Министерство науки и высшего образования Российской Федерации
Институт проблем управления им. В.А. Трапезникова
Российской академии наук

Институт прикладной математики им. М.В.Келдыша
Российской академии наук

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
XXX МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ
14 декабря 2022 г., Москва

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

НАУЧНОЕ ЭЛЕКТРОННОЕ ИЗДАНИЕ

Москва
ИПУ РАН
2022

УДК 658.012:658.382.2 **DOI: 10.25728/iccss.2022.26.77.074**
ББК 65.9:66.2:68.9
П78

Проблемы управления безопасностью сложных систем : материалы XXX Международной конференции, 14 декабря 2022 г., Москва / под общей редакцией А.О. Калашникова, В.В. Кульбы; Институт проблем управления им. В.А. Трапезникова РАН Минобрнауки РФ [и др.] . – Электрон. текстовые дан. (10,0 Мб). – Москва : ИПУ РАН. – 2022. – 1 электрон. опт. диск (CD-R). – Систем. требования: Pentium 4; 1,3 ГГц и выше; Windows XP/7/8; Acrobat Reader 4.0 или выше. – Загл. с титул. экрана. – ISBN 978-5-91450-263-5. ï ¯ ctsfn tej cc[fljstcO ųcc[0322204178. –Текст : электронный.

Научное электронное 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.

Материалы представлены в авторской редакции

Утверждено к печати Программным комитетом конференции

ISBN 978-5-91450-263-5

СОДЕРЖАНИЕ

I. Общетеоретические и методологические вопросы обеспечения безопасности

DOI: 10.25728/iccss.2022.40.32.001

Малинецкий Г.Г., Кульба В.В.

Военные конфликты и промышленная политика в контексте теории управления рисками

Аннотация: За последние десятилетия изменился и характер войн, и способы их ведения. Сфера силового противостояния значительно расширилась. Активная борьба сегодня ведется в киберпространстве, в информационном пространстве, в сфере смыслов и ценностей, широко используются технологии «переписывания истории», делающие вчерашних побежденных сегодняшними победителями. Важной сферой противостояния становится биологическое пространство. Все более важную роль начинают играть космические системы, ориентированные на поддержку боевых действий. По-прежнему ахиллесовой пятой нашей армии является связь, разведка и целеуказание. Всё, что требует форсированного развития ряда инженерных разработок и научных направлений, быстрого выпуска ряда вооружений. Необходимо преодолеть острый дефицит подготовленных людей и в армии, и в оборонно-промышленном комплексе. Мы имеем дело с войной нового поколения, в которой есть множество ограничений, связанных с использованием военных технологий, – это требует широкого междисциплинарного подхода, касающегося многих сфер жизнедеятельности. Ход и результаты специальной военной операции меняют приоритеты решения многих проблем в данной области. Ряд возникающих здесь вопросов рассмотрен в данной работе.

Ключевые слова: война нового поколения, научная поддержка военных действий, оборонно-промышленный

комплекс, самоорганизация, образовательный вызов России, цивилизационные войны, междисциплинарные подходы, постиндустриальное развитие, гуманитарно-технологическая революция

Военные императивы

> Следующая война в Европе будет войной между Россией и фашизмом, только фашизм будет называться демократией.
>
> Фидель Кастро

> Поверьте, в наше время самый большой подвиг для тех, кому есть что сказать, – это прикусить язык.
>
> А. Ходаковский

О войне естественно писать историкам или тем, кто участвует в боевых действиях. Однако несколько соображений о специальной военной операции можно высказать уже сейчас.

Необходимость осознания, что воюет вся страна. Россия ведет цивилизационную войну и противостоит Западу. Значение этого трудно переоценить. В этой войне решается во многом будущее мира, наших детей и внуков. Нельзя жить так, как будто в одной части страны всё, как всегда, другая находится под обстрелами, а третья воюет. Нельзя одновременно устраивать день Москвы с гуляниями и салютами и сдавать города, которые брались месяцами. Это путь к распаду. Нынешняя война должна быть делом всей страны.

На Донбассе сейчас есть прекрасные видео, песни, поэзия. Их исполняет молодежь. Они должны идти по первым каналам. Это изменит страну!

Следует отказаться от идеи «специальной военной операции», которую мы можем вести, имея впятеро или втрое меньшим контингентом, чем наш противник. «Перемалывание оружия противника» обозначает оборону. Движение по несколько сотен метров в день – путь к поражению. Необходимо существенное

увеличение числа *подготовленных людей*, участвующих в операции.

Нужен перевод экономики на военные рельсы и рывок в создании вооружений для локальных конфликтов. Мы воюем с Западом и противостоим ему. Следует отдать себе отчет, что в первые месяцы конфликта стороны воевали оружием, созданным в советские времена. Отсутствие оружия, которое было бы намного лучше, чем у противника, заставляло солдат и ополченцев решать свои задачи, опираясь в основном на свои морально-волевые качества. Министр обороны говорит, что у Запада нет «супероружия». Однако Хаймерсы (производятся с 2003 года), Джавелины (1996 год), Байрактары (2014 год), системы космической разведки и дешифровки создают серьезные проблемы для наших солдат и ополченцев. Использование тувинцев в переговорах означает, что наши системы связи противником открыты. Нам нужно больше оружия и оружия лучшего качества.

Совершенствование системы управления, налаживание эффективной обратной связи. Обратим внимание на формулировку классика военной науки А.А. Свечина, данную в начале XX века: «Всё военное искусство заключается в соединении усилий для поражения врага, а могут ли лгуны и лицемеры произвести общее усилие… Достоинство и сила военного заключается в оружии, которое он носит при себе, и в его правдивости. Безоружный боец – бесчестен; также бесчестен и боец-лгун… Гибель народа начинается тогда, когда он теряет способность смотреть в лицо действительности; когда он факты действительной жизни начинает подменять фантазией; начинает мечтать и засыпать» [1]. Ещё хуже, если общие мысли и ценности, необходимые для обеспечения безопасности государства, заменяется корпоративными интересами.

«Одна из основных бед замкнутой системы, формировавшейся десятилетиями и пронизанной нитями влияния клубов по интересам – паника перед негативными докладами. Честно признавая те или иные проблемы в узком кругу, иной значительный генерал на вопрос, – А почему не докладываете? – отвечает: «Так ведь снимут…», – пишет командир батальона «Восток» А. Ходоковский.

Формирование идеологии, понимаемой как синтез долгосрочного прогноза и образа желаемого будущего. У людей не должно возникать диссонанса – они должны ясно понимать, за что идет борьба, и как они будут жить после победы над фашизмом на

Украине. Это очень важно и для граждан России, и для жителей украинских регионов, ориентирующихся на Россию. Точными представляются слова главы Чечни Рамзана Кадырова: «Мы боремся не только за освобождение мирных людей от многолетнего нацистского произвола. Мы боремся за будущее нашей страны – России, за свои традиции, идентичность, за духовно-нравственные ценности, за религию, за торжество справедливости» [2].

Командир батальона «Восток» А. Ходаковский так очертил мотивы, поднимающие людей в атаку: «… я бы примерно так разложил факторы влияния: я бы провел верхнюю горизонтальную черту, которая символизировала бы сто процентов, и под ней самым длинным столбцом был бы столбец с надписью «приказ», который не дотягивал бы до верхней планки процентов сорок – не всегда и приказ способен поднять людей в атаку. Потом бы шел столбец с надписью «убей, чтобы выжить»; за ним – с сокращенной надписью «игра», – переиграть противника всегда интересно… И только последний ступенькой этой нисходящей лестницы я бы поставил высокий мотив: «За Родину!»… не раз и не два я слышал выражение: за кого умереть, – за Миллера с Сечиным???» [3]. Эту ситуацию надо изменить.

Развертывание по всей стране военно-спортивных клубов, ориентированных на обучение молодежи военному делу, работе с техникой и компьютерными системами. Система ДОСААФ России должна быть существенно увеличена. Молодежь должна уметь защищать Родину и своих близких. Иначе возникает диссонанс между обыденностью и задачами, которые решает страна. Те, кто сдавал деньги на беспилотники и на гуманитарную помощь Донбассу, понимают, как важна в этой сфере ясность и простота. Такая система организаций могла бы взять на себя эти задачи.

Развитие систем разведки, связи и управления. История показывает, что к большинству войн отечественная армия оказывалась не готова, и проблемы приходилось восполнять после начала боевых действий. Ахиллесовой пятой в этом конфликте оказалась разведка, связь и управление. Украинцы с помощью западной техники определяют координаты целей быстрее и точнее, чем мы. Несмотря на то, что в нашей стране действительно давно была создана контрбатарейная РЛС «Зоопарк», многое здесь оставляет желать лучшего. Хотелось бы, чтобы борьба с артиллерией

противника была более эффективной. Важнейшей частью вооруженной борьбы сегодня являются беспилотники. России нужно как можно скорее научиться производить набор *своих* аппаратов такого типа. Классики и теоретики военного дела обращали внимание на ключевое значение времени в ходе боевых действий. В армиях, построенных по стандартам НАТО, время между обнаружением цели и её атакой артиллерией гораздо меньше, чем в российской армии. И это тоже надо изменить. Очень важным является использование информации в системах управления. Современные технологии привели к тому, что скрыть массированное сосредоточение войск невозможно. Остается удивляться, что информация о готовящихся наступлениях украинской стороны использовалась недостаточно эффективно. И здесь нужны перемены.

