметр, характеризующий конкретный, например, физический, социально-экономический, экологический процесс. Измеримость параметра не предполагает обязательность его объективного измерения. Количественная оценка может быть получена экспертным путем. Примерами факторов в технических системах могут служить давление, температура, скорость; в социально-экономических системах – численность населения, средний доход на душу населения, социальная напряженность. Значение фактора меняется под действием внутренних процессов и внешних воздействий. Внутренние процессы связаны с природой фактора и не зависят от внешних воздействий. Внешние воздействия связаны с взаимодействием факторов. Отношение между факторами *(взаимодействие факторов)* – количественное или качественное описание влияния изменения одного фактора на изменение других факторов.

Сценарный подход включает реализацию следующих функций:

- сбор и анализ данных, а также получение экспертных оценок;
- разработку модели системы или ситуации и представления ее на языке знаковых, знаковых взвешенных и функциональных графов;
- автоматическую генерацию, представление и оценку альтернативных сценариев поведения управляемого объекта или обстановки в

соответствии с принятыми решениями с точки зрения реализации поставленных целей и разрушения замысла противника;

- оценку эффективности управленческих воздействий, их последствий и выбор наиболее эффективных решений.

Входной информацией при построении и исследовании модели является совокупность исследуемых объектов, их характеристик и причинно-следственные связи между ними, имеющиеся количественные данные или их экспертные оценки, нормативная или регламентная информация, а также знания, полученные средствами Data Mining. Таким образом, входной информацией является структура моделируемой системы, ее характеристики и варианты управленческих решений. Структура модели является гибкой и может меняться в соответствии с изменяющейся обстановкой.

Выходными результатами являются сценарии развития обстановки, т.е. последовательность значимых событий и изменений их характеристик во времени. Анализ сценариев развития позволяет оценивать эффективность и согласованность множества распределенных во времени и пространстве управленческих решений в случае, когда экспериментирование на реальных объектах практически невозможно, экономически и политически нецелесообразно или представляет опасность.

Для реализации целей формирования и анализа альтернативных сценариев развития обстановки выбран аппарат функциональных графов, представляющих собой развитие аппарата знаковых и взвешенных знаковых графов. Целесообразность и перспективность использования этого аппарата определяется, во-первых, его относительной математической простотой, что позволяет преодолеть известный барьер высокой вычислительной трудоемкости, возникающей из-за необходимости учета множества существенных факторов, характеризующих и влияющих на развитие обстановки; во-вторых, слабой чувствительностью к точности исходных данных и возможностью построения адекватных моделей процессов развития качественного типа.

При отрицательной качественной оценке характеристик полученных сценариев следует перейти к решению обратной задачи – поиску эффективных управлений, т.е. перейти к генерации аттрактивных сценариев. Управленческие воздействия могут быть ресурсными или структурными. Ресурсные управленческие воздействия осуществляются в форме внешних импульсных воздействий (административных, экономических, информационных и т.п.) на выбранные факторы модели. Структурное управление заключается в изменении взаимосвязей между существующими факторами модели, а также в добавлении новых факторов или выводе старых за пределы модели. Эти два вида управления могут быть статическими (неизменными или однократными в течение всего

процесса моделирования) или динамическими (могут неоднократно изменяться на всем временном интервале моделирования).

В процессе моделирования управляющие воздействия при автоматической генерации сценариев обеспечиваются выбором следующих действий:

- изменение состояния факторов и их взаимосвязей;
- введение новых параметров в существующую модель с целью ее детализации;
- изменение характера и интенсивности взаимосвязей;
- добавление/исключение факторов и их взаимосвязей;
- исключение некоторых параметров, например, путем определения жесткой функциональной зависимости между заданными параметрами.

Разработанная первоначальная модель обладает необходимой гибкостью и способна автоматически настраивать свою структуру в соответствии с измененной обстановкой.

Предложенная методика сценарного анализа реализована в рамках программно-аналитического комплекса «Полюс», реализующего методы сценарного анализа социально-экономических систем и синтеза альтернативных сценариев их поведения при оказании внешних воздействий.

Литература:

1. George Westerman, Didier Bonnet, Andrew McAfee. Leading Digital: Turning Technology into Business Transformation// Harvard Business Review Press, 2014. – 292 p.
2. *Паклин Н. Б., Орешков В. И.* Бизнес-аналитика: от данных к знаниям. Санкт-Петербург: Питер, 2010.
3. *Шульц В.Л., Кульба В.В., Кононов Д.А., Косяченко С.А., Шелков А.Б., Чернов И.В.* Модели и методы анализа и синтеза сценариев развития социально-экономических систем: в 2-х кн. / под ред. В.Л.Шульца, В.В. Кульбы; Москва: Наука, 2012. – 662 с.
4. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Сценарный анализ в управлении геополитическим информационным противоборством. Москва: Наука, 2015.

VI. Автоматизированные системы и средства обеспечения безопасности сложных систем

Kasimov A. M., Balabanov A.V.

Method of designing microfluidic operational units of robust reserve control systems of critical objects

Abstract: A method of designing microfluidic operational units of robust reserve control systems of critically important objects is devised. The method is based on the forming of the multidimensional network models that are generalized structures of the operational units to be designed, and represent these units in the form of the structural-class instance sets organized by specified characteristics and operations on the instances.

Keywords: robustness, reserve control system, critical (critically important) object, microfluidic operational unit, design implementation, multidimensional network model, structural class

Required levels of the fault tolerance of critical objects (air vehicles, NPPs, technological equipment for extremely dangerous processes, etc.) can be provided by means of reserve non-electronic control systems that keep the operability while being influenced by the factors resulting in failures of electronics (electromagnetic and corpuscular radiations, low or high temperatures, and so on). The above mentioned control systems can be of microfluidic nature and operate on the basis of gas dynamics laws. It is the tolerance to electromagnetic disturbances that is a distinctive feature of the microfluidics. In addition, microfluidic elements are highly manufacturable and can be made of both metals and different non-metallic materials by means of advanced techniques of molding and stamping. There are the microfluidic unit implementations requiring no electronics and electrical products.

Most important characteristics of reserve control systems are the overall dimensions and the power consumption. These characteristics, as a rule, should be minimized at the development stage. V. A. Trapeznikov Institute of Control Sciences has been carrying out researches in the field of microminiaturization of operational units of fluidic control systems. For example, prototypes of the microfluidic base elements of the characteristic 100 μm size that is resistant to

both electromagnetic radiation of high powers and high temperatures have been created [1, 2]. Images of three of the prototypes are given in Fig. 1.

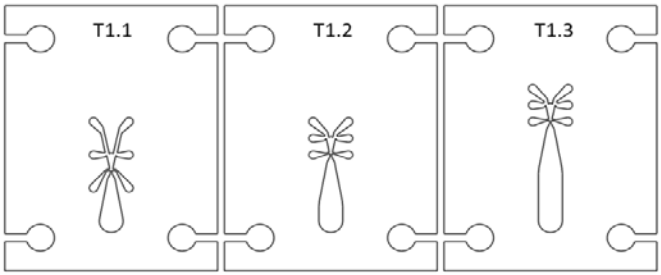


Fig. 1 – Microfluidic base elements of characteristic 100 μm size

Experimental researches have revealed high characteristics of the base elements (frequency, operating range, consumption). The advantages of these characteristics can result in improved robustness of reserve microfluidic control systems. Therefore, a most important aim is to hold these advantages within the operational units and even the whole control system. To approach the aim (or, at least, to make it closer), the authors have devised the method of designing microfluidic operational units of robust reserve control systems, using the base constructive elements.

As an example of applying the method, the design of the microfluidic three-stage oscillator has been created on the basis of the elements represented in Fig. 1.

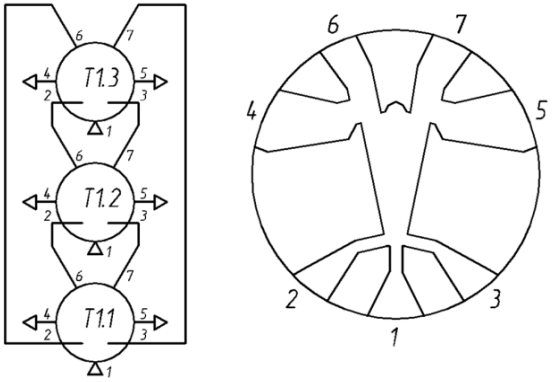


Fig. 2.– Schematic circuit of microfluidic three-stage oscillator (on the left) and operational geometry of base elements (on the right)

Represented in Fig. 2 are the schematic circuit of the microfluidic three-stage oscillator (on the left) and the operational geometry of the base elements (on the right). The oscillator operating is provided by the following in-circuit processes. The power of the oscillator (input 1) having been provided, the gas flow can equiprobably occupy the left channel 6 or the right channel 7 of the first stage T 1.1. For the gas to easily flow from the input to the output, the microfluidic elements should have the atmosphere channels 4, 5 that provide the removing of the redundant gas from the operating chamber. The outputs 6, 7 of the first stage are connected to the inputs 2, 3 of the second stage, and the outputs of the second stage are connected to the inputs of the third stage. The circuit includes the two feedback paths connecting the outputs 6, 7 of the third (end) stage to the inputs 2, 3 of the first stage. This provides sustainable operating of the oscillator. The feedback channels are matched to the oscillator inputs and outputs by hydrodynamic impedances, using the method described in [3].

An analysis of possible design implementations and a synthesis of the best design implementation of the oscillator can effectually be performed by means of *Multidimensional Network Models (MNM)* [4, 5].

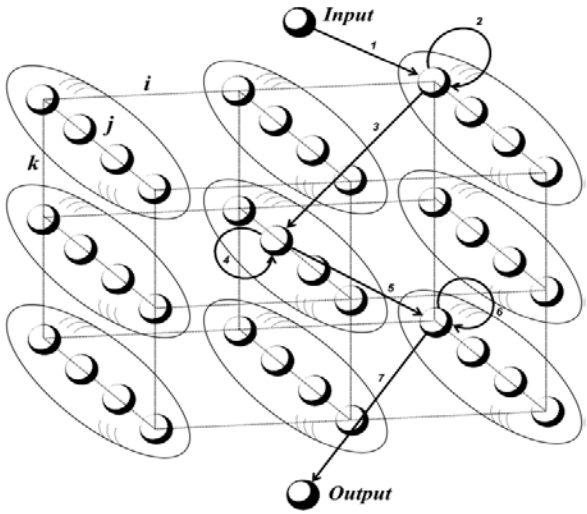


Fig. 3 – Multidimensional network model of microfluidic oscillator

MNM of the microfluidic three-stage oscillator being designed (see Fig. 2) is given in Fig. 3. The network model is three-dimensional (***i***, ***j***, ***k***). Generally, the amount of dimensions varies and is to choose in terms of both complexity and carefulness of the analysis.

The nodes of MNM are instances of the structure classes. As an example, MNM given in Fig. 3 includes three structure classes, which corresponds to the three node sets toward ***i***, and to the three base elements represented in Fig. 1. Each of the structure classes is attributed with the parameter vector that can include both constant (fixed) parameters and variable ones. The constant parameters specified in designing the oscillator are the geometries of the base elements (see Fig. 2 on the right), the element thickness, the element area, and the connection sizes. Four spatial orientations of the base elements are specified as the variable parameters, which corresponds to the four node sets toward ***j***.

The ellipsoids render the strongly connected graphs of the operations of transforming the structure class instances: during these operations, the variable parameters run through the sets of their values.

MNM given in Fig. 3 includes tree levels, which is rendered with the three node sets toward ***k***. The network levels correspond to the design levels of the oscillator. The maximum number of the levels equals the number of the base elements of the oscillator, which corresponds to placement of each of the elements at its own (separate) level.

The loops of MNM render the operations of creating the structure class instances, which corresponds to the installing of the base elements into the assembly. The other edges (excepting the input and the output) render the operations of transiting between pairs of the structure class instances (for example, forming a communication element, interlayer spacers, etc.). The most relevant condition for the transitions to be performed is that the end nodes of the edges (transition operations) are to be matched by the main characteristics attributed to the information signals (*representation forms*, *codes*, and *coding precision*). The input and output edges render the complex operations of forming the terminal and fastening elements of the design. For example, the input edge would correspond to the operation of installing the bottom and the pins to position the microfluidic elements as precisely as required. The output edge would render the operation of installing the cover, the screws, and the connectors to carry out data exchange with peripheral devices.

The edges are to associate with the weights that reflect contributions of the corresponding operations to the quality of the design implementation. The best design implementation is synthesized by means of calculating the shortest path within MNM. The path calculated is represented with the end node and edge set in Fig. 3. The edge 1 corresponds to the technological operation of installing the bottom equipped with the connective input elements delivering the power gas. The {2, 4, 6} and {3, 5} edge sets render the operations of mounting the three base elements as well as the connector spacers. The edge 7 represents the assembling operations for the cover, the fastening details, and the connective output elements to transmit the informational signals to pneumoelectric converters.

Thus, MNM is a generalized design model of the microfluidic operational unit to be designed, and render this unit in the form of the arranged set of structural-class instances and the operations on the instances. The method of designing microfluidic operational units of robust reserve control systems of critically important objects, represented in this paper, is based on MNM. This allows the possible design implementations to be systematized within the single multidimensional network, and provides the choice of the best design implementation by means of calculating the shortest path within this network.

References:

1. *Kasimov A. M., Mamedli E. M., Mel'nikov L. I.* Issues of Design and Production of Heterogeneous Control System of Aircrafts // Sensors & Systems. – 2012. – № 5. – P. 2-6.
2. *Belyaev M. M., Kasimov A. M., Popov A. I.* Measurements of Physical Parameters by Means of Pneumatic Devices with Frequency Output // Sensors & Systems. – 2017. – № 1. – P. 49-56.
3. *Kasimov A. M., Balabanov A. V., Dolgov I. V.* Method of calculating design parameters of communication and throttle channels of microfluidic system // Sensors & Systems. – 2018. – № 5. – P. 39-44.
4. *Balabanov A. V.* Structured synthesis of 3D-models with primitive instances // Information Technology of CAD/CAM/CAE. – 2017. – № 2. – P. 50-54.
5. *Balabanov A. V.* Structured synthesis of dynamic 3D-models of spatial mechanisms // Information Technology of CAD/CAM/CAE. – 2017. – № 3. – P. 44-46.

Иванов В.П., Каблова Е.Б., Кленовая Л.Г., Фомичев И.В.

Информационно-аналитическое обеспечение терминальных систем СУРТ и ПГСП для повышения безопасности жидкостных средств выведения

Аннотация: Статья посвящена описанию информационно-аналитического обеспечения систем СУРТ и ПГСП ракет-носителей при проведении наземных, стендовых и летно-конструкторских испытаний для повышения безопасности запусков ракет-носителей и разгонных блоков.

Ключевые слова: терминальные системы, наземные, стендовые, летные испытания, безопасность запусков, ракета-носитель, разгонный блок

Управление внутрибаковыми процессами ракет-носителей (РН) оказывает существенное влияние на надежность и безопасность средств

выведения [1]. Внутрибаковые процессы определяют условия устойчивой работы жидкостных двигателей (ЖРД), безаварийность их запуска и выключения. Желаемое протекание этих процессов обеспечивается путем управления расходованием компонентов топлива и наддувом баков на основе систем управления расходованием топлива (СУРТ) и пневмогидравлических систем подачи (ПГСП).

Надежность функционирования этих систем в значительной степени определяется качеством их наземной и стендовой отработки.

Решающая роль в решении этих задач принадлежит информационно-аналитическому обеспечению систем в части адекватности аналитического описания функционирования данных систем и отсутствия ошибок реализации в процессе отработки.

Информационно-аналитическое обеспечение систем СУРТ и ПГСП, помимо формульных блок-схем бортовых алгоритмов и параметрического обеспечения, включает в себя контрольно-тестовое обеспечение автономной отработки бортовой программной реализации алгоритмов и математическое описание внутрибаковых процессов, являющихся объектом управления этих систем. Кроме того, сюда входят методики анализа результатов испытаний и методика расчета параметров алгоритма, которые позволяют адаптировать систему к конкретным условиям полета РН и могут вводиться в бортовую вычислительную машину (БЦВМ) непосредственно перед запуском ракеты-носителя. Ошибки отработки в процессе испытаний, при анализе результатов испытаний, при расчете массива данных на пуск (ДНП) могут привести к нештатным ситуациям в работе систем СУРТ и ПГСП и невыполнению задачи пуска.

Основным инструментом проверки правильности программной реализации алгоритмов является контрольно-тестовое обеспечение.

Разработка контрольных тестов для проверки бортового программного обеспечения (БПО) производится путем моделирования работы системы на заданном интервале времени на универсальной вычислительной машине. Современные бортовые алгоритмы СУРТ и ПГСП представляют собой широко разветвленную сеть каналов формирования управления. Тестовые примеры должны обеспечить проверку функционирования всех каналов управления в штатных и нештатных режимах работы системы. Каждый тестовый пример представляет собой временную последовательность входных сигналов алгоритма управления и соответствующую этой таблице последовательность выходных сигналов. Правильность программной реализации определяется на основе сравнения результатов моделирования БПО и таблицы выходных сигналов тестовых примеров.

Аналогичная тестовая проверка проводится для программной реализации алгоритмов управления стендового изделия. Стендовое

изделие подвергается огневым испытаниям при подаче топлива из баков и работающем двигателе. В процессе огневых испытаний проверяется функционирование систем ПГСП и СУРТ с программным обеспечением, разработанным для стендового изделия. Это программное обеспечение должно быть максимально приближено к штатному БПО систем СУРТ и ПГСП.

Важным этапом в процессе отработки бортового программного обеспечения является имитационное моделирование полета ракеты-носителя.

Моделирующий комплекс (МК), предназначенный для имитации процессов управления полетом ракеты-носителя, состоит из имитационных моделей объекта управления, измерительных и исполнительных устройств, реализуемых на универсальных вычислительных средствах, и бортового программного обеспечения всех систем носителя, которое может быть реализовано на бортовой вычислительной машине.

Возможность некорректности и неадекватности аналитического описания внутрибаковых процессов связана со сложностью уравнений массо-теплообменных процессов при непрерывной подаче жидких компонентов топлива из баков ракеты в работающий двигатель, с учётом конденсации или испарения жидкости и уравнений, характеризующих зависимость расходов компонентов топлива через работающий двигатель от возмущающих факторов и воздействия регулирующих органов. Теплообменные процессы между газом, жидкостью и стенками баков на границе раздела между газом и жидкостью [2] описываются уравнениями в частных производных. В итоге, расход топлива из баков определяет тягу двигателя и изменение кажущегося ускорения ракеты-носителя.

Другим источником ошибок является неполнота исходных данных. С целью недопущения работы имитатора с испорченными или недостоверными исходными данными, или для контроля выхода основных характеристик системы за допустимые пределы, а также с целью упрощения дальнейшей отработки совместного комплекса всех используемых программных средств, в имитационном программном обеспечении стенда (ИмПО) СУРТ и ПГСП предусмотрены защитные и диагностические средства.

Условия проверки бортового программного обеспечения системы при совместных отработочных испытаниях (СОИ) на моделирующем комплексе максимально приближены к реальным условиям ее эксплуатации. При проведении СОИ на моделирующем комплексе БПО всех систем носителя функционирует в замкнутой схеме, получая входные сигналы от программных имитационных модулей измерительных трактов и управляя моделями соответствующих объектов управления. Это

позволяет проверить правильность взаимодействия БПО различных подсистем (в том числе правильность данных на пуск, вводимых оперативно для конкретного изделия), оценить результаты моделирования пуска изделия по величинам обеспечиваемой конечной точности и контролируемым характеристикам динамики процесса управления.

Правильность функционирования БПО проверяется путем проведения на моделирующем комплексе нескольких испытаний, имитирующих полет РН с различным составом возмущающих факторов. Поскольку имитация полета РН на моделирующем комплексе является достаточно трудоемкой процедурой, общее число испытаний, проводимых на моделирующем комплексе, как правило, существенно ограничено.

Одной из основных задач испытаний является проверка энергетической безопасности запуска возмущенных режимов работы.

С учетом сложившейся практики проведения совместных отработочных испытаний на моделирующем комплексе проверяются номинальный режим полета РН и несколько возмущенных статистически-предельных режимов полета, характеризующихся различными условиями по потребной энергетике для успешного решения задачи выведения. Как правило, в число таких возмущенных режимов включаются испытания с наборами возмущений, требующих минимально-потребную и предельную энергетику РН.

Современные бортовые системы используют отказоустойчивые алгоритмы управления, позволяющие диагностировать аппаратные отказы, адаптировать систему к нештатным ситуациям и сохранять ее работоспособность.

В плане контроля надежности и безопасности полета при имитационном моделировании анализируется функционирование бортовых систем в различного рода нештатных ситуациях. В процессе таких испытаний подтверждается возможность решения задачи пуска в ряде нештатных ситуаций. Проверяется возможность частичного решения задачи и экологическая безопасность в аварийных ситуациях.

Применительно к системе СУРТ имитируются отказы дискретных измерительных точек датчиков уровней в различных комбинациях, отказы в цепях исполнения регулировки режима двигателя по параметру Km и по тяге. В части системы ПГСП имитируются отказы каналов функциональных датчиков измерения давления в баках, отказы исполнительных органов ПГСП (электро-пневмо клапана и дренажно-предохранительного клапана).

В заключение отметим, что информационно-аналитическое обеспечение в части систем СУРТ и ПГСП разработано для РН «Протон-М», РН «Союз», РН «Зенит» РН «Ангара-1.2» и РН «Ангара-А5».

Литература:
1. *Иванов В.П., Завадский В.К., Каблова Е.Б., Кленовая Л.Г.* Управление массо- и теплообменными процессами в баках и магистралях двигателя, определяющими устойчивый режим образования (выделения) энергии большой мощности в жидкостных двигателях Труды XX международной конференция «Проблемы управления безопасностью сложных систем». Москва, декабрь 2012 г. ИПУ РАН. С. 262-264.
2. *Гордеев В.А., Фирсов В.П.* Комплект математических моделей ПГСП криогенного разгонного блока. Юбилейный сборник трудов, посвященный 90-летию ГКНПЦ им. М.В. Хруничева и 55-летию ОКБ-23-КБ Салют». М.: Воздушный транспорт, 2006, с. 320 – 333.

Мавлянкариев Б.А., Пен А.Ю., Хатамов Б.Б., Талибджанов И.Р.

Многофункциональная интегрированная система безопасности

Аннотация:Предлагаются особенности построения и развития многофункциональных интегрированных систем безопасности на объектах производства с повышенным уровнем опасности в Республики Узбекистан.

Ключевые слова: интегрированная система безопасности, аварийная ситуация, мониторинг, защита персонала

Для повышения эффективности производства при обеспечении технологической и производственной безопасности многофункциональная интегрированная система безопасности (МИСБ) промышленных комплексов должна обеспечивать: контроль и управление технологическими и производственными процессами в нормальных условиях; аварийное оповещение; поиск застигнутых аварией людей в аварийных ситуациях, при проведении спасательных работ и ликвидации аварий; контроль за возникновением гремучих смесей и автоматическую газовую защиту; наблюдение (контроль за обслуживающим персоналом и проникновением на объект посторонних); оперативную связь; оценку и прогноз различных опасностей в любых условиях.

Вышеперечисленное делится на задачи управления технологическими и производственными процессами и задачи противоаварийного управления и защиты, при этом принципиально важным является техническое разделение систем противоаварийной защиты и систем автоматики и связи. Правильность такого подхода подтверждается многолетней инженерной практикой реализации систем автоматизации и противоаварийной защиты на различных опасных производствах в

нефтегазовой, нефтехимической, нефтеперерабатывающей, энергетической и других отраслях промышленности.

Анализ тяжести последствий аварий и требований к МИСБ, призванных исключить аварии или минимизировать их последствия, показывает, что ни существующие, ни перспективные электрические, электронные и программируемые системы защиты не способны сами по себе обеспечить безопасную работу [1]. Эти системы защиты эффективны только тогда, когда они дополняют и контролируют реализацию соответствующих проектных решений, технологических и организационных мероприятий, обеспечивающих снижение уровня риска аварий до приемлемого.

Противоаварийное управление и защита промышленных комплексов должны осуществляться с использованием МИСБ, которая объединяет в единый комплекс системы и средства, обеспечивающие решение задач организации безопасного производства и информационной поддержки управления технологическими и производственными процессами в нормальных и аварийных условиях, в частности:

- оперативный мониторинг за соблюдением проектных решений, предотвращающих условия возникновения различных видов опасности промышленного и техногенного характера;

- предотвращение условий возникновения различных видов опасностей в виде аварий за счет организации технологических и производственных процессов и применения систем, осуществляющих противоаварийное управление и защиту людей, оборудования и сооружений;

- минимизацию ущерба от реализованной в виде аварии опасности за счет средств, обеспечивающих предотвращение развития аварии, распространения и снижения степени влияния опасных факторов.

Объектами мониторинга и управления, оценки и прогноза служат техническое состояние производства, технологическое оборудование, сооружения и обслуживающий персонал предприятия, системы и средства, связанные с безопасностью, другие процессы производственного цикла.

МИСБ должна обладать свойством «гибкости», т.к. может изменяться в ходе эксплуатации. В состав МИСБ должны входить электрические, электронные и программируемые системы, обеспечивающие:

- оперативное срабатывание систем безопасности при образовании паровоздушных смесей повышенной концентрации, особенно в случаях внезапных выбросов пожаровзрывоопасных смесей (разливов);

- противопожарную защиту систем обнаружения пожаров и их ранних признаков, контроля и управления системами пожаротушения;

- систем наблюдения, сигнализации, аварийного оповещения и оперативной связи;

- индивидуальную и групповую защиту обслуживающего персонала.

Учитывая технологическую сложность и техническую проблематику совмещения систем безопасности «старой» (оставшейся в наследство) и «новой» (современнейшей) модификации, которая вобрала бы в себя полный спектр требований по автоматизации и безопасности всех технологических процессов, разумным методом построения единой МИСБ является глобализация существующих на предприятии систем (подсистем) безопасности и обеспечение их взаимной интеграции с новейшими [2].

Перспективы построения и развития МИСБ связаны с разработкой и внедрением многокомпонентных многоуровневых программных (информационных) комплексов, обеспечивающих одновременное повышение экономической эффективности и уровня безопасности за счет предоставления в нормальных и аварийных ситуациях оперативной и достоверной информации, содержащей данные о состоянии, тенденциях и признаках опасных ситуаций и явлений, получаемых за счет комплексной обработки данных от различных информационных, измерительных, управляющих и противоаварийных систем. Подобные комплексы весьма актуальны для предприятий с повышенной пожаровзрывоопасностью и обеспечивают [2]: интеграцию данных от различных информационных, измерительных и управляющих программных и технических подсистем в едином информационном поле и использование оптимальных методов обработки и предоставления информации для эффективного управления на различных уровнях; структурную, информационную, организационную и территориальную компонентность; углубленную детальную обработку данных на основе использования математических моделей, баз данных и знаний для выявления признаков, взаимосвязей, последствий и т.п.; применение логических алгоритмов и спецификаций информационного взаимодействия с произвольными программными компонентами; интерфейсы с различными информационными системами (ситуационными центрами).

Литература:

1. *Мавлянкариев Б.А* Информационно-аналитическое обеспечение при создании многофункциональной пожарно-спасательной техники// Мат.межд.НПК при ИПБ МВД РУз "Реформы в службе пожарной безопасности-переход на новый этап" 30.03.2018. Ташкент, с.39-41.
2. *Мавлянкариев Б.А*., *Кулдашев А.Х.* Развитие научно-технического обеспечения пожарной безопасности на инновационной, многофункциональной основе//Мат.респ. НПК при ИПБ 14.12.2017, с.27-33.
3. http://masters.donntu.edu.ua/ (Дата обращения:10.09.2018).

Сафронов А.И.

Составляющие автоматизации построения плановых графиков движения поездов метрополитена, нацеленные на обеспечение безопасности перевозки пассажиров

Аннотация: Статья посвящена современному состоянию развития Московского метрополитена, тенденциям его развития, а также тенденциям развития автоматизации технологических процессов, прямо и косвенно влияющих на безопасность перевозки пассажиров. Вместе с тем рассмотрены базовые составляющие комплексной автоматизации технологического процесса, связанного с составлением расписания движения пассажирских поездов метрополитена.

Ключевые слова: безопасность, движение поездов, метрополитен, планирование, перевозочный процесс, расписание, график движения поездов

Московский метрополитен является сложной транспортной системой, которая со времён запуска для пассажиров и до настоящего момента продолжает непрерывно развиваться. За последние несколько лет усилиями строителей и инженеров-проектировщиков крайне успешно реализуется государственный заказ по программе «2012-2020», которую выполняет ГУП «Московский метрополитен» совместно с АО «Мосметрострой», АО «Мосинжпроект», другими подрядными строительными организациями Российской Федерации, а также ближайшего зарубежья. В частности, строительство южного участка Большой кольцевой линии (БКЛ) сейчас проводится при участии специалистов и строителей из Китайской Народной Республики «China Railway Construction Corporation» (CRCC) [1].

Выбранная стратегия развития метрополитена оказалась весьма успешной – 2018-й год уже побил рекорды по количеству открытых для пассажиров новых станций. До этого рекорд по количеству открытых для пассажиров за год станций не был побит с самого момента запуска Московского метрополитена, а именно с 15 мая 1935 года. В тот день пассажиры могли воспользоваться сразу тринадцатью станциями «подземки». Этот год подарил жителям мегаполиса пять станций БКЛ, три станции продления Люблинско-Дмитровской линии (ЛДЛ) на север, семь станций Солнцевской линии. Известно, что в графике мэра города Москвы на конец 2018-го года записаны мероприятия по открытию ещё одной станции на БКЛ, одной станции на Замоскворецкой линии и трёх станций новой, Некрасовской линии. В совокупности – это 20 станций.

И без того разветвлённая система Московского метрополитена становится всё больше и больше. Это, безусловно, положительно сказывается на качестве жизни людей в мегаполисе – скоростной транспорт начинает появляться в шаговой доступности от мест их проживания и работы. Однако, существует и обратная сторона вопроса – со временем звенья этой разветвлённой системы становятся всё менее и менее надёжными. Они могли бы стать таковыми без должного обслуживания. Но система не приходит в упадок благодаря усилиям огромного штата сотрудников, поддерживающих и днём, и ночью, ежедневно метрополитен в надёжном и безопасном состоянии. Метрополитен продолжает расти, не снижая своих качественных показателей по безопасности перевозки пассажиров – и это крайне важно.

Показатель безопасности функционирования метрополитена напрямую зависит, в частности, от деятельности сотрудников Службы Движения – составителей плановых графиков движения пассажирских поездов (ПГД), то есть нормативных документов, позволяющих организовать эффективное взаимодействие Службы Движения с другими Службами метрополитена, от которых зависит качественная перевозка пассажиров.

В области построения плановых графиков движения пассажирских поездов (ПГД) или, попросту, в области составления поездного расписания, велика роль автоматизации технологических процессов. Именно комплексная автоматизация позволяет существенно снизить показатели большинства известных на сегодняшний день рисков (термин употреблён на бытовом уровне), связанных с влиянием человеческого фактора.