Формулировка ограничений в сфере использования военных. Конфликт на Украине – гражданская война с международным участием. Задачи демилитаризации и денацификации нетрадиционны для военных действий. В XX веке, в особенности после появления ядерного оружия, стало понятно, что, начиная конфликт, следует очертить и ограничения в области используемых вооружений, и цели, которые будут поражаться. Понятно, например, что мегаполисы защитить невозможно, и что поражение атомных станций, чревато «новым Чернобылем» неприемлемо. По-видимому, именно об этом сейчас надо договариваться с Западом.

Разработка инструментов противодействия «дирижерам», а не только «оркестрантам». «Режиссером» войны на Украине являются политические элиты США и ряд транснациональных корпораций. Они создают множество неудобств и препятствий России в экономической, финансовой, военной, дипломатической, информационной сферах, будучи уверенными, что их «не достанут». Эта неприемлемая для нас ситуация давно понята, исследована и описана европейскими учеными [4]. Важная научная задача – разработка инструментов, позволяющих изменить эту ситуацию и не играть по чужому, разрушительному для нас сценарию. Мы должны научиться создавать проблемы «дирижерам».

Использование новых подходов в ходе боевых действий. Ученые, инженеры, военные России знают и умеют очень многое из того, что может пригодиться в ходе войны. Система управления должна это увидеть, помочь реализовать и использовать в массовом порядке.

Заметим, что это делается в ряде стран. К примеру, в США, офицеры рассказывают о киберугрозах в военных сферах, используя графическую форму и фантастические сюжеты [5]. Пусть военные вникают, придумывают, используют новое.

Очевидно, и нам надо использовать новые инструменты для достижения целей защиты России.

Мне доводилось писать о том, что можно сделать на «быстрых» и «медленных» временах в спецоперации на Украине [6, 7]. Однако наиболее важными сейчас представляются моменты, представленные выше.

Большая часть пути к победе над фашизмом на Украине уже пройдено. Осталось пройти остальную часть.

Промышленная политика в коротком времени

> Хороший план сегодня лучше безупречного плана завтра.
>
> Джордж Паттен

Исторический эксперимент последних 30 лет показал, что Россия и олигархический капитализм как гений и злодейство – «две вещи несовместные».

Промышленная политика определяет пути реализации стратегии страны на 10-15 лет. Однако сейчас Россия ведет войну с Западом, поэтому разумно поступить так, как делают математики. Определить политику для «коротких» времен (несколько лет), имея в виду военную ситуацию, и политику «длинных» времен.

Следует иметь в виду историческую традицию. Огромную роль в победе России в Отечественной войне 1812 года сыграл генерал Е.Ф. Канкрин (1774-1845), координировавший снабжение армии и финансы империи. Мы видим, что в настоящее время на Украине российской армии и ополченцам с трудом удается оборонять фронт. Поэтому необходимо срочное формирование новой промышленной политики, позволяющей более эффективно поддерживать армию России.

Коротко сформулируем основные предложения, разделив их на две группы – «сверху вниз» – то, что должно делаться на уровне первых лиц, и «снизу вверх» – инициативы, которые должны быть осуществлены другими структурами.

Формирование Ставки верховного главнокомандования, которая объединит в одних руках военную, политическую, экономическую власть в стране.

Формирование и работа Государственного комитета обороны. Планирование, управление и контроль за всем, что необходимо для войны.

Формирование независимой структуры Росстата. Это структура должна быть самостоятельным органом и давать объективную картину происходящего в стране, а не служить инструментом отстаивания ведомственных интересов, как в настоящее время.

Формирование Госплана и проектирование войны. Мы должны быть готовы к ведению «долгой войны». Это требует переориентации значительной части промышленности страны в контексте реализуемой военно-политической стратегии.

Формирование Госкомитета по науке и технологиям. Война показала, что мы существенно отстали по ряду видов вооружений от образцов, используемых Западом, и не используем в интересах обороны большой научно-технический потенциал, имеющийся в России.

Формирование Министерства электронной промышленности и ряда министерств «военной девятки», существовавших в СССР. От 80 до 95 % возможностей современного оружия определяется электроникой, которая в него «зашита». Хаос в этой области, как и в ряде других, имея в виду военную ситуацию, необходимо как можно скорее устранить.

Решение проблем цивилизационной достаточности. В условиях жестких санкций необходимо выделить контуры производства жизненно важных типов продукции. Лечить, защищать, обогревать, обеспечивать, инфраструктуру, учить и делать ряд других необходимых вещей мы должны сами, не надеясь на поставки извне. Именно в этом и состоит реальный, а не бумажный суверенитет нашей цивилизации – мира России.

Организация военно-технической революции. На Украине Россия в большой степени воюет советским оружием. В ряде случаев оно уже отстает от того, что использует Запад. При этом в мире происходит научно-техническая революция – акцент на разведывательно-ударных комплексах, новых инструментах

разведки, системах искусственного интеллекта – проявление этого. России нужен рывок в будущее, создание новых инструментов вооруженной борьбы. Говоря словами академика И.В. Курчатова, надо «обгонять, не догоняя».

Промышленная политика «снизу вверх» на коротких временах должна включать следующие пункты.

Замыкание обратной связи в планировании, управлении и расходовании государственных средств. И медведевские «четыре И», и «Цифровая экономика», и работы по нанотехнологиям и искусственному интеллекту, и «Национальные проекты» не дали желаемых результатов. Нельзя управлять промышленностью, не подводя итоги и не извлекая ошибок, исходя из полученных результатов.

Демонополизация производства оружия. В годы Великой Отечественной войны работали конструкторские бюро Антонова, Туполева, Поликарпова, Илюшина и ряд других. Дело не в обилии денег, а в том, что наличие альтернатив позволяет выявить лучший вариант и делать для фронта именно его. Слияние множества организаций в настоящее время в гигантские структуры не дало эффекта. Очевидно, к содержательной конкуренции в этой области придется возвращаться.

Открытые конкурсы по проблемам производства оружия и импортозамещения. Привлечение малого бизнеса и конкретных людей. Нужно искать новые эффективные решения, а не только делать старое во всё больших количествах.

Организация системы фондов, ориентированных на решение цивилизационных задач. К сожалению, в России был ликвидирован гуманитарный научный фонд (РГНФ) Российский фонд фундаментальных исследований (РФФИ). Такие структуры как «Роснано» и «Сколково» не дали ожидаемого эффекта, создать аналог американского DARPA (Управление перспективных исследовательских проектов Министерства обороны США) не удалось. Опыт показывает, что самоорганизация в научно-техническом пространстве играет огромную роль. Этим надо пользоваться и поддерживать её, имея в виду задачи военного времени.

Организация государственной экспертизы и контроля результатов. Государственные интересы и задачи обороны должны

быть поставлены выше корпоративных выгод. Из 1000 предложений в Кремниевой долине на основе всесторонней экспертизы поддержку в среднем получают 7. Это позволяет снизить риски реализации инновационных проектов до приемлемого уровня.

Открытие военных училищ и военных кафедр в вузах России. В рамках «демилитаризации» в ходе реформ в стране было закрыто значительное число военных училищ. По инициативе руководства Высшей школы экономики (ВШЭ) были ликвидированы военные кафедры в большинстве вузов страны, а в сохранившихся в них существенно сократили набор. Военные кафедры, по сути, давали ещё одну специальность и позволяли готовить командиров. Сейчас в армии РФ не хватает командиров – надо срочно открывать ранее закрытые училища и воссоздавать военные кафедры в вузах.

Подготовка перехода от контрактной к призывной системе. Специальная военная операция показала, что надежды реформаторов на то, что страна обойдется малой, высококвалифицированной контрактной армией не оправдываются. Контрактная армия не дает достаточного резерва для возможных больших конфликтов. Угрозы национальной безопасности требуют гораздо бо́льшей армии, её вооружения и обеспечения. Очевидно, это необходимо учитывать в промышленной политике на «коротких временах».

Очень многое в войне происходит стремительно на коротких временах. Чем быстрее, точнее и лучше мы сделаем необходимое, тем ближе окажемся к Победе.

В промышленной политике на «длинных временах» можно выделить следующее.

Выявление реальных, а не «имитационных» приоритетов и действий систем управления. Реализация государственной политики требует доверия населения. Превращение за 30 лет России в сырьевого донора, имитационные экономика, наука, культура и связанные с ними неудовлетворительные результаты требуют понимания обществом происходящего, без чего трудно надеяться на его серьезную поддержку. Почему, например, стратегические приоритеты, обозначенные в Послании Президента Федеральному собранию 01.03.2018, остались на бумаге? Министры и вице-министры регулярно отвечают, что они исполняют решения. Но кто принимал и принимает эти решения и несет за них ответственность? Ситуация требует более простой и легкой системы управления.

Иную на «длинных временах» общество не поддержит.

Кадровые изменения. Доверие общества к власти может вернуть увольнение знаковых фигур, проваливших порученное им дело. Страна вполне может обойтись без присутствия Эльвиры Набиуллиной, Германа Грефа, Александра Фурсенко и ряда других лиц на руководящих постах. «По плодам узнаете их», – говорится в Нагорной проповеди. Плоды деятельности многих руководителей для России стали очевидны. Необходима обратная связь.

Обеспечение системной достаточности цивилизации. Жесткая связь между финансами, технологиями и людьми, приходящими извне, и достижениями России должна быть разорвана. Нам необходим реальный суверенитет во многих областях.

Протекционизм. В качестве правила следует поддерживать отечественного производителя, не полагаясь на дешевизну импорта. Война это ещё раз подтвердила.

Проценты банков по кредитам промышленным предприятиям должны быть ниже 3 %. При более высоком проценте основная часть промышленности, прежде всего высокотехнологичной, в которой Россия особенно нуждается, не выживает.

Налоговая реформа. Отмена налога на добавленную стоимость, переход к налогу на потребление. Дополнительные вложения в повышение уровня жизни детей и пожилых людей. Соответствующие расчеты были проведены в Институте прикладной математики им. М.В. Келдыша и в Институте проблем управления им. В.А. Трапезникова. Они показали, что такая реформа благотворно отразится на всей экономической системе.

Курс на переход страны к ситуации равновесия между покупками и продажами товаров и ресурсов. Продавая гораздо больше ресурсов, чем закупая товаров, мы развиваем экономику других стран и разоряем следующие поколения граждан России. Ситуация должна быть иной.

Тридцатилетний форсайт развития России и пятилетний индикативный план. Наша страна жила будущим, и нам очень важно понять, куда мы идем, где хотим оказаться и каким будет наше место в мире. Это должен определять форсайт. Пятилетний индикативный план, итоги которого через пять лет непременно подводятся, определяет путь к намеченным целям. Опыт Японии, Южной Кореи и Китая показывает, что такой подход является важным

инструментом формирования промышленной политики.

Введение продуктовых карточек для беднейшей части населения России. (15 тысяч рублей в месяц для 21 миллиона человек). Расчеты и опыт других стран показывают большое социально-экономическое значение подобных мер.

Ликвидация «ножниц цен» между отечественными и зарубежными товарами. Эти ножницы сформировались благодаря дорогим отечественным кредитам. Такие ножницы лишают стимулов и возможностей для развития большинства производств. Российские кредиты должны быть дешевыми.

Выделение и развитие локомотивных отраслей экономики с ориентацией на VI технологический уклад. Экономика должна жить не только настоящим, но и будущим. Системный анализ показывает, что особое значение в ближайшее десятилетие будет иметь развитие компьютерной реальности, начиная с производства собственных компьютеров, мобильников и кончая развитым программным обеспечением и системами искусственного интеллекта, а также биотехнологий (новая медицина, новое природопользование, сельское хозяйство нового поколения).

Формирование индикативного плана подготовки специалистов, исходя из принимаемой промышленной политики. В настоящее время имеет место образовательный хаос. Мы имеем дело с острым дефицитом пилотов, представителей компьютерных специальностей, школьных учителей и т.д. Промышленная политика позволяет оценить когда, сколько и каких специалистов понадобится. Такой подход позволяет решить многие социально-экономические проблемы и обойтись без гастарбайтеров в ключевых областях. Кроме того, нельзя эффективно развиваться, не имея собственных специалистов.

Модернизация Аналитического центра Правительства РФ. Нам необходима система математических моделей развития России и баз данных и информационных потоков современного уровня, позволяющих заглядывать вперед.

Переход к оценке и организации науки как к непосредственной производительной силе, а не как к элементу системы образования. Наука обеспечивает инновации, развитие и защиту страны. На решение этих задач, а не на создание информационного шума, ее и надо сориентировать.

Критерием успешного развития страны в целом и промышленной политики в частности очень просты. Наша цивилизация должна воспроизводить себя. Для этого суммарный коэффициент рождаемости должен превышать 2,1 ребенка на женщину, сейчас он у нас 1,50, а в ходе реформ опускался до 1,16. Мы не должны вымирать! По прогнозу великого химика, а также демографа и экономиста Д.И. Менделеева, данному в 1906 году, к 2000-му году население России должно было составить 594 миллиона человек.

Другим ключевым критерием является валовый внутренний продукт на душу населения. По данным Всемирного банка, в 2000-м году наша страна находилась на 83 позиции. Это очень мало для страны, имеющей, по оценкам экспертов, около трети минеральных ресурсов мира. Украина находится на 132-й позиции. Естественно, другие страны ориентируются, прежде всего, на тех, кто живет хорошо. Если бы мы занимали место в первой тридцатке, то отношения с сопредельными государствами были бы иными. Исходя из этого, и надо строить промышленную политику.

Завершить текст можно известной восточной пословицей: «Когда караван поворачивает назад, то хромой верблюд становится первым». Ситуация в мире сейчас кардинально меняется. История распорядилась так, что во многих отношениях мы оказались первыми. Осталось перестать хромать.

Сильных будущее за собой ведет, а слабых тащит. Нам стоит быть сильными.

Литература:

1. *Свечин А.А.* «Предрассудки и военная действительность» / Е.И. Мартынов, А.А. Свечин, С.Ф. Ахромеев. «…хорошо забытое старое». / Сб. статьей. – М.: Воениздат, 1991. – С. 107-137.

2. Кадыров назвал истинные цели СВО на Украине. – URL: https://prokazan.ru/news/161709?utm_source=yxnews&utm_medium=desrtop&utm_referrer=https://yandex.ru/news/story/Glava_Chechni_Radurov_nazval_istinnoj_celyu_specoperacii_borbu_za_budushhee_Rossii__a9a912f41097467faa009d2425d235bf (дата обращения 15.10.2022).

3. Сайт А. Ходаковского. [Электронный ресурс]. – URL: https://dzen.ru/id/635236d9a4a3c632e6e5a851 (дата обращения

15.10.2022).

4. *Мюнклер Г.* Осколки войны: эволюция насилия в XX и XXI веках. / Пер с нем. А.И. Лакутовой. – М.: Кучково поле, 2018. – 384 с.

5. Киберугрозы в военной сфере. Собрание американских графических рассказов. Часть I. / Пер. с англ. АНО «Институт стратегий развития». – М.: Институт стратегий развития, 2022. – 48 с.

6. *Малинецкий Г.Г.* Стратегическая стабильность и спецоперация России на Украине. Часть I. – URL: https://yandex.ru/turbo/regnum.ru/news/3637280.html (дата обращения 15.10.2022).

7. *Малинецкий Г.Г.* Стратегическая стабильность и спецоперация России на Украине. Часть II. – URL: https://yandex.ru/turbo/regnum.ru/news/3637946.html (дата обращения 15.10.2022).

DOI: 10.25728/iccss.2022.81.49.002

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

Наука и образование как объекты управления сложными системами

Аннотация: В настоящее время происходит гуманитарно-технологическая революция. Она существенно меняет способы силового противостояния государств, блоков, цивилизаций, а также внутренний мир людей. Специальная военная операция на Украине сделала очевидными тенденции, формировавшиеся десятилетиями. Эти качественные изменения требуют существенных преобразований не только научного, образовательного и военного пространства, но и всей России, направленных на обеспечение безопасности и создание условий для развития нашего Отечества.

Революция в создании систем «грязного» искусственного интеллекта, развитие вычислительных систем в соответствии с законом Мура, совершенствование средств дистанционного зондирования Земли и открывают

перспективу «безлюдных войн». Огромное значение приобретает сфера гуманитарного обеспечения военного противостояния. Это очень серьезный вызов для российской науки, нынешняя организация которой не позволяет на него эффективно ответить. Здесь необходимы серьезные организационные преобразования, контуры которых намечены в данной работе.

СССР имел одну из лучших в мире систем образования, ориентированную на развитие высокоиндустриальной страны и подготовку творцов, способных создавать и развивать собственные технологии, продукты, алгоритмы, стратегии. Российские образовательные реформы были ориентированы на подготовку «квалифицированного потребителя» в стране, которая является сырьевым донором ведущих государств. Был произведен переход от «культуры полезности к культуре достоинства», от предметоцентрического к личностно-ориентированному подходу. Это предопределило развал средней и высшей школы, представляющий серьезную угрозу для национальной безопасности. Обсуждаются срочные меры, которые надо осуществить в образовательной сфере.

Ключевые слова: война нового поколения, научная поддержка военных действий, оборонно-промышленный комплекс, самоорганизация, образовательный вызов России, цивилизационные войны, междисциплинарные подходы, постиндустриальное развитие, гуманитарно-технологическая революция

Введение. Почему к нам пришла война?

> Заключайте союзы с кем угодно, развязывайте любые войны, но никогда не трогайте русских.
>
> О. Бисмарк

В ходе специальной военной операции Россия ведет цивилизационную войну с Западом, готовым «воевать до последнего украинца». В этой войне выясняется, сможет ли наша цивилизация –

мир России – быть субъектом, а не объектом мировой истории. Сможет ли наше Отечество самостоятельно определять наши смыслы, ценности, путь в будущее, тип жизнеустройства?