В данной статье рассматриваются составляющие комплексной автоматизации для процесса построения плановых графиков движения поездов метрополитена, нацеленные на обеспечение безопасности при перевозке пассажиров. Это следующие составляющие:

- модуль для автоматизации построения плановых графиков движения поездов для линий радиального типа [2];
- модуль для автоматизации построения плановых графиков движения поездов для линий радиального / диаметрального / хордового типов с зонированием («зонное» движение) [3];
- модуль для автоматизации построения плановых графиков движения поездов для радиальных линий с «вилочным» движением [3];
- модуль для автоматизации построения графика движения поездов для линий кольцевого типа [4];
- модуль для анализа качества составленных плановых графиков движения пассажирских поездов метрополитена, снабжённый компонентами электронного документооборота [5];

- модуль для блочного дополнения и развития структуры «подложки» (бланка) для построения графика движения поездов по продлённой линии метрополитена [6].

Упомянутые модули основываются на классификации, составленной в [4] и дополненной в [7, 8]. Модули и их специфика подробно описаны в отмеченных выше трудах учёных и разработчиков, занимавшихся и продолжающих заниматься соответствующими вопросами.

До настоящего момента внимание в ранее опубликованных трудах в меньшей степени уделено только:

- модулю для анализа качества составленных плановых графиков движения пассажирских поездов метрополитена, снабжённому компонентами автоматизации электронного документооборота;

- модулю для блочного дополнения и развития структуры «подложки» (бланка) для построения графика движения поездов по продлённой линии метрополитена (этот модуль договоримся далее называть «конструктором»).

Тенденция развития и функционирования Московского метрополитена на сегодня такова, что построенные отдельные фрагменты будущих новых и достаточно протяжённых линий руководители ГУП и, в частности, Службы Движения, стремятся максимально увязывать между собой при организации пассажирского движения по ним. Это делается, зачастую, из-за отсутствия возможности, например, ввода в эксплуатацию депо в поставленные сроки, или вовсе из-за отсутствия депо в плане развития инфраструктуры на данном участке в принципе (депо этой линии запланировано только на участке перспективного продления, и до момента открытия участка продления линия ещё не может считаться самостоятельной). Так характеризуется вынужденная мера Служб метрополитена по объединению двух участков разных перспективных линий в одну длинную линию.

Ныне известно и об утилитарном объединении участков линий. Это тот случай, когда участки будущих длинных линий, в принципе, способны существовать независимо друг от друга, но перевозочный процесс на них согласно решению Службы Движения, осуществляется единый, организованный по принципу «вилочного» движения [3]. Это позволяет максимально удлинить линию и эффективно использовать ресурсы электроподвижного состава, сокращая общее количество оборотов по тупикам и ремонтов в пунктах осмотра.

Очевидно, что лучше составить один плановый график движения пассажирских поездов и прилагающийся к нему график оборота электроподвижного состава на объединённую линию, нежели составить два плановых графика на каждый участок и к каждому их них приложить свой график оборота электроподвижного состава. Последний вариант

неэффективен с точки зрения затрат человеческих ресурсов на выполнение работ по составлению графиков. Вдобавок, раздельный случай обладает меньшей надёжностью и большими затратами электроэнергии на тягу в виду увеличения количества оборотов по тупикам. Как следствие снижение надёжности может приводить и к ухудшению безопасности, которой метрополитен не пренебрегает. По этой причине в настоящее время заметно увеличение числа линий с «вилочным» движением на схеме метрополитена. С точки зрения навигации и комфорта – этот вид движения вносит путаницу, но с точки зрения безопасности перевозки пассажиров он более надёжен.

Подобные манипуляции слиянием и последующей расцепкой линий метрополитена оправдывает трудозатраты на создание модуля «конструктор» в системе. Модуль «конструктор» нацелен на развитие структуры линии метрополитена в самой системе для автоматизированного построения плановых графиков движения пассажирских поездов метрополитена, а не в СУБД, подключаемой к ней. При внесении изменений в хранимые данные посредством СУБД велика вероятность нарушения целостности этих данных в процессе развития структуры линии метрополитена. Существующие алгоритмы содержат в основе объектно-ориентированный подход и реализуют «клонирование» существующих станций. Подход требует работы только со структурой очищенной «подложки» (бланка) для нанесения на неё элементов расписания. В настоящее время модуль нацелен на взаимодействие с базой данных линии метрополитена, не содержащей в себе ни единого элемента расписания.

Автором планируется развитие модуля «конструктор» с целью выполнения продления линий с сохранением всех элементов расписания. Для решения такой задачи за основу взята графовая модель. В ней вершины графа – станции, рёбра – перегоны и оборотные тупики. При переходе к графовой модели структуру линии и нанесённое на неё расписание следует рассматривать как связанные слои, где элементы одного слоя отслеживают происходящие изменения в соседних слоях и автоматически дублируют структуру слоя по аналогии со своими «соседями». В этом случае объекты не клонируются, а являются новыми вполне определёнными элементами цепи, препятствующими нарушению целостности данных.

Сохранённое расписание для продлённых линий метрополитена в перспективе поспособствует ускорению составления ПГД, обуславливая для сотрудников Службы Движения ситуации, аналогичные обновлению ПГД для линий, не меняющих своей структуры. Подход должен:

- сократить количество возникающих стрессовых ситуаций, предоставив составителям плановых графиков движения больше времени на выполнение их работы;

- минимизировать ошибки, классифицируемые как человеческий фактор.

Подход нацелен на повышение надёжности составляемого графика движения и, как следствие, безопасности перевозочного процесса.

Взаимодействие оператора с модулем «конструктор» проводится без участия в процессе продления линии метрополитена лица, сопровождающего систему, что означает буквально следующее – процесс продления линии на «подложке» автономен. Он облегчает работу оператора и не позволяет затормозиться процессу составления расписания при плановом развитии инфраструктуры метрополитена, как это могло случаться ранее.

Использование модуля «конструктор» исключает ситуации возникновения ошибок от неправильного взаимодействия оператора с базой данных. Структура «подложки» (бланка) для построения нового планового графика движения пассажирских поездов благодаря «конструктору» развивается штатно, своевременно, в технологическом процессе минимизируются всплески, связанные с необходимостью создания графиков в авральном режиме, что повышает качественные показатели систем не только на практическом, инженерном уровне, но и на уровне эргономики.

Перспективный анализ предполагает выявление куда большего числа положительных сторон в работе модуля «конструктор» с возможным составлением новых классификационных схем для предметной области. Принятый подход обладает масштабируемостью, он эффективен, надёжен и безопасен.

Литература:

1. Комплекс градостроительной политики и строительства города Москвы. [Электронный ресурс]: Китайский щит начал строить еще один тоннель Большого кольца метро. URL: *https://stroi.mos.ru/photo_lines/kitaiskii-shchit-nachal-stroit-ieshchie-odin-tonniel-bol-shogho-kol-tsa-mietro* (Дата обращения: 24.11.2018).
2. *Сидоренко В.Г.* Принципы построения автоматизированных средств планирования перевозочного процесса на метрополитене / В.Г. Сидоренко // Проблемы управления безопасностью сложных систем: материалы XII Международной конференции. – М.: РГГУ, 2004. – С. 413–416.

3. *Сидоренко В.Г.* Синтез планового графика движения зонного типа / В.Г. Сидоренко, М. В. Новикова // Мир транспорта. – 2010. – № 4. – С. 128–134.
4. *Сафронов А.И.* Построение планового графика движения для метрополитена / А. И. Сафронов, В. Г. Сидоренко // Мир транспорта. – 2010. – № 3. – С. 98–105.
5. *Сафронов А.И.* Развитие методики расчёта эксплуатационных показателей в системе автоматизированного построения плановых графиков движения пассажирских поездов метрополитена / А.И. Сафронов // Интеллектуальные системы на транспорте: Материалы IV международной научно-практической конференции «ИнтеллектТранс-2014» / Под редакцией доктора технических наук, профессора А.А. Корниенко. – СПб.: ПГУПС, 2014. С. 367-374.
6. *Сафронов А.И.* Обеспечение безопасности движения пассажирских поездов на этапе планирования при продлении линий метрополитена / А. И. Сафронов // Труды. Восемнадцатой научно-практической конференции. "Безопасность движения поездов" – 2017. С. VIII-20-VIII-21.
7. *Сафронов А.И.* Автоматизация планирования работы ЭПС метрополитена / А.И. Сафронов, В.Г. Сидоренко, К.М. Филипченко // Мир транспорта. 2015, №4(59). - С.154-165.
8. *Чжо М. А.* Методика автоматизации построения планового графика движения пассажирских поездов метрополитена / М.А. Чжо, А.С. Петров, А.И. Сафронов, В.Г. Сидоренко // Транспорт и образование: актуальные вопросы и тенденции: материалы международной научно-практической конференции – Челябинск: ЧИПС УрГУПС, 2015.С. 74-80.

Исмаилов Ж.И., Кононов Д.А.

Новый шелковый путь: безопасность и оперативность железнодорожных перевозок

Аннотация: Рассмотрено текущее состояние формирования контейнерных поездов по маршруту и транспортно-логистических центров. Предложены принципы формирования поездов на железнодорожном транспорте стран, формирующих грузопотоки. Предложены перспективные модели и методы, позволяющие осуществлять непрерывный поток контейнерных перевозок в международном сообщении в целях повышения эффективности управления. Изучены влияния временных требований на формирование контейнерных поездов.

Ключевые слова: новый шелковый путь, железнодорожный транспорт, контейнерные перевозки, логистика, оптимизация, эффективное управление.

I. Введение

На фоне быстрого развития IT-технологии и интернет-продаж в последнее время, в целях сокращения времени поставки, наблюдается резкий рост контейнеризации грузов на железнодорожном транспорте.

Объём транзитных перевозок ПАО «ТрансКонтейнер» только за 2017 год вырос на 69,9% и составил 126 тыс. TEU против 74,2 тыс. TEU годом ранее. Контейнерные грузы весьма привлекательны для железных дорог, так как они относятся к грузам II тарифного класса наравне с нефтью и зерном. Продолжается дальнейшее контейнеризация грузопотоков на железнодорожном транспорте – коэффициент контейнеризации 2017 года вырос почти на 17%.

Железнодорожный транспорт постоянно увеличивает скорость доставки грузов, в том числе контейнерных отправок, а также оптимизирует процесс работы станций и контейнерных терминалов так как, определённое отставание динамики объёмов терминальной переработки транспортно-логистических центров от темпов роста рынка контейнерных перевозок не соответствует опережающим темпам роста экспортных и транзитных перевозок. Количество контейнерных поездов, прошедших по сети маршрутов, связывающих Китай и Европу, превысило в прошлом году 3,27 тыс. рейсов. Рост количества рейсов за прошлый год составило 52% от совокупного трафика за весь период с начала запуска сервиса в 2011 году (6,24 тыс. рейсов). На 2018 год China Railway прогнозирует рост трафика до 4 тыс. рейсов, сообщает в Комитете экономики и информатизации города центрального подчинения Чунцин (Юго-Западный Китай). Общее количество железнодорожных составов, формируемых из более чем 250 грузоотправителей для следования по магистрали Чунцин – Дуйсбург, по итогам 2017 года превысило 650 поездов. В частности, по этому маршруту налажено движение контейнерных поездов по расписанию.

II. Постановка задачи

Все виды грузов, перевозимые стандартными контейнерами, можно отнести к категории однородного груза, по правилам перевозок и по габаритам.

Классически, основной задачей математического моделирования транспортных перевозок является построение оптимального плана перевозок, предполагающий оптимизацию по времени или по стоимости перевозок однородного груза без учета временных требований заказчика, то есть требований поставки в определенное время. Этот ограничение значительно сужает возможности использования классической

транспортной задачи при решении задач железнодорожных перевозок. Также в ряде задач организации перевозок качество плана оценивается временем, затраченным на перевозки. Для практического применения математической модели железнодорожных перевозок необходимо составлять транспортные задачи с учетом времени поставок.

Пусть t_{ij} – время, необходимое на перевозку продукта из i-го пункта грузоотправителя в j-й пункт грузополучателя. При этом объем перевозок – x_{ij}. Цель задачи – обеспечить удовлетворение спроса логистических центров грузополучателя B_j ((j=1,…n) контейнером. Стратегии управления – формирование плана перевозок X={x_{ij}.}. Критерий эффективности – лучшим будем считать план, самая продолжительная перевозка которого имеет минимальную длительность.

При выбранном показателе эффективности задача планирования перевозок решается при ограничениях: отгрузка в логистических центров A_i составляет a_i единиц (i=1,…m).

Формальная постановка задачи не укладывается в рамки линейного программирования. Тем не менее, можно показать, что решение этой задачи может быть сведено к последовательному решению серии транспортных задач.

Планирование по минимуму времени осуществления наиболее длительной перевозки актуально при перевозки контейнерных перевозок. В то же время следует учесть, что необходимо

– осуществлять отправку контейнерных поездов по расписанию;

– организовать движение поездов на совмещенных грузо-пассажирских магистралях, где каждый поезд имеет свой график движения, т.е. транспортно-логистические центры должны организовывать прием контейнеров с учетом времени отправки поездов.

III.Заключение

Решение транспортной задачи с учетом времени поставок оказывает существенное влияние на безопасное и оперативное распределение грузоперевозок и позволяет минимизировать транспортные затраты.

Следует отметить, что с возрастанием возможностей поставок решение транспортной задачи с учетом времени поставок будет стремиться к решению классической транспортной задачи. В случае, когда отгрузка будет не меньше потребностей соответствующего заказчика, эти ограничения будут автоматически выполнены и решения обеих задач совпадут. Если исходная транспортная задача является открытой, то следует ввести дополнительного (фиктивного) заказчика с объемом заказов, делающих задачу замкнутой. Тарифы перевозок к этому заказчику задаются равными нулю, а время поставок к нему достаточно большим.

Учет времени поставок при моделировании транспортных перевозок позволит находить комплексные оптимальные решения с учетом

возможностей всех заинтересованных сторон в процессе формирования контейнерных поездов в транспортно-логистических центрах «Нового Шелкового Пути».

Литература:
1. *Гоголин В.А., Николаева Е.А.* Транспортная задача с учетом времени поставок // Современные наукоемкие технологии. – 2017. – № 7. – С. 23-26.
2. *V.V. Kulba, D.A. Kononov and R.O. Ponomarev*, «A scenario research of the vulnerability of socio-economic s ystems,» 2 017 Tenth International Conference M anagement o f L arge-Scale S ystem D evelopment (MLSD), Mos-cow, Russia, 2017, pp. 1-5.
3. *Кононов Д.А.* Синтез эффективных структур управления на основе структурно-сценарного анализа /Труды 23-й Международной конференции «Проблемы управления безопасностью сложных систем» (Москва, 2015). – М.: РГГУ, 2015. С. 51-54.
4. *Архипова Н.И., Кульба В.В., Кононов Д.А.* Проблемы и задачи сценарного исследования безопасности региональных социально-экономических систем /Материалы Международной научной конференции «Актуальные проблемы управления» (Москва, 2015). – М.: Издательский Центр РГГУ, 2015. С. 3-9.
5. *Кононов Д.А., Лепе Н.Л., Пономарев Р.О.* Управление чрезвычайными ситуациями в региональных системах методами ситуационного анализа //Вестник РГГУ. Серия «Управление». 2016. № 4 (6). С. 58-70.

Торгашев Р.Е.

К вопросу аналитического обеспечения управления городами при использовании smart-технологий

Аннотация: В настоящей статье автор раскрывает стратегию развития курса использования smart-технологий в крупных городах Российской Федерации в современных условиях. Теория и практика аналитического обеспечения управления городами опирается на внедрение smart-технологий. Для обеспечения внедрения и развития smart-технологий необходимо всесторонне анализировать и давать объективную оценку российской муниципальной реформы и предлагать научно обосновывать меры для продвижения и укрепления местного самоуправления, в частности, по повышению эффективности управления современными городами, а также и агломерациями.

Ключевые слова: аналитическое управление, «умный» город, smart-технологии, местное самоуправление, агломерация

В последнее время мы наблюдаем процесс рождения «умных городов». «Умные города растут, несмотря на серьёзные проблемы в правовой и нормативно-технической базе, а также недостаточных инвестиций или их отсутствий вовсе. Самые успешные примеры связаны с решением конкретных муниципальных проблем или созданием новых сервисов для горожан. Для примера, можно взять столицу Каталонии – Барселону. В этом городе, одном из самых богатых и развитых городов Европы есть уникальные тенденции и передовые smart-технологии, в частности, Барселону можно считать первопроходцем внедрения высоких технологий, где датчиками оборудованы не только уличные фонари и остановки городского транспорта, но и даже мусорные баки. Они оперативно сообщают городским службам об их заполнении. Городским коммуникационным и инженерным службам стоит освобождать заполненные баки только по сигналу, - экономия вырастает.

В современной России много политических акторов, пытающихся всесторонне анализировать и давать объективную оценку российской муниципальной реформы и предлагать научно обосновывать меры для продвижения и укрепления местного самоуправления, в частности, по повышению эффективности управления современными городами, а также и агломерациями. Но в РФ пока Москва и Санкт-Петербург стали самыми «умными» российскими городами, по версии Национального исследовательского института технологий и связи (НИИТС). К эффективно развивающимся причислены Казань, Екатеринбург, к ним приближается Новосибирск, в которых технологии заметно развиваются относительно возможностей бюджета. Самара и Волгоград отнесены к начинающим. Следует отметить, что все названные города России относятся к городам миллионикам (крупные города, населения которых превышает 1 млн жителей). С 23 сентября 2018 года в РФ насчитывается уже 16 городов миллионеров, но меньшая их часть относится к «умным» городам, где развиваются Smart-технологии. Большинство проблем с отставанием остальных крупнейших городов России по численности населения в сфере smart-технологий считаем кроется в отсутствии ясности в вопросах дальнейшего развития местного самоуправления в Российской Федерации на средне и долгосрочную перспективу. Отсутствуют современные «стандарты развития городов разных типов» о которых говорил в августе 2016 года Председатель Правительства РФ Д. А. Медведев на форуме ВСМС «Городское развитие и совершенствование качества городской среды».

На практике происходит периодическое перераспределение полномочий между государственным и муниципальным уровнем власти, «перекройка границ» и слияние (укрупнение) муниципальных образований, приводящие преобразованию муниципальных районов в

округа, «к централизации» полномочий субъектов РФ, ущемляющие права местного самоуправления. Происходит отставании не только в информационном и экономическом потенциале у городов РФ, но и в интеллектуальном капитале аналитических служб бизнеса и некоммерческих организаций, где выделяются два компонента: человеческий капитал и структурный капитал [1, с. 71]. Структурный капитал включает все, что обеспечивает аналитикам возможность реализовывать свой потенциал в конкретной деятельности. В нем, как минимум, выделяют клиентский и организационный капиталы.

Клиентский капитал аналитических служб – это отлаженное эффективное взаимодействие с заказчиками. Он включает не только имидж у заказчика и деловую репутацию в целом, но и адекватные аналитические идеи, концепции, стратегии, деловые связи, сети распространения своей аналитической продукции и др.

К организационному капиталу относятся: информационные технологии, электронные сервисы и ресурсы службы, организационную структуру, систему управления аналитическими исследованиями, созданные организацией сетевые структуры для участия внешних аналитиков и экспертов и др.

Обычно организационный капитал аналитических бизнес служб разделяют на инновационный и процессный [3, с. 228].

Уместно подчеркнуть важность организационной структуры и системы управления аналитическими исследованиями, наиболее сильно влияющих на возможности и мотивацию аналитиков оперирующих знаниями, эффективно использовать свои знания [6, с. 122].

Человеческий капитал аналитической службы это не только реальные и потенциальные интеллектуальные способности и соответствующие практические навыки, умения работников аналитической службы, но и другие личные качества (креативные таланты, благоприятные психологические качества и др.). Понятие «человеческий капитал» предназначено для описания ценности того, что может произвести отдельный аналитик. В экономическом смысле человеческий капитал включает индивидуальную ценность аналитика. Этот капитал включает в себя накопленную стоимость инвестиций в подготовку и обучение работников, в их компетентность и их будущее. Его можно обозначить как совокупность компетентности аналитиков, их способности формировать взаимоотношения и ценности. Сюда же мы включаем креативность аналитиков.

Работа с человеческим капиталом аналитической службы часто направлена на трансформацию индивидуальных знаний в коллективные, а, следовательно, в более длительно сохраняющийся организационный капитал, что снижает риски организации, и определяет одну из тенденций

развития отечественной аналитики. Аналитик может уволиться. Если аналитик креативный, то потенциал креативности у аналитической службы естественно уменьшится, но она сохранит когнитивный потенциал и будет использовать результаты его креативного труда (на правовой основе). Поэтому для руководства любой аналитической службы важно сохранить ценных креативных сотрудников, а также организовать рабочий процесс так, чтобы происходило обучение других аналитиков, чтобы знания оставались в аналитической службе.

Для оценки аналитического капитала коммерческие и некоммерческие организации в основном используют методы, основанные на рыночной стоимости или экспертных оценках [2, с. 61].

Отметим некоторые тенденции развития государственной и муниципальной аналитики.

1. Повышается важность символичности и политического дискурса по критериям результативности, эффективности и качества муниципального и государственного управления.

2. Отдается приоритет групповой работе над индивидуальной (в частности, потому, что требования заказчика часто не даны априори, а вырабатываются в процессе совместного анализа).

3. Используются комплексные инструменты различных школ, многоуровневой, междисциплинарной и трансдисциплинарной аналитики.

4. Недостаточное внимание уделяется системному анализу и долгосрочному прогнозированию.

Повышение качества государственной и муниципальной аналитики связывают с внедрением в рамках электронных правительств аналитических систем типа B2B (заимствование государством опыта бизнеса) и B2G (в частности, в рамках аутсорсинга).

В рамках административной реформы [4, с. 225] аналитику рассматривают как функцию управления, иногда – как государственную услугу, если выполнение функционала инициируется вторым сектором (бизнесом) или третьим сектором (некоммерческими организациями, гражданами, мигрантами и др.). Эта функция (услуга) фиксируется в регламентах (органов власти, их подразделений, должностных регламентах аналитических подсистем типа G2G, G2B, G2C) и связана в основном с аналитическим обеспечением должностных лиц (в подсистемах типа G2G) или заявителей государственной услуги (в подсистемах типа G2B и G2C).

Обозначим подчеркиванием снизу подсистемы, включаемые в региональные сегменты национальной инновационной системы и инфраструктуры [7, с. 11].

Именно системы типа G2B и ряд систем типа B2B, B2G лежат в основе структурных каркасов глобальных инновационных 3К-факторов

(Креативность, Коммуникации, Когнитивность) в глобальной инновационной экономике регионов. На данный момент реально этими факторами в России в полной мере характеризуются Санкт-Петербург, Москва и частично Московская область [5, с. 59].

Литература:

1. *Торгашев Р.Е.* Государственная региональная политика и стратегическое управление экономикой региона. – Учебник. – Ульяновск: Зебра. – 2017. – 131 с.
2. *Торгашев Р.Е.* Государственное стратегическое управление, прогнозирование и планирование. – Учебник. – М.: Перо. – 2017. – 98 с.
3. *Торгашев Р.Е.* Комплексный подход при изучении геопространства. В книге: Пилотируемые полеты в космос Материалы XI Международной научно-практической конференции. 2015. - С. 226-228.
4. *Торгашев Р.Е.* Методические рекомендации по изучению регионов России. В книге: Пилотируемые полеты в космос Материалы XI Международной научно-практической конференции. 2015. - С. 225-226.
5. *Торгашев Р.Е.* Региональное управление и социально-экономическое развитие субъектов Российской Федерации. – Учебник. – Ульяновск: Зебра. – 2016. – 99 с.
6. *Торгашев Р.Е.* Формирование структуры управления территориальным хозяйством субъекта федерации. В сборнике: Актуальные проблемы управления Сборник статей Международной научной конференции. Сер. "Гуманитарные чтения РГГУ - 2015". 2015. - С. 114-123.
7. *Торгашев Р.Е.* Экономика и управление природопользованием Российской Федерации. – Учебник. – Ульяновск: Зебра. – 2016. – 51 с.

Завадский В.К., Стаменкович Н.

Обеспечение устойчивой работы маршевых ЖРД большой мощности перспективных ракет-носителей с широким диапазоном регулирования тяги

Аннотация: Рассмотрены вопросы обеспечения устойчивой работы маршевых ЖРД большой мощности в условиях регулирования тяги и соотношения расходов компонентов топлива в широком диапазоне.

Ключевые слова: режимы работы по тяге, устойчивость работы ЖРД, ограничения регулирования ЖРД.

Важнейшей частью жидкостных ракет-носителей (РН(и разгонных блоков (РБ) являются маршевые ЖРД, которые определяют

тяговооруженность ракеты-носителя, а, следовательно, его энергетические характеристики. Современные отечественные ЖРД РД170, РД180, РД191 с тягой от 200 до 700 тонн, представляют собой источник большой кинетической энергии, которая потенциально может стать причиной катастрофической ситуации в нештатных режимах работы. В связи с этим возникает проблема обеспечения устойчивой работы двигателя, в том числе средствами управления. ЖРД как объект регулирования представляет собой сложную динамическую систему, переходные процессы в которой характеризуются постоянным запаздыванием и широким спектром частотных характеристик.

В связи с развитием ракетно-космической техники существенно расширились задачи, возлагаемые на маршевые ЖРД. В настоящее время вместо одного или двух базовых режимов, оптимизация траектории полета РН требует от двигателя возможности постоянного регулирования тяги и соотношения расходов компонентов топлива в широком диапазоне [1].

В этих условиях актуальным является анализ наиболее критичных режимов работы современных ЖРД в контуре систем управления тягой, расходованием компонентов топлива. На основании такого анализа формулируются требования к этим системам, выполнение которых позволяет исключить критические режимы, и задача управления, обеспечивающая выполнение требований безаварийного функционирования ЖРД.

Исследования, проведенные КБ «Энергомаш» для двигателя РД 191, показали значительное влияние входных давлений компонентов на соотношение компонентов топлива на режимах глубоко дросселирования (<30% по тяге). Изменение давления окислителя на входе в двигатель на +1 кгс\см^2 соответствует изменению тяги на 0.2% и соотношения компонентов на 1.82% а изменение давления горючего на входе в двигатель на +1 кгс\см^2 соответствует изменению тяги на – 0.06 % и соотношения компонентов на 1.54% от нормальных величин.

Сочетание высоких входных давлений окислителя и горючего на низких режимах работы двигателя (27%) приводят к существенному росту значения соотношения расходов компонента по сравнению с номинальной величиной.

Подобное условие возникает на РН блочной компоновки (Ангара А5) для двигателя центрального блока, в циклограмме работы которого предусмотрен эффективный в плане энергетики режим глубокого дросселирования (30%) и с последующим возвращением на основной режим 100%-ой тяги. Для парирования существенного роста Km на режиме глубоко дросселирования в алгоритм управления двигателя вводится поправка на изменение Km с учетом изменения входных давлений компонентов топлива. Величина изменения определяется по

информации об измеряемом давлении наддува в подушках баков, продольной перегрузке, уровню столба жидкости в баках и плотности компонентов топлива [2]. Непрерывная информация о текущем уровне жидкости в баке может быть сформирована в алгоритме системы СУРТ с использованием дискретных датчиков измерения.

Наиболее эффективным средством своевременного парирования роста Km является способ регулирования Km на основе измерения расходов компонентов топлива датчиками расходов, установленными в магистралях двигателя. Такой способ широко используется в системах управления расходованием топлива семейства ракет-носителей «Союз».

Система управления расходованием топлива синхронизирует выработку окислителя и горючего путем изменения коэффициента соотношения компонентов. По результатам моделирования и огневых испытаний РД191 на некоторых образцах этого двигателя была выявлена склонность к возбуждению низкочастотных колебаний по тяге, возникающих под действием команд на уменьшение Km. Тенденция к возбуждению таких колебаний и их амплитуда увеличиваются с уменьшением расхода окислителя, то есть с уменьшением суммарного расхода и уменьшением коэффициента Km соотношения расхода компонентов топлива.

Для снижения вероятности возбуждения низкочастотных колебаний целесообразно использовать ряд алгоритмических мер ограничительного характера, не допускающих чрезмерного снижения расхода двигателя на этом участке.

В режиме глубокого дросселирования ЖРД по тяге возникает задача выбора алгоритма управления коэффициентом соотношения расходов из условия обеспечения устойчивой работы ЖРД. Суть этой задачи заключается в определении программы управления Km, обеспечивающей одновременность выработки компонентов топлива к моменту выключения двигателя при ограничении изменения Km на участке регулирования, критичном для устойчивой работы ЖРД.

Литература:

1. *Колбасенков А.И., Лёвочкин П.С., Пушкарев Д.С.* и др. Настройка современных ЖРД для обеспечения высокой точности при управлении и регулировании. // Общероссийский научно-технический журнал «Полет» - М., 2013. - №10. – С. 57-60.
2. *Колбасенков А.И., Пушкарев Д.С., Семенов В.И. и др.* Влияние входных давлений компонентов при работе двигателя на режиме дросселирования // Общероссийский научно-технический журнал «Полет» - М., 2013. - №11. – С. 34-36.

Скворцов О.Б.

Вибрационная безопасность больших энергетических агрегатов

Аннотация: Защита энергетического оборудования от аварий, начиная с незапланированных остановов и вплоть до масштабных катастрофических событий, имеет важнейшее значение для обеспечения безопасности. Быстрое развитие современных систем вибрационного мониторинга на основе *SCADA* и *IIoT* технологических решений, большая часть которых ориеbнтирована на использование современных методов вибрационной диагностики, не может полностью гарантировать своевременное выявление всех возникающих опасных нарушений режимов и дефектов. Для снижения риска крупных аварий такие системы должны включать эффективные быстродействующие средства противоаварийной защиты (СПАЗ), имеющие высокий уровень достоверности срабатывания. Разработка новых современных структур СПАЗ, возможна на основе систем, ориентированных на решение задач вибрационной диагностики. При этом не требуются существенные дополнительные затраты, чтобы обеспечить одновременно требования к СПАЗ, которые существенно отличны от предъявляемых к системам вибрационной диагностики. Получаемые при этом СПАЗ имеют повышенную достоверностью функционирования, которая ранее могла быть получена только в существенно более затратных решениях, основанных на многократном резервировании.

Ключевые слова: противоаварийная защита, вибрационный мониторинг, энергетический агрегат, промышленный интернет вещей, векторный анализ, достоверность функционирования

Надежная работа энергетического оборудования является необходимым условием безопасности любого современного государства. Вибрация является одним из важнейших факторов, влияющих на работоспособность основного и вспомогательного оборудования систем энергетического обеспечения. Для выполнения дистанционного контроля вибрационного состояния оборудования, диагностики исправностей и прогнозирования остаточного ресурса используют системы вибрационного мониторинга (СВМ). Обязательное использование таких систем предусмотрено действующими нормативными документами. СВМ также должны обеспечивать аварийную защиту агрегатов в условиях быстрого развития опасных ситуаций. С учетом требований нормативной документации для энергетического оборудования, как механического, в

виде различных роторные агрегатов, так и электрического, в виде мощных трансформаторов, вибрационный контроль обычно ограничивается измерением интенсивности вибрации. В большинстве случаев контроль выполняют по среднему квадратичному значению вибрационной скорости. Современные решения в области вибрационной диагностики требуют исследования вибрации в широкой полосе частот и интенсивностей вибрации. Это не может быть обеспечено, если ограничиться только требованиями нормативных документов. При разработке методов диагностирования и прогнозирования оборудования по вибрационному состоянию можно выделить три направления. В соответствии с первым на основе опытных данных и их статистического анализа формируется набор диагностических признаков, контроль за изменениями которых позволяет выявить зарождающиеся и развивающиеся дефекты и по тренду параметров формируется вероятностная оценка остаточного ресурса. Для второго направления прогноз остаточного ресурса с учетом используемых в оборудовании материалов и действующих на них нагрузок строится как оценка вероятности возникновения и развития повреждений. Такая возможность основана на использовании методов прогнозирования по вероятностным зависимостям для *S-N* диаграмм. Еще одно направление основано на использовании обучаемых нейронных сетей, для которых в явном виде не требуется описание процесса постановки диагноза. Некоторые типы дефектов сравнительно просто диагностируются с высокой достоверностью. например, такие как возникновение дисбаланса, , то распознать ряд других с высокой достоверностью и на ранних этапах развития достаточно сложно. Важное значение имеет тот факт, что развитие аварийной ситуации в энергетическом оборудовании может происходить очень быстро. Часто интервал времени от возникновения дефекта до аварии измеряется минутами или секундами. Задачи систем противоаварийной защиты (СПАЗ) по вибрационному состоянию имеют существенные особенности (меньшие требования к разрешающей способности и точности измерения, при необходимости повышенной надежности и сокращении времени отклика на возникновение аварийных ситуаций), желательно решать в единой системе вибрационного мониторинга. Построение высоконадежно системы вибрационного мониторинга, обеспечивающей диагностирование состояния оборудования. Обеспечить соответствие противоречивым требованиям возможно за счет увеличения объема собираемых на объекте данных о его вибрационном состоянии, эффективных передачи, хранения и анализа данных в центрах обработки при естественном желании сокращения затрат на СМВ. Обеспечение высокой надежности и достоверности функционирования СПАЗ за счет резервирования на практике не нашло

сколько-нибудь заметного распространения, поскольку требует кратного увеличения затрат на реализацию СМВ.