Почему война пришла в наш дом? Почему поражение в этой операции может привести к распаду нашей страны? Почему для масштабного военного противостояния был выбран настоящий момент? Чтобы выяснить это, надо разобраться со смыслом термина «цивилизация». Среди многочисленных определений нынешнюю реальность точнее других определяет концепция американского футуролога Э. Тоффлера: «Мы мчимся к полностью иной структуре власти, которая создаст мир, разделенный не на две, а на три четко определенные, контрастирующие и конкурентные цивилизации. Первую из них символизирует мотыга, вторую – сборочная линия, третью – компьютер.

Термин «цивилизация» звучит несколько претенциозно, особенно для американского уха, но нет другого термина достаточно всеобъемлющего, чтобы он охватывал такие разные вопросы, как технологии, семейная жизнь, религия, культура, политика, экономика, иерархическая структура, руководство, система ценностей, половая мораль и эпистемология.

Измените все эти социальные, технологические и культурные элементы одновременно – и вы получите не переход, а преображение; не просто новое общество, но начало как минимум – полностью новой цивилизации.

Однако ввести на планете новую цивилизацию и ожидать мира и спокойствия – это верх политической наивности. У каждой цивилизации есть свои экономические (не говоря уже о политических и военных) требования.

В разделенном натрое мире сектор Первой волны поставляет сельскохозяйственные и минеральные ресурсы, сектор Второй волны дает дешевый труд и массовое производство, а быстро расширяющийся сектор Третьей волны восходит к доминированию, основанному на новых способах, которыми создается и используется знание.

Страны Третьей волны продают всему миру информацию и новшества, менеджмент, культуру и поп-культуру, передовые технологии, программное обеспечение, образование, профессиональное обучение, здравоохранение, финансирование и другие услуги. Одной их этих услуг может оказаться военная защита,

основанная на владении превосходящими вооруженными силами Третьей волны» [1].

Современный мир – большая, сложная, многоуровневая система. В нем около 200 государств, однако геополитику, геоэкономику и геокультуру в нем всё чаще рассматривают, используя цивилизационный подход. Почему?

Бисмарку принадлежит циничное высказывание (впоследствии повторенное Стэнли Кубриком): «Большие государства ведут себя как бандиты, а маленькие ведут себя как проститутки, пытаясь ублажить большие». Последние ищут у первых военной защиты, предоставляют свои рынки, их элиты стремятся влиться в высший свет больших стран. Всё это длится не век и не два. «Нужно, чтобы владыки не презирали малых, которые под ними: ведь малые уже не малые, когда полезны великим», – писал богослов, архиепископ Константинопольский Иоанн Златоуст (347-407). Для больших государств малые – инструмент для расширения экономического пространства, для неравноправных договоров, способ трансляции своих смыслов и ценностей всему миру как «общечеловеческих». Кроме того, это дает новые плацдармы и рынки сбыта своего оружия.

Война – это суровый экзамен для страны. «Война есть испытание всех экономических и организационных сил каждой нации» [2].

Однако создано очень мощное оружие, и за спиной у человечества трагический опыт двух мировых войн. Поэтому, как писала Х. Арендт: «Война в XX веке – это роскошь, доступная лишь малым нациям». Поэтому большие могущественные государства пробуют свои силы на территории своих союзников. Вспомним Корейскую, Вьетнамскую, Афганскую войны.

Тем не менее, в виде «игроков» на исторической сцене сегодня видятся не государства, а более крупные образования – цивилизации. Дело в самоорганизации – расширяется пространство взаимодействий между разными обществами, процессы становится более быстрыми и рефлексивными. Для соперничества на больших временах нужно быть сильными и эффективными в нескольких областях, – число ведущих игроков на исторической сцене уменьшается.

Кроме того, ключевое значение приобретает научно-техническое развитие, определяющее настоящее и будущее общества. По сути, разные страны и цивилизации живут, несмотря

на взаимодействие, в разных исторических временах. Этот подход был развит около полувека назад американским социологом Д. Беллом в теории постиндустриального развития. В этой теории мировая история предстает следующим образом: «На протяжении большей части человеческой истории *реальностью была природа*: и в поэзии, и в воображении люди пытались соотнести своё «я» с окружающим миром. Затем *реальностью стала техника*, инструменты и предметы, сделанные человеком, однако получившие независимое существование вне его «я», в овеществленном мире. В настоящее время *реальность является, в первую очередь, социальным миром* – не природным, не вещественным, а исключительно человеческим – воспринимаемым через отражение своего «я» в других людях… Поэтому неизбежно, что постиндустриальное общество ведет к появлению нового утопизма, как инженерного, так и психологического. Человек может быть переделан или освобожден, его поведение – запрограммировано, а сознание изменено. Ограничители прошлого исчезли вместе с концом эры природы и вещей» [3].

СССР – одна из ведущих индустриальных держав, имевших вторую экономику мира и очень сильную армию, возглавлявший мировую социалистическую систему, формировал цивилизацию Третьей волны. Наша страна имела идеологию мирового уровня, науку и образование, занимавшие ведущие места. Военно-стратегический паритет с США показал огромные достижения и большие перспективы мира России.

Более тридцати лет в России проводился большой исторический эксперимент. Он связан со сменой социальной системы – от социалистической к капиталистической. С отказом от поддержки мировой социалистической системы и передачей многих стран под влияние Запада. Особую роль в этом проекте играла «демилитаризация» страны и создание «небольшой армии контрактников» – численность Вооруженных сил СССР к концу 1991 года составляла 3 млн 760 тыс. человек. В начале 2022 года количество действующих военнослужащих составляло 1 млн 014 тыс. человек.

Правящая элита России в 1990-х годах предполагала, что в результате реформ наше отечество станет «обычной капиталистической страной», «энергетической империей»,

«штрафным батальоном Запада в борьбе с Востоком» и т.д. Горбачевщина и политический авантюризм привели к распаду великой страны.

В ходе этого исторического эксперимента в нашей стране была развалена значительная доля обрабатывающей промышленности. Россия стала сырьевым донором Запада, поставщиком минеральных ресурсов и людей за границы, настежь открывшим свои рынки. Был сделан огромный шаг в прошлое, в направлении цивилизации Первой волны.

Результатом этого исторического эксперимента является экономическая слабость России (рисунок 1). По данным Всемирного банка, в 2019 году валовый внутренний продукт (ВВП) США составлял $21,43 трлн и доля в глобальном продукте – 24,42 %. Китай – $14,334 трлн и 16,34 %; Япония – $5,08 трлн, 5,79 %; Германия – $3,85 трлн, 4,385; Индия – $2,88 трлн, 3,28 %; Великобритания – $2,83 трлн, 3,22 %; Франция – $2,72 трлн, 3,09 %; Италия – $2,88 трлн, 2,28 %; Россия $2,88 трлн, $1,7 трлн, 1,94 %.

Наполеон говорил: «Для ведения войны мне необходимы три вещи: во-первых, – деньги, во-вторых – деньги и, в-третьих, – деньги». Важнейшая причина, по которой ведущие страны Запада решились на военный конфликт с Россией – представление о том, что нашей стране не хватит средств для масштабных, длительных военных действий. Ситуация усугубляется тем, что у нас нет ряда жизненно важных отраслей промышленности. Следовательно, ряд видов продукции, необходимых для армии, начиная от компьютеров и кончая шарикоподшипниками, мы должны втридорога закупать за рубежом. Поэтому 10 тысяч санкций, наложенных на нашу страну, не улучшают положение отечественной экономики в военный период.

Рисунок 1 – Доля разных стран в глобальном продукте

В начале XX века предполагалось, что есть идеологии – единые рецепты для всего мира – либеральная, коммунистическая, консервативная и другие. Прошедший век показал, что мир стал иным – разные цивилизации имеют свои рецепты развития, свои смыслы, ценности и проекты будущего. По мнению американского социолога С. Хантингтона, взгляды которого разделяет значительная часть элиты США, нынешний век станет столетием схватки цивилизаций в борьбе за тающие ресурсы Земли. Он выделил 8 цивилизаций, называя мир России восточно-христианской цивилизацией. Её он считал «слабой», «расколотой», в которой 10-15 % населения ориентируется на Запад и готовы быть «европейцами второго сорта». В то же время 70-75 % населения близки советские

смыслы и ценности, и олигархический капитализм им не близок. Поэтому ставка делается на социальную нестабильность и демонстрацию населению неуспешности проекта новой России.

О качестве и уровне жизни позволяет судить показатель внутреннего валового продукта на душу населения (рисунок 2). По этому показателю наша страна, располагая третью минеральных ресурсов мира, находится на 83-й позиции. Можно обратить внимание на ожидаемую продолжительность жизни. При лидерстве Японии (84,62 года) и среднемировом показателе (72,75 года) Россия находится на 122-й позиции (71,34 года; 66,49 г. у мужчин, 76,43 года у женщин). Это данные Всемирного банка за 2020 год [4]. Имеют место неблагоприятные демографические тренды – доля граждан России в мировом населении падает. Естественно, война на Украине ухудшит социально-экономические показатели страны, и, как ожидает Запад, увеличит социально-политическую напряженность. Исторический опыт показывает, что война приближает революцию. Русско-японская война привела к революции 1905 года и во многом изменила историю России. Участие нашей страны в Первой мировой войне привело к Февральской, а затем и к Октябрьской революции.

Американская стратегия исходит из того, что их страну «не достанут», и можно свободно вмешиваться в дела других государств, не ожидая адекватного ответа. Кроме того, их целью является война чужими руками и идеально в рамках одного и того же народа. Корейцы воевали с корейцами, вьетнамцы, – с вьетнамцами, сейчас русские воюют с русскими… Запад не может воевать против России, Украина тоже не может, но Украина с оружием Запада делает это.

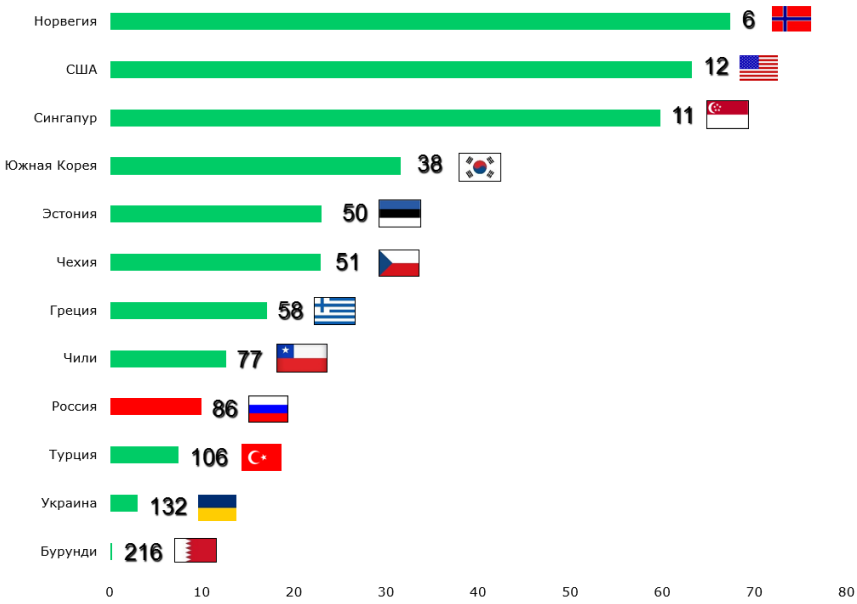


Рисунок 2 – ВВП на душу населения в 2020 году

Стоит обратить внимание ещё на один момент «режиссуры» Америкой Украинской войны. Реалии современного мира таковы, что мы в значительной мере возвращаемся к стратегиям, описанным китайским стратегом и военачальником Сунь-Цзы (VI-V в. до н.э.). Этот мыслитель пишет: «При рассмотрении искусства войны в полном объеме существенно следующее: предпочтительнее захватывать государство целиком, а не разбивать его, лучше захватывать армию целиком, а не уничтожать её по частям… Руководствуясь этим принципом, вы поймете, что одержать сто побед в ста сражениях – не высшее достижение: высшее достижение – победить неприятеля не переходя к бою. Таким образом, из этого следует, что высшая форма войны – думать за противника, затем нарушать его союзы; затем – побеждать его армию в сражении; самой низшей формой войны является осада города противника. Блокада в войне должна применяться только тогда, когда она становится неизбежной» [5].

Опыт Первой мировой войны подтверждает это утверждение

Сунь-Цзы. Битва при Вердене (21.02 – 18.12.1916) вошла в историю как хрестоматийный пример *войны на истощение*. Целью операции был прорыв германской армией Верденского укрепленного района и удара по войскам, оборонявшим Париж. С французской стороны был задействовано 1140 тыс. человек, 75 дивизий, потери 377 тыс. (из них 162 тыс. убито). С немецкой – 1 млн 250 тыс. (из них убито 143 тыс.). Форты, артиллерия, огнеметы, борьба за господство в воздухе, использовавшиеся в Вердене, удивительно напоминают основные военные инструменты, используемые в Украинской войне. Результат тоже можно предвидеть – тяжелая длительная военная компания, большие жертвы, огромные экономические потери, большая работа по восстановлению хозяйства, социально-психологическая травма миллионов людей, меняющая их отношение друг к другу, которая может продолжаться несколько поколений. «Победителем» в этой войне (как и во Второй мировой войне) будет «режиссер» этого конфликта – США.

Стоит обратить внимание на речь Президента РФ В.В. Путина на Мюнхенской конференции по вопросам политики безопасности 10.02.2007: «Считаю, что для современного мира однополярная модель не только неприемлема, но и вообще невозможна. И не только потому, что при единоличном лидерстве в современном мире – именно в современном мире не будет хватать ни военно-политических, ни экономических ресурсов. Но что ещё важнее: сама модель является неработающей, так как в её основе нет и не может быть морально-нравственной базы современной цивилизации… Мы видим все больше пренебрежение основополагающими принципами международного права. Больше того, отдельные нормы, да и, по сути, чуть ли не вся система права одного государства, прежде всего, конечно, Соединенных Штатов, перешагнула свои национальные границы во всех сферах: и в экономике, и в политике, и в гуманитарной сфере – и навязывается другим государствам. Но кому это нравится?»

Как видим, речь идет о морально-нравственной основе цивилизации. Как выясняется, не только ограничения, но и пределы допустимого у мира России и Запада принципиально различны. В ходе Второй мировой войны американские психологи и аналитики выясняли, какая доля гражданского населения Германии должна быть уничтожена, чтобы это повлияло на действия немецкой армии.

Можно вспомнить уничтоженный Дрезден, сожженный Токио, ядерные бомбардировки Хиросимы и Нагасаки.

«Нарушители», которые отрицают западные «правила», должны быть наказаны. Вероятно, Украинская война задумывалась лидерами Запада уже тогда.

В математике есть метод последовательных приближений. Вначале получается простейшее, первое приближение к решению исходной задачи. Затем оно уточняется и получается второе, и мы так действуем до тех пор, пока мы не получим ответ с достаточной степенью точности.

В первом приближении мы рассматривали цивилизации как действующих игроков на исторической сцене. Но эти общности неоднородны. Существенны элиты. Если общество сравнить с оркестром, то ему нужны дирижеры, которые направляют ключевые процессы в желаемом направлении. Они влияют на самые существенные параметры, характеризующие общество – в терминах синергетики их называют *параметрами порядка* [6].

Не вдаваясь в детали, обратим внимание на это приближение: «Разумеется, в основе кризисов и революций лежат объективные системные причины. Никто не отменял массовые процессы. Но мир – понятие не количественное, а качественное, как любил говорить Эйнштейн. В мире небольшая, но хорошо организованная группа, в руках которой огромные средства (собственность, финансы), власть и контроль над знанием и его структурами, а также над СМИ весит намного больше, чем масса людей и даже целая страна – достаточно почитать исповедь «экономического убийцы» Дж. Перкинса.

«Современная политическая экономия, – пишет нобелевский лауреат по экономике П. Кругман, – учит нас, что маленькие, хорошо организованные группы зачастую превалируют над интересами более широкой публики». Эти слова принадлежат не конспирологу, а известному либеральному американскому экономисту и экономическому обозревателю, нобелевскому лауреату по экономике. Он прямо пишет о том, что, например, в Америке правые радикалы, будучи небольшой группой, но, контролируя при этом Белый дом, Конгресс и в значительной степени юстицию и СМИ, стремятся изменить как нынешнюю американскую, так и мировую систему» [7].

Не все американцы знают, на каком континенте находится

Украина, но при Байдене на военную помощь этой стране уже было затрачено $10 млрд. Закон о ленд-лизе, принятый в США, позволяет существенно увеличить эту сумму: «Каждый день украинцы борются за свою жизнь… Цена борьбы недешевая, но поддаваться агрессии ещё дороже», – заявили представители американской администрации [8].

Следующее приближение связано с перспективой. В мировой социально-экономической системе и в системе международных отношений происходит самоорганизация, определяемая экономическим, политическим, военным влиянием. Влияние центров силы растет. Например, Украину сейчас поддерживают около 50 государств, находящихся в зоне влияния США. Этот тип самоорганизации рассматривался в динамической теории информации, основы которой были заложены Д.С. Чернавским [9].

За 30 лет, прошедших после исследований С. Хаттингтона, число ведущих игроков на мировой сцене уменьшилось. Результаты моделирования и сделанные оценки показывают, что ведущими игроками на мировой арене XXI века будут центры силы, которые можно было бы назвать *сверхцивилизациями*, население которых превышает 400 млн человек, а валовый внутренний продукт составляет не менее $20 трлн.

Очевидных кандидатов здесь три – США с их провинциями – Мексикой и Канадой. Сильная сторона этого субъекта – военные базы. Пентагон признает, что их за границами страны более 700, они составляют 95 % от всех баз вместе взятых. В Германии их насчитывается более 200, а контингент военнослужащих на них составляет примерно 250 тыс. человек; в Японии 94 базы и около 50 тысяч военнослужащих, множество баз и в других странах. Это обеспечивает контроль за территориями и существенное влияние на политический режим.

Другой кандидат – стремительно растущий Китай. Его население составляло в июле 2022 года около 1 млрд 450 млн человек. За 18 лет Китаю удалось увеличить свой ВВП в 10 раз; США понадобилось 40 лет, чтобы увеличить свой ВВП в 13 раз. Поистине Китай является мастерской мира и в ближайшие десятилетия будет претендовать на лидирующее положение на планете.

Следующим центром силы является Европейский Союз.

Есть ли у мира России шанс стать гигантом такого масштаба?