Удовлетворить требования к современной СМВ можно, если реализовать ее с использованием инновационных подходов, как при выборе структурных решений, так и за счет применения достижений в используемых аппаратных средствах. На уровне структуры системы такие возможности сбора и обработки информации СМВ реализуют с применением принципов промышленного интернета вещей (*IIoT*). Технологии *IIoT* являются версией широко применяемых решений *SCADA*. Дополнительные преимущества обеспечиваются одновременным использовании в СВМ специализированных решений. К таким решениям относятся адаптируемые в процессе работы структуры сбора вибрационных сигналов, что позволяет более полно и оптимально использовать возможности измерения вибрации в расширенном частотном и динамическом диапазонах [1-4]. Другое инновационное направление связано с учетом пространственного характера процессов вибрации. Это позволяет, используя один набор датчиков максимально приблизиться к получению полного объема диагностической информации и обеспечить повышенную достоверность работы при выполнении противоаварийной защиты [5, 6].

Обеспечение повышенной достоверности ПАЗ при этом обеспечивается тем, что данные с датчиков соответствующие вибрации в направлениях для которых механические свойства отличаются в максимальной степени и используются для диагностики состояния, одновременно преобразуются в набор измерений нескольких направлений которые с равными вкладами характеризующих вибрацию во всех направлениях. Пример структурной схемы аппаратуры для контроля вибрации подшипникового узла представлен на рис. 1. Сравнение таких данных фактически эквивалентно резервированному контролю при использовании их в СПАЗ. Также можно обеспечить возможность использования малобюджетных многокомпонентных датчиков вибрации, что в значительной степени позволяют существенно упростит систему. Снижение затрат на такую систему может быть обеспечено не только за счет применения дешевых *MEMs* вибрационных датчиков, но и применить для их подключения модификаций двухпроводных интерфейсов. Такие интерфейсы аналогичны *IEPE*, которые получили широкое распространение, но более экономичны и надежны. Использование инновационных подходов позволяет принципиально расширить возможности СВМ как при решении задач диагностики, так и противоаварийной защиты критически важного оборудования.

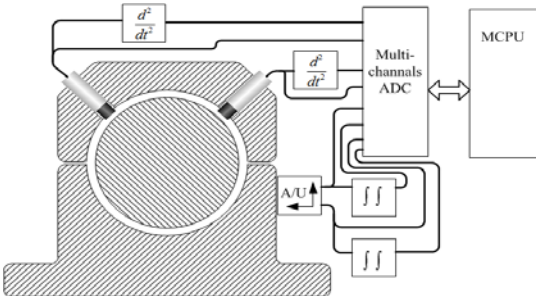


Рис. 1 – Структура измерительной схемы для мониторинга вибрации подшипникового узла с расширенным диапазоном измерения и поворотом осей чувствительности

Заключение

Комплексное использование инновационных решений при создании СМВ позволяет при общем снижении затрат обеспечить повышение эффективности как при обнаружении и распознавании дефектов, при одновременном сокращении времени реакции на развитии аварийной ситуации с улучшенной достоверностью ее обнаружения.

Литература:

1. Патент RU 2644620, кл. G01M 7/02, БИ № 5. 2018. — 14 с.
2. Патент RU 2658569, кл. G01M 1/00, БИ № 18. 2018. — 14 с.
3. Патент RU 2658570, кл. G01M 1/00, БИ № 18. 2018. — 13 с.
4. Патент RU 2658575, кл. G01P 3/36, БИ № 18. 2018. — 10 с.
5. Патент RU 2658568, кл. G01P 15/09, БИ № 18. 2018. — 22 с.
6. Патент RU 2658577, кл. G01H 11/06, БИ № 18. 2018. — 26 с.

Маций В.С., Кацко Д.И.

Геотехническая безопасность и субъективная оценка факторов оползневого риска

Аннотация: Предлагается для оценки геотехнической безопасности при изучении оползневого риска использовать субъективные знания специалистов по геотехнике, представленные в виде байесовских сетей доверия.

Ключевые слова: геотехническая безопасность, оползневый риск, субъективная вероятность, байесовская сеть, эффективность

Природно-технические системы сегодня возводятся в тяжелых условиях, поэтому проблемы геотехнической безопасности очень важны. Одним из центральных направлений является противооползневая защита, которая требует определенных действий [2]: оценка устойчивости склонов; проектирование, сооружение и эксплуатация. Актуальность заявленной темы подтверждается как природными катаклизмами (например, подъем рек на побережье Краснодарского края в октябре 2018 г.), так и частыми оползнями автомобильных дорог (рис. 1-2).

Рис. 1 – 5-й км А-147 Джубга – Сочи

Рис. 2 – А/д Хоста – Верхняя Хоста

Формализованные методы предельного равновесия оползневого массива многообразны и используют различные допущения. Автором [2] в рамках метода линий скольжения получены закономерности, позволившие

уточнить методику оценки устойчивости оползневых склонов. В работах [1, 3] разработаны методологические аспекты оценки и управлением рискам на транспортных природно-технических системах. Необходимость системного подхода, учитывающего как формализованные процедуры получения моделей принятия решений при оценке экономического риска, так и не формализованные, отражена в [4]. Вариативные подходы к оценке и управлению оползневым риском транспортных систем, рассмотрены в работе [5].

Как известно, основой доформального исследования является когнитивная структуризация наших (экспертных) знаний, представленная в виде когнитивной карты. Фрагменты когнитивной карты представляют собой фрагменты знаний, характеризующие связи между несколькими концептами (утверждениями), например, при изучении оползнеопасного участка автодороги нами были рассмотрены следующие концепты: F1 – наличие растительности, слабая расчленённость рельефа, блюдца замокания, на отдельных участках грунт влажный; F2→F1 и/или F3: участки застоя воды, участки отсутствия растительности, выходы выветрелых пород, бровки срыва грунта, эрозионные борозды; F3 →F1 и/или F2: рельеф расчленен эрозийными промоинами, глубиной более 0,5м, «пьяный лес», осыпи, оползневые накопления в подошве, рыхлый, водонасыщенный грунт, неурегулированный водоток в подошве, выходы струйных течений, мульда, утечки хозяйственно-бытовых вод; Investment – инвестиции в противооползневые мероприятия (водоотведение, дренаж, подпорные и удерживающие стены); Road – дорожное полотно требует ремонта или находится в аварийном состоянии. Предварительное отображение фрагмента знаний представлено на рисунке 3.

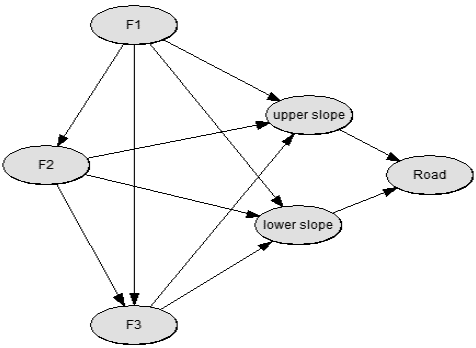


Рис. 3–Граф фрагмента знаний

Опрос экспертов, работающих в сфере геотехнического мониторинга, позволил получить субъективные оценки доверия влияния отдельных

концептов друг на друга (фрагменты знаний). В результате были получены таблицы вероятностей и условных вероятностей вершин при условии состояния их родителей, фрагменты которых представлены ниже:

F2	F="F2"		F="нет"	
F1	F1="нет"	F1="F1"	F1="нет"	F1="F1"
F3="нет"	0,2	0,15	0,1	0,05
F3="F3"	0,8	0,85	0,9	0,95

	P(lower slop)			
F2	F2="F2"			
F1	F1="нет"	F1="F1"		
F3	F3="нет"	F3="F3"	F3="нет"	F3="F3"
lower slopp = ="нет"	0,01	0,05	0,85	0,1
lower slop = ="поврежден"	0,99	0,95	0,15	0,9

Lower slope	Lower slope= ="0"		Lower slope= ="1"	
Upper slope	Upper slope= ="нет"	Upper slope= ="да"	Upper slope= ="нет"	Upper slope= ="да"
Road= ="нет"	0,95	0,3	0,1	0,02
Road= ="требует ремонта"	0,05	0,7	0,9	0,98

Полученные с помощью экспертов, оценки доверия на основе когнитивной карты оползнеопасного участка автодороги (Рис.3) использовались при построении Байесовской сети доверия для двух этапов мониторинга в программном комплексе «*Hugin*» (рис 4), которую можно назвать базой фрагментов знаний (БФЗ) в изучаемой предметной области «оползневого риска». Байесовская сеть доверия (БСД)— вероятностная модель, представленная в виде графа и состоящая из множества переменных и их вероятностных зависимостей *по Байесу:*

$$P(H/E) = \frac{P(E/H)P(H)}{P(E/H)P(H) + P(E/\bar{H})P(\bar{H})} \quad (1)$$

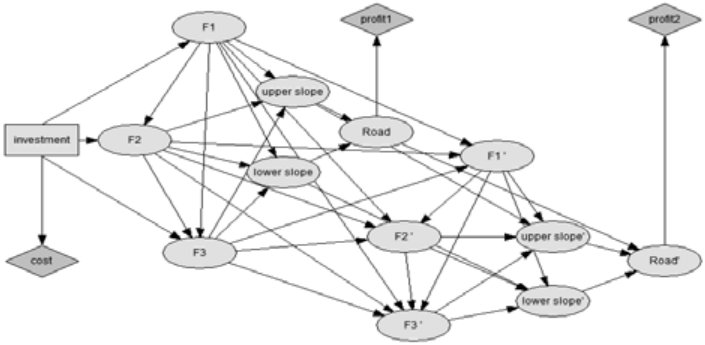


Рис. 4 – *БСД* для участка автомобильной дороги

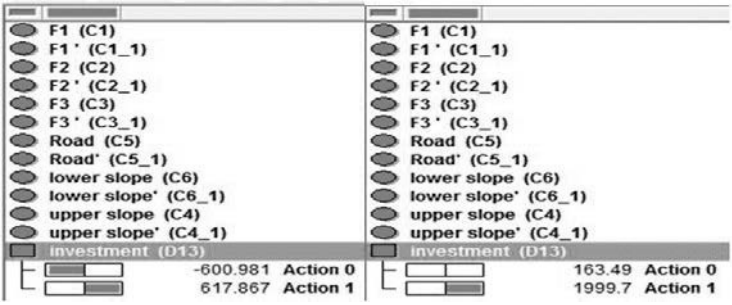


Рис. 5 – Оценка эффективности инвестиций

В нашем случае «если событие H истинно, то событие E будет наблюдаться с вероятностью P», а «если событие E уже произошло, то какова вероятность истинности H?».

Обобщение формулы на случай множества гипотез (H_1, H_2, ... , H_m) и множества независимых свидетельств (E_1, E_2, … ,E_n) (подход называют наивный Байес – *naive Bayes*):

$$P(H_i / E_1E_2 \dots E_n) = \frac{P\left(E_1E_2 \dots \frac{E_n}{H_i}\right)P(H_i)}{\sum_{k=1}^{m} P\left(\frac{E_1/ H_i)P(E_2}{H_i}\right) \dots P\left(\frac{E_n}{H_k}\right)P(H_k)}. \quad (2)$$

Полученная база фрагментов знаний может совершенствоваться, уточняться и использоваться в качестве основы для создания диаграмм влияния, позволяющих оценить необходимость противооползневых мероприятий и их эффективность (рис 5), наряду с известными процедурами оценки оползневого риска [1-4].

Литература:
1. *Безуглова Е.В.* Оползневый риск транспортных природно-технических систем: монография / Е. В. Безуглова, С. И. Маций, В. В. Подтелков. – Краснодар: КубГАУ, 2015. – 239 с.
2. *Маций С.И.* Противооползневая защита: монография. – Краснодар: АлВи-дизайн, 2010. – 288 с.
3. *Маций С.И.* Оценка оползневого риска транспортных сооружений: монография / С. И. Маций, Е. В. Безуглова, Д. В. Плешаков. – Краснодар: КубГАУ, 2015. – 120 с.
4. *Маций С.И.* Принятие решений при формировании при формировании природно-технических систем в условиях неопределенности и риска / С.И. Маций, Д.И. Кацко В сборнике: Системный анализ в проектировании и управлении. Сборник трудов XXII международной научно-практической конференции. – СПБ: СПбГПУ, 2018. С.268-273.
5. *Маций В.С.* Вариативные подходы к оценке и управлению оползневым риском транспортных систем / В.С. Маций, Д.И. Кацко. В сборнике трудов: IV Международной научно-практической молодежной конференции по геотехнике Тюмень: ТИУ, 2018. С.47-51.

Сидоренко В.Г., Кулагин М.А.

Прогнозирование совершения нарушения безопасности движения по вине локомотивной бригады с использованием современных методов машинного обучения

Аннотация: Статья посвящена вопросам определения и сбора показателей, влияющих на безопасность движения, а также расчету вероятности совершения нарушения локомотивной бригадой. В работе разработаны и проанализированы разнообразные алгоритмы машинного обучения, а именно: нейронные сети, градиентный бустинг над решающими деревьями и случайные леса.

Ключевые слова: локомотивная бригада, расчет вероятности, оценка влияния человеческого фактора, машинное обучение, искусственный интеллект

На данный момент в компании ОАО «РЖД» подавляющий объем перевозок выполняется людьми, от которых зависит высокое качество и безопасность работы железной дороги. Для того чтобы управлять целым составом требуются специалисты с высоким уровнем профессионализма. В компании ОАО «РЖД» насчитывает порядка 100 тысяч работников, управляющих локомотивом. Большинство нарушений, совершаемых

локомотивными бригадами, влечет за собой серьезные экономические потери для компании. Поэтому задача прогнозирования совершения нарушения по вине локомотивной бригады является актуальной на данный момент.

В рамках данной статьи представлен способ расчета вероятности совершения нарушения машинистом локомотива с использованием современных методов машинного обучения. Процедуру расчета вероятности можно разделить на следующие этапы:

1. Постановка задачи и определения допустимых критериев качества работы алгоритма.
2. Получение и исследование данных о машинисте.
3. Подготовка данных для алгоритмов машинного обучения.
4. Обучение и анализ качества работы разнообразных алгоритмов.
5. Проверка качества работы наилучшего с точки выбранного критерия алгоритма или композиции алгоритмов на тестовой выборке.

Схема разрабатываемой процедуры приведена на рис. 1.

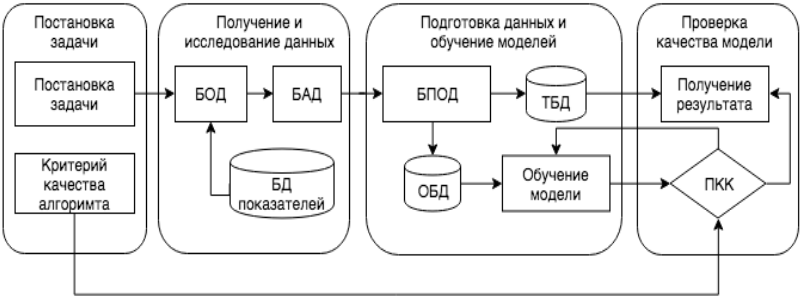


Рис. 1 – Блок-схема получения математической модели
(БОД – блок обработки данных; БАД – блок анализа данных; БД – база данных; БПОД – блок предварительной обработки данных; ОБД/ТБД – обучающая/тестовая база данных; ПКК – проверка критерия качества алгоритма)

Любое исследование начинается с постановки цели и задачи. В данной статье представлена классическая задача обучения с учителем [1]. В качестве признаков выступают показатели машиниста, собранные из различных автоматизированных систем. Меткой каждого маршрута выступает факт наличия вины машиниста в совершении нарушения (0 – вины машиниста нет; 1 – вина машиниста есть). В терминах машинного обучения можно данную задачу можно отнести к сфере задач бинарной классификация.

Критерием оценки качества алгоритма будет выступать:

– Accuracy – доля верного срабатывания алгоритма;

– AUC-ROC – площадь по ROC кривой (соотношение между долей объектов от общего количества носителей признака, верно классифицированных как несущих признак, и долей объектов от общего количества объектов, не несущих признака, ошибочно классифицированных как несущих признак) [2];
– F-мера – гармоническое среднее между Precision (доля действительно верного определения нарушения алгоритмом к общему количеству выявленных нарушений) и Recall (доля найденных классификатором нарушений относительно всех нарушений в тестовой выборке) [3].

В качестве объекта исследования был выбран машинист и все его поездки за 2017-2018 год. Машинист - это работник, осуществляющий обслуживание и управление локомотивом, ведение поезда с точным соблюдением графика движения поездов, обеспечивающий требования безопасности, безусловное выполнение установленного регламента переговоров, сохранность грузов и подвижного состава, а также рациональный режим ведения поезда при минимальном расходе топлива и электроэнергии. У машиниста было выделено порядка 50 признаков, характеризующих его работу. Все признаки машиниста можно разбить на группы:

1. Медицинские показатели.
2. История нарушений машиниста.
3. История нарушений, зафиксированных машинистом-инструктором при проверке.
4. Уровень знаний.
5. Личные показатели машинистов (депо, стаж, класс и другие).
6. Время работы и время отдыха.

В исследовании использовались базовые алгоритмы: искусственная нейронная сеть (ИНС), градиентный бустинг (ГБ), случайные леса (СЛ).

На момент написания статьи алгоритм проходил обучение на выборке размером около 500 тысяч поездок и тестировался на выборке 100 тысяч поездок. Ключевой проблемой решаемой задачи является несбалансированность обучающей выборки (рис. 2).

Из рисунка 2 можно заключить, что количество случаев с нарушениями по вине машиниста занимают около 7,5 % места в выборке (597247 – поездок без вины; 45109 – поездок с виной). Данная проблема является ключевой трудностью на пути к получению рационального математического алгоритма. К основным приемам, которые используются учеными и специалистами по анализу данных, относятся:

Поиск возможностей получения дополнительных данных о минорном классе [3].

Размножение малочисленного целевого (минорного) класса путем копирования. Количество элементов минорного класса за счет

множественного дублирования приравнивается к количеству доминирующего [3,4].

Балансирование обучающей выборки до уровня целевого класса. Количество элементов доминирующего класса приравнивается количеству объектов минорного [3,4].

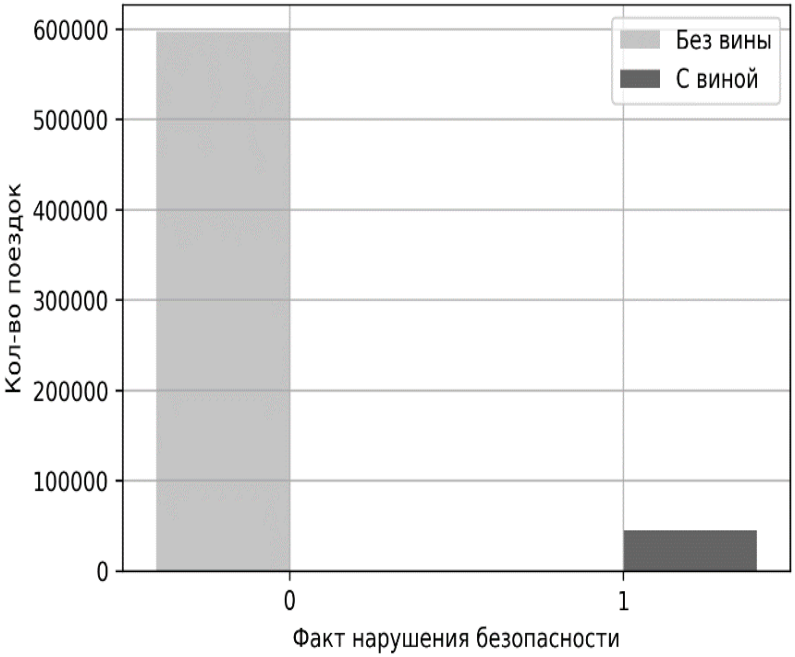


Рис. 2 – Гистограмма распределения меток в базе данных

Создание синтетических образцов. Данный способ подходит к задачам, связанным с компьютерным зрением, так как суть метода заключается в увеличении минорного класса за счет небольших изменений значений признаков объектов. Например, поворот или зеркальное отображение. В нашей задаче данный подход не имеет большого смысла [4].

Увеличение штрафа за ошибки на целевом классе. При обучении алгоритма за каждую ошибку на минорном классе штрафовать алгоритм сильнее, чем за ошибки на доминирующем [3].

Построение композиции алгоритмов и усреднение результатов обучения. Суть метода заключается в балансировании выборки, но только не один раз, как это было описано в пункте 4, а несколько, при этом каждый раз с разным набором доминирующего класса. Затем каждая выборка используется для обучения, а результаты усредняются [3].

Использование алгоритмов обучения без учителя (поиск аномалий). Зачастую, в зависимости от задачи, необязательно строить алгоритм классификации по классическому принципу. Достаточно отыскать признаки с аномальными значениями, которые и являются представителями минорного класса [5].

Увеличение числа минорного класса происходит за счет искусственной генерации новых объектов. Новые объекты генерируется путем поиска для каждого объекта k-ближайших соседей, из которых выбирается один случайным образом, а затем новый объект строится как среднее между текущим объектом и случайно выбранным [6].

В рамках данной статьи были проведены исследования с применением нескольких способов.

Результаты обучения после применения различных способов представлены в таблице 1.

Таблица 1. Сравнительная характеристика работы алгоритмов

Алгоритмы	Метрики	Результат на исходных данных, %	Результат на балансированных данных, %	Результат при увеличении числа меток, %	Результат при композиции моделей, %
ИНС	Accuracy	95,1	67,4	76,1	79,2
	F-мера	25,5	32.1	62,1	68,7
	AUC-ROC	52,5	68,6	73,2	71,2
ГБ	Accuracy	96,3	70,2	76,5	77,2
	F-мера	30,2	45.7	66,3	69,2
	AUC-ROC	56,2	76,9	72,6	70,3
СЛ	Accuracy	93,6	62,7	68,1	70,2
	F-мера	22.4	40.8	56,5	54,9
	AUC-ROC	51,0	66,2	70,8	69,6

При решении задачи бинарной классификации требуется использовать только тот способ оценки качества работы модели, который отражает объективную ситуацию. Например, в данной задаче корректнее использовать AUC-ROC и F-меру. Согласно полученным результатам, следует, что ни один способ работы с несбалансированными выборками не показывает хороший результат для данного набора данных. Отсюда следует, что проблема несбалансированной выборки остается актуальной, как минимум, для решаемой задачи.

Метод уменьшения 0-го класса до уровня 1-го приводит к тому, что мы строим вероятностную модель только на выборочной совокупности данных, которая значительно меньше всей, а это значит, что модель не видела всех данных в выборке, и в будущем появится много ложных срабатываний алгоритма.

Два последних метода показали наилучшие результаты на тестовой выборке. Причины успеха, возможно, связаны с тем, что алгоритмы используют всю выборку, но при этом сохраняется баланс классов.

Проблема несбалансированной выборки до сих пор присутствует в области машинного обучения, так как большинство данных, используемых для решения разного рода задач, имеют смещение в сторону одного доминирующего класса.

На данный момент стоит задача разработки нового или адаптации старого метода работы с несбалансированной выборкой к решаемой задаче. Кроме того, очевидно, требуется увеличение обучающей выборки.

В рамках данной статьи предложен способ обучения, поднята проблема несбалансированной выборки, а также представлен возможный алгоритм предсказания совершения нарушения безопасности движения локомотивной бригадой.

Литература:

1. *Muller* A.*C*., *Guido* S. Introduction to machine learning with Python: a guide for data scientists. O'Reilly Media, Inc., — 2016.
2. *Boyd* K., *Eng* K. H., *Page* C. D. Area under the precision-recall curve: Point estimates and condence intervals / /Joint E uropean Conference on Machine Learning an d K nowledge D iscovery i n D atabases. S pringer, B erlin, Heidelberg — 2013. — C. 451-466.
3. *Powers D.M.* Evaluation: from p recision, r ecall an d F -measure t o R OC, informedness, markedness and correlation — 2011.
4. *Lemaitre*, *Guillaume*, *Fernando Nogueira*, a nd *Christos* K. Ar idas. Imbalanced-learn: A p ython t oolbox t o t ackle t he cu rse o f i mbalanced datasets i n machine learning. T he J ournal o f M achine Learning Research 18.1— 2017. C. 559-563.
5. *He*, *Haibo*, a nd *Yunqian* Ma, ed s. I mbalanced l earning: foundations, algorithms, and applications. John Wiley & Sons, — 2013.
6. *Chawla* N., *Bowyer* K., *Hall* L., Kegelmeyer W . S MOTE: S ynthetic Minority O ver-sampling T echnique. // J ournal o f A rtificial I ntelligence Research, — 2002. — C. 321–357.

Морозов Д.В.

Алгоритм повышения надежности функционирования системы управления беспилотным летательным аппаратом

Аннотация: Алгоритм позволяет, при обнаружении отказа в контрольно-проверочной аппаратуре, произвести анализ принадлежности отказа функциональной части и реализовать соответствующие решения. Решение продолжить выполнение целевой задачи системой управления беспилотного летательного аппарата, сопровождается оптимальной глубиной самоконтроля контрольно-проверочной аппаратуры. Выбор очередной элементарной самопроверки производится на основании методики определения риска потерь. В качестве потерь используется вероятностный показатель достоверности контроля (вероятность ложного забракования). Методика решения задачи основана на использовании комбинированного метода ветвей и границ. Элементарные самопроверки являются пересекающимися по комбинаторным подмножествам элементов.

Ключевые слова: контролируемая область элементов, подозреваемая на отказ область элементов, самоконтроль, система управления, беспилотный летательный аппарат

Успех выполнения стоящих перед беспилотным летательным аппаратом (БЛА) задач зависит от безотказной работы всех бортовых систем. БЛА часто функционирует в сложной электромагнитной обстановке. Это, как следствие, привело к увеличению отказов в системе управления (СУ) БЛА. Бортовая СУ БЛА состоит из контрольно-проверочной аппаратуры (КПА), системы ее самоконтроля (ССК) и бортовой аппаратуры (БА) выполнения задач целевого применения. Представляя СУ, как многофункциональную систему, становится очевидным тот факт, что отказ не любого функционального элемента СУ БЛА ведет к невозможности выполнения задач целевого применения. В [1] поставлена задача по изменению алгоритма работы СУ БЛА в полете, в случае возникновения отказа в аппаратуре КПА.

Целью данной работы является разработка оптимального алгоритма повышения надежности функционирования, заключающаяся в изменении программы полета СУ БЛА при ее отказе, для выполнения конечных задач целевого применения. Обобщенная блок-схема оптимального алгоритма повышения надежности функционирования системы управления беспилотным летательным аппаратом (СУ БЛА) приведена на рисунке 1. В качестве исходных данных для построения алгоритма используется [2] бинарная иерархическая модель (БИМ) СУ БЛА, бинарная

диагностическая модель системы самоконтроля (БДМ ССК) КПА, время, прошедшее после проведения последнего контроля БА СУ и самоконтроля КПА и требуемый уровень вероятности выполнения задачи P^*.