По-видимому, есть. Конечно, за это идет борьба. В случае успеха Евразийского проекта возникает социальная структура с численностью населения в 250 миллионов человек. Этого недостаточно. Нужны стратегические союзники. Таковыми могут быть Индия и ряд стран Латинской Америки, которые решают схожие стратегические задачи и достаточно близкие к России в пространстве смыслов и ценностей. Стоит обратить внимание также на поддержку ряда стран Латинской Америки действий России в ходе специальной военной операции.

Тем не менее, здесь принципиально видение будущего, большой проект, который бы осуществляла Россия. Пока этого нет. Потеряно несколько десятилетий исторического времени. Созданный «хаос в головах», горбачевщина, попытки «жить по-западному», кризис общественного сознания отбросили нашу страну на много десятилетий назад [10]. Попытка опираться на региональные националистические элиты в ходе преобразований оказалось стратегической ошибкой, привела к распаду страны. На кафедре истории Педагогического университета в Москве мне показали коллекцию школьных учебников истории, выпущенных в постсоветских странах. Все они, за исключением белорусских, были антироссийскими, антисоветскими, антикоммунистическими. Национализм буржуазных элит постсоветских стран, ставший основой их государственности, корни локальных конфликтов вокруг России выковались еще в 1991 году, да и в последующие годы тоже.

Война на Украине остро поставила ряд мировоззренческих вопросов. Очень важной стала проблема единства народа и направления дальнейшего развития страны.

Победа и решение многочисленных проблем может сделать нашу страну лидером движения неприсоединения на новом уровне, одним из ведущих центров силы.

Нынешние лидеры «первой лиги» – США, ЕС и Китай активно соперничают между собой, или, как говорили в детстве, играют в игру «царь горы».

Китайский проект «Один пояс – один путь» резко повысит возможности и Китая, и Европейского союз (ЕС). В 2021 году их товарооборот составил $8288,1 млрд, увеличившись на 27,5 % в годовом исчислении. Грузовые поезда Китай-Европа курсировали по 73 маршрутам, достигали 175 городов в 23 европейских странах с 50

тысячами видов товаров [11]. Проект «Один пояс – один путь» позволил бы вывести торговлю и связи Китая и ЕС на другой, гораздо более высокий уровень (рисунок 3) [12].

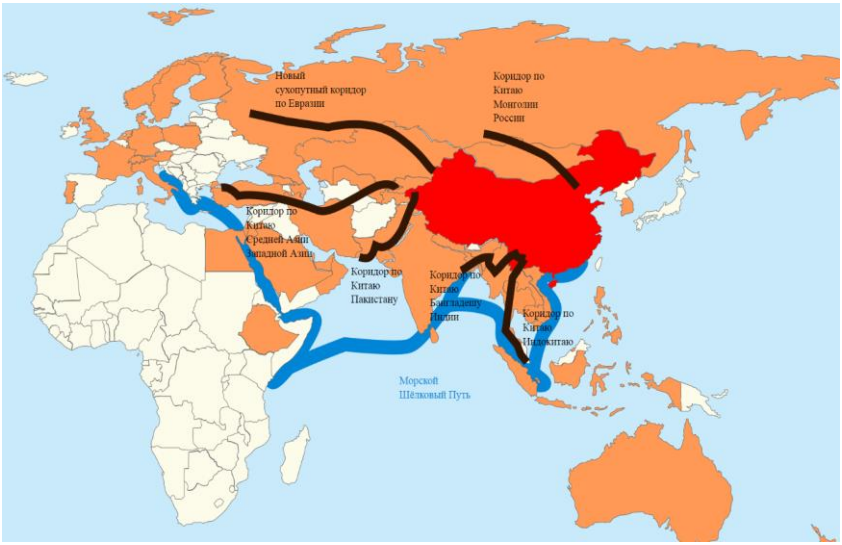


Рисунок 3 – География проекта «Один пояс – один путь»

Естественно, США пытались сорвать этот проект различными способами. Один из них – Украинская война. И чем дольше она будет продолжаться, чем более кровопролитной она будет, чем больше разрушений она принесет, тем бо́льшим будет геополитический и геоэкономичский выигрыш США. Испорченные отношения России и ЕС, проблемы с поставками энергоносителей должны существенно отбросить Европу назад. Секретарь Совбеза России Н.П. Патрушев заявил, что именно Вашингтон виноват в том, «в какой беспрецедентный кризис сегодня погружается Европа», что все проблемы вызваны санкциями «которые американцы навязали своим партнерам в ущерб самим» [13]. Кроме того, он отметил, что госдолг США превысил $30 трлн, а Японии приблизился к $10 трлн.

Следует отметить внутреннюю нестабильность Америки, разочарование граждан в демократии и своем правительстве. США являются единственной страной в мире, где от COVID-19 умерло

более миллиона человек. Существенная доля американцев допускают войну в своей стране [14]. США разжигают сейчас конфликты на Тайване и в Косово, режиссерами и бенефициарами которых они надеются стать.

Американская администрация, не способная решить внутренние проблемы, надеется перенести внимание граждан страны вовне. В новейшей истории такой маневр ей не раз удавался.

Есть риск, что война на Украине станет прологом для мирового конфликта. В свое время была начата исследовательская программа, связанная построением математической истории, ориентированной на исторический прогноз [15].

Развитие этого подхода американскими исследователями показало глубокую аналогию между предвоенной ситуацией начала XX века и нынешними реалиями. Слабеющий доминант стремится сохранить устраивающую его систему международных отношений. Тогда таким доминантом была Великобритания, сейчас США. Новые центры силы имеют более высокую производительность труда и претендуют на более значительную роль в мире. Тогда такой страной была Германия, сейчас – Китай. При этом очень важен переход от одного технологического уклада к другому. Война позволяет «сжечь» старую промышленность и открыть пространство для новой. Очень существенна смена главного энергоносителя эпохи. Тогда – угля на нефть. Сейчас происходит переход вначале от нефти к газу, а затем к «зеленой» энергетике.

Война на Украине была предопределена глубокими системными процессами, на многие из которых Россия не могла повлиять. Кроме того, народная мудрость гласит – где тонко, там и рвется.

Реанимация науки России

Таким образом, мы можем сказать, что, зная самих себя и зная своего неприятеля, вы достигните победы и в ста случаях из ста. Если же вы знаете себя, но не знаете своего неприятеля, у вас на каждую победу будет приходиться одно поражение. Если вы не знаете ни себя, ни неприятеля, побед вам не видать никогда.

Сунь Цзы

Эту часть текста мы построим иначе, чем предыдущую. Вначале мы очертим общую картину, а затем сформулируем предложения с коротким обоснованием.

Науку, образование, технологии относят к «медленным переменным», определяющим развитие стран и цивилизаций. Но современная война ускоряет процессы в этих сферах, которые во многом начинают определять и ход, и развитие военных конфликтов. О значении и сценарии развития этих сфер уже приходилось писать [16], но к обсуждению этих проблем стоит вернуться, – война не только ускоряет, но и упрощает решение многих проблем.

Влияние науки на общество состоит в том, что можно замкнуть круг воспроизводства изобретений, инноваций, технологий (рисунок 4). Выделим в нем ключевые элементы. Важнейший элемент – *целеполагание*, выработка ясного понимания того, что наша страна или цивилизация хочет достичь в долговременной перспективе, соотнесение целей и стратегий общества с новыми продуктами, технологиями, алгоритмами, которые позволили бы решить поставленные задачи.

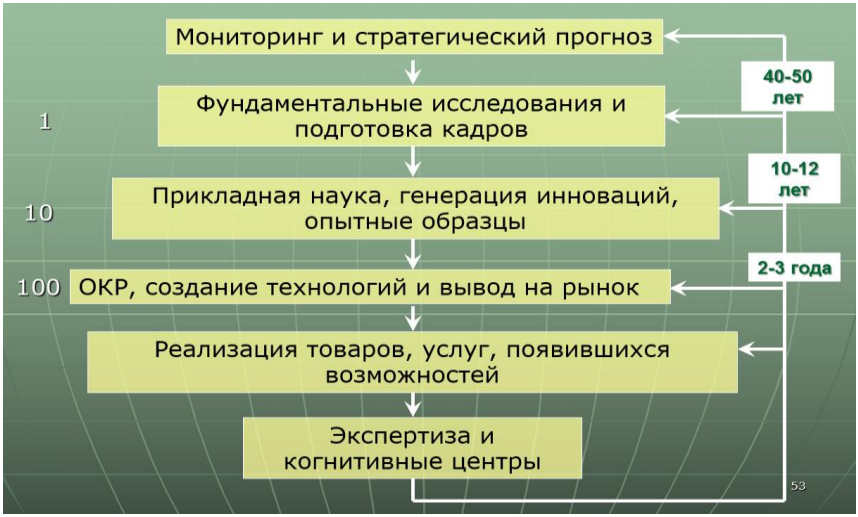


Рисунок 4 – Цикл воспроизводства инноваций

Исходя из этих целей, организуются фундаментальные исследования и готовятся специалисты. Условно говоря, эта сфера «стоит» один рубль. Фундаментальная наука занимается изучением *неизвестных* свойств Природы, Общества и Человека. Здесь, как

правило, мы не знаем, когда будет получен результат и каких усилий потребует его получение. Более того, характерное время, за которое сделанное открытие дойдет до уровня новых продуктов, – это 40-50 лет. По сути, это работа «за горизонт». Целью усилий в этой сфере является новое знание. Однако в предвоенный и военный период это знание, причем в достаточно неожиданных областях, может быть востребовано и оказаться очень важным для решения стратегических задач. Разработчики сейчас часто жалуются на дефицит фундаментальных оснований для создания новых поколений военной техники. Сказанное отлично иллюстрирует история Атомного и Космического проекта и в СССР, и в США, и в Германии. Слова о «создании оружия на новых физических принципах» не должны завораживать. Беспилотники строятся на «старых», давно известных принципах, но на новой технологической базе. Роль этого оружия, тем не менее, оказалась очень велика.