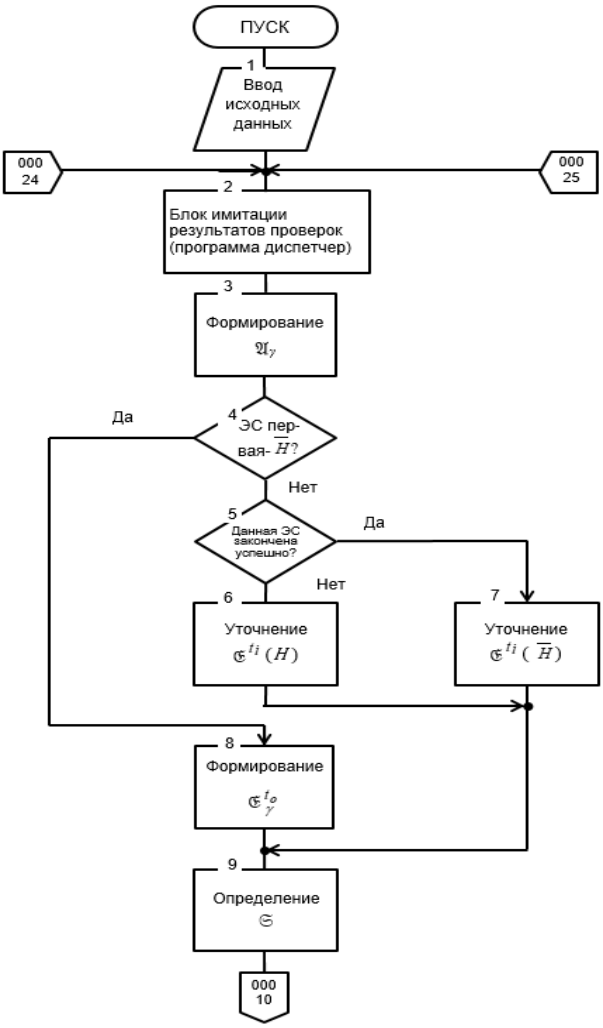


Рис. 1 – Обобщенная блок-схема алгоритма повышения надежности функционирования СУ БЛА

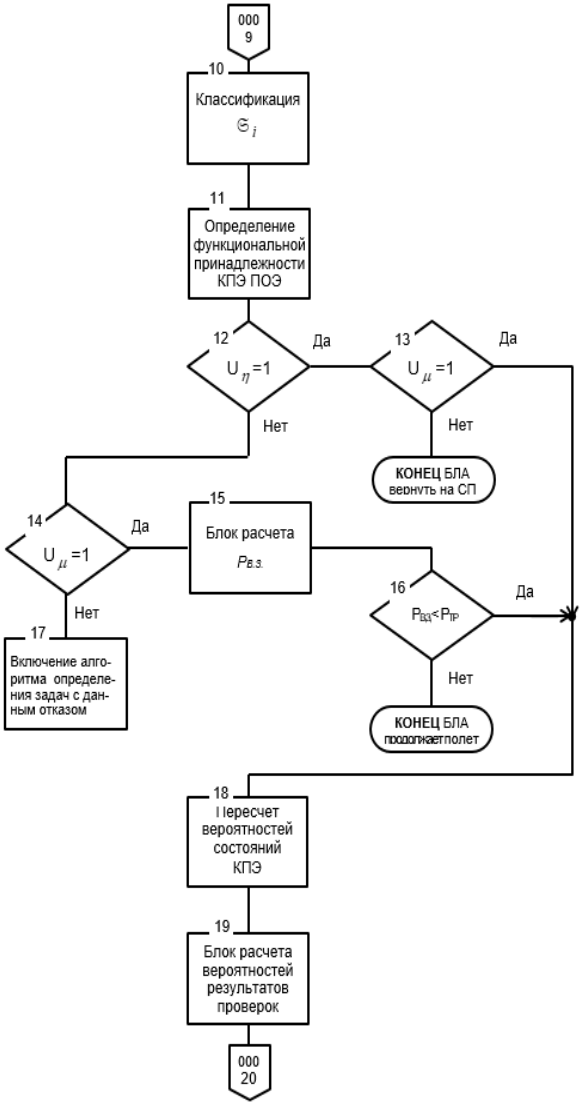


Рис. 1 – Обобщенная блок-схема алгоритма повышения надежности функционирования СУ БЛА (Продолжение)

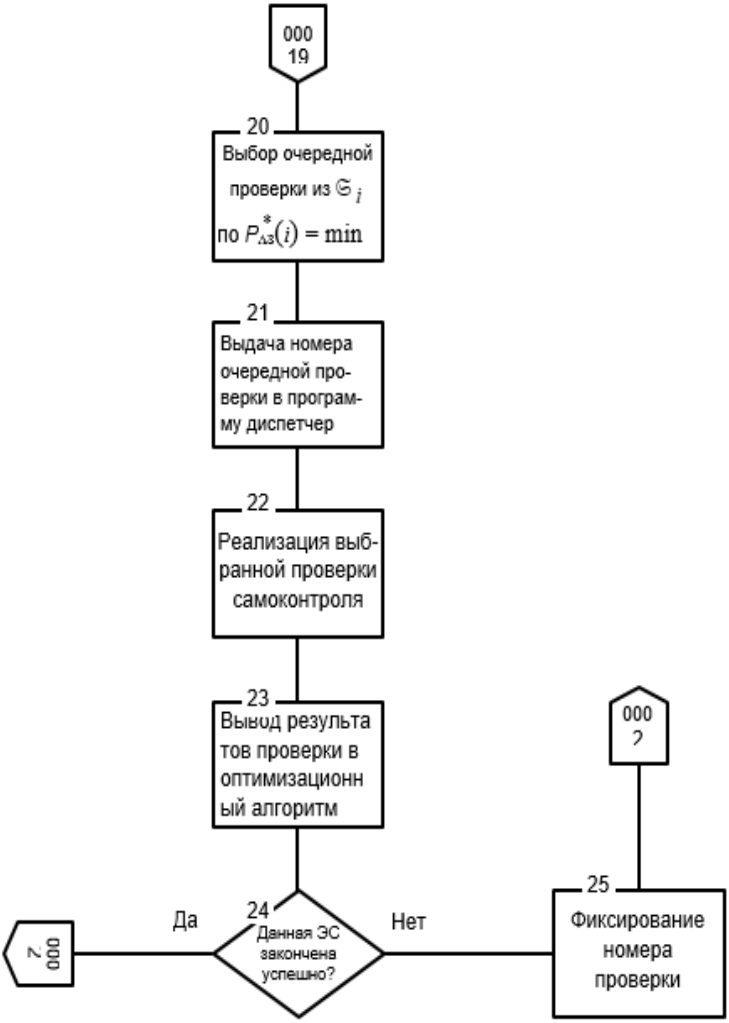


Рис. 1 – Обобщенная блок-схема алгоритма повышения надежности функционирования СУ БЛА (окончание)

1.Определение. Контролируемая область элементов (КОЭ) - совокупность (подмножество) КПЭ КПА, покрываемая *i*-ой ЭС

$\{ b_i, \ldots, b_i \} \in \mathfrak{A}_i$

2.Определение. Подозреваемая на отказ область элементов (ПОЭ) - это область КПЭ(а), образованная в результате пересечения $\bar{\mathfrak{A}}_i$ *i* - ой ЭС, в которой зафиксирован отказ с $\mathfrak{A}_j$ предыдущих ЭС

$\{ b_j \} \in \bar{\mathfrak{A}}_i \cap \mathfrak{A}_j \in \mathfrak{C}$,

где $\bar{\mathfrak{A}}_i$ КОЭ *i* - ой ЭС, в которой зафиксирован отказ;

$\mathfrak{A}_j$, $j = \overline{1, i-1}$ - КОЭ ЭС, выполненных до проведения *i* -ой ЭС и, в которых получен результат "годен".

При проведении рабочей программы полета (или самоконтроле КПА) по одной из ЭП (допустим π_γ) получен результат "не норма". В этом случае фиксируется ее номер γ и заносится в *мас.* **А.** В блоке 3 производится формирование $\mathfrak{A}_\gamma$ (КОЭ) отказовой ЭП (ЭС) – π_γ . Блок 8 осуществляет формирование одного из наблюдаемых процессов – $\mathfrak{C}_\gamma$ (ПОЭ). Из определения $\mathfrak{C}_\gamma$ [3,4] следует и алгоритм его формирования. Причем, если π_γ , γ = 1, то $\{ \bar{b}_j \} \subset \mathfrak{C}_\gamma$, $j = \overline{1, N}$. Следующим этапом работы алгоритма (блок 9), является определение $\mathfrak{S}$ (область проверок покрывающая (ОПП) ПОЭ), изменение содержания которого является вторым наблюдаемым процессом, на начальном этапе формирования алгоритма, самоконтроля КПА. В блоке 10 производится классификация ЭС на основные и вспомогательные, составляющих $\mathfrak{S}$ на данном шаге локализации отказа. В блоке 10 формируются и определяются основные ЭС (Σ = 01) и вспомогательные ЭС (Σ = 10, Σ = 11). Причем вспомогательные ЭС подразделяются на ЭС, в КОЭ, которых содержатся только $\{ b_j \} \in$ *АК* КПА (10) $j = \overline{1, K}$ и $\{ b_j \} \in$ *АК*, *АПП* КПА (11), $j = \overline{1, K}$. В блоке 11 производится определение функциональной принадлежности КПЭ, составляющих $\mathfrak{C}^{t_i}$. Если результат логического суммирования 01, это означает, что $\{ b_j \} \in \mathfrak{C}_\gamma^{t_o}$ (на начальном этапе локализации отказа в КПА), $j = \overline{1, u}$, т.е. $\mathfrak{C}_\gamma^{t_o} \in$ *АПП* КПА. При результате 10 – $\mathfrak{C}_\gamma^{t_o} \in$ *АК* КПА, а если результат равен 11, то ПОЭ состоит из $\{ b_j \} \in$ *АК, АПП* КПА. На следующем этапе работы алгоритма самоконтроля КПА, на основании анализа функциональных составляющих $\mathfrak{C}_\gamma^{t_o}$, производится принятие

решения. На основании анализа результатов логического суммирования в блоках 12, 13, 14, 15, 16 принимаются следующие решения:

1. Если Σ = 01, d_3^{01} (решение №1. Прекратить проверки и забраковать КПА);

2. Если Σ = 10, d_n^{10} (решение 2. Продолжить локализацию отказа)

3. Если Σ = 11, решение 2.

Выводы

Разработан алгоритм повышения надежности функционирования СУ БЛА. На каждом цикле выполнения алгоритма наблюдаемыми областями являются ПОЭ и ОПП. В качестве потерь принимается вероятность ложного забракования КПА по выполняемой ЭС, выбираемой из области ОПП ЭС, покрывающую подозреваемую на отказ область комбинаторных подмножеств элементов. Применение алгоритма позволяет решить задачу определения оптимальной глубины локализации отказов, с учетом пересечения элементарных самопроверок и применить гибкий алгоритм функционирования системы управления беспилотным летательным аппаратом в полете, для выполнения конечной задачи целевого применения.

Литература:

1. *Морозов Д.В*. Методика повышения надежности функционирования системы управления летательного аппарата// V Международная научно-практическая конференция ITS Forum-Kazan «Современные проблемы безопасности жизнедеятельности: интеллектуальные транспортные системы и ситуационные центры». 27–28 февраля 2018 г. – С.123–138.
2. *Морозов Д.В*. Бинарная иерархическая модель системы управления беспилотного летательного аппарата. Системы управления беспилотными космическими и атмосферными летательными аппаратами: Тезисы докладов IV научно-технической конференции. – М.: МОКБ «Марс», 2017. – С. 132–133.
3. *Морозов Д.В.* Методика определения потерь в решении задач повышения надежности функционирования системы управления беспилотного летательного аппарата в полете//Труды Международного симпозиума надежность и качество (Пенза, 21–31 мая 2018 г.). – 2018. – т. 1. – С.139–144.

Пицык В.В., Суховерхова Л.В.

Обоснование информационных свойств извещателей в системах пожарной сигнализации

Аннотация: Описаны процедура обоснования порога срабатывания пожарных извещателей на основе свойств преобразования случайных процессов в линейных и нелинейных устройствах и процедура обоснования точности фиксации значения полезного сигнала, несущего в себе информацию о факте возникновения очага пожара, пользуясь интервальной формой выражения точности.

Ключевые слова: пожарный извещатель, порог срабатывания, случайный процесс, точность измерения

Важным фактором повышения эффективности эксплуатации систем пожарной сигнализации является совершенствование информационных свойств извещателей. Ниже рассматривается метод их обоснования.

Вначале изложим процедуру обоснования порога их срабатывания. Будем рассматривать пожарный извещатель, как простое линейное устройство – ограничитель с порогом насыщения a, которое осуществляет преобразование во времени t входной величины $z(t)$ с помощью линейного оператора [1,2]:

$$F\left[z(t)\right]=\begin{cases} -a \text{ при } z(t)<-a, \\ z(t) \text{ при } \left|z(t)\right|<a, \\ +a \text{ при } z(t)>a. \end{cases} \qquad (1)$$

Если значения a становятся бесконечными, то в пределе функция $F\left[z(t)\right]$ будет линейной, и можно считать, что такое устройство пропустит входной сигнал $z(t)$ без искажения. И тогда корреляционная функция $K_w(t_1,t_2)$ выходной величины $w(t)=F\left[z(t)\right]$ будет совпадать с корреляционной функцией $K_z(t_1,t_2)$ входной величины $z(t)$.

Поскольку пожарный извещатель имеет конечное значение порога a, то обоснование конкретных его значений является важной задачей, решаемой на стадии обоснования технического задания на его разработку.

Опишем задачу. Пусть на вход устройства поступает сигнал:

$$z(t)=x(t)+y(t), \qquad (2)$$

представляющий собой аддитивную смесь полезного сигнала $y(t)$, как неслучайной функции, описывающей изменение во времени контролируемого параметра, и стационарного гауссова случайного процесса $x(t)$ с плотностью вероятности

$$f(t)=\frac{1}{\sqrt{2\pi}\sigma_x}\mathrm{e}^{-\frac{t^2}{2\sigma_x^2}}, \qquad (3)$$

где σ_x – известное среднее квадратическое отклонение случайной величины $x(t)$.

Рассматривая полезный сигнал $y(t)$ как неслучайную функцию, можно понимать под линейным оператором (1) линейный однородный оператор. Поэтому корреляционная функция $K_w(t_1,t_2)$ его выходной величины $w(t)$ не меняется от прибавления к случайной величине $x(t)$ неслучайного слагаемого $y(t)$ [3]. И так как абсолютная величина сигнала на выходе устройства не может превышать величины a, то с некоторой (ненулевой) вероятностью можно считать, что эта величина может принимать значения $\pm a$.

Отношение среднего квадрата выходного сигнала устройства к среднему квадрату входного сигнала можно выразить равенством [2]:

$$\frac{K_w(0)}{\sigma_x^2}=x_a^2\left[1-P(x_a)\right]+P(x_a)-\sqrt{\frac{2}{\pi}}x_a\,\mathrm{e}^{-\frac{x_a^2}{2}}, \qquad (4)$$

где $x_a=\dfrac{a}{\sqrt{\varphi_{11}}}$; $P(x_a)=\sqrt{\dfrac{2}{\pi}}\int\limits_0^{x_a}\mathrm{e}^{-\frac{x^2}{2}}dx$; $\varphi_{11}=M\left[x(t_1),x(t_1)\right]$; M – знак математического ожидания.

И тогда для заданного отношения $\dfrac{K_w(0)}{\sigma_x^2}$ и гауссова распределения случайного процесса $x(t)$ с известным корреляционным моментом ρ можно определить порог насыщения a пожарного извещателя.

Например, для отношения $\dfrac{K_w(0)}{\sigma_x^2}=0,04$, коэффициента корреляции $\rho=1$ и элемента $\varphi_{11}=1$ корреляционной матрицы случайного процесса $x(t)$ величина порога будет равной $a\approx 0,2$ [2].

Таким образом, пользуясь свойствами преобразования случайных процессов в линейных и нелинейных устройствах [1-3], можно обосновать

для требуемого значения величины $\frac{K_w(0)}{\sigma_x^2}$ пределы срабатывания извещателей в системе пожарной сигнализации.

Рассмотрим далее процедуру обоснования точности фиксации (измерения) значения полезного сигнала, несущего в себе информацию о факте возникновения очага пожара, пользуясь интервальной формой выражения точности.

Для этого зададим интервал значений величин α и β ($[\alpha,\beta]\subseteq[-a,a]$), в котором с заданной наперед вероятностью P_0 должны находиться значения величины $w(t)$ на выходе порогового устройства, и будем считать, что требования к точности выполняются, если выполняется соотношение $P_0 \le P(-a<\omega<a)$, где $P(A)$ обозначает вероятность события A.

Опишем задачу. Пусть на вход устройства сравнения поступает гауссов случайный процесс, описываемый известной плотностью распределения $f(w,K_w(0))$ его значений $w(t)$ с известным параметром $K_w(0)$. Выходная величина $\tilde{w}(t)$ устройства сравнения представляет собой аддитивную смесь полезного сигнала $w(t)$ и его погрешности измерения $\Delta w=\tilde{w}-w$.

Случайная погрешность Δw распределена по известному закону $\varphi(\Delta w,\sigma)$ с неизвестным заранее, в общем случае векторным, параметром σ, характеризующим точность устройства сравнения (иначе, результата измерения).

Задача обоснования точности измерения заключается в нахождении параметра σ распределения $\varphi(\Delta w,\sigma)$, удовлетворяющего соотношению

$$\int_{-a}^{a}[\int_{\alpha}^{\beta} f(w,K_w(0))*\varphi(\Delta w,\sigma)dw]d\tilde{w}=\int_{\alpha}^{\beta} g(\tilde{w},K_w(0),\sigma)d\tilde{w}=P_0, \qquad (5)$$

где $g(\tilde{w},K_w(0),\sigma)$ – функция плотности распределения результатов измерения $\tilde{w}$, как композиция законов распределения $f(w,K_w(0))$ и $\varphi(\Delta w,\sigma)$.

В частности, для нормальных распределений значений w и Δw:

$$f(w,K_w(0))=\frac{1}{\sqrt{2\pi K_w(0)}\sigma}e^{-\frac{(w-m_w)^2}{2K_w(0)}}, \qquad (6)$$

$$\varphi(\Delta w,\sigma)=\frac{1}{\sqrt{2\pi}\sigma}e^{-\frac{(\Delta\omega-m_{\Delta w})^2}{2\sigma^2}} \quad (7)$$

с параметрами $m_w,\sigma,m_{\Delta W},\sigma_{\Delta\omega},K_w(0)$ и $m_{\Delta\omega},\sigma_{\Delta\omega}$ их композиция описывается плотностью распределения

$$g(\tilde{w},K_w(0),\sigma)=\frac{1}{\sqrt{K_w(0)+\sigma^2}}\frac{1}{\sqrt{2\pi}}e^{-\frac{[\tilde{\omega}-(m_w+m_{\Delta w})]^2}{2(K_w(0)+\sigma^2)}}. \quad (8)$$

Таким образом, пользуясь описанными процедурами, можно обоснованно предъявлять требования к свойствам пожарных извещателей для достижения требуемого качества функционирования систем пожарной сигнализации.

Литература:

1. *Пугачев В.С.* Теория случайных функций. М.: ГИФМЛ., 1960. - 884 с.
2. *Лэнинг Дж., Бэттин Р.Г.* Случайные процессы в задачах автоматического управления. М.: Изд-во ИЛ., 1958. - 3884 с.
3. *Вентцель Е.С.* Теория вероятностей: Учеб. для вузов. М.: Высш. шк., 2002. - 575 с.

Плотников Н.И.

Проблемы идентификации предмета безопасности авиации

Аннотация: Вопросы идентификации предмета безопасности авиации являются актуальной проблемой современной гражданской авиации. Понятийная ясность предмета безопасности полетов необходима для потребителя услуг воздушных перевозок. Для выполнения задачи предлагается подход и методологические требования логики в теории понятия.

Ключевые слова: безопасность, нормативное регулирование, гражданская авиация, безопасность полетов

Содержание проблемы. Исследования и разработки современных методов управления безопасностью и экономической эффективностью в мировой практике ВТ направлены на выявление так называемых факторов опасности (ФО) и установление авиационных событий (АС), расследование авиационных происшествий (АП), исследование статистики. Данный подход основан на причинной (каузальной) логике установления связей причин и следствий исходов деятельности, называемые АС. Подобные логики имеют неопределенные выводы и наименования неклассических, парадоксальных, основанных на

ограниченности знаний, нечеткости объектов предметного мира. Наименования предметной деятельности составляются не только для внутреннего использования производителя продукции и услуг, а главным образом для потребителя. Потребитель воздушных перевозок имеет право знать, как различать качество услуги, предлагаемой авиаперевозчиком в полете, и как можно определить качество услуги до полета.

Определения безопасности авиации формировались в понятиях «безопасность полетов» (БП) и «авиационная безопасность» (АБ). До настоящего времени мировое авиационное сообщество ведет поиск приемлемых определений безопасности в авиации, что подтверждается постоянными поправками формулировок в стандартах ИКАО по безопасности полетов (БП), авиационной безопасности (АБ) [1, 2, 3]. Понимание важности безопасности полетов подтверждается тем, что основные определения доступны общественности на сайте Минтранса РФ. Обзор проблемы показывает несводимость словарного описания и нормативной базы предмета безопасности, безопасности транспорта и безопасности в авиации.

Проблема определений безопасности авиации. Определение ИКАО «Авиационная безопасность» [2]: 1. Комплекс мер, а также людские и материальные ресурсы, предназначенные для защиты гражданской авиации от актов незаконного вмешательства. 2. Состояние защищённости авиации от незаконного вмешательства в деятельность в области авиации. Понятие «акт незаконного вмешательства» (АНВ) означает противоправные действия, в том числе террористические акты, которые могут угрожать безопасности ТК. АНВ определяются как «акты или попытки совершения актов, создающие угрозу безопасности гражданской авиации и ВТ» и подразделяются на шесть групп.

Определение безопасности полетов. В отечественной практике длительное время использовалась формулировка НПП ГА-85: «Безопасность полетов - комплексная характеристика ВТ и авиационных работ, определяющая способность выполнять полеты без угрозы для жизни и здоровья людей». Исследуем формулировку. Словосочетание «комплексная характеристика» содержит два отвлеченных понятия: «комплексная» и «характеристика». Понятие характеристики несет смысл общего описания свойств (величин) и состояний объекта. Понятие комплексной, то есть, сложной деятельности еще более делает словосочетание размытым. Данное обобщение отождествляет полет со всей деятельностью. Полет является концентрированным воплощением всех процессов участников ТК. Однако в хозяйственной деятельности организации существует другие процессы и функции, которые в ином содержании не менее «комплексно характеризуют» качество деятельности: стратегическое управление, администрирование, управление персоналом,

коммерция, финансы, информационные технологии. Вторая часть формулировки «способность выполнять полеты без угрозы для жизни и здоровья людей» также составляет проблему. Слово *способность* более применимо к субъекту деятельности, к людям, а не к сложным объектам, каким является ВТ. Выполнять полеты без угрозы, то есть, гарантировать исключение любого ухудшения качества деятельности, принципиально невозможно.

Определения БП ИКАО. Международным сообществом ИКАО приняты несколько последовательно корректируемых определений. Руководство по управлению безопасностью полетов (РУБП) ИКАО Doc 9859 AN/460-2006: «Безопасность полетов - состояние, при котором риск причинения вреда лицам или нанесения ущерба имуществу снижен до приемлемого уровня и поддерживается на этом либо более низком уровне посредством непрерывного процесса выявления источников опасности и контроля факторов риска» [4]. РУБП ИКАО Doc 9859 AN/474-2009: «Безопасность. Состояние, при котором возможность причинения ущерба лицам или имуществу снижена до приемлемого уровня и поддерживается на этом или более низком уровне посредством постоянного процесса выявления факторов опасности и управления факторами риска для безопасности полетов» [4]. Приложение 19 к Конвенции ИКАО 2013 года [3]: «*Безопасность полетов*: состояние, при котором риски, связанные с авиационной деятельностью, относящейся к эксплуатации воздушных судов или непосредственно обеспечивающей такую эксплуатацию, снижены до приемлемого уровня и контролируются».

Проблемы определений. Размытость, нечеткость определений понятий безопасности имеет крайне негативные последствия для деятельности ГА. В современных классификациях и нормативных определениях понятий безопасности авиации не соблюдаются логические законы деления понятий по объему на классы: непрерывность, несовместимость видов класса, совпадение объемов класса и суммы видов, наличие основания (признака) деления.

Определение ИКАО авиационной безопасности в [3] состоит из двух пунктов, содержание которых по смыслу идентичны и практически сводятся к защите от АНВ. Понятие «авиация» является понятием несравненно большего объема, чем понятие АНВ. АНВ направлены на производство полетов, а также в части аэропортовой инфраструктуры. Наибольшая часть всех процессов авиации, в частности в авиастроении, не может быть объектом АНВ. Таким образом, свертка понятий АБ к АНВ не имеет теоретических и логических оснований.

Рассмотрим определения безопасности полетов. Определения [3, 4] тождественны. Только во втором изменена последняя часть предыдущего содержания: «…посредством постоянного процесса выявления факторов

опасности и управления факторами риска для безопасности полетов». Совокупность предлагаемых стандартами понятий: *безопасности, приемлемости, риска, ущерба, выявления или управления факторами на этом или более низком уровне* – собранных в одной формулировке, до сих пор обсуждается авиационной общественностью.

В [3] также очевидны размытые формулировки, например: «*Инцидент*: любое событие, кроме авиационного происшествия, связанное с использованием ВС, которое влияет или могло бы повлиять на безопасность эксплуатации. *Показатель эффективности обеспечения безопасности полетов*: основанный на данных параметр, используемый для мониторинга и оценки эффективности обеспечения безопасности полетов. *Риск для безопасности полетов*: предполагаемая вероятность и серьезность последствий или результатов опасности». Что означает «риск для (?) безопасности…», «…последствий или результатов (?) опасности», «состояние, при котором риск…», «показатель …, основанный на данных параметр…». Параметр и показатель – разные понятия. Пара́метр (от др.-греч. παραμετρέω — соразмеряю) — величина, значения которой служат для различения групп элементов некоторого множества между собой; Параметр. Величина, используемая в описании распределения вероятностей некоторой случайной величины (ГОСТ Р 50779.10-2000); π – характеристика свойств и состояний объекта. Пример.: скорость движения, температура, давление, масса. Показатель: (σ) структурные количественные характеристики и степень проявления параметра какого-либо свойства объекта. Пример: свойство ЛА перемещаться в трехмерном пространстве структурируется на параметры: направление, высота, скорость. Параметр скорости структурируется: скорость взлета, скорость набора высоты, скорость снижения, скорость посадки.

Таким образом, предписания ИКАО «Стандарты и рекомендованная практика» в данном изложении представляют собой непреодолимый барьер понимания как исследователям, так и практикам ВТ.

Обсуждение. Определения сформированы в *концепции приемлемого уровня рисков полетов.* Введение данной концепции отвечает необходимости использовать подход, основанный на показателях, *уровнях* и *требованиях* безопасности. Показатели являются мерой результатов, достигнутых в безопасности полетов. В настоящее время приняты четыре основных и четыре дополнительных показателей, которые показывают меру ущерба уже свершившихся происшествий. Под уровнем понимается достигнутое состояние, рассчитываемое как совокупность показателей. Для достижения соответствующих показателей безопасности и заданных уровней безопасности полетов устанавливаются требования. Они включают эксплуатационные процедуры, технические средства, системы и программы, для которых устанавливаются показатели.

Мы рассматриваем назначение (качества, свойства) ТК в параметрах или состояниях безопасности, надежности, риска. Совокупность этих трех важнейших понятий в настоящее время составляет дефицит современных теоретических разработок и серьезную теоретическую проблему. Пусть множество хозяйственных функций авиаперевозчика описываются линейной функцией

$W(w_1x_1, w_2x_2, \dots, w_ix_i, \dots, w_nx_n)$,

где w_i и x_i – функция и вводимая переменная i-й структуры бизнеса.

Приемлемые и задаваемые уровни (levels) безопасности полетов являются тождественным целям и задачам общей деятельности авиакомпании. Уровень может быть рассчитан натуральным числом $\bar{L}$. Установленное число показателей (performances) также рассчитывается четким значением $\bar{P}$. Требования (requirements) $\tilde{R}$ - нечеткие величины, являются рекомендациями к разработке программ безопасности и исключительной ответственностью авиаперевозчиков. Иначе:

$\bar{P}\{\tilde{R}(W)\}: \rightarrow \bar{L}$.

В данном выражении предписывается достижение уровня безопасности одного процесса одной функции производства (полетов) через наблюдение ограниченного числа показателей, формируемых нечеткими требованиями всех процессов и функций. То есть, наблюдение единичного через общее. Авиаперевозчику необходимо решать задачу: структурировать хозяйственные функции таким образом, чтобы их любое множество $определенно$ сводилось к показателям и уровням безопасности.

Таким образом, совокупность проблемы идентификации предмета безопасности в авиации, понятийных описаний, определений и терминов состоит в дефиците теоретических разработок, следствием которого является нормативная нечеткость стандартов безопасности в авиации.

Решение проблемы и задачи. Задачей по разрешению проблемы является идентификация предмета безопасности авиации путем логического анализа и установления определений ключевых понятий безопасности авиации: безопасность, авиация, полет. Для выполнения задачи излагаются методологические требования логики к объемам и содержанию, видам и отношениям понятий, к определению понятия. Составляется предварительная логическая оценка понятий безопасности, что позволяет установить их родовидовые отношения и определения [7].

Литература:

1. ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты. - М.: Стандартинформ, 2006.
2. Приложение 17 к Конвенции о международной гражданской авиации. Безопасность. Защита международной гражданской авиации от актов незаконного вмешательства. – Монреаль: ИКАО, 2011. – 62 с.

3. Приложение 19 к Конвенции о международной гражданской авиации. Управление безопасностью полетов. – Монреаль: ИКАО, 2013. – 44 с.
4. Руководство по управлению безопасностью полетов (РУБП) Doc 9859 AN/460 ИКАО. - 2006. – 364 с.
5. Руководство по управлению безопасностью полетов (РУБП) Doc 9859 AN/474 ИКАО. – 2009. – 318 с.
6. ГОСТ-Р 53480-2009. – Надежность в технике. Термины и определения. - М.: Стандартинформ, 2010.
7. *Плотников Н.И.* Ресурсы безопасности транспортных комплексов. Монография. – Новосибирск: ЗАО ИПЦ «АвиаМенеджер», 2013. – 286 с.
8. Скачать: http://aviam.org/images/sampledata/book/pilot_resources.pdf.

Анохин А.М.

Проблемы надежности измерительных преобразователей

Аннотация: Рассмотрены ключевые проблемы, связанные с развитием измерительно-преобразовательной техники в направлении повышения качества физических измерений и обеспечения метрологической надежности измерительных преобразователей (датчиков) физических величин. Показана первостепенная роль метрологических характеристик первичных преобразователей (сенсоров) в обеспечении качества измерений. Предложен вариант использования термодатчика в медицинской практике.

Ключевые слова: сенсорезистор, пороговый переключатель, самонагрев, терморегулирование, измерительный ток.

Введение.

Качество физических измерений оценивается по степени присутствия в результатах измерений систематических погрешностей методического и инструментального происхождения. Особенно опасными среди них являются те погрешности, которые имеют неисключаемый или трудно исключаемый характер. Они требуют послеоперационной (после процедур наблюдения) корректировки с применением методов рандомизации или расчетов по аппроксимирующим моделям. При этом очевидно, что чем упрощеннее модель, тем большую методическую погрешность привносит моделирование в результаты измерений. Но, чем сложнее и адекватнее модель, тем сложнее и дороже аппаратно-компьютерное обеспечение, а также длительнее процесс измерения.

Такого рода взаимные альтернативы влияют на направленность процесса дальнейшей компьютеризации в технологиях физических

измерений. В этом контексте выявлена тенденция – динамика развития электронной сенсорики на современном этапе ориентирована главным образом на расширение и совершенствование за счет компьютерных технологий разного рода сервисных возможностей. Это микропроцессорная обработка измерительного сигнала, его унификация и введение в интеллектуальную измерительную систему, компьютерный анализ измерительной информации, ее отображение на дисплее и. т. д.

Объясняется такое положение тем, что абсолютное большинство применяемых в электронной сенсорике первичных преобразователей является сенситивными резисторами, то есть резисторами, активное сопротивление которых чувствительно к измеряемой физической величине какой-либо природы.

Традиционно сенситивные резисторы включают в цепь измерительного моста и по характеру изменения рабочего тока резистора, модулируемого воздействием физической величины, судят об этой физической величине. То есть, физическим носителем измерительного сигнала традиционно является рабочий ток сенсорезистора. При этом достаточный уровень мощности сигнала первичного преобразователя определяется величиной рабочего измерительного тока. Это приводит к выделению в преобразователе тепловой энергии, т.е. к его самонагреву и росту избыточной температуры. Фактор самонагрева особенно негативен в плане обеспечения качества метрологических характеристик и функциональной надежности измерительных преобразователей. Его последствия таковы:

- тепловая инерционность, то есть потребность в дополнительном времени выхода на установившийся тепловой режим работы преобразователя, соответствующий заданному уровню мощности измерительного сигнала;
- температурный «смаз» характеристики преобразования, то есть неуправляемый переход рабочей точки с одной характеристики на другую в температурном семействе характеристик при изменении уровня (мощности) измерительного сигнала;
- повышение порога чувствительности и общей погрешности измерения вследствие увеличения тепловых и токовых шумов преобразователя;
- влияние повышенной (избыточной) температуры первичного преобразователя на температуру измеряемой среды или объекта в точке измерения, искажающее объективность показаний;
- ускорение процесса старения структуры первичного преобразователя, интенсификация отказов в его работе и общее снижение достоверности результатов измерений.

Перечисленные факторы приводят к определенным трудностям в развитии непосредственно сенсорных функций измерительных

преобразователей и главной проблемой, препятствующей улучшению их метрологических характеристик, является фактор самонагрева первичного преобразователя рабочим, т.е. измерительным током.

В контексте данной проблемы эффективным представляется путь исключения систематических погрешностей измерений еще до начала измерений, т.е. на этапе проектирования измерительных средств. В работе предпринята попытка практической реализации такого подхода к построению измерительных преобразователей.

Для этого предлагается:

- отказаться от использования рабочего тока первичного преобразователя в качестве физического носителя измерительной информации, то есть в качестве информативного параметра измерительного сигнала;
- использовать в качестве информативного параметра измерительного сигнала преобразователя порогового потенциала переключения бистабильной полупроводниковой структуры из закрытого состояния в открытое.
- применить в качестве бистабильных полупроводниковых структур схемы негатронов с переключательной вольтамперной характеристикой S-типа (однопереходные транзисторы, S-диоды, тиристоры и схемы транзисторно-резисторных эквивалентов тиристора);
- исследовать зависимости порога переключения S-негатрона от воздействия физических величин различной природы и применить их для построения измерительных преобразователей;
- организовать импульсный режим измерения путем опроса состояния проводимости S-негатрона нарастающими по амплитуде счетными импульсами со стробированием по пороговой амплитуде.

1. Самонагрев - ключевая проблема качества измерительных преобразователей.

Традиционно, сенситивные резисторы включают в цепь измерительного моста и по характеру изменения рабочего тока резистора, модулируемого воздействием физической величины, судят об этой физической величине. То есть, физическим носителем измерительного сигнала традиционно является рабочий ток сенсорезистора. При этом мощность измерительного сигнала должна быть достаточной для выполнения двух условий – обеспечения необходимого соотношения сигнал/шум (условие помехоустойчивости) и обеспечения уверенного восприятия сигнала схемой вторичной обработки.

Для увеличения мощности измерительного сигнала и повышения крутизны характеристики преобразования сигнал первичного преобразователя усиливают. Но при этом повышается общий порог

чувствительности измерительного преобразователя и растет суммарная погрешность измерения за счет шумов, вносимых усилителем. Увеличение мощности непосредственно первичного измерительного сигнала за счет увеличения тока первичного преобразователя приводит к дополнительному повышению уровня поглощаемой им мощности, т.е. к самонагреву и росту избыточной температуры. Фактор самонагрева особенно негативен в плане обеспечения качества метрологических характеристик и функциональной надежности измерительных преобразователей. Его последствия таковы:

- тепловая инерционность выхода на установившийся тепловой режим работы преобразователя;
- температурный «смаз» характеристики преобразования, то есть неуправляемый переход рабочей точки с одной характеристики на другую в температурном семействе характеристик при изменении уровня (мощности) измерительного сигнала;
- повышение порога чувствительности и общей погрешности измерения вследствие увеличения тепловых и токовых шумов преобразователя;
- влияние повышенной (избыточной) температуры первичного преобразователя на температуру измеряемой среды или объекта в точке измерения, искажающее объективность показаний;
- ускорение процесса старения структуры первичного преобразователя, интенсификация отказов в его работе и общее снижение достоверности результатов измерений.

Все вышеперечисленные факторы приводят к определенному застою в развитии непосредственно сенсорных функций измерительных преобразователей и ключевой проблемой, препятствующей улучшению их метрологических характеристик, является эффект самонагрева первичного преобразователя рабочим, т.е. измерительным током.

2. Методика порогово-переключательной потенциометрии на сенсорных S-негатронах.

Бистабильное состояние в работе присуще полупроводниковым приборам класса «негатрон», то есть приборам на вольтамперной характеристике (ВАХ) которых имеется участок с отрицательным дифференциальным сопротивлением [1]. Среди них различают Λ-, N- и S-типы в зависимости от формы ВАХ. В качестве сенсорной бистабильной структуры целесообразно использовать S-негатроны, на ВАХ которых начальный участок высокоомный (соответствует закрытому состоянию) и протяженный.

К подклассу S-негатронов относятся S-диоды, однопереходные транзисторы (ОПТ), тиристоры и их транзисторно-резисторные аналоги.

Традиционная область применения S-негатронов по их прямому функциональному назначению – построение разного рода генераторных схем, а также силовых переключателей на тиристорах [2]. По этой причине разработчики аппаратуры применяли к ним всевозможные приемы температурной стабилизации характеристик и в первую очередь температурной стабилизации порогового потенциала переключения. Однако, если вместо обеспечения температурной инвариантности, еще более активировать температурную зависимость порога переключения, то таким образом можно получить температурочувствительный пороговопереключательный первичный преобразователь. Его удобно и логично назвать «свитч-сенсор». Такого рода температурные и световые свитч-сенсоры были совместно разработаны московскими институтами ИПУ РАН и ГИ-РЕДМЕТ на базе технологии S-диода. Они обладают уникальной чувствительностью, в несколько раз превышающей чувствительность лучших аналогов (за это качество удостоены множества высших наград на международных форумах), и вполне могут быть применены для построения на их основе измерительных преобразователей нового типа.

Заключение.

Рассмотрены современные методы совершенствования по следующим направлениям:

- в метрологическом аспекте – повышения чувствительности и линейности (главных факторов статической точности), снижения инерционности и повышения быстродействия (главного фактора динамической точности), повышения соотношения сигнал/шум (фактора помехоустойчивости), повышения режимной стабильности, отказоустойчивости и долговечности (факторов метрологической надежности) и расширения динамического диапазона;
- в эксплуатационном аспекте – унификации (способности к встраиванию в универсальные информационно-измерительные системы), повышения технологичности, снижения себестоимости и массогабаритных показателей.

Внедрение прецизионного цифрового термометра в биомедицинское приборостроение позволит реализовать на практике потенциал уникальных диагностических и лечебных возможностей методов хронобиологии, например, создать сеть высокоэффективных мобильных автоматизированных медико-биологических комплексов (АМБК) (по типу службы скорой помощи) для массовой экспресс-диагностики и терапии среди населения [3].

Литература:
1. *Биберман Л.И.* Широкодиапазонные генераторы на негатронах. – М.: Радио и связь, 1982.
2. *Кравченко А.М., Анохин А.М.* Новый подход к построению терморегуляторов на основе S-негатрона // Датчики и системы. 2013. № 1. С. 34-38.
3. *Анохин А.М., Кравченко А.М.* Прецизионный термомониторинг в медицинских задачах массовой экспресс диагностики / Труды 3-й Международной конференции “Управление развитием крупномасштабных систем“ (MLSD-2009, Москва). М.: ИПУ РАН, 2009. С. 412-420.

Сомов С.К.

Резервирование взаимосвязанных массивов данных в распределенных системах обработки данных

Аннотация: В работе рассмотрены вопросы применения резервирования информации в распределенных системах обработки данных, функционирующих на основе компьютерных сетей, с целью повышения безопасности и производительности их работы. Рассмотрены проблемы и задачи оптимизации резервирования массивов данных в распределенных системах с учетом их взаимосвязи между собой.

Ключевые слова: безопасность распределенных систем, резервирование взаимосвязанных массивов данных, компьютерные сети

Распределенные системы обработки данных (РСОД) представляют собой сложные аппаратно-программные комплексы. Компоненты этих систем как правило распределены на больших расстояниях друг от друга и объединяются единую систему программными и техническими средствами компьютерных сетей.

Во время работы РСОД в силу различных причин могут возникать негативные инциденты, которые могут приводить к возникновению искаженных данных, ошибочным результатам решения задач и обработки запросов. В самом неблагоприятном случае последствия серьезных инцидентов могут привести к невозможности нормального функционирования системы, т.е. к отказу и даже потере работоспособности системы.

Эффективным методом повышения безопасности и работоспособности систем обработки данных является применение информационной избыточности (создание и хранение резервных данных) [1]. В РСОД основным методом обеспечения сохранности данных служит метод резервирования, который предполагает использование следующих видов избыточности: создание и хранение копий массивов данных и/или создание и хранение предысторий массивов данных (предыдущие версии массива вместе с журналами их изменений).

В работе [2] представлены особенности и сформулированы задачи оптимального резервирования в компьютерных сетях, сделанные в предположении, что массивы данных используются независимо друг от друга. Это позволило упростить проблему повышения безопасности систем обработки данных и сформулировать и представить решения задач оптимального резервирования отдельно для каждого массива данных. На практике же в системах обработки данных разного класса и назначения чаще всего решаются задачи и обрабатываются запросы, для которых требуется использование некоторого множества массивов данных, взаимосвязанных между собой по ссылкам или алгоритмически.

Использование резервирования в распределенных системах обработки данных имеет ряд особенностей, обусловленных большим количеством возможных вариантов размещения резерва по узлам компьютерных сетей, на основе которых работают эти системы [3-5].

В частности, при размещении резерва данных в нескольких узлах сети для обработки запросов к данным можно использовать различные дисциплины их обработки. Например:

1. Запрос пересылается и обрабатывается в ближайшем (согласно некоторому критерию) узле с резервом массива данных.

2. Запрос пересылается для обработки одновременно в несколько узлов с требуемым резервом.

3. Запрос, возникший в узле j, последовательно пересылается по узлам пути длины K, начинающегося в узле j и состоящим из узлов с резервом требуемого массива. Запрос пересылается по узлам этого пути до тех пор, пока он или не будет успешно обработан в одном из узлов, либо не будет пройден весь путь без получения ответа на запрос.

4. Запрос, возникший в узле j, поочередно посылается для обработки в K ближайших узлов с необходимым резервом. Запрос посылается в ближайшие узлы до тех пор, пока из очередного узла не будет получен ответ, либо все узлы не будут опрошены без получения требуемого ответа.

Сформулируем задачу оптимального резервирования взаимосвязанных массивов данных в РСОД.

Рассмотрим компьютерную сеть, состоящую из N узлов, на базе которой работает РСОД. В системе при решении J различных задач

используется M массивов данных. При этом каждая из задач системы может решаться в нескольких различных узлах сети и использовать данные из нескольких массивов данных. Пусть W_j это количество решений в системе задачи j $(j = \overline{1-J})$, которое выполняется за некий интервал времени (например, час, сутки, неделя, месяц, квартал и т.п.).

Будем использовать следующие обозначения:

-ψ_{jn} - переменная такая, что $\psi_{jn} = 1$, если задача с номером *j* решается в *n*-м узле сети;

- x_{nm}- объем резерва массива *m*, который размещен в *n*- м узле сети;

- L_m- размер *m*-го массива данных;

- U_{jm}- среднее число информационных запросов задачи j к m-му массиву данных;

- V_{jm} - среднее число запросов на модификацию *m*-го массива данных, которые возникают при решении задачи *j*.

Предположим, что задача в системе успешно решена только в том случае, если на все запросы, возникающие в процессе ее решения ко всем необходимым для решения массивам данных, получены ответы. В этом случае вероятность $P_{nj}(X)$ решения задачи j в узле n при распределении резерва $X = \|x_{nm}\|$ будет равна:

$$P_{nj}(X) = \sum_{m=1}^{M} [\rho_{nm}(X)]^{U_{jm}} \left(\beta_{nm}(X)\right)^{V_{jm}}$$

Здесь $\rho_{nm}(X)$ - это вероятность получения ответа на информационный запрос, выданный в узле сети *n* к массиву *m*. Значение данной вероятности зависит от того, какая используется дисциплина обработки запроса, и определяется по соответствующей формуле, приведенной в таблице 2 в работе [2]; $\beta_{nm}(X)$ - это вероятность успешной обработки запроса на обновление *m*-го массива данных, выданного в узле *n* сети. Предположим, что значение этой вероятности равно вероятности события, заключающегося в успешном обновлении, по крайней мере, одного из массивов данных, размещенного в одном из узлов сети с резервом, с последующим получением подтверждения об обновлении массива. Тогда вероятность успешной обработки запроса на обновление массива данных будет равна:

$$\beta_{nm}(X) = 1 - \prod_{i=1}^{N} [1 - r_{ni} \mathrm{P}_i(x_{im}) r_{in}]$$

Здесь $P_i(x_{im})$ - вероятность успешной обработки запроса в узле i, который содержит размещенный в нем резерв объемом x_{im}, а r_{ni} – надежность канала связи между узлами *n* и *i* сети (при этом будем считать, что $r_{ni} = r_{in}$).

Обозначим через $T_{nj}(X)$ суммарное время ожидания ответов на все запросы, выданные в узле *n* при решении задачи *j*. Оно равно:

$$T_{nj}(X) = \sum_{m=1}^{M} \{U_{jm} t'_{nm}(X) + V_{jm} t''_{nm}(X)\}$$

Здесь $t'_{nm}(X)$ - время получения ответа на запрос к массиву *m*, который был сформирован в узле *n*; $t''_{nm}(X)$ - это время обработки запроса на модификацию данных массива *m*, в соответствии с запросом, выданным в узле *n*.

Стоимость затрат $S(X)$ на функционирование системы в течение рассматриваемого периода времени состоит из стоимости хранения резерва в узлах сети и стоимости решения всех задач системы. Стоимость затрат равна:

$$S(X) = \left\{ \sum_{j=1}^{J} W_j \sum_{n=1}^{N} \varphi_{jn} \left[V_{jm} \sum_{i/x_{im} \neq 0} ZP_{ni}(x_{im}) + + U_{jm} \min_{i/x_{im} \neq 0} ZP_{ni}(x_{im}) \right] + L_m \sum_{n=1}^{N} S_n x_{nm} \right\}$$

Здесь:

$ZP_{ni}(x_{im})$ - величина средних затрат на обработку запроса, посланного из узла *n* на обработку в узел *i*, которая равна:

$ZP_{ni}(x_{im}) = 2D_{ni} + E_i(x_{im})h_i$;

S_n - стоимость хранения одного бита информации в узле *n* в течение рассматриваемого периода времени;

Задача поиска размещения в узлах сети резерва для *M* взаимосвязанных массивов данных, оптимального по критерию минимума стоимостных затрат $S(X)$ на функционирование распределенной системы будет иметь следующую формулировку.

Необходимо найти такое оптимальное размещение резерва взаимосвязанных массивов данных по узлам компьютерной сети, которое обеспечит минимум стоимости затрат на функционирования системы. При этом найденное решение задачи должно соответствовать ряду ограничений: на вероятность успешной обработки запроса в узлах сети; решение должно обеспечивать затраты времени на ожидание ответов на запросы не более заданного лимита; ограничение на объем резерва, размещаемого в каждом из узлов сети. Таким образом, задача имеет формулировку:

$S(X) \rightarrow min$

при ограничениях:

$P_{nj}(X) \geq \bar{P}_j$;
$T_{nj}(X) \leq \bar{T}_j$;
$\sum_{m=1}^{M} x_{nm} L_m \leq Q_n$

Аналогично формулируются задачи поиска оптимального размещения резерва взаимосвязанных массивов, используемых в распределенной системе, при применении других критериев оптимальности. В частности, при использовании такого критерия оптимальности, как максимум вероятности успешного решения всех задач системы за заданный период времени, задача оптимизации размещения резерва будет иметь следующую формулировку:

$$P(X) = \prod_{j=1}^{J} \prod_{n=1}^{N} \left[P_{nj}(X)\right]^{W_j} \rightarrow max$$

При следующих ограничениях:
$S(X) \leq \bar{S}$;
$T_{nj}(X) \leq \bar{T}_j$;
$\sum_{m=1}^{M} x_{nm} L_m \leq Q_n$

Здесь $j = \overline{1,J}; n = \overline{1,N}$.

В силу большой размерности сформулированных задач для их решения целесообразно использовать эвристические алгоритмы.

Приведенные выше формулировки задач сделаны в предположении, что они решаются в два этапа. На первом этапе определяется множество N^* узлов сети, в которых должны разместиться копии массивов данных (при этом в одном узле размещается не более одной копии массива). Это размещение находится в результате решения задач с помощью известных алгоритмов [6-8].

В случае, если найденное на первом этапе решение не обеспечивает выполнение ограничений задачи, то выполняется второй этап решения задачи. На этом этапе для каждого узла из множества N^* решается своя задача определения оптимального объема резерва в этом узле. Для решения этих задач на втором этапе используются традиционные методы (методы решения задач распределения ограниченных ресурсов) [2].

Литература:

1. *Кузнецов Н.А., Кульба В.В., Микрин Е.А.* и др. Информационная безопасность систем организационного управления. Теоретические

основы в 2 т./ под ред. Н.А. Кузнецова, В.В. Кульбы. Ин-т проблем передачи информации. РАН. – М.: Наука, 2006. – 427с.
2. *Кульба В.В., Сомов С.К., Шелков А.Б.* Резервирование данных в сетях ЭВМ. – Казань: Издательство казанского университета. – 1987. – С. 175.
3. *Микрин Е.А., Сомов С.К.* Оптимальное оперативное резервирование информации в системах обработки данных на базе вычислительных сетей // Проблемы управления. – 2016. – №5. – С. 47-56.
4. *Кульба В.В., Сомов С.К* Повышение надежности функционирования распределенных СОД методами резервирования и восстановления информации.// Информатизация и связь. – 2016. – №3. – С. 86-94.
5. *Микрин Е.А., Сомов С.К.* Оптимизация резервирования информации в распределенных системах обработки данных реального времени // Проблемы управления. – 2016. – №6. – С. 47-52.
6. *Machmoud S., Riordon J.S.* Optimal Allocation of Resources in Distributed Information networks. //ACM Transactions on Database Systems. – 1976. – Vol.l, N.4. – P. 66-78.
7. *Chu W.W.* File Allocation in a Multiple Computer System.//IEEE Transactions on Computers. – 1969. – Vol. C-18. – №. 10. – P. 885-889.
8. *Casey R.G.* Allocations of copies of a file in an Information Network. //AFIPS Conference Proceedings, – 1972. – Vol. 40. – P. 617-625.

Мусаев В.К.

Моделирование нестационарных упругих волн напряжений в консоли (соотношение ширины к высоте один к десяти) с основанием (полуплоскость) с помощью волновой теории сейсмической безопасности

Аннотация: Рассматриваются вопросы численного моделирования сейсмической безопасности консоли с основанием в виде упругой полуплоскости при волновых воздействиях. Программный комплекс позволяют решать задачи при нестационарных воздействиях на объекты сложной формы. На основе метода конечных элементов в перемещениях разработаны алгоритм и комплекс программ для решения линейных плоских двумерных задач волновой теории упругости. Упругое контурное напряжение на гранях консоли является почти зеркальным отражением одна другой, то есть антисимметричным.

Ключевые слова: математическое моделирование, контурные напряжения, волновая теория сейсмической безопасности, динамическая теория упругости, сейсмическое воздействие, функция Хевисайда, фундаментальное воздействие, консоль, контурное напряжение, изгибные волны

Некоторые вопросы в области моделирования нестационарных динамических задач с помощью применяемого метода, алгоритма и комплекса программ рассмотрены в следующих работах [1–6].

На основе метода конечных элементов в перемещениях разработаны алгоритм и комплекс программ для решения линейных плоских двумерных задач, которые позволяют решать задачи при нестационарных волновых воздействиях на сложные системы. При разработке комплекса программ использовался алгоритмический язык Фортран-90. Исследуемая область разбивается по пространственным переменным на конечные элементы первого порядка. По временной переменной исследуемая область разбивается на конечные элементы первого порядка.

В работах [1, 3–6] приведена информация о физической достоверности и математической точности моделирования нестационарных волн напряжений в деформируемых телах с помощью рассматриваемого численного метода, алгоритма и комплекса программ.

Расчеты проводились при следующих единицах измерения: килограмм-сила (кгс); сантиметр (см); секунда (с). Для перехода в другие единицы измерения были приняты следующие допущения: 1 кгс/см^2 ≈ 0,1 МПа; 1 кгс с^2/см^4 ≈ 10^9 кг/м^3.

Рассматривается задача о воздействии плоской продольной упругой волны в виде функции Хевисайда на консоль с основанием (соотношение ширины к высоте один к десяти) (рис. 1).

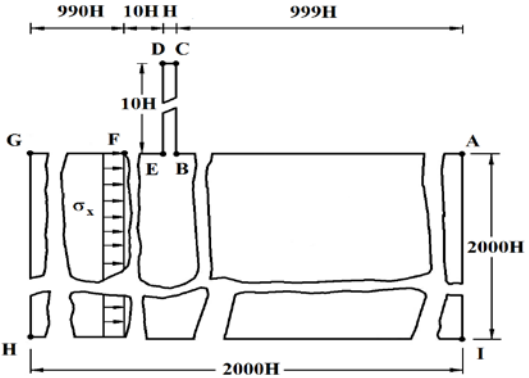


Рис. 1 – Постановка задачи для консоли (соотношение ширины к высоте один к десяти) с упругим основанием (полуплоскость)

Начальные условия приняты нулевыми. От точки F параллельно свободной поверхности ABEFG приложено нормальное напряжение σ_x, которое при $0 \le n \le 11$ ($n = t/\Delta t$) изменяется линейно от 0 до P, а при $n \ge 11$ равно P ($P = \sigma_0$, $\sigma_0 = 0{,}1$ МПа (1 кгс/см^2)).

Граничные условия для контура GHIA при $t > 0$ $u = v = \dot{u} = \dot{v} = 0$. Отраженные волны от контура GHIA не доходят до исследуемых точек при $0 \le n \le 500$. Контур ABEFG свободен от нагрузок, кроме точки F.

Решается система уравнений из 4004021 неизвестной.

В характерных областях исследуемой задачи получены контурные напряжения и компоненты тензора напряжений.

На рис. 3–5 показано изменение контурных напряжений $\overline{\sigma}_k$ в консоли (рис. 2) во времени $t/\Delta t$.

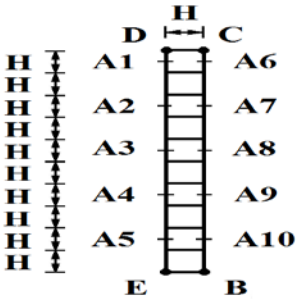


Рис. 2 – Точки, в которых получены контурные напряжения в консоли

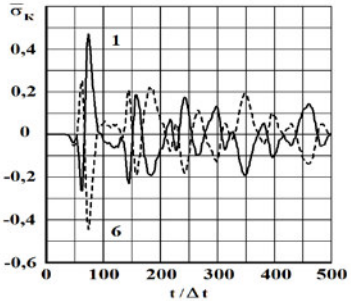


Рис. 3. Изменение упругого контурного напряжения $\overline{\sigma}_k$ в точках 1 и 6 на контуре консоли во времени $t/\Delta t$

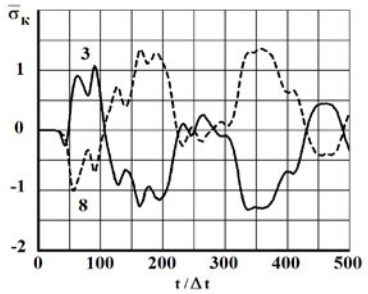


Рис. 4. Изменение упругого контурного напряжения $\bar{\sigma}_k$ в точках 3 и 8 на контуре консоли во времени $t/\Delta t$

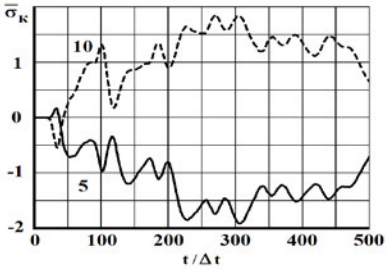


Рис. 5. Изменение упругого контурного напряжения $\bar{\sigma}_k$ в точках 5 и 10 на контуре консоли во времени $t/\Delta t$

На основании проведенных следований можно сделать следующие выводы:

Консоль (соотношение ширины к высоте один к десяти) моделируется с упругим основанием в виде упругой полуплоскости.

Упругое контурное напряжение на гранях консоли является почти зеркальным отражением одна другой, то есть антисимметричным.

Консоль при сейсмическом воздействии работает как стержень переменного сечения, то есть если на одной грани растягивающие напряжения, то на другой сжимающие напряжения.

На контурах консоли при сейсмическом воздействии в основном преобладают изгибные волны.

Литература:

1. *Мусаев В.К.* О достоверности результатов численного метода решения сложных задач волновой теории упругости при ударных, взрывных и сейсмических воздействиях // Ученые записки Российского государственного социального университета. – 2009. – № 5. – С. 21–33.

2. *Мусаев В.К.* Моделирование нестационарных упругих волн напряжений в деформируемых областях с помощью метода конечных элементов в перемещениях // Современные наукоемкие технологии. – 2014. – № 12–1. – С. 28–32.
3. *Musayev V.K.* Estimation of accuracy of the results of numerical simulation of unsteady wave of the stress in deformable objects of complex shape // International Journal for Computational Civil and Structural Engineering. – 2015. – Volume 11, Issue 1. – P. 135–146.
4. *Musayev V.K.* On the mathematical modeling of nonstationary elastic waves stresses in corroborated by the round hole // International Journal for Computational Civil and Structural Engineering. – 2015. – Volume 11, Issue 1. – P. 147–156.
5. *Стародубцев В.В., Мусаев А.В., Куранцов В.А., Мусаева С.В., Кулагина Н.В.* Оценка точности и достоверности моделирования плоских нестационарных упругих волн напряжений (треугольный импульс) в полуплоскости с помощью численного метода, алгоритма и комплекса программ Мусаева В.К. // Проблемы управления безопасностью сложных систем. Материалы XXIV Международной конференции. – М.: РГГУ, 2016. – С. 352–355.
6. *Стародубцев В.В., Акатьев С.В., Мусаев А.В., Шиянов С.М., Куранцов О.В.* Моделирование упругих волн в виде импульсного воздействия (восходящая часть – четверть круга, нисходящая часть – четверть круга) в полуплоскости с помощью численного метода Мусаева В.К. // Проблемы безопасности российского общества. – 2017. – № 1. – С. 36–40.

Стародубцев В.В., Мусаев А.В., Шиянов С.М., Крылов А.И., Куранцов В.А.

Применение численного метода Мусаева В.К. для моделирования несущей способности (прочности) уникальных объектов с помощью волновой теории взрывной безопасности

Аннотация: Рассматриваются некоторые вопросы решения задач о воздействии упругой взрывной волны на уникальные объекты. Применяется волновая теория взрывной безопасности. Поставленная задача решается с помощью методов вычислительной механики. Для решения поставленных задач используется численный метод, алгоритм и комплекс программ Мусаева В.К. Приведена некоторая информация о постановке решаемых задач.

Ключевые слова: компьютерное моделирование, взрывная волна, воздействие в виде треугольника, дельта функция, волновая теория взрывной безопасности, численное моделирование, контурное напряжение, компоненты тензора напряжений, несущая способность, безопасность окружающей среды

В работах [1–6] приведена информация о моделировании нестационарных волн напряжений в деформируемых телах сложной формы.

Некоторая информация о физической достоверности и математической точности рассматриваемого численного метода, алгоритма и комплекса программ приведена в следующих работах [5].

Применение численного моделирования в задачах управления безопасности сложных объектов при взрывных воздействиях рассмотрено в следующих работах [1–4, 6].

Решена задача о воздействии сосредоточенной взрывной волны на свободной поверхности упругой полуплоскости с полостью (соотношение ширины к высоте один к пяти) (рис. 1) [3]. Исследуемая расчетная область имеет 2004002 узловых точек. Решается система уравнений из 8016008 неизвестных. Рассматриваются некоторые точки в окрестности полости на свободной поверхности упругой полуплоскости.

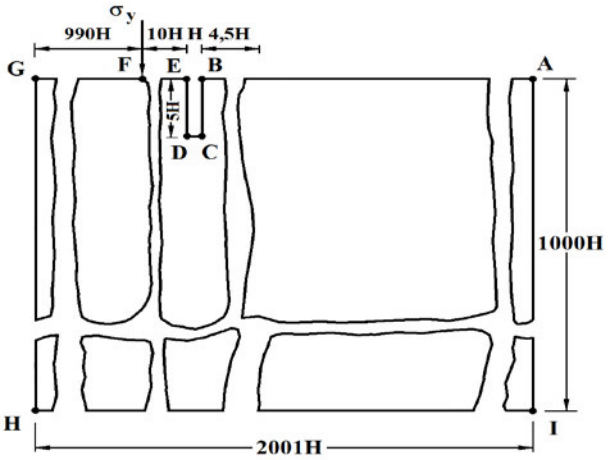


Рис. 1 – Постановка задачи о воздействии сосредоточенной взрывной волны на свободной поверхности упругой полуплоскости с полостью (соотношение ширины к высоте один к пяти) [3]

Решена задача о воздействии взрывной волны в сооружении неглубокого заложения на окружающую среду с полостью в виде прямоугольника (соотношение ширины к высоте один к пяти, десяти и пятнадцати). Исследуемая расчетная область имеет 17112 узловых точек. Решается система уравнений из 68448 неизвестных. Рассматриваются точки на свободной поверхности упругой полуплоскости, которые находятся в окрестности полости.

Рассматриваются вопросы моделирования упругих волн напряжений в упругой полуплоскости с дымовыми трубами при сосредоточенном взрывном воздействии в виде дельта функции (рис. 2) [1–2, 4]. Исследуемая расчетная область имеет 2004032 узловых точек. Решается система уравнений из 8016128 неизвестных. Полученные результаты показывают, что дымовые трубы уменьшают нормальные напряжения на границе сред в окрестности сооружения.

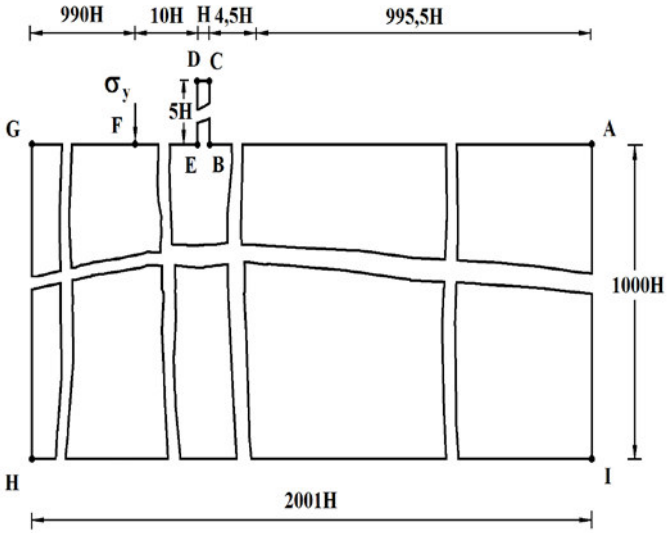


Рис. 2 – Постановка задачи о сосредоточенном упругом взрывном воздействии на грунтовой среды с дымовой трубой (соотношение ширины к высоте один к пяти) [1–2, 4]

Решена задача о воздействии упругой взрывной волны в объекте хранения опасных веществ с полостью в виде прямоугольника (соотношение ширины к высоте один к пяти, десяти и пятнадцати).

Исследуемая расчетная область имеет 14250 узловых точек. Решается система уравнений из 57000 неизвестных. Получены напряжения в точках на поверхности упругой полуплоскости около объекта хранения опасных веществ с полостью.

Рассмотрена задача о воздействии сосредоточенной взрывной волны на свободной поверхности упругой полуплоскости с надземным нефтепроводом (рис. 3) [6]. Взрывное воздействие моделируется в виде треугольного импульса, которое приложено на расстоянии одного среднего диаметра от края трубы (рис. 3). Исследуемая расчетная область имеет 2004072 узловых точек. Решается система уравнений из 8016288 неизвестных.

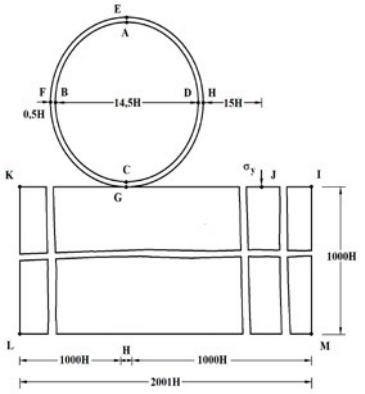


Рис. 3. Постановка задачи о воздействии сосредоточенной взрывной волны на надземный нефтепровод с основание в виде упругой полуплоскости (воздействие приложено на расстоянии одного среднего диаметра от края трубы) [6]

Авторы выражают благодарность Мусаеву В.К. за оказанную помощь и внимание к работе.