Другой важный пункт – прикладная наука. Здесь выясняется, как можно превратить новое знание в действующие образцы техники, в новые алгоритмы или стратегии. Характерное время здесь – 10-12 лет, и «стоит» этот сектор научной отрасли, условно говоря, 10 рублей. Именно в нем и делается примерно 75% изобретений. Огромную роль в нем играет работа инженеров.

Наконец, далее следует опытно-конструкторские разработки (ОКР), делающие придуманное эффективным, конкурентоспособным и достаточно дешевым. Именно здесь создаются технологии, позволяющие сделать всё это. Этот сектор «стоит» уже 100 рублей, и характерное время здесь 2-3 года. Именно в этой сфере обычно и происходит соперничество «щита» и «меча» в военное время.

Иными словами, переведя сказанное на «автомобильный язык», представленное разделение научной области таково. Информация и целеполагание – ветровое стекло и навигатор, фундаментальные исследования – руль, прикладные – мотор, ОКР – колеса. В ходе проведенных реформ наш научный «автомобиль» оказался без руля, без мотора, без колес.

Российская научная отрасль в настоящее время развалена. По закону, принятому в 2013 году, Российская академия наук лишилась институтов и права заниматься научной деятельностью и превратилась в клуб заслуженных ученых. В советские времена именно Академия наук занималась фундаментальными

исследованиями. Масштаб этих перемен и отсутствие Академии в качестве научной организации до сих пор не понимаются в обществе, поэтому поясню произошедшее цитатой из беседы научного журналиста А.В. Ваганова и президента РАН А.М. Сергеева:

А.В. *Вам не кажется, что это какой-то оксюморон: академия наук просит (борется!) чтобы ей разрешили заниматься наукой?*

А.С. – *Кажется, конечно! Да, это так и есть с 2013 г. точнее с 2014 г., когда был принят новый устав академии наук. Но я не хочу снимать с академии наук ответственность за настоящее положение дел. Ведь это академия приняла тот устав, в котором нет пункта «научная работа» в основных видах деятельности. И, заметьте, за этот устав голосовали практически единогласно. Против, если я не ошибаюсь, было 10-12 голосов. Я был среди этого небольшого числа людей. А все остальные проголосовали за…* [17].

Прикладная наука – «мотор» – была разрушена по большей части еще в 1990-е, и вопрос о её восстановлении за эти десятилетия даже не ставился.

«Колес» тоже нет – высокотехнологичных корпораций мирового уровня, которые могли бы вести ОКР на современном уровне, в стране практически нет.

Бывшие академические институты подчинены Министерству науки и образования, которое платит ученым за число выполненных и опубликованных научных работ. Особо ценятся те, которые упоминаются в международных базах знаний Scopus и Web of Science. О чем эти работы неважно. Все как у классика «числом поболее, ценою подешевле». Образование и наука – принципиально разные виды деятельности. В преподавании важно хорошо научить людей тому, что известно и понятно. Это нелегкая работа. В науке нужно пробовать и создавать новое. Естественно, Министерство образования хочет, чтобы преподаватели имели какое-то отношение к науке, и действует, исходя из этого. Пусть публикуют что-нибудь и желательно за границей.

В СССР круг воспроизводства инноваций замыкался одним способом, в Китае – другим, в США – третьим. У нас он сейчас не замыкается никак – обратные связи разорваны. Была сделана ставка на «инновации», но и она оказалась бита. Вспомним грустный опыт «Роснано». Летопись инновационной политики России можно сравнить с коллекцией сделанных ошибок [18]. В своё время

А.А. Фурсенко предлагал «обуниверситечить» науку, «омолодить» её и «сопрячь с малым бизнесом» и тогда будет пройдена «точка росы» и мы окажемся среди инноваций. Не получилось, не оказались.

Ориентировка на страну-сырьевого донора, вероятно, и заставила махнуть рукой на науку. В развитии космической отрасли Россия вкладывает 1/90 от мировых вложений. В Китае на работы в области искусственного интеллекта тратится в 350 раз больше, чем в России. Там, где у нас сидит один сотрудник, там создается институт.

Какими будут войны в обозримой перспективе? Не первое десятилетие эксперты пишут, что это будут *войны разведывательно-ударных комплексов*. Важнейшая часть этих систем – электроника и программное обеспечение. В свое время академик Ж.И. Алферов не раз говорил мне, что лучший способ позаботиться о национальной безопасности – вложить деньги в создание *собственной* элементной базы, поскольку от 80 до 95 % эффективности современного оружия определяется электроникой, которая в него «зашита». К сожалению, мы до сих пор не имеем электронной промышленности, которая удовлетворяет потребности российской армии.

Что же делать в этой ситуации?

Создание Госкомитета по науке и технологиям и назначение вице-премьера, курирующего эту сферу, реализацию научной и технологической стратегии страны.

Стратегия развития России и ключевые задачи, стоящие перед нашей страной, были определены в Послании Президента Федеральному собранию 01.03.2018: «Дело в том, что скорость технологических изменений нарастает стремительно, идет резко вверх. Тот, кто использует эту технологическую волну, вырвется далеко вперед. Тех, кто не сможет этого сделать, она, эта волна, просто захлестнет, утопит. Технологическое отставание, зависимость означают снижение безопасности и экономических возможностей страны, а в результате – потерю суверенитета. Именно так, а не иначе обстоит дело… Мы обязаны сконцентрировать все ресурсы, собрать все силы в кулак, проявить волю для дерзновенного, результативного труда. Не сделаем этого – не будет будущего ни у нас, ни у наших детей, ни у нашей страны. И вопрос не в том, что кто-то придет, захватит и разорит нашу землю. Нет, дело совершенно не в этом. Именно отставание – вот главная угроза, вот наш враг. Если не переломим ситуацию, оно будет неизбежно

усиливаться» [17].

Важнейший фактор ликвидации отставания – развитие науки, определяющей ключевые технологии России, прежде всего, в оборонном комплексе. Именно этого сейчас не делается.

Подробно необходимые действия мы описали в книге [16], но коротко говоря, надо:

– создать организационную структуру, позволяющую решать поставленные научно-технические задачи и использовать полученные результаты. Особенно это касается прикладной науки. Военная ситуация требует координации усилий. Возможно, не следует «возрождать» ранее созданные структуры, такие как Академия наук и иные. Вероятно, надо создавать новые организации, которые могут в нынешних реалиях заниматься фундаментальными исследованиями, прикладной наукой, ОКР. Есть большой опыт отличной работы научно-технологического комплекса в СССР, в США и в Германии в годы войны [19], и многими «заготовками» можно воспользоваться. Советский Союз выиграл научно-техническую гонку в годы Великой Отечественной войны у Германии, и сейчас, когда России противостоит Запад, перед нами встала та же проблема;

– выделить приоритеты в данной сфере, сделав акцент на двух ключевых вопросах – военных технологиях и узловых точках в импортозамещении;

– предложить и реализовать в промышленной и технологической политике меры, позволяющие производить новое и эффективное вместо старого и неэффективного.

– выработать стратегию опережающего развития в ряде областей мирового научно-технологического пространства. Повторяя в ухудшенном варианте то, что нам позволяет Запад, отсталости мы не преодолеем;

– развитие науки и технологий является важнейшим фактором формирования производительных сил, а значит, и всей экономики, а также ключевым элементом национальной безопасности. Важно было бы создать Госкомитет по науке и технологиям. Госкомитет должен быть ориентирован на утверждение и реализацию этого императива. История показывает, что в ходе реформ был взят курс на ликвидацию отечественной науки [20] – например, численность людей, занятых в научной сфере в России, уменьшилась почти втрое (рисунок 5) [21], в то время как в ведущих странах эта численность

увеличилась. Госкомитет должен переломить нынешнюю тенденцию к деградации.