Литература:

1. *Мусаев В.К.* Моделирование безопасности по несущей способности дымовых труб с основанием при взрыве атомной бомбы в Нагасаки // Международный журнал прикладных и фундаментальных исследований. – 2014. – № 12. – С. 198–203.
2. *Мусаев В.К.* Моделирование безопасности по несущей способности дымовой трубы с основанием при взрыве атомной бомбы в Нагасаки // Проблемы управления безопасностью сложных систем. Материалы XXII Международной конференции. – М.: РГГУ, 2014. – С. 372–376.

3. *Мусаев В.К.* Применение нестационарной волновой теории взрывной безопасности к моделированию волн напряжений в упругой полуплоскости с вертикальной прямоугольной полостью (соотношение ширины к высоте один к восьми) // Проблемы безопасности российского общества. – 2017. – № 1. – С. 74–80.
4. *Мусаев В.К.* Моделирование безопасности по несущей способности дымовой трубы с основанием (полуплоскость) при взрыве атомной бомбы в Нагасаки (Япония) // Проблемы безопасности российского общества. – 2017. – № 2. – С. 19–25.
5. *Мусаев В.К.* Сопоставление численного метода с результатами динамической фотоупругости при решении задачи о воздействии плоской продольной волны на свободное круглое отверстие // Высшая школа. Новые технологии науки, техники, педагогики: материалы Всероссийской научно-практической конференции «Наука – Общество – Технологии – 2018». – М.: Московский политех, 2018. – С. 303–313.
6. *Мусаев В.К.* Моделирование нестационарных изгибных волн напряжений в надземном нефтепроводе при внешнем сосредоточенном взрывом воздействии // Высшая школа. Новые технологии науки, техники, педагогики: материалы Всероссийской научно-практической конференции «Наука – Общество – Технологии – 2018». – М.: Московский политех, 2018. – С. 374–380.

Маклаков В.В., Христофоров О.Б.

Исследование квантовомеханических процессов формирования идентификаторов для безопасности сложных систем

Аннотация: Исследован метод срытой маркировки, основанный на неразрушающем воздействии лазерного УФ излучения. Маркировка может быть нано-структурированной, не нарушающей внешний вид изделий и служить элементом их дизайна. В вариантах реализации метода скрытую маркировку можно обнаружить только приборными методами. Маркировка, выполненная с использованием различных длин волн лазерного УФ излучения, отличается контрастом и спектрами УФ флуоресценции, что позволяет реализовать многоуровневую кодировку. Исследован метод скрытой лазерной маркировки материалов, прозрачных в УФ области спектра. Развитые методы могут служить основой развития новой технологии защиты от фальсификации изделий, документов, носителей информации и ценных предметов.

Ключевые слова: маркировка, квантовые эффекты, УФ флуоресценция, модификация, наноструктуры, скрытое изображение.

Введение. Формирование наноидентификаторов в элементах сложных систем обеспечивает возможность определения их подлинности и, соответственно, надежность и безопасность эксплуатации. Новые возможности открываются при использовании радиофизических эффектов управления квантовомеханическими процессами в различных материалах [1]. Практическое решение этой задачи возможно с использованием когерентного лазерного излучения с высокой энергией квантов [2- 5]. В настоящей работе представлены результаты исследований развиваемого нами подхода к созданию технологии защиты от фальсификации, идентификации и установления подлинности различных объектов.

Методы. В исследованиях использовались электроразрядные эксимерные лазеры УФ - диапазона (248, 308, 350 нм. Доза облучения образца для получения скрытой маркировки обычно не превышала 10 Дж/см^2. Использовались контактные маски, либо изображение формировались сканированием сфокусированного лазерного пучка. Для детектирования скрытой маркировки с помощью УФ подсвета обычно использовались УФ лампы с максимальной спектральной интенсивностью на 366 нм. С помощью флуориметров (Hitachi и NTX2000) проводилось сравнение спектров флуоресценции образцов до и после их обработки лазерным УФ излучением.

Результаты. Исследования показали, что в различных по окраске и прозрачности образцах пластиков, в частности поливинилхлорида (*ПВХ*), фото-модифицированные области образцов не обнаруживаются в видимом свете, но наблюдаются при освещении УФ лампой.

В ряде случаев скрытое изображение визуализируется способом, не требующим ни УФ освещения, ни сложных спектральных приборов. Скрытое изображение проявляется при селективной конденсации паров влаги на необработанных участках поверхности при дыхании на нее. Этот способ, основанный на пространственно-селективном изменении поверхностной энергии материала, может быть применяться для создания элементов дизайна изделия.

В других случаях фото-модифицированные области регистрируются приборными методами. Рис. 1 иллюстрирует спектральные характеристики сформированных в поликарбонате CD-диска идентификаторов, не визуализируемых при УФ подсвете, но наблюдаемых с помощью УФ- спектрометра. Как видно из рис. 1, спектральные различия наблюдаются в УФ диапазоне 310-400 нм.

Варьируя длину волны УФ-излучения $\lambda_{УФ}$, которым индуцируют флуоресценцию, может быть получен 3D- спектр флуоресценции I ($\lambda_{ФЛ}$, $\lambda_{УФ}$). На рисунке 2 представлены 3D- спектры флуоресценции образца силиконовой резины, показывающие, что максимальные спектральные отличия скрытой маркировки наблюдаются в УФ - диапазоне.

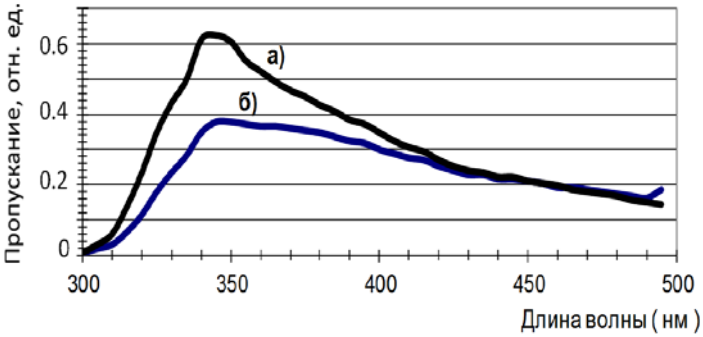
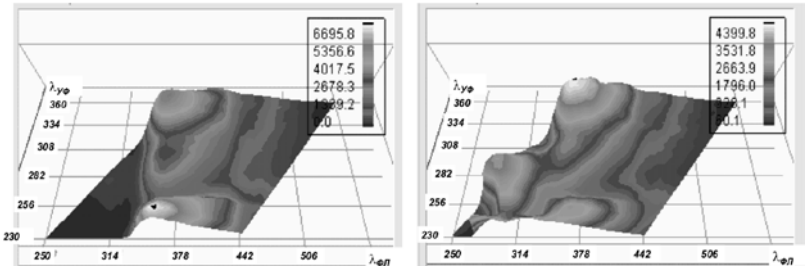


Рис 1 – Спектральный сигнал флуоресценции материала CD-диска: (а)- исходного, (б) – модифицированного



а) б)

Рис. 2 – 3D- спектры флуоресценции образца силиконовой резины: а) - исходного, б) - модифицированного УФ излучением XeCl лазера.

При определенном сочетании материала образца и условий воздействия коротковолнового излучения модификация материалов может быть реализована с различными свойствами, например, быть многоуровневой. Так, в образцах пластика (*ПВХ*) были получены скрытые изображения, имеющие различную топологию, выполненные последовательно облучением образца монохроматическим излучением сначала с одной (248 нм), а затем с другой длиной волны (351 нм) лазерного УФ – излучения. При УФ подсвете две скрытые структуры визуализировались в различных областях видимого спектра [3].

Исследования показали, что скрытые изображения можно выполнять с варьируемым в широких пределах контрастом, зависящим от величины энергетической экспозиции. К настоящему времени возраст некоторых образцов со срытой маркировкой превысил десять лет, что свидетельствует о большом времени жизни выполненных в соответствии с разработанной технологией идентификаторов.

В образцах с достаточно высокой однородностью материала, в частности, в пластиковых картах были сформированы скрытые устойчивые идентификаторы с тонкой периодической структурой, характерный размер которой составлял 10 мкм. Идентификаторы при их освещении пучком монохроматического излучения, в частности, от лазерной указки проявлялись в виде дифракции монохроматического пучка на тонкой периодической структуре модифицированной части образца. При наблюдении в белом свете под скользящим углом к поверхности такие скрытые идентификаторы визуализировались в виде радужной дифракционной картины модифицированной части образца.

Также показана возможность формирования скрытых изображений на прозрачных объектах, например, кварце за счет их облучения корпускулярными потоками из лазерной плазмы металлических мишеней, как это показано на рис. 3.

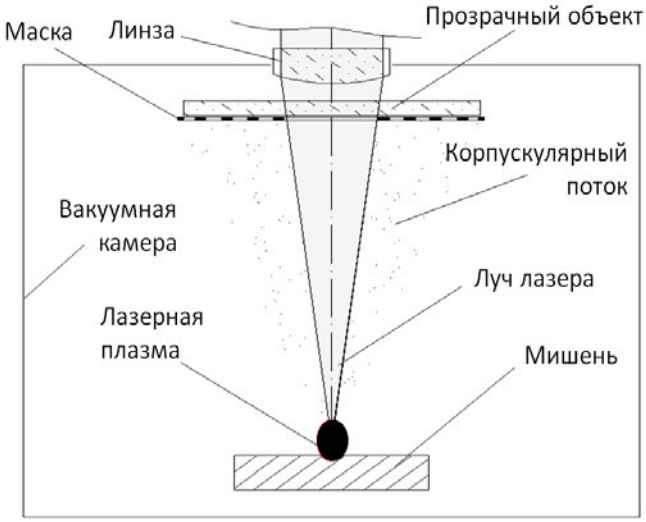


Рис. 3 – Схема, поясняющая вариант метода формирования скрытого изображения на прозрачном объекте за счет его облучения потоком высокоэнергетичных ионов из лазерной плазмы

Показано, что идентификаторы рассеивающие, поглощающие или прозрачные для заданного диапазона волн достоверно обнаруживаются. Это является следствием того, что идентификаторы с индуцированными периодическими структурами модулируют фазу когерентного электромагнитного излучения и формируют бегущие волны интенсивности интерференционных когерентных полей.

Выводы. Результаты работы показывают новые возможности защиты изделий от фальсификации на основе скрытой лазерной маркировки методом неразрушающего пространственно - селективного воздействия коротковолновым лазерным излучением.

Разработанные методы реализованы в воздухе при нормальных условиях. Однако они могут быть осуществлены и в газовых средах, вступающих в фото-инициируемую химическую реакцию с материалом, как это показано в работе [6], в которой формирование изображений на поверхности электролюминесцентных полимеров осуществлялось за счет их УФ инициируемой модификации в атмосфере органосиланов.

Формирование структур модифицированного вещества нанометрового масштаба в промышленных масштабах для изготовлении интегральных схем осуществляется методом проекционной литографии с применением сложных и дорогих оптико-механических систем- нанолитографов. В [7] формирование двумерных периодических модифицированных наноструктур было продемонстрировано при использовании интерференции пучков излучения XeCl- лазера на поверхности таких материалов как полиимид, фоторезист и поликристаллический алмаз. Подобная сравнительно простая и дешевая нанотехнология применима и для исследуемого в данной работе метода скрытой лазерной маркировки.

Литература:

1. *Бутковский А.Г., Самойленко Ю.А.* Управление квантовомеханическими процессами. – М.: Наука, 1984. – 256 с.
2. Способ маркировки объектов//Патент России № 2165359. 2001. Бюл. № 11 / Маклаков В.В.
3. *Маклаков В., Христофоров О., Мошников А.* Селективная модификация материалов неразрушающим потоком высокоэнергетичных фотонов//Наноиндустрия. – 2011. – Т. 29. № 5. – С. 66–70.
4. *Ershov Yu.A., Maklakov V.V., Khristoforov O.B.* Photochemical Technology of t he F ormation o f P olymer M aterials' Nanomarkers//Theoretical Foundations of Chemical Engineering. –2016. Vol. 50. No. 1. – P. 76–82
5. *Маклаков В.В., Христофоров О.Б.* Исследование методов формирования скрытых изображений для идентификации ценных материальных объектов. //Приднепровский научный вестник. 2018. Т.7. № 3. С. 47-55.

6. Spanring J ., B uchgraber C ., E bel M. F., et al . U V assisted s urface modification o f p olystyrene i n t he p resence o f trialkylsilanes//Macromolecular c hemistry a nd phy sics. – 2005. – V. 2 06. № 22. – P. 2248-2256.
7. *Веревкин Ю.К., Бронникова Н.Г., Королихин В.В,* и др. Формирование двумерных периодических наноструктур на поверхности плавленого кварца, полиимида и поликристаллического алмаза с помощью метода импульсной четырехлучевой интерференционной лазерной модификации//ЖТФ. – 2003. – Т. 73. – С. 99-102.

Авдеева З.К., Филиппов В.А.

Применение элементов умных образовательных сред в экспертно-аналитических центрах поддержки принятия решений по обеспечению безопасности

Аннотация: В современных условиях требования к уровню подготовки аналитиков, потребность в подготовке экспертов для современных центров поддержки принятия решений (ситуационных центров) требует использования современных образовательных технологий, которые могут использовать накапливаемую в системах информацию, опыт по анализу и решению проблем, внешние источники для формирования навыков и умений по анализу в новых или сложных кризисных ситуациях и подготовки соответствующих управленческих решений.

Ключевые слова: аналитический центр, умная среда, интеллектуальная обучающая система, профиль эксперта

Центры поддержки принятия решений должны обеспечивать работу в трех основных режимах: плановом, проблемном, чрезвычайном и кризисном [1]. Усиление и даже изменение характера угроз государственной безопасности требует постоянной поддержки ситуационных центров и их сети в соответствующих министерствах и ведомствах. При этом выросла потребность в поддержке проблемного и кризисного режима, что вызвано следующими причинами: уникальностью (неповторимостью) каждой ситуации и решений по ним; фрагментарностью и противоречивостью исходной информации; интуитивностью критериев оценки ситуаций и принятия решений; необходимостью большего внимания к поддержке процессов постановки задач, чем к их решению; необходимостью выхода за рамки стереотипных решений, рассмотрения маловероятных альтернативных ходов; влиянием

отклоняющих (от ранее намеченного плана) тенденций на ход управленческих процессов.

Поэтому возникает острая потребность в кадрах, способных ориентироваться в быстро изменяющейся проблемной ситуации с совершенно новыми условиями и возможностями. В этой связи, требуются специальные средства и методы подготовки специалистов, специфичные для экономических, правовых и политических условий функционирования развивающегося государства. Объективно и комплексно оценивать ситуацию сложно вследствие ее многоаспектности и наличия большого числа заинтересованных субъектов. Государственные органы действуют в реальном времени и поэтому вынуждены своевременно принимать решения в динамике, достигать поставленных целей, должны хорошо оценивать динамические характеристики управляемых процессов, их инерционность и ресурсоемкость (в смысле тех затрат, которые необходимы для направления процесса к желаемой цели). Сейчас по существу единственным и очень дорогим способом подготовки кадров является - практическая работа. Для обучения искусству постановки и достижения стратегических целей различной природы (социально-политических, криминальных и пр.) необходимо дополнить практику как слишком медленный и "дорогой" способ приобретения необходимых знаний и навыков.

Система поддержки группового принятия решений для ситуационных центров должна включать в себя интеллектуальную обучающую систему пользователей в смешанном (оффлайн/онлайн) информационном пространстве, которая [4,6] состоит из: модуля поддержки процесса обучения пользователей (аналитиков и экспертов), в котором формируется и визуализируется модель знаний и компетенций пользователя, дополняется модель знаний с учетом новых ключевых понятий , планируется процесс обучения и погружения в проблемную ситуацию, формируется база информации, возможных методов и экспертов, связанных с проблемой; модуль интерактивной поддержки работы тьютора, который содержит инструменты для мониторинга информационного пространства, как отношение между фактическими знаниями и результатами дидактической обработки таких знаний для определенной предметной области, которые синхронизированы с прикладными аспектами (практической полезностью). В таком случае, электронная среда строится на базе знаний всех источников знаний в разных проблемных областях [3], обучающих материалов или виртуальных ссылок на них в рамках программы подготовки экспертов. Таким образом, необходимая функциональность такой информационно-аналитической системы на основе I-агентов для динамического формирования виртуальной обучающей среды должна реализовывать

следующие стратегии работы с информацией в ходе обучения: поиск, серфинг, рекомендации и навигации.

Заключительные выводы. В докладе проведен анализ современных ситуационных центров поддержки принятия решений в области управления стратегическим развитием, обеспечения безопасностью региональных систем. В связи с нарастающей скоростью изменения внешней обстановки, потребностью работы с новыми проблемными ситуациями, объемом данных для всестороннего анализа типовых ситуаций, проблемой с достаточностью и качеством кадров в ситуационных центрах, обновлением и доступностью современных технологии поиска структуризации и анализа информации и данных обоснована потребность включения в структуру типового ситуационного центра подсистем обучения пользователей с применением технологий формирования умных образовательных сред. Такие подсистемы должны решать задачи ускоренного «тренинга» аналитиков при возникновении новых проблемных или сложных кризисных ситуаций, по которым оперативно нужно составить представление и сформировать принципы анализа и поиска решений.

Литература:

1. *Ильин Н.И., Демидов Н.Н., Новикова Е.В.* Ситуационные центры: опыт, состояние, тенденции развития. М.: МедиаПресс, 2011. – 336 с.
2. *Филиппов В.А.* Аналитические центры - стратегический интеллектуальный ресурс. М.: URSS, 2007. – 104 с.
3. Атлас российских «фабрик мыслей» - Центр изучения кризисного общества, 2018. – 37 с.
4. *Филиппов В.А., Авдеева З.К.* The main functionality o f s mart t raining system f or e xperts i n an alytical ce nters / P roceedings o f t he 1 0th International C onference "Management o f Large-Scale S ystem Development" (M LSD). M oscow: IE EE, 2 017. C. http://ieeexplore.ieee.org/document/8109596/.
5. Conati, C. I ntelligent T utoring Systems: New Challenges a nd D irections. Proceedings o f t he 2 1st I nternational J oint Conference o n Artificial Intelligence, Pasadena, California, 2009. – P. 2-7
6. *Avdeeva Z., Taratuhina Y. V., Omarova N.O.* Smart E ducational Environment as a Platform for Individualized Learning Adjusted to Student's Cultural-Cognitive P rofile, i n: Smart E ducation a nd S mart e -learning. Switzerland: Springer International Publishing, 2015. – P. 219-231.

VII. Правовые вопросы обеспечения безопасности сложных систем

Пискурева Т.А., Завидова М.Ю., Сергеев М.С.

Вопросы кадровой безопасности. Зоны ответственности при обеспечении комплексной безопасности ядерного объекта

Аннотация: В статье рассматриваются вопросы кадровой безопасности, роль которой заключается в упреждении негативных воздействий на безопасность за счет снижения угроз, связанных с персоналом, его квалификацией и компетенциями, интеллектуальным потенциалом и трудовыми отношениями. Обращается внимание на необходимость использования риск-фильтров при приеме на работу, постоянного мониторинга нарушений, связанных с человеческим фактором, на важность построения сквозной защиты, необходимость четкого распределения зон ответственности и интегративную функцию культуры безопасности на всех уровнях управления ядерным объектом.

Ключевые слова: кадровая безопасность, риск-фильтры, зоны ответственности, сквозная защита, человеческий фактор, надежность персонала, социотехническая система, культура безопасности

В системе управления ядерным объектом подсистема обеспечения безопасности тесно связана с подсистемой управления персоналом. Никто не может нанести большего ущерба ядерному объекту, чем ее работник, допущенный практически ко всем средствам и системам предприятия. Кадровая безопасность - это процесс предотвращения негативных воздействий на безопасность ядерного объекта за счет ликвидации или снижения рисков и угроз, связанных с персоналом. При этом, предметом в обеспечении кадровой безопасности с одной стороны выступает выявление непрофессионализма и деструктивного профессионализма сотрудников, с другой – сохранение и наращивание профессионального потенциала посредством эффективной кадровой политики. Когда мы говорим о кадровой безопасности, то обращаем внимание на угрозы, связанные с человеческим фактором. При этом различаем внешние и внутренние угрозы [1]. К внутренним негативным воздействиям со

стороны человеческого фактора приводят пробелы со стороны системы управления персоналом, такие как слабая система подбора и отбора персонала, неэффективная организация системы подготовки и обучения персонала, ошибки в планировании ресурсов персонала, отсутствие стратегии в планировании человеческих ресурсов предприятия, неэффективная система мотивации для инициатив и рационализаторских предложений, кадровая текучесть, уход квалифицированных сотрудников, слабая корпоративная культура и культура безопасности.

К внешним угрозам относятся такие факторы как давление на сотрудников извне, изменения во внешней экономической среде, попадание сотрудников в различные виды зависимости, высокая мотивационная составляющая конкурентов.

При обеспечении кадровой безопасности необходимо учитывать и потенциальные источники угроз, к которым относятся персонал и техника, выступающие как материальные объекты, информация об источниках потенциальной опасности и угрозах, включающая возможности реализации потенциальной опасности и меры предотвращения их реализации. Поведение персонала - источник опасности, основанный на профессиональных знаниях, компетенциях, психологических аспектах, взаимоотношениях персонала, личной ответственности и этики. Все эти негативные воздействия внешней и внутренней среды оказывают влияние на процессы внутри предприятия, в целом, и на ее безопасность по кадровой составляющей.

Как повысить кадровую безопасность? Какие факторы влияют на кадровую безопасность?

Деятельность по обеспечению кадровой безопасности начинается уже на этапе отбора кандидатов. Важной составляющей при подборе кандидатов является использование риск – фильтров. Первоочередной из них – оценка резюме. Резюме не рассматривается, если в нем есть грамматические ошибки. Резюме проверяется по базе данных с целью выявления его наличия ранее, при этом выясняется история кандидата на должность. Оценивается поведение претендента на должность, оцениваются вопросы, которые задает претендент на должность, при приглашении на собеседование по телефону. Опоздание на собеседование расценивается как предпосылка к нарушению дисциплины и трудового распорядка в дальнейшем. Важное значение имеет оценка влияния на должность, при которой производится аудит потенциального риска вакансии (должностной позиции). Немаловажен и анализ личности кандидата: анализ трудовой биографии кандидата, анализ хобби, увлечений, выявление вредных привычек, проверка возможности

пристрастия кандидата и/или его близких к азартным играм и наркотикам, наличие крупных денежных долгов. Беседы с кандидатом при приеме на работу предполагают подробное выяснение его взглядов на жизнь, профессиональных мотивов (что побуждает его поступать на работу в данную организацию), самооценки сильных и слабых сторон.

Немаловажным фактором в обеспечении кадровой безопасности является надежность персонала [2]. В связи с этим, при приеме на работу необходимы беседы с лицами, знающими работника и выяснение их мнений о нем, в том числе, с точки зрения его надежности. Надежность персонала – комплексная характеристика, зависящая как от внешних (управление, организация труда, социально-экономические условия и др.), так и внутренних (профессиональные знания и умения, функциональное состояние, личностные качества, мотивация и др.) факторов.

Как правило, подходы к повышению надежности персонала нацелены на обеспечение безопасности оборудования от неверных действий персонала и написание всеобъемлющих инструкций на все случаи жизни. Но вариативность развития событий, несовершенство инструкций, а главное - социально-психологическая природа человека как субъективного фактора нестабильности и неоднозначности и в восприятии и в оценке событий - приводит к необходимости учета человеческого фактора и к формированию культуры безопасного производства посредством отбора, воспитания, обучения и мотивации, что входит в кадровую составляющую.

Надежность сотрудника указывает на степень нормативности его поведения по отношению к безопасности. Не допускается прием на работу лиц, имеющих серьезные личностные недостатки, социальные связи, порочащие их, биографию, свидетельствующую о наличии у них моральных дефектов. Целесообразно дополнить общие условия такими мерами, как тестирование кандидата на должность, личное поручительство работников, по рекомендации которых берется на работу кандидат, получение информации с прежних мест учебы или работы, анализ результатов его предыдущей деятельности и т.д.

Помимо проведения комплекса мер при кадровом подборе и отборе, необходимы условия, при которых работнику будет невыгодно осуществлять действия, наносящие ущерб предприятию [3]. Эти условия включают согласованную систему мер по моральному и материальному стимулированию, формированию престижности работы на предприятии, заботе о внешнем и внутреннем имидже предприятия, созданию в ней комфортного социально-психологического климата: сотрудники знают условия карьерного роста и свои шансы на карьерный рост. Им хорошо известна структура предприятия и условия, необходимые для занятия

конкретной должности. При этом, критерии карьерного роста основываются на чётких и объективных показателях успешной работы за предыдущий период, существует возможность горизонтальной карьеры, когда с ростом опыта и квалификации растет материальное и моральное вознаграждение, существует система оценки эффективности деятельности персонала Замещение вакантных руководящих должностей производится, прежде всего, за счёт внутренних человеческих ресурсов.

Еще одной из составляющих кадровой безопасности является установленный на объекте режим безопасности и контроля, который представляет собой комплекс мер из установленных для персонала, в том числе и для администрации, регламентов, ограничений, режимов, технологических процессов, оценочных, контрольных и других процедур безопасности. Этот комплекс уже непосредственно нацелен на ликвидацию возможностей причинения ущерба и находится в зоне ответственности, как правило, служб различных видов обеспечения безопасности. При этом, создаются условия для предупреждения и выявления случаев алкоголизма, наркомании, религиозного сектантства, патологических депрессий. Такая помощь должна реализовываться профессионально и конфиденциально, за разглашение которой должна быть предусмотрена соответствующая ответственность [4].

Важна совместная оптимизация усилий различных служб, которая подразумевает, что система безопасности, как социотехническая система, будет функционировать наилучшим образом только тогда, когда социальная и техническая системы построены таким образом, чтобы служить потребностям друг друга. Техническая подсистема: включает устройства, инструменты и технологии, которые улучшают безопасность,· социальная подсистема включает управленческую структуру, персонал, их знания, умения, настрой, ценностные ориентиры, отношение к выполняемой работе, следование правилам и процедурам, систему поощрений [5]. Специфическими чертами социотехнической системы безопасности является их открытый, незавершенный характер, развитие, непрерывная адаптация, многоуровневость, ориентация на человека. И здесь необходимо обратить внимание на четкое распределение зон ответственности при их тесном взаимодействии.

Зоны ответственности распределяются следующим образом:

- Физическая безопасность занимаются физической охраной объекта, противодействием внешним угрозам.
- Информационная безопасность занимается защитой конфиденциальной информации.

- Технико-технологическая безопасность опирается на создание и использование такой технической базы, оборудования и основных средств производства, и таких технологий и бизнес-процессов, которые усиливают безопасность.
- Финансовая безопасность занимается вопросами финансово-экономической составляющей предприятия, обеспечивая его устойчивость к банкротству, определяет параметры платежеспособности и другие экономические характеристики.
- Правовая безопасность подразумевает всестороннее юридическое обеспечение деятельности предприятия, грамотную правовую работу с контрагентами и властью, решение правовых вопросов.
- Экологическая безопасность осуществляет комплекс мер, направленных на приведение деятельности предприятия к соответствию природоохранным нормам.
- Кадровая безопасность направлена на предотвращение угроз со стороны персонала.
- Культура безопасности создаётся и функционирует в социотехнических системах в процессе деятельности предприятия и призвана ограничить объективно существующие потенциальные опасности на уровне социально приемлемого риска.

Таким образом, кадровая безопасность распространяется на все сферы кадровой и управленческой работы. Особое значение кадровая безопасность принимает в высокотехнологичных областях и на ядерно-опасных объектах и направлена на поиск способов по минимизации риска и угроз со стороны сотрудников. Необходимо постоянное усовершенствование стратегии кадрового обеспечения, при котором особое внимание уделяется вопросам формирования системы ядерных знаний и ядерных компетенций, необходима работа по противодействию угрозам внутренней безопасности в тесном взаимодействии различных служб обеспечения безопасности.

Постоянное внимание должно уделяться обеспечению внутренней безопасности на всех уровнях, развитию система сквозной защиты, постоянный контроль зон риска, отработка до автоматизма сценарии действий в чрезвычайных ситуациях. Большое значение имеет работа по формированию корпоративной культуры, препятствующей злоупотреблениям, благоприятный моральный климат, стабильный коллектив, отлаженные процедуры увольнений, высокая требовательность к кандидатам, тщательная проверка при приеме на работу. Немаловажное значение имеет внедрение инноваций, формирование кадрового резерва, а

также понимание сотрудниками стратегии развития предприятия, при которой действует развитая система сохранения критически важных знаний, наставничество, формируется культура безопасности.

Литература:
1. *Ландерс Д.* Снижение угрозы со стороны внутреннего нарушителя с помощью бихевиоризма, семинар, 28-29 июня 2010, г. Санкт-Петербург, Россия.
2. *Харский К.И.* Благонадёжность и лояльность персонала, СПб: Питер, 2003, 496с.
3. *Пискурева Т.А., Членов А.М.* Человеческий фактор и его роль в долгосрочном обеспечении работоспособности системы учёта контроля и физической защиты ядерных материалов // Сборник материалов международной конференции Института управления ядерными материалами (INMM), США, 2012.
4. *Климов Е.А.* Психология профессионального самоопределения. - М.: Академия, 2007 – 302 с.
5. *Пискурева Т.А.* Совершенствование управленческих систем как условие успешного функционирования организации //Евразийский международный научно-аналитический журнал «Проблемы современной экономики», № 2 (30), СПб: Питер, 2009. С. 461 – 464.

Кротова М.В.

Роль нормативно-методических материалов в обеспечении экономической безопасности (на примере оценки экономической эффективности инвестиционных проектов)

Аннотация: Экономическая эффективность и экономическая безопасность – категории, между которыми всегда существует выбор при принятии управленческих решений в крупных компаниях и организациях. Наука и импортозамещающие инновации обеспечивают решающий вклад в экономическую (и иные) виды безопасности России. Однако в настоящее время не достает адекватных методических документов по оценке и легитимизации этого вклада.

Ключевые слова: экономическая безопасность, экономическая эффективность, инвестиционные проекты, эффективность НИОКР, фундаментальные исследования

В настоящее время оценка эффективности инвестиционных проектов проводится в соответствии с Методическими рекомендациями по оценке эффективности инвестиционных проектов и их отбору для финансирования, утвержденными Госстроем России, Министерством экономики РФ, Министерством финансов РФ, Госкомпромом России 31 марта 1994 г., № 7-12/47.

Документ, являющийся рамочным для других нормативных материалов, обеспечивает – а точнее, на момент его принятия в 1990-е гг. – вернее сказать, обеспечивал унификацию методов оценки эффективности инвестиционных проектов в условиях перехода России к рыночным отношениям. В условиях, когда становление современного типа экономики России завершено, да и сами основы рыночной экономики подвергаются обоснованным сомнениям, как, например, [1], остро стоит вопрос о соответствии действующих нормативных документов в области экономики и финансов таким основополагающим понятиям Российской цивилизации, как суверенитет, экономическая и энергетическая безопасность, стратегическое импортозамещение и развитие научно-технологического потенциала.

Особенностью же действующего рамочного документа является его ориентация на сугубо финансово-экономические и коммерческие параметры, связанные с действующими в международной практике принципы и подходы к оценке эффективности инвестиционных проектов, равно как и его адаптация к условиям рыночного транзита. К ним, в частности, относятся:

- моделирование потоков продукции, ресурсов и денежных средств;
- учет результатов анализа рынка, финансового состояния предприятия, влияния реализации проекта на окружающую природную среду и т.д.;
- определение эффекта посредством сопоставления предстоящих интегральных результатов и затрат с ориентацией на достижение требуемой нормы дохода на капитал или иных показателей;
- приведение предстоящих разновременных расходов и доходов к условиям их соизмеримости по экономической ценности в начальном периоде;
- учет влияния инфляции, задержек платежей и других факторов, влияющих на ценность используемых денежных средств;
- учет неопределенности и рисков, связанных с осуществлением проекта.

Выбор между экономической эффективностью и экономической безопасностью присущ практически любому инвестиционному проекту. Непосредственно в «Методических рекомендациях…» обращает на себя внимание то, что проблематика безопасности сведена здесь к факторам риска, т.е., самого «нижнего» этажа иерархии показателей безопасности «Вызовы – Угрозы – «Риски». Поэтому при формальном соответствии

всем критериям экономической, финансовой, коммерческой и социальной эффективности, проект может быть отклонен по соображениям безопасности, если создает дополнительные риски, стратегические риски или даже угрозы, описание которых выходит за рамки требований «Методических рекомендаций…».

В процессе развития практики инвестиционно-инновационных проектов сформировалась целая серия методических материалов и рекомендаций, которые можно классифицировать следующим образом:

1. Международные, рассчитанные на привлечение иностранных инвестиций (ЮНИДО, ЕБРР и т.п.) – в связи с введением санкций со стороны Запада, непосредственное применение этих документов сопряжено с рядом стратегических рисков.
2. Материалы ЕврАзЭс, Таможенного союза, БРИКС, банка развития БРИКС, частично ШОС – многие находятся в настоящее время в стадии разработки или даже проработки самой концепции документа, но являются серьезным стратегическим заделом на будущее.
3. Отраслевые (ведомственные или корпоративные) материалы, включая отдельные находящиеся в открытом доступе через юридическую базу «Консультант» - как показала работа автора, на этом уровне принятия решений проблематика экономической и ряда других видов безопасности прорабатывается ;
4. Электронные платформы и программные пакеты, используемые при составлении бизнес-планов – при применении этого класса методических материалов важна сертификация программных продуктов и их соответствие обычаям делового оборота и интересам инвестора в конкретном сегменте бизнеса, как правило, среднего и малого;
5. Закрытые материалы и документы, к которым относятся также банковские методы и технологии оценки потенциальных заемщиков, т.к., многие Российские банки обладают стратегической значимостью.

Ключевым вопросом является здесь логика формирования самого понятия «экономический эффект» от инвестиционной и инновационной деятельности. Здесь одной из главных проблем является сложность самого понимания и «распознавания» в хозяйственной практике – экономических эффектов от научно-исследовательских работ. Параметры коммерческой и финансовой эффективности в целом не чувствительны к тому – кто является владельцем либо поставщиком технологии, т.е., контролируется ли технология из-за рубежа?

Более глубокий уровень той же проблемы состоит в том, что отечественные по исполнению оборудование, технологии, комплектующие, программные пакеты и т.п., – могут, в свою очередь являться материальным воплощением иностранных разработок не только

прикладного, но и фундаментально-ориентированного класса, а в отдельных случаях и фундаментальных исследований.

Не менее важен вопрос об учете стратегических рисков – т.е., таких рисков, реализация которых привести к невосполнимому снижению потенциала и ликвидации технологий, хозяйственных объектов, имеющих стратегическое значение. Работы коллектива исследователей [2; 3] приводят к вопросу о том, что ущерб от стратегических рисков, т.е, величина обратная эффекту, должен оцениваться полностью, а не вероятностно. Данный подход соответствует концепции суверенитета и безопасности и может быть применим в стратегических отраслях.

Отраслевые методические и нормативные документы, как правило, связывают затраты на НИОКР с увеличением выпуска или реализации (экспорта) целевой, профильной продукции. Существуют определенные наработки оценки эффективности увеличения доли не одного только отечественного оборудования, но и отечественных комплектующих в оборудовании, изготовляемом по программам импортозамещения для ПАО «Газпром»; см., например, [4]. Разговор идет о сугубо промышленных разработках. Зачастую в отношении исследовательских организаций доминирует подход, представляющий их объектами своего рода благотворительности, не имеющей непосредственного практического эффекта. Основные положения Методических рекомендаций и ряда документов, имеющихся в доступе в базе «Консультант», проанализированы в Таблице 1 – на предмет их эффективного применения не к одним только прикладным, но и к фундаментальным разработкам.

Таблица 1

Основные логические составляющие структуры документа	**Действующие характеристики, требования документов**	**Основные проблемы применения документов к проектам с участием научных организаций**
Характер эффекта:	Специализированный, относящийся к профильной деятельности	Не учитываются эффекты (как положительные, так и отрицательные) в других сферах деятельности интегрированной компании

Основные логические составляющие структуры документа	Действующие характеристики, требования документов	Основные проблемы применения документов к проектам с участием научных организаций
Виды научно-технической продукции	1. Документы концептуального характера 2. Нормативно-техническая документация 3. Информационно-технологическая продукция: программы, базы данных, мат. модели 4. Нематериальные активы (НМА)	Нет условий для передачи созданных в результате НИОКР как материальных активов В качестве НМА классифицируется опытный образец, зачастую представляющий собой актив материальный – за исключением программного обеспечения
Критерий обоснования необходимости выполнения НИОКР	Принятие крупномасштабных стратегических решений, по сферам применения	Во многом игнорируется эффект на комплекс решений инженерно-технологического свойства по технологической цепочке
Факторы, влияющие на ценность НИОКР с точки зрения заказчика	Масштаб, уникальность, сроки исполнения, количество задействованных участников потенциальный эффект	Масштабность НИОКР определяется по юридическим и организационным критериям, слабо отражающим производственную специфику

Основные логические составляющие структуры документа	Действующие характеристики, требования документов	Основные проблемы применения документов к проектам с участием научных организаций
Факторы, влияющие на масштаб объекта, охваченного НИОКР	Масштаб объекта внедрения, также масштаб рынка	Масштабность НИОКР определяется по юридическим и организационным критериям, слабо отражающим производственную специфику
Метод оценки эффективности НИОКР (НИР)	NPV за весь период эксплуатации НИОКР / стоимость проведения НИОКР	Упрощенный подход к расчету NPV может приводить к невозможности численной оценки эффективности НИОКР
Метод формирования стоимости НИОКР	Базовая цена уровня фиксированного года Ч поправочные коэффициенты, включая инфляцию	Фактически, базовые цены на НИОКР зафиксированы в тех пропорциях, в каких соотносились между собой аналогичные работы в нормативно-установленном фиксированном году

Изложенное выше позволяет сделать следующие выводы. В настоящее время исследовательская проблематика анализа вызовов, угроз и рисков в экономической и энергетической безопасности недостаточно связана – методологически и методически – с общедоступной базой оценки

экономической эффективности. Последняя остается ориентированной на рыночный транзит и опыт стран Запада.

Наука, включая фундаментальные и фундаментально-ориентированные исследования, направленные на решение перспективных практических задач в крупных отраслях и ведомствах (ОПК, ТЭК, МЧС и др.) и импортозамещающие инновации являются необходимым условием обеспечения суверенитета, безопасности и развития России в направлении реализации ее национальных интересов. Однако в настоящее время не достает адекватных методических документов по оценке и легитимизации этого вклада в безопасность сложных систем, на которых можно было бы не только осуществлять специализированные ведомственные оценки, но и формировать соответствующее мировоззрение у специалистов в сфере экономики, управления и финансов.

Литература:

1. Кара-Мурза С.Г. Русская матрица: будет ли перезагрузка? М.: «Алгоритм» : «ЭКСМО», 2012. – 240 с.
2. Воробьев Ю.Л., Малинецкий Г.Г., Махутов Н.А. Теория риска и технологии обеспечения безопасности. Подход с позиций нелинейной динамики // Проблемы безопасности в чрезвычайных ситуациях. Часть 1 1998 № 11 С. 5-21 и Часть 2 1999 № 1. С. 18-41.
3. Крылов В.Ю., Курдюмов С.П., Малинецкий Г.Г. Психология и синергетика. Препринт ИПМ им. М.В. Келдыша АН СССР № 41, 1990
4. Голова придумала – руки сделали. Для обеспечения полномасштабного импортозамещения необходимо начинать с развития Российских НИОКР. Интервью с начальником Департамента технологических партнерств и импортозамещения ПАО «Газпромнефть» С. Архиповым // Нефть России: аналитич. журн. – 2018.— № 1-2. – Режим доступа: http://neftrossii.ru. – (Дата обращения: 05.09.2018)

Кафидов В.В.

Роль общественности в контроле за обеспечением безопасности муниципального образования

Аннотация: Рассматриваются вопросы участия общественности в обеспечение безопасности муниципального образование в рамках территориального общественного самоуправления.

Ключевые слова: безопасность, общественность, поселение, территориальное общественное самоуправление, органы местного самоуправления

Обычно, обсуждая проблемы опасности и безопасности объекта защиты, не рассматривается специфика организации и управления социальными системами. В отличие от технических систем, социальные системы не управляются извне. Поэтому приходится модифицировать общепринятое кибернетическое определение управления. Управление заключается не в воздействии на систему для перевода ее в заданное состояние или поддержания в заданном состоянии. Управление заключается во взаимодействии субъекта и объекта управления (которые находятся внутри системы) для достижения поставленной цели.

Соответственно указанной специфике следует уточнить и определения опасности и безопасности. Если согласиться с тем, что расхожее мнение о том, что безопасность – это отсутствие опасности, не точно, то можно предложить следующее определение: опасность – это, во-первых, возможность (или способность) нанесения вреда любому объекту защиты и, во-вторых, это свойство окружающей среды. Опасность – это явление, способное нанести вред (ущерб) жизненно важным интересам личности, общества и государства. Однако, справедливо и обратное.

Для социально-экономических систем необходимо учитывать влияние опасных факторов и внутренней среды, действиями подсистем и элементов подсистем разного уровня, связанных с возможными кризисами, описанными в моделях жизненного цикла организации (например, жизненный цикл Ицхака Адизеса). При этом нужно учитывать требования системного подхода, заключающиеся в рассмотрении того уровня систем, на котором возникает проблема.

В отличие от опасности, безопасность – это не свойство элементов среды, а состояние защищенности объектов, связанных с жизненно важными интересами личности, организации, общества и государства.

Безопасность означает допустимый уровень опасности во внутренней и внешней среде системы, допустимый риск ее воздействия на объект защиты или уровень защиты этого объекта. В зависимости от иерархии систем необходима защита и от действий групп организации и отдельных индивидов.

В каждом конкретном случае может определяться приемлемый риск. В коммерческих организациях диапазон риска может быть больше, так как это зависит от требуемой и допустимой предприимчивости. В бюджетных организациях он должен быть фиксированным.

Понятие жизненно важных интересов может применяться и относительно организаций, ее собственников, сотрудников, смежников, потребителей продукции и других заинтересованных лиц и организаций.

В связи с отмеченными обстоятельствами важное значение приобретает привлечение общественности к решению вопросов безопасности как во внутренней, так и во внешней среде организации. На уровне предприятий

и организаций роль общественности в контроле за безопасностью внутренней среды весьма ограничена. Во внешней среде возникают независимые общественные организации, заинтересованные во взаимодействии с органами местного самоуправления (МСУ) для контроля за обеспечением безопасности на территории муниципального образования.

Поселение является формой включения индивида в общественную жизнь, средой его социализации. Оно формирует у него определенные социальные качества. Любой тип поселения – это непосредственная среда жизнедеятельности человека. В данном плане социальная функция поселения выражает его место в границах общества.

Хотя официально провозглашается, что население является непосредственным субъектом управления муниципального образования, реально это невыполнимо, но население является источником власти.

Субъектом управления в системе является руководство муниципального образования (руководитель муниципального образования и руководитель администрации). Сама администрация муниципального образования представляет собой элемент объекта управления. Объектом управления является муниципальное хозяйство.

Заказчиком и потребителем услуг МСУ выступают жители и население муниципального образования, а так же субъекты хозяйствования, находящиеся и ведущие бизнес на его территории. Выразителем интересов жителей и населения, их представителем в органах власти является муниципальное собрание депутатов со своим председателем. Руководитель муниципального образования формально подотчетен населению и муниципальному собранию, хотя по закону может быть председателем муниципального собрания.

Среда муниципального образования как системы управления имеет сложное строение. С одной стороны, само поселение является средой социализации для жителей и населения. С другой стороны, само поселение имеет внутреннюю и внешнюю среду.

Если рассматривать уровень поселения, то функции по обеспечению безопасности осуществляются органами МСУ. Вместе с тем все большее значение приобретают территориальные органы самоуправления (ТОС).

В качестве гипотезы можно сформулировать некий предполагаемый парадокс. С одной стороны, потребность в возникновении ТОС появляется в том случае, когда не работают или работает не достаточно активно орган МСУ. С другой стороны, как показывает статистика, успешное развитие ТОС и наблюдается в случае активной работы муниципалитетов. Получается так, что ТОС, с одобрения муниципальных властей берут на себя решение социально важных вопросов на конкретной территории. Одной из функций ТСО может являться и контроль, через мониторинг

принимаемых на муниципальном уровне решений и выявление случаев не принятия решений, за деятельностью органов МСУ. Возникает вопрос, а зачем этот контроль органам МСУ? Что за механизмы заставляют власть заботиться об обратной связи в управлении? Безопасность, самосохранение власти. Есть мнение, что условия для осуществления общественного контроля создает правящая элита. «Правящий класс становится по-настоящему элитой тогда, когда он отождествляет свои эгоистические интересы с национальными интересами страны, которые заключаются в обеспечении безопасности и благополучия народа, верховенства права, исполнения закона, защиты прав и свобод человека, формирования широкого слоя среднего класса – основы сильного гражданского общества, развития демократии и эффективной экономики» [1].

Создание системы общественного контроля (ОК) позволяет обеспечивать управляемую и предсказуемую обратную связь в управлении.

На муниципальном уровне власть ближе к народу и, казалось бы, должно быть больше внимания к ОК, но дальше контроль вышестоящих органов, вместо элит появляется местничество. Контроль не предполагает сами действия по приведение в должное состояние контролируемого объекта или процесса, этим занимается объект контроля. Контроль – одна из важнейших функций управления.

Законодательством предусмотрено право на осуществление ОК на федеральном уровне, уровне субъекта федерации и муниципальном уровне. Право участия в ОК может быть поручено в соответствующих рамках группам общественности. Это контроль сверху. А через ТСО может быть осуществлен контроль снизу. Народ не может вырабатывать идеи, это удел просвещенной, нравственной и т.д. общественности.

Очень важная функция ОК и формирование этой общественности. Вырабатываются консолидированные решения, общественное мнение благодаря взаимодействию и самоорганизации.

Законодательные нормы не предусматривают конкретные направления совершенствования работы органов местного самоуправления и технологии использования результатов общественного контроля в деятельности органов власти, не определяют формы взаимодействия субъектов общественного контроля, не регламентируют санкции по итогам реализации контрольных действий. Появляется возможность привлекать общественность для контроля за деятельностью самих органов МСУ по обеспечению безопасности на территории муниципального образования.

Различают общественный и социальный контроль. Это почти синонимы, но возможна такая трактовка: социальный – со стороны общества, общественный со стороны групп общественности. А это может

быть общественная палата, общественные организации, организации местного самоуправления, общественные советы и др. Их деятельность законодательно и нормативно регулируется, существуют нормы, определяющие деятельность общественных групп, имеющих право контроля. Обычно ОК направлен на виды деятельности, а в данном случае нас интересует деятельность по обеспечению безопасности. Однако не менее важен и более доступен с точки зрения профессиональной подготовки контроль за организацией муниципалитетами условий для этой деятельности.

«К сожалению, контроль и надзор за деятельность органов местного самоуправления в настоящее время основываются главным образом на количественном подходе, целью которого является не столько обеспечение качества оказания муниципальных услуг, сколько количество мер реагирования» [2].

Какие же возможности ОК за деятельностью органов МСУ в вопросах обеспечения безопасности появляются с созданием ТОС. ТОС – это углубление самоуправления, придаток официальной власти или компенсация недостатков власти, вынужденная мера самоорганизации общества. Любое управление, включая самоуправление, представляет процесс, состоящий из выполнения ряда функций: планирование, организация, мотивация и контроль. В случае ТОС группы общественности, представляющие население или его часть под свою ответственность берутся за решение социально важных вопросов, но с ведома ОМСУ. Функции организации, мотивации и контроля за деятельностью ТОС являются внешними. Фактически нет обратной связи населения с органами МСУ через деятельность ТОС.

Анализ отчетов о работе ТОС ряда муниципальных образований позволяет утверждать, что основные усилия ТОС сосредоточены на тех вопросах, которые не делают органы МСУ или до которых не доходят руки. Получается, что ТОС самоуправлением не занимается, а решает вопросы самоорганизации и самодеятельности. Т.е. если самоуправление представляет собой единство субъекта и объекта управления, то в деятельности ТОС проявляются функции преимущественно объекта управления. Советы ТОС мобилизуют усилия населения, привлекают спонсоров. Однако совершенно отсутствует информация о мерах ТОС по контролю за деятельностью органов МСУ, о постановке вопросов, почему эти вопросы не решаются, хотя средства выделяются. Эти вопросы не решают депутаты и не решают органы ТОС. Фактически ТОС выполняют работу, которую должны организовывать и возглавлять депутаты. На практике получается так, что ТОС является придатком ОМСУ и не выполняет функции самоуправления. Этому способствует и финансовая зависимость от администрации. И все же, несмотря на рассмотренные

недостатки, ТОС могут взять на себя очень важные в настоящее время функции по контролю за безопасностью, в частности, за пожарную безопасность жилого сектора, особенно в сельской местности, и совместно с депутатами по контролю за деятельностью органов МСУ по обеспечению безопасности муниципального образования.

Литература:
1. *Аринин А.* Мировой опыт общественного контроля над деятельностью власти: уроки для России 22.03.2010 Часть первая. Автор: Александр Аринин доктор политических наук // Режим доступа: URL:http://www.lawinrussia.ru/ (Дата обращения: 12.10.2018).
2. Российское местное самоуправление: итоги муниципальной реформы 2003-2008 гг. Аналитический доклад Института современного развития» [электронный ресурс] // Режим доступа: URL: http://www.riocenter.ru/ru/programs/doc/3928 (Дата обращения: 12.10.2018).

Кононов Д.А.

Правовая система обеспечения государственной безопасности: методология исследования

Аннотация: Рассмотрены проблемы и задачи совершенствования правоохранительной системы как подсистемы обеспечения государственной безопасности. На основе стратификации социально-экономической системы рассмотрены историко-философские основы права, правовые аспекты организационного управления. Предложена методология исследования.

Ключевые слова: государственная безопасность, правовая система, методология исследования

I. Введение

Исследование государственной безопасности представляет собой важную и достаточно неоднозначную задачу. В общем случае безопасность следует понимать как «отсутствие опасности». Следовательно, необходимо изучить те опасности, которые возникают в реальной действительности (или их виртуальные, кажущиеся аналоги), в том числе в деятельности Общества. Изучение проводят на основе построения модели посредством выявления и определения ее системных параметров. Они представляют собой основные свойства и определяют

возможности эффективного функционирования и развития. В Социуме наиболее общей системой является социально-экономическая система (СЭС).

Социально-экономическая система характеризуется большим числом существенных параметров функционирования и развития. Следовательно, при моделировании ее поведения целесообразно выделять различные ее компоненты, или страты.

В работе [1] предложена стратификация СЭС, представленная в виде определенной иерархии подсистем. Указанные подсистемы имеют характерные особенности, средства исследования, критерии функционирования и развития.

Технологическая страта представляет собой комплекс технологий (в том числе логистику), которыми располагает и/или использует СЭС для функционирования и развития.

Организационная страта – формализованное описание организационной и функциональной структур, т.е. информационных и управленческих отношений между субъектами деятельности.

Правовая страта описывает законодательное регулирование деятельности субъектов деятельности СЭС.

Экономическая страта описывает отношения, которые регулируются категорией стоимости. Здесь выделим производственные и финансовые связи, контрактные условия с контрагентами, возможности их модернизации и развития.

В культурологической страте рассмотрим специфические для СЭС этнические, исторические, религиозные и культурные особенности, которые могут существенно влиять на развитие.

К социальной страте отнесем совокупность необходимых данных, описывающих протекание социальных процессов как внутри СЭС, так и во внешней среде. Социальная страта описывает социальную структуру, характер выполняемой деятельности, характерные экономические и культурные связи, основные показатели социального развития и т.п.

Процессы преобразования подсистем социально-экономической системы и условий их развития в целях наиболее эффективного функционирования хозяйственного механизма в Российской Федерации связаны со значительными трудностями. Во многом они определяются необходимостью проведения крупномасштабных, в том числе структурных, изменений в ведущих отраслях промышленности, реконструкции и модернизации производственных процессов, перехода на новые технологии и отношения, обеспечивающие удовлетворение потребностей в высокотехнологичной и качественной продукции,

конкурентоспособной на мировом рынке, тщательного научного анализа эффективности использования материальных, финансовых и общественных ресурсов. Указанные частные цели развития затрагивают все страты СЭС России и интегрируются в понятии «безопасность функционирования и развития системы». Последнее требует систематизированного аналитического исследования на основе математического моделирования. В настоящей работе рассмотрим вопросы сценарного моделирования правовой страты.

II. Историко-философские основы правовых отношений

Понятие «право» возникло при феодализме и представляет собой производственные отношения. Юридическое законодательство фиксирует условия их осуществления.

«В отличие от Закона, жестко предписывающего, регламентирующего определенные действия, Право лишь устанавливает систему ограничений, в пределах которых возможны любые действия, не выходящие за их рамки. Только начиная с этой ступени возможно говорить о «правах и обязанностях», «индивидуальной свободе», «взаимных обязательствах» и т.п. Смешение «Закона» с «Правом» в обыденном понимании является следствием того, что Право… по отношению к Закону выступает как форма по отношению к содержанию: закон как свод регламентации превращается в закон как свод ограничений, т.е. закон, в котором фиксируется право» [2].

Право – основные производственное отношение феодального способа производства, выступая в форме вассалитета, феодального права.

«Между феодализмом и капитализмом… находится еще один переходный способ производства – абсолютизм…

При абсолютизме право из господствующего производственного отношения превращается в то, что можно купить. Основной формой зависимости крестьян становится денежная рента. С другой стороны, благодаря деньгам образуется новый слой аристократии («дворянство плаща» наряду с «дворянством шпаги»). Деньги становятся средством перехода в более высокое сословие. Массы выкупившихся крестьян пополняют ряды свободных ремесленников, объединяющихся в цехи. В городах под сенью Магдебургского права расцветают могущественные купеческие гильдии, расширение торговли приводит к образованию национального рынка. И все это торгашеское буйство поощряется абсолютным монархом, расширяя, в свою очередь, его финансовую мощь, которую, в опоре на наемное войско и свободные города, он использует для ликвидации феодальной раздробленности.

Основным производственным отношением абсолютизма как способа производства является товарно-денежное отношение...

При капитализме деньги – это средство делать деньги, и это свойство они приобретают только в качестве капитала. При абсолютизме деньги – это только средство купить себе право перейти в более высокое сословие. С другой стороны, для высших сословий, нуждающихся в деньгах, средством их получения является сословное право. Деньги обмениваются на право, а право обменивается на деньги. Имеющие деньги постепенно приобретают права, имеющие права спускают их за деньги. Эти два встречных потока медленно просачиваются сквозь систему сословных плотин и шлюзов, которая, наконец, взрывается буржуазной революцией» [2].

Эти исходные философские позиции далее претворяются ныне в организационные и юридические формы.

III. Правовые аспекты организационного управления

В процессе управления национальной экономикой и обеспечения безопасности важное место занимает право. С помощью права в управление вносится необходимая мера нормативного регулирования, формальной определенности и упорядоченности, закрепляется объем полномочий и ответственности звеньев управления и четкий порядок их взаимоотношений.

Право охватывает, по существу, всю систему и весь процесс управления. Правовое регулирование субъектов и объектов управления дополняется регламентацией сфер государственной и общественной жизни, в том числе и экономики. Поэтому от умелого решения юридических вопросов во многом зависит качество управленческой деятельности и эффективность развития хозяйства. Любая недооценка юридических стадий организационного управления отрицательно сказывается на его эффективности, дезорганизуя его, порождая безответственность, дублирование, субъективизм и бюрократизм.

Единообразное понимание и применение законов, а также их точное и неуклонное исполнение – важнейшая составная часть всего правового регулирования в сфере производственно-хозяйственной деятельности. Следует также подчеркнуть, что принятие и наличие самых совершенных законов само по себе еще не гарантирует надлежащего уровня правопорядка и организованности. Для того чтобы законы до конца выполнили свою целевую функцию в обществе, чтобы достичь реализации главных целей законодательной деятельности в государстве, необходим четко отлаженный механизм их реализации, стройная иерархия методов

правового регулирования общественных отношений и прежде всего в сфере управления производством.

Правовое регулирование осуществляет государство, которое не только вводит юридические средства воздействия на общественные отношения, но и гарантирует общеобязательность их исполнения (применяет государственное принуждение). Правовое регулирование необходимо постольку, поскольку созревшие экономические и политические условия делают необходимым такое поведение людей, которое закреплено нормами права. Предметом правового регулирования являются фактические общественные отношения, которые могут быть различными по своей природе и содержанию.

Суть воздействия права на экономику заключается в том, что производственная деятельность людей закрепляется соответствующими нормами. Таким образом, если экономика – суть, то право – это совокупность норм, определяющих формы общественных процессов.

Правовое воздействие направлено прежде всего на регулирование целесообразной, экономически обоснованной деятельности, поэтому юридические нормы с запрещающими, карающими, т.е. олицетворяющими применение государственного принуждения санкциями, не занимают ведущего положения.

Виды правовых норм по характеру их воздействия можно разделить на следующие группы: а) нормы-цели; б) плановые нормы; в) нормы-предписания (ГОСТы, регламенты и т. п.); г) нормы-ориентиры (методики, рекомендации и т. п.); д) нормы-запреты; е) нормы-разрешения.

Такая классификация дает представление о содержании и формах выражения правовых воздействий как управлений.

Наступающая ответственность закреплена правом в нескольких видах: имущественная (гражданская), материальная, дисциплинарная, административная и уголовная.

Анализ причин нарушений законности позволяет суммировать их следующим образом. Прежде всего, к ним относятся недооценка роли права в управлении и игнорирование юридических предписаний в решении управленческих и хозяйственных задач. Не налажена должным образом четкая правовая регламентация функций, взаимоотношений и ответственности звеньев управления. В ряде случаев задержка процесса обновления правовых актов и изменения устаревших также может порождать нарушение законности.

Структура и содержание информационного обеспечения, которое используется при решении задач выработки и реализации управляющих воздействий правового характера приведена в [3].

IV. Заключение

В настоящее время отсутствуют теоретические и методологические основы исследования правовой системы как подсистемы обеспечения государственной безопасности. В основу предлагаемой методологии исследования предлагается положить компоненты: модель системы безопасности; модель правового обеспечения безопасности; методология построения и анализа сценариев функционирования и развития системы; сценарные модели системных параметров (характеристик) безопасности государственной системы; модели реализации угроз и распространения возмущений при принятии Закона; модель уязвимости.

Общая идея заключается в построении системы государственной безопасности как динамической социально-экономической системы с выделенной правовой стратой. Последняя должна быть представлена динамической моделью с компонентами – Участниками системы (МВД, СК, Прокуратура…), связанными показателями и характеристиками функционирования и развития.

Создание такой динамической модели позволит на основе методологии сценарного исследования

– проводить анализ эффективности изменений функционирования системы безопасности при введении новых Законов;

– проводить анализ перестройки структуры правовой системы;

– проводить анализ реализации угроз системе безопасности;

– выявлять места уязвимости в системе безопасности;

– строить сценарии эффективного правового управления.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16151

Литература:

1. Модели и методы анализа и синтеза сценариев развития социально-экономических систем. Кн. 1, 2 /Под редакцией чл.-корр. РАН Шульца В.Л., д.т.н., проф. Кульбы В.В. – М.: Наука, 2012.
2. Платонов С. После коммунизма: Кн., не предназнач. для печати /Предисл. В. Аксенова и др. 2-е изд.; Второе пришествие: беседы. – М.: Молодая гвардия. 1991.
3. Информационное обеспечение систем организационного управления (теоретические основы). В 3-ч частях Ч.1. Методологические основы организационного управления /Под ред. Е.А. Микрина и В.В. Кульбы. – М.: Физматлит, 2011. - 464 с.

Гориславец А.Ю.

Современные аспекты нормативно-правового регулирования деятельности хозяйствующих субъектов в Российской Федерации – как фактор обеспечения экономической безопасности государства

Аннотация: Обеспечение экономической безопасности современного правового государства невозможно представить без комплексного подхода к вопросу нормативно-правового регулирования деятельности одних из основных его элементов и объектов – хозяйствующих субъектов. В статье рассматриваются основные современные российские тенденции в области правового регулирования различных аспектов хозяйственной деятельности юридических лиц и индивидуальных предпринимателей, которые направлены на повышение эффективности их функционирования, а также определение наиболее перспективных направлений дальнейшего работы по совершенствования законодательства в целях обеспечения экономической безопасности государства.

Ключевые слова: нормативно-правовое регулирование, хозяйствующие субъекты, фактор, экономическая безопасность, государство

При определении уровня развития современного правового государства, с точки зрения обеспечения его экономической безопасности, особого внимания заслуживает рассмотрение актуальных тенденций совершенствования законодательной базы в области регулирования деятельности хозяйствующих субъектов.

За период с 2016 по 2017 годы профильные субъекты законодательной инициативы проделали огромную работу в этом направлении. Ими были реализованы очень важные законодательные предложения и инициативы, направленные на улучшение положения субъектов малого и среднего предпринимательства в Российской Федерации.

Предпринимательское сообщество всегда очень осторожно относится к любым предложениям субъектов законодательной инициативы в сфере совершенствования аспектов его хозяйственной жизни, вынося наиболее значимые из них на широкое обсуждение.

Сегодня всё большее значение в вопросах поддержки российских предпринимателей имеют различные общественные организации и ассоциации, институты развития, штабы по защите предпринимателей. Отдельно следует выделить активную работу Уполномоченного при Президенте России по защите прав предпринимателей. Институт уполномоченных появился в России относительно недавно, но результаты

его работы уже сегодня свидетельствуют о существенной поддержке со стороны представителей бизнеса.

Прежде всего, бизнес-сообщество заинтересовано в продуманной и глубоко проработанной комплексной программе поддержки со стороны государства.

Несмотря на достаточно большое количество существующих форм государственной поддержки предпринимателей, актуальной остается проблема выбора наиболее оптимальных из них с точки зрения минимизации предпринимательских рисков, под которыми принято понимать степень наступления негативных последствий, являющихся результатом влияния факторов внешней и внутренней среды.

Анализ эффективности нормативно-правового регулирования деятельности хозяйственных субъектов представляется сложной и комплексной задачей для разработчиков законодательных инициатив, которая требует непосредственного диалога с представителями делового сообщества.

За последние два года в России на законодательном уровне было принято огромное количество документов, призванных защищать и охранять права предпринимателей.

Цель таких документов – помочь предпринимателям в сложных социально-экономических условиях российской действительности.

Отдельного внимания заслуживает Стратегия развития малого и среднего предпринимательства в Российской Федерации до 2030 года, которая была принята Правительством России в 2016 году, целью которой является развитие сферы малого и среднего предпринимательства в качестве одного из факторов инновационного развития страны и улучшения отраслевой структуры российской экономики.

В качестве основных направлений Стратегии следует отметить следующие:

1. объединение функций поддержки малого и среднего предпринимательства;
2. активное стимулирование спроса на выпускаемую продукцию малых и средних компаний (в том числе благодаря расширению доступа таких компаний к закупкам товаров, работ, услуг организациями государственного сектора экономики);
3. создание и обеспечение условий для повышения производительности труда на малых и средних предприятиях;
4. существенное повышение качества государственного регулирования в сфере малого и среднего предпринимательства;
5. повышение доступности финансовых ресурсов для малых и средних компаний;

6. повышение эффективности государственной политики в области налогообложения;
7. активное развитие предпринимательской деятельности на отдельных территориях страны («Территории опережающего социально-экономического развития»).

Благодаря реализации этой Стратегии планируется:

- увеличение доли малых и средних предприятий в валовом внутреннем продукте страны в два раза с 20 до 40%;
- увеличение оборота малых и средних предприятий в 2,5 раза;
- увеличение доли количества занятых в сфере российского малого и среднего предпринимательства в общей численности занятого населения до 35%;
- увеличение доли обрабатывающей промышленности в обороте сектора малого и среднего предпринимательства без учёта индивидуальных предпринимателей до 20%;
- повышение производительности труда в этом секторе в два раза.

Кроме этого, Стратегией предусматривается введение трехлетнего моратория на организацию и осуществление плановых проверок со стороны контрольно-надзорных государственных органов в отношении субъектов малого предпринимательства, формирование, систематизация и ведение единого сводного реестра проверок, внедрение риск-ориентированного подхода проверок.

Органами государственной власти, которые наделены полномочиями по выработке государственной политики в сфере предпринимательской деятельности совместно с различными институтами поддержки бизнеса проводится серьезная работа, результатом которой должен стать рост интереса общества к предпринимательству, выработке мер поддержки и её совершенствования, в том числе информационной, технической и финансовой.

Современный предприниматель, сталкиваясь в повседневной работе, с самыми разными ситуациями, должен все свои усилия направлять на развитие своего дела и быть уверенным, что его интересы надежно защищены на законодательном уровне.

Таким образом, совершенствование нормативно-правового регулирования предпринимательской деятельности на сегодняшний день представляется важнейшим аспектом в работе профильных органов государственной власти.

Вместе с тем, проводя сравнительный анализ состояния малого и среднего предпринимательства за рубежом, наблюдается значительный разрыв в таких показателях как:

1) доля малого и среднего предпринимательства в валовом внутреннем продукте страны;

2) доля общей занятости населения в малом и среднем предпринимательстве;

3) доля МСП в количестве компаний.

Обращает на себя внимание отсутствие достаточно профессиональных исследовательских трудов, посвященных изучению вопросов предпринимательства, в которых экспертами, в том числе, анализируются законодательные новшества и даются оценки от их внедрения в хозяйственную практику компаний.

В 2017 году вышел Обзор Организации экономического сотрудничества и развития (ОЭСР) «Панорама предпринимательства 2017», в котором нашли отражение основные тенденции в сфере предпринимательства в странах ОЭСР. А также российский национальный отчёт «Глобальный мониторинг предпринимательства. Россия 2016», который выполнен в рамках международного проекта «Глобальный мониторинг предпринимательства» (Global Entrepreneurship Monitor).

Сегодня проект GEM – это наиболее влиятельное исследование, посвященное изучению взаимоотношений между предпринимательством и экономическим ростом, а также в котором представлена информация для организации и проведения сравнительных исследований об уровнях предпринимательской активности не только на этапе создания, но и на этапе развития предпринимательской фирмы.

Подобные исследования непосредственно играют большую роль при оценке в том числе возможных аспектов правового регулирования вопросов предпринимательства и позволяют получить экспертное мнение у представителей различных отраслей национальной экономики.

Безусловно, говорить об эффективности реализуемых нормативно-правовых мер, направленных на повышение эффективности деятельности российских хозяйствующих субъектов, можно только исходя из анализа последующей правоприменительной практики.

Артемов О.Ю., Овчинникова Н.В., Овчинников С.А.

К вопросу о структуре и содержании Концепции безопасности компании

Аннотация: В статье раскрываются сущность, место и роль Концепции безопасности в системе управления современными организациями.

Ключевые слова: защита информации, злоупотребления, коммерческая тайна, концепция, личная безопасность, механизм обеспечения безопасности, превентивные меры, режим безопасности

С целью более четкого и качественного планирования мероприятий по обеспечению безопасности является разработка соответствующей Концепции, представляющей собой официально утвержденный документ, в котором отражаются цели и задачи, принципы и способы противодействия различного рода опасностям, определяется система требований и условий для защиты собственности компании. Ее предназначение – сделать нарушения режима безопасности максимально затруднительными для злоумышленников и нерадивых работников.

Структура Концепции безопасности включает следующие части [1].

1. *Описание проблемных ситуаций в данной сфере*. В «идеале» оно должно содержать: а) перечень потенциальных и реальных угроз безопасности, а также их ранжирование; б) причины и факторы появления различного рода опасностей; в) их негативные последствия.

2. *Выбор механизма обеспечения безопасности*, предусматривающего: а) определение объектов защиты компании; б) формулирование политики и стратегии безопасности; в) принципы, цели и задачи ее обеспечения; г) критерии и показатели безопасности; д) создание структуры по управлению системой безопасности.

3. *Определение мер по реализации мер безопасности*, включающих: а) формирование подсистем общей системы безопасности компании; б) определение субъектов безопасности компании и их ролей; в) расчет средств и определение методов обеспечения безопасности; г) контроль и оценка процесса реализации Концепции.

Очень важно при этом очень важно определить способы защиты материальных ресурсов и имеющейся информации, а также усилить личную безопасность сотрудников. Так, к примеру, в первом случае необходимо ответить на следующие вопросы: Достаточно ли надежно охраняется оборудование, ценности, информация? Насколько просматриваются помещения снаружи и из каких зон? Работает ли сигнализация? Какие осуществляются противопожарные мероприятия? Как будет действовать охрана, если сработает сигнализация? Имеются ли резервные копии информации? Где и как они хранятся? Как скоро можно восстановить работоспособность компании, если случится то или иное форс-мажорное событие? Это не банальные вопросы. Ряд простых превентивных мер в ответ на них позволит снизить уровень потенциальных угроз. Это: обустройство «зон» для конфиденциальных бесед с клиентами; оборудование защищенных помещений для операций с крупной наличностью; обустройство внешнего периметра компании и его внутренних помещений современными средствами сигнализации и защиты; разработка системы доступа лиц, обслуживающих технические

средства охраны и компьютеры; продумывание расположения постов охраны в рабочее и нерабочее время. Все эти меры направлены на снижение рисков в случае силового покушения на собственность компании и в некоторой степени на предотвращение утечки информации. Наибольшую часть в решении этих вопросов может взять на себя охранная организация.

Очевидно, не все потенциальные угрозы разрешаются традиционными мерами безопасности. Например, внутреннее мошенничество и злоупотребления. Для этого требуется организовать контроль над доходами и расходами сотрудников, имеющих право финансовой подписи или допущенных к конфиденциальной информации. Появление у работника сумм, не отраженных в его налоговой декларации, должно стать сигналом к проведению мероприятий по установлению источников его непомерно возросших доходов. Вместе с тем персонал часто совершает те или иные поступки в качестве мести за несправедливость и жесткость со стороны администрации, притеснение в коллективе. Поэтому, чтобы исключить их, необходимо создавать благоприятный социально-психологический климат внутри компании. Предотвратить внутренние мошенничества можно за счет недопущения узурпации власти одним из топменеджеров. Вот почему в состав всех подразделений, участвующих в решении стратегических вопросов, должны включаться юристы, экономисты и сотрудники службы безопасности.

Если фирма только начинает собственное дело, и в ее штате всего несколько сотрудников, то и в этом случае желательно предпринять хотя бы следующий минимум защитных мер, а именно: разработка простых соглашений о неразглашении частной информации для персонала, использование штампа «секретно» на деловых планах, списках покупателей, чертежах и другой технической документации.

Если вопросом защиты информации занимается более крупная компания, и руководством принято решение о создании полноценной системы ее безопасности, то необходимо: а) оценить важность и ценность информации, чтобы понять, какие данные, для чего и от кого нужно защищать; б) внести дополнения в уставные документы и подготовить перечни сведений, составляющих коммерческую тайну; в) обозначить защищаемую информацию соответствующими указателями на ее носителях, организовать их учет, а также разграничить доступ персонала; г) организовать минимум физической защиты помещений и хранилищ данных; д) регламентировать использование средств их связи и передачи; е) подобрать специалистов и начать работу по защите с помощью средств вычислительной техники; ж) заручиться поддержкой профессионалов в области защиты информации и юриста.

Как уже было отмечено, необходимо разработать «Перечень сведений, составляющих коммерческую тайну компании и основные требования к сотрудникам по ее защите», а также «Перечень сведений, которые не

должны разглашаться посторонним лицам в целях личной безопасности сотрудников компании». Оба эти локальных акта следует закрепить в приказе и дать под расписку каждому работнику. Так, к примеру, первый документ является прямой основой для возникновения юридической ответственности в соответствии с гражданским законодательством. Второй нужен в связи с тем, что некоторую информацию трудно отнести к коммерческой тайне, но сохранять ее весьма важно (например, место нахождения руководителя в конкретное время, планируемые совещания, переговоры, сведения о личной жизни сотрудников).

Ещё одним полезным документом является «Договор-обязательство о сохранении коммерческой тайны и другой служебной информации». Это может быть как отдельный акт, так и специальный раздел в трудовом договоре о найме на работу. Предложив сотруднику подписать договор-обязательство, администрация предупреждает последнего о том, что в дело вступает целая система мероприятий по защите информации: правовых, организационных, технических.

Для построения системы защиты коммерческой тайны в компании очень полезно определить источники и соответствующие им каналы утечки информации, перечень которых на каждом конкретном объекте носит индивидуальный характер, что определяется спецификой его деятельности. Носителями коммерческой тайны могут быть: сотрудники, документы, изделия / продукция, процессы [2].

Сотрудники. Круг лиц, причастных к служебным тайнам, должен быть максимально сужен. Получать конфиденциальные документы должны только те лица, кому действительно необходимо знать содержащиеся в них сведения. Если в компании не отработана система определения такого круга лиц, то любая система контроля за движением документов будет бессмысленной.

Документы. Следует завести специальный журнал учета входящих, исходящих и внутренних документов, содержащих конфиденциальную информацию. Его наличие позволит периодически проводить инвентаризацию и своевременно уничтожать бумаги, потерявшие для компании (но не для ее соперников на рынке) значение. Кроме того, для документов, содержащих сведения, разглашения которых администрация хотела бы избежать, следует установить специальный порядок подготовки, маркировки (т.е. присвоения соответствующего грифа), размножения, рассылки, приема и учета, группировки в дела, использования, хранения, уничтожения и проверки наличия. В договорах с контрагентами компании также необходимо специально оговаривать обязательства о соблюдении условий конфиденциальности и предусмотреть последствия нарушения принятых обязательств. Актуально вести защиту компьютерных сетей и персональных компьютеров сотрудников посредством различных ограничений доступа к информационным базам, а также введением специальных паролей и кодов.

Изделия / Продукция. Требуется вести надежный учет всех товаров, промышленных и экспериментальных образцов, сведения о которых не должны стать достоянием конкурентов. Охрана изделий необходима на всех этапах их движения внутри компании (в том числе приобретения или изготовления, испытаний либо проверки качества, транспортировки, хранения, эксплуатации, ремонта и пр.).

Технические каналы передачи информации. Следует установить систему ограничений на использование телефоном, факсом, Интернетом, компьютерными сетями и пр. для передачи конфиденциальных сведений. Охранять от возможного подслушивания или сканирования необходимо не только служебные помещения, но и личные квартиры, автомобили, ПК, для чего можно использовать засекречивающую аппаратуру связи, генераторы помех, приборы для обнаружения «жучков» и сканирующих устройств, а также применять условные кодовые обозначения.

Требуется также разработать меры по обеспечению личной безопасности. Последняя в определяющей степени зависит от самого человека, соблюдения им соответствующих правил предосторожности и форм поведения, которые усваиваются в процессе воспитания, обучения и накопления опыта. Важнейшей стратегией личной безопасности является информационная защита, включающая: а) сокрытие личных данных, которые в случае их оглашения могут нанести ущерб; б) четкий инструктаж родственников и ближайшего окружения о том, какие сведения о сотрудниках им не следует сообщать; в) своевременное информирование службы безопасности компании обо всех фактах подозрительного, необоснованного интереса, указывающих на сбор досье; г) доведение до окружения заранее обработанных данных, которые могут ввести злоумышленников в заблуждение или усилить у них чувство неуверенности (страха) в возможности реализации преступных намерений.

Следующий шаг – это выбор мер противодействия, так как по каждому из элементов реагирования необходимо создать детальное описание предпринимаемых действий. В качестве мер противодействия выступают: *электронные системы безопасности* (объединяют системы контроля доступа, обнаружения, наблюдения и сбора свидетельских показаний; в число их подсистем могут входить тревожные кнопки, охранное телевидение, проводные и радиопереговорные устройства, громкоговорящие системы, средства индивидуальной защиты и телефонные комплексы) *физические и психологические барьеры* (применяются для затруднения доступа к объекту; так, к примеру, в число физических барьеров входят: хранилища, сейфы, шлагбаумы, ограждения и ворота, колючая проволока, ловушки для транспортных средств, бронезащита автомобилей, механические замки, средства освещения, щиты, панели из прочных материалов и специальные элементы ландшафта), *персонал службы безопасности* (исполняет различные

охранные функции, включая оперирование электронными системами, несение вахты на постах и осуществление патрулирования; большинство действий охраны предусматривают наблюдение за событиями и, в случае инцидента, постановка в известность правоохранительных органов; в некоторых случаях охранники могут быть вооружены, иметь специальную подготовку и обладать правом вмешиваться в ход событий) и *политики* (устанавливают позицию управляющего звена и общий подход к практике разрешения бизнес-проблем; считаются наиболее критичной частью программы безопасности, поскольку определяют программы и процессы, необходимые для того, чтобы эффективно работали все возможные механизмы защиты [3].

Далее идет внедрение, когда рекомендации преобразуются в спецификации и инструкции, направленные на действия людей и систем, а также формирование правил и политики компании. Задачей внедрения является перевод плана безопасности в организационные программы, процессы, процедуры и регламентирующие их документы.

Литература:

1. *Александровская, Л.Н.* Статистические методы анализа безопасности сложных технических систем / Л.Н. Александровская и др.– М., 2001.
2. *Каталевский, Д.Ю.* Основы имитационного моделирования и системного анализа в управлении / Д.Ю. Каталевский. – М., 2015. – С. 247 – 249.
3. *Бакланов, В.В.* Введение в информационную безопасность. Направления информационной защиты / В.В. Бакланов. – Екатеринбург, 2007. – С. 82.

Широкий А.А., Финьков В.Н.

Игра с природой как инструмент оценки рисков при реализации охранных мер

Аннотация: В работе предложен подход для оценки рисков охраняемым объектам и выбора оптимального набора охранных мер на основе теоретико-игровой модели со схемой учёта неопределённости «игра с природой». Применение модели позволяет прогнозировать вероятные потери заказчика охранных услуг для произвольного сочетания событий неопределённости и применяемых охранных мер.

Ключевые слова: охрана, риск, неопределённость, матричные игры, игра с природой

Введение

Методы теории игр традиционно используются для оценки рисков при выборе решения из некоторого множества альтернатив. Наиболее часто такой подход можно встретить в работах по обеспечению безопасности информационных систем [1, 3], при решении задач оценки моделей возникновения террористических угроз [2] и охраны государственной границы [4, 5]. Для оценки рисков при выборе мер охраны коммерческих объектов эти методы тоже вполне подходят. Эта задача актуальна для любой владеющей недвижимостью организации. Тем не менее, их руководители на практике редко представляют себе актуальные источники угроз их объектам, что приводит к перерасходу средств на их охрану или повышенным затратам на устранение последствий реализовавшейся угрозы. Методы моделирования угроз применяются для таких задач крайне редко, притом, что устойчивость малых и средних предприятий несравнима с государственными организационными системами и ожидаемый ущерб может легко превысить стоимость всего бизнеса.

Особенность задачи принятия решения о формировании набора охранных мер для коммерческих объектов, на взгляд авторов, заключается в том, что попытка атаки периметра подготовленным злоумышленником маловероятна – охранник главным образом должен предотвращать несанкционированный проход случайных людей и оперативно реагировать на угрозы природного и техногенного характера. Для описания этих условий антагонистические матричные игры (с активным противником) не вполне подходит, поэтому мы предлагаем применить схему учёта неопределённости типа «Игра с природой».

Постановка задача оценки и минимизации рисков при определении набора охранных мер

Зададим частоту дискретизации временным промежутком Δt. В течение каждого такого Δt происходит розыгрыш одной и только одной партии матричной игры. Пусть T – множество угроз. Для каждого неблагоприятного события $\tau \in T$ зададим вероятность p_τ его наступления в течение времени Δt и величину риска $R(\tau)$. Будем считать, что все элементы множества T являются независимыми событиями.

Зададим множество наборов охранных мер M. Применение набора $\mu \in M$ изменяет (обычно снижает) риск, но его реализация требует некоторых ресурсов. Будем описывать это изменение функцией $f_\mu(\tau)$, а стоимость реализации набора мер μ в течение времени Δt примем константой c_μ. Таким образом, вероятные потери предприятия при реализации набора охранных мер μ в случае наступления события τ составят $c_\mu + f_\mu(\tau)$.

Добавим ещё одно – фиктивное – неблагоприятное событие T_0, соответствующее ситуации, когда за время Δt ни одна угроза не реализовалась. Вероятность его наступления определяется как $p_0 = 1 - \sum_\tau p_\tau$, что автоматически влечёт за собой требование

$\sum_{\tau \neq T_0} p_\tau < 1$ (1)

При этом $\sum_{\tau \in T} p_\tau = 1$ и величину риска предприятия при реализации набора охранных мер μ можно определить по формуле Байеса:

$R_\mu = c_\mu + \sum_{\tau \in T} p_\tau f_\mu(\tau)$ (2)

Таким образом, задача минимизации риска заключается в нахождении

$R = \min_{\mu \in M} R_\mu = \min_{\mu \in M} \left(c_\mu + \sum_{\tau \in T} p_\tau f_\mu(\tau) \right)$ (3)

Отметим, что если требование (1) не выполняется, то следует уменьшить Δt. Для лучшего результата следует подбирать Δt таким образом, чтобы p_0 была больше 0,5.

В таблице 1 приведёт общий вид матрицы игры с природой в нормальной форме для m неблагоприятных событий и n наборов охранных мер.

Таблица 1. Матрица игры с природой для m угроз и n наборов контрмер

Наборы контр-мер	Угрозы	T_1	T_2	…	T_m	Нет угроз (T_0)
	Вероят-ность реализа ции	p_1	p_2		p_m	$p_0 = 1 - \sum_\tau p_\tau$
M_1		$c_1 + f_1(T_1)$	$c_1 + f_1(T_2)$	…	$c_1 + f_1(T_m)$	c_1
M_2		$c_2 + f_2(T_1)$	$c_2 + f_2(T_2)$	…	$c_2 + f_2(T_m)$	c_2
…		…	…	…	…	…
M_n		$c_n + f_n(T_1)$	$c_n + f_n(T_2)$	…	$c_n + f_n(T_m)$	c_n
Нет контрмер (M_0)		$R(T_1)$	$R(T_2)$	…	$R(T_m)$	0

В такой постановке для решения задачи минимизации риска достаточно придерживаться байесовской стратегии, которая гарантирует максимальный средний выигрыш в матричной игре с природой.

Заключение

Предлагаемый подход позволяет оценивать риски при определении набора охранных мер для широкого класса объектов. Для получения прогнозов высокого качества важно не только правильно выбрать временной промежуток дискретизации модели и верно оценить вероятность наступления неблагоприятных событий в нём, но и получить адекватные оценки величин вероятных потерь от наступления этих

событий. Это является отдельной и во многих случаях очень непростой задачей.

Кроме того, результаты моделирования могут быть использованы в качестве прогноза только в случае, когда внешние условия более-менее стабильны. Решение задачи выбора охранных мер в условиях постоянно изменяющегося набора угроз потребует существенной модификации предлагаемой модели.

Литература:

1. *Алехин И. В.*, *Голубинский А. Н.* Модели параметров оценки изменения риска возникновения угроз в информационных и технических системах // В сб. Актуальные проблемы деятельности подразделений УИС. Сборник материалов Всероссийской научно-практической конференции, 2015. – С. 247–249.
2. *Кадочникова Е. Н.*, *Фетисов А. В.*, *Черных А. К.*, *Гарькушев А. Ю.* Оценка эффективности применения математических моделей, реализуемых в структурах министерства внутренних дел при возникновении террористических угроз // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – № 3–4 (81–82), 2015. – С. 92–97.
3. *Калашников А. О.* Пример использования теоретико-игрового подхода в задачах обеспечения кибербезопасности информационных систем // Вопросы кибербезопасности. – № 1 (2), 2014. – С. 49–54.
4. *Шумов В. В.* Механизм ранжирования пограничных средств // В сб. Теория активных систем. Материалы международной научно-практической конференции / под общ. ред. В. Н. Буркова. – 2014. – С. 193–194.
5. *Шумов В. В.* Теоретико-игровая модель пограничного сдерживания // Управление большими системами: сборник трудов. – № 42, 201 3. – С. 217–232.

СОКРАЩЕНИЯ

АГПС МЧС России	ФГБОУ ВО «Академия Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий»
АО ГНЦ РФ ТРИНИТИ»	Акционерное общество «Государственный научный центр Российской федерации Троицкий институт инновационных и термоядерных исследований»
АО «НИИП»	Акционерное общество «Научно-исследовательский институт приборов»
АО «ЦНИИ ЭИСУ»	АО «Центральный научно-исследовательский институт экономики, информатики и систем управления»
АО НИПИ ГА «АвиаМенеджер»	Акционерное общество Научно-исследовательский проектный институт гражданской авиации «АвиаМенеджер»
ВАГШ ВС РФ	Военная академия Генерального штаба Вооруженных Сил Российской Федерации
ВТИ НГ РУз	Военно-технический институт Национальной Гвардии Республики Узбекистан
ИЗМИРАН	ФГБУН Институт земного магнетизма, ионосферы и распространения радиоволн им. Н.В.Пушкова РАН
ИНП РАН	ФГБУН Институт народнохозяйственного прогнозирования РАН
ИПБ МВД РУз	Институт пожарной безопасности МВД Республики Узбекистан
ИПМ им. М.В. Келдыша РАН	Институт прикладной математики им. М.В. Келдыша РАН

ИПУ РАН	ФГБУН Институт проблем управления им. В.А. Трапезникова
ИСПИ РАН	Институт социально-политических исследований
КНИТУ - КАИ	Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ
МАИ	ФГБОУ ВО «Московский авиационный институт (Национальный исследовательский университет)»
МКПП	Международный Конгресс промышленников и предпринимателей
Мосполитех	Московский политехнический университет
НИЯУ «МИФИ»	Национальный исследовательский ядерный университет «Московский инженерно-физический институт»
НТЦ «Балансмаш»	Научно-технический центр «Завод балансировочных машин»
ООО «ИнТех»	ООО «Инженерно-Техническая Компания»
РАНХиГС при Президенте РФ	Российская академия народного хозяйства и государственной службы при Президенте РФ
РГГУ	ФГБОУ ВО Российский государственный гуманитарный университет
РУТ (МИИТ)	ФГБОУ ВО «Российский университет транспорта (МИИТ)»
СГУ	Сухумский государственный университет
ФГБОУ ВПО РГСУ	ФГБОУ ВПО «Российский государственный социальный университет»
ФИЦ ИУ ВЦ РАН	ФГУ Федеральный исследовательский центр «Информатика и управление», Вычислительный центр им. А.А. Дородницына РАН
ФИЦ ИУ РАН	ФГУ Федеральный исследовательский центр «Информатика и управление» РАН

ФИЦ КНЦ РАН	Федеральный исследовательский центр «Кольский научный центр Российской академии наук»
Центральный филиал ФГБОУ ВО «РГУП»	Центральный филиал ФГБОУ ВО «Российский государственный университет правосудия»
ЮФУ	Южный Федеральный университет

АВТОРЫ

Balabanov A.V.	ИПУ РАН
Kasimov A. M.	ИПУ РАН
Авдеева З.К.	ИПУ РАН
Агаев Р.П.	ИПУ РАН
Акатьев С.В.	Мосполитех
Алексейчук А.Е.	ИПУ РАН
Аникина Е.В.	ИПУ РАН
Анохин А.М.	ИПУ РАН
Артемов О.Ю.	РГГУ
Асратян Р.Э.	ИПУ РАН
Ахромеева Т.С.	ИПМ им. М.В. Келдыша
Баранов Л.А.	РУТ (МИИТ)
Богатырева Л.В.	ИПУ РАН
Бочкарев А.П.	ВАГШ ВС РФ
Быстров В.В.	ФИЦ КНЦ РАН
Горелова Г.В.	ЮФУ
Гориславец А.Ю.	ИЭУП РГГУ
Грузман В.А.	ИПУ РАН
Гучук В.В.	ИПУ РАН
Дикова Е.В.	Мосполитех
Еременко В.А.	ИЗМИРАН
Еремин М.С.	Мосполитех
Жеков В.И.	Institute for economic development, Bulgaria
Завадский В.К.	ИПУ РАН
Завидова М.Ю.	АО «НИИП»
Зимин А.М.	Мосполитех
Иванов В.В.	Президиум РАН
Иванов В.П.	ИПУ РАН
Исаков Д.А.	Фонд инвестиций в национальную экономику
Исмаилов Ж.И.	Акционерное общество «КТЖ-ГРУЗОВЫЕ ПЕРЕВОЗКИ»
Каблова Е.Б.	ИПУ РАН
Калиниченко А.И.	ЮФУ
Карпов В.В.	ВАГШ ВС РФ
Касабов Г.А.	Университет национального и мирового хозяйства, Болгария
Кафидов В.В.	РАНХиГС при Президенте РФ
Кацко Д.И.	ФГБОУ ВО Кубанский государственный аграрный университет им. И.Т. Трубилина
Кереселидзе Н. Г.	СГУ

Кленовая Л.Г.	ИПУ РАН
Коврига С.В.	ИПУ РАН
Козлов А.Д.	ИПУ РАН
Комков Н.И.	ИНП РАН
Кононов Д.А.	ИПУ РАН
Кормилицин А.И.	Мосполитех
Косачев Ю.В.	РГГУ
Косяченко С.А.	ИПУ РАН
Кротова М.В.	ИНП РАН
Крылов А.И.	Мосполитех
Кузьминов А.Н.	ЮФУ
Кулагин М.А.	РУТ (МИИТ)
Кулагина Н.В.	Мосполитех
Кульба В.В.	ИПУ РАН
Курако Е.А.	ИПУ РАН
Куранцов В.А.	Мосполитех
Куранцов В.В.	Мосполитех
Куранцов О.В.	Мосполитех
Кусакина Ю.Н.	МАИ
Лазарев А.В.	ИНП РАН
Логинова Л.Н.	РУТ (МИИТ)
Людаговская М.А.	РУТ (МИИТ)
Мавлянкариев Б.А.	ИПБ МВД РУз
Маклаков В.В.	ИПУ РАН
Малинецкий Г.Г.	ИПМ им. М.В. Келдыша
Манаенкова Н.И.	ИЗМИРАН
Маслобоев А.В.	ФИЦ КНЦ РАН
Маций В.С.	ФГБОУ ВО Кубанский государственный аграрный университет им. И.Т. Трубилина
Мачкин П.И.	МКПП
Мелихов А.А.	АО «ЦНИИ ЭИСУ»
Мирошник С.Н.	ФИЦ ИУ РАН
Мистров Л.Е.	Центральный филиал ФГБОУ ВО «РГУП»
Морозов Д.В.	КНИТУ - КАИ
Муромцев В.В.	РГГУ
Муромцева А.В.	РГГУ
Мусаев А.В.	Мосполитех
Мусаев В.К.	Мосполитех
Назаркин А.С.	Мосполитех
Неизвестный С.И.	ФГБОУ ВПО РГСУ
Никифоров С.В.	РГГУ
Нога Н.Л.	ИПУ РАН

Овчинников С.А.	РГГУ
Овчинникова Н.В.	РГГУ
Орёл Е.Н.	Финансовый университет
Орлов В.Л.	ИПУ РАН
Пен А.Ю.	ВТИ НГ РУз
Пискурева Т.А.	АО «НИИП»
Пицык В.В.	АГПС МЧС России
Плотников Н.И.	АО НИПИ ГА «АвиаМенеджер»
Посашков С.А.	Финансовая академия при Правительстве РФ
Почхуа Г.Р.	СГУ
Прошина О.М.	АГПС МЧС России
Райков А.Н. (Raikov A.N.)	ИПУ РАН
Рожнов А.В.	ИПУ РАН
Рыженко А.А.	АГПС МЧС России
Саак А.А.	РГСУ
Сакрутина Е.А.	ИПУ РАН
Сафронов А.И.	РУТ (МИИТ)
Сергеев М.С.	НИЯУ «МИФИ»
Сидоренко В.Г.	РУТ (МИИТ)
Сиротский А.А.	ФГБОУ ВО РГСУ
Сиротюк В.О.	ИПУ РАН
Скворцов О.Б.	НТЦ «Балансмаш»
Сомов С.К.	ИПУ РАН
Сорокин Л.А.	ООО «ИнТех»
Стаменкович Н.	ИПУ РАН
Стародубцев В.В.	Мосполитех
Суховерхова Л.В.	АГПС МЧС России
Талибджанов И.Р.	ИПБ МВД РУз
Товмасян Т.А.	ИПУ РАН
Торгашев Р.Е	РГГУ
Торопыгина С.А.	ИПМ им. М.В. Келдыша
Тюрин С.А.	ИПУ РАН
Усманова Т.Х.	ИНП РАН
Финьков В.Н.	Индивидуальный предприниматель
Филиппов В.А.	ИПУ РАН
Фомичев И.В.	ИПУ РАН
Фуругян М.Г.	ФИЦ ИУ ВЦ РАН
Хатамов Б.Б.	ВТИ НГ РУз
Христофоров О.Б.	АО "ГНЦ РФ ТРИНИТИ"
Цыганов В.В.	ИПУ РАН
Чекаданова М.В.	ИНП РАН

Чернов И.В.,	ИПУ РАН
Чилачава Т.И.	СГУ
Шелков А.Б.	ИПУ РАН
Широкий А.А.	ИПУ РАН
Шиянов М.И.	Мосполитех
Шиянов С.М.	Мосполитех
Шульц В.Л.	ИСПИ РАН

СОДЕРЖАНИЕ

Научное издание

ПРОБЛЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ

Материалы
XXVI международной конференции
19 декабря 2018 г., Москва

Под общей редакцией
д.т.н. Калашникова А.О., д.т.н. Кульбы В.В.

В печать от 06.12.2018
Формат 60×90/16. Усл. печ. л. 25,69
Тираж 100. Заказ 353

117997, Москва, Профсоюзная, 65
Федеральное государственное бюджетное учреждение науки
Институт проблем управления им. В.А.Трапезникова
Российской академии наук
www.ipu.ru