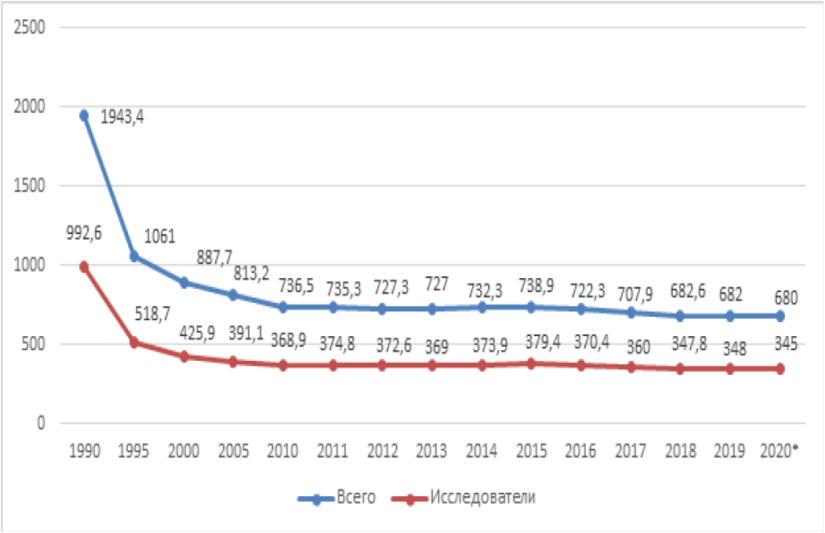


Рисунок 5 – Численность персонала, занятого исследования и разработками, и исследователей, в тыс. чел.

Вернувшись к «автомобильной» аналогии, можно сказать, что нужно уменьшить люфт руля, чтобы можно было управлять, создать двигатель – прикладную науку и сделать кардан, позволяющий передать усилия на существующие «колеса» и обновить их.

Реанимация прикладной науки России. Война ускоряет исследования и технологическое развитие. Становится понятно, что у нас должно появиться. Нынешняя стратегия импортозамещения: «Были под Западом, будем под Востоком», является тупиком. Она оставляет нас в положении игрушки более сильных центров силы. Именно в сфере прикладной науки делается 75 % изобретений. Порочна мысль «спустить» прикладную науку на уровень университетов (тем более, в условиях кризиса российского образования), технопарков, малых фирм и т.д.

Вспомним министерства «военно-промышленной 9-ки» СССР, подчинявшиеся *Военно-промышленной комиссии: – общего*

машиностроения, авиационной промышленности, оборонной промышленности, среднего машиностроения, радиопромышленности, судостроительной промышленности, промышленности связи, тяжелого машиностроения, электронной промышленности. При каждой из них были научные институты, обеспечивавшие научно-технологическое развитие этих отраслей. Ликвидировав эти институты или «слив» отрасли друг с другом, мы наказали сами себя. В Китае и США всё устроено в промышленности точно так же – там есть и свои структуры, и огромные прикладные институты, обсуживающие эти отрасли. Попытки их копировать оказались неудачны. По-видимому, стоит опираться на советский опыт.

В конце школьных задачников есть ответы. Ученики могут рассуждать по-разному, но если задачу они решили правильно, то ответы должны совпадать. Это касается и научно-технологической сферы. Конечно, исходящие из иных, по сравнению с описанными, представлений, дают ту же рекомендацию: «Необходимо сформулировать концепцию развития прикладной науки в современных условиях. Модели её в разных отраслях могут существенно отличаться, однако необходимы координация и методологическое сопровождение этого процесса на уровне правительства РФ в тесном взаимодействии с корпоративным сектором» [18].

Проблема постановки задачи. Найти хорошего заказчика сейчас нелегко. Нет ясной постановки проблем перед учеными и инженерами и представлений, что можно сейчас сделать в стране, в что нет. Военно-промышленная комиссия СССР работала в тесном контакте в Госпланом. В военное и предвоенное время никакие рыночные механизмы тут не работают. Структуры уровня Госплана сейчас необходимы России. Минэкономразвития, на которое возложены задачи стратегического планирования экономики России, не справляется с этими задачами. Нет прогноза на 10-15 лет, нет перспективы, нет математических моделей, межотраслевого баланса, нет таких корпораций как RAND в США, которые ориентированы на стратегический прогноз, нет системы 5 и 30-летнего форсайта и индикативного планирования как в Японии. В организационном плане мы оказались на уровне страны третьего мира, ждущих указаний от других или от первых лиц своей страны.

Ученые, инженеры, руководители могут писать прекрасные доклады, статьи, книги, выдвигать проекты – их некому читать и воплощать в конкретные дела. Всё это, как правило, блуждает в бюрократических структурах, не давая желаемого эффекта. В борьбе между современными технологиями принятия, реализации и контроля управленческих решений и сложившейся бюрократией последняя быстро и решительно побеждает.

Наглядный пример – реализация императивов Послания 01.03.2018. Очень важные политические решения, представленные в этом документе, не находят практического воплощения в необходимом объеме.

Для решения проблем национальной безопасности нужен не только ГКНТ, но и Госплан. Правильная постановка задачи – половина её решения.

Необходимость конкуренции в сфере ОПК. Перед Великой Отечественной и во время войны в нашей стране работало несколько конструкторских бюро, проектировавших самолеты. Это происходило не от избытка денег, а потому что разные научные и инженерные школы предлагали свои конструкции, решения, образцы техники. Можно было для массового производства выбрать лучшие образцы. Советские ракеты делали в конструкторских бюро С.П. Королева, М.К Янгеля, В.Н. Челомея. Попытка «собрать воедино» оборонные предприятия и конструкторские коллективы в «Ростехе» или «Алмаз-Антее», «Объединенной авиастроительной корпорации» и т.д., чтобы «Уменьшить трансакционные издержки», и издержки не уменьшила, и привела к монополизации. Это привело к тому, что «малые» и «средние» компании, работающие в ОПК, часто боятся вступить со своими разработчиками и проектами на поле, которое занимают «сильные». Технологическая реальность требует разнообразия и демонополизации.

Еще более грустная ситуация возникает, когда какой-то вид вооружений оказывается «не замечен» заказчиками и в результате не произведен для армии в то время, когда он был нужен. Типичный пример – беспилотники, барражирующие снаряды, в начале разработки которых наша страна занимала лидирующие позиции. Первый отечественный беспилотник успешно прошел испытания в 1968 году. Но в течение десятилетий наши заказчики так и не смогли определиться, какие аппараты нужны будут нашей армии и флоту.

Турецкий ударный оперативно-тактический средневысотный беспилотный летательный аппарат (БПЛА) Байрактар ТБ-2 с четырьмя ракетами, дальностью управления до 150 км, способный находиться в воздухе от 12 до 24 часов, выпускаемый с 2014 года, не является чудом техники. Судя по открытой прессе, не являются чудом и иранские беспилотники. Набор возможных дронов широк [20]. Несколько открытых конкурсов между отечественными производителями, готовыми работать в этой сфере, сняли бы массу проблем. DARRA это делает по многим технологиям двойного назначения. Почему же нам нельзя? Сейчас многое приходится делать срочно.

Такая же ситуация с нанотехнологиями, военные приложения которых в создании разведывательно-ударных комплексов и в сохранении жизни людей, подробно описаны в [22].

Еще Шарль де Голль писал, что только война помогает справиться с бюрократией в военной сфере. Иначе выясняется, что никто ни за что не отвечает, все просто исполняют указания и законы, а организации, которые должны помогать, отслеживают, чтобы всё делалось по инструкции и было правильно оформлено [23]. Есть известная пословица – пока гром не грянет, мужик не перекрестится. Но гром уже грянул.

Формирование Спецкомитета, ориентированного на выявление и курирование особо важных разработок. Следует на самом высоком уровне организовать Спецкомитет, выявляющий и обеспечивающий выполнение особо важных научно-технических работ, которые могут иметь стратегический эффект. Перед Второй мировой войной и в ходе этой войны такие структуры были созданы в СССР, США, Великобритании, Германии. Их работа дала большой эффект. В СССР и США на такой основе создавалось ядерное оружие и ещё несколько типов вооружений. В Великобритании по указанию премьера была создана небольшая комиссия, призванная среди имеющихся военных разработок выделить то, что сыграет ключевую роль в предстоящей войне. Они выделили радиолокацию и методику дешифровки сообщений противника, и оказались правы. Чтение немецких сообщений в течение войны позволило многократно увеличить объем доставки грузов морем и сберечь людей. В Германии на такой основе создавались ракеты ФАУ, реактивные самолеты, подводные лодки.

Организация инновационной деятельности и её экспертиза в сфере обороны и импортозамещения. Необходим широкий конкурс изобретений, инноваций, технических решений, которые могут быть использованы в военной сфере, а также в области импортозамещения с последующей экспертизой и реализацией наиболее интересных проектов. Необходимость создания реальной инновационный системы, а не её имитация. Для этого необходим поток предложений. Советский, китайский и американский опыт показывает, как это можно организовать и как поддержать людей, предлагающих новые решения насущных проблем. Не менее важна экспертиза. В США – стране с сильной инновационной системой среди 1000 проектов поддержку получают 7. Научная, технологическая, маркетинговая и иные виды экспертизы позволяют сократить риски вложения средств в реализацию выдвинутых предложений. И здесь необходим ГКНТ, работа которого позволяет воплотить, реализовать проекты, а не оставить их на бумаге.

Перед Великой Отечественной войной работа по сбору предложений от ученых была проведена в Академии наук СССР (численность которой тогда составляла около 5000 человек). Она дала большой эффект. Реализация оригинальных, парадоксальных предложений ученых оказалась очень важна для обороны страны.

Есть и ещё один аспект – для России в глобальном валовом продукте составляет 1,94 %, в объеме мировой торговли – 2,6 %. По военному бюджету Россия отстала от США более, чем в 10 раз. И такая ситуация будет иметь место на один десяток лет. Это определяет ключевое значение инновационного сектора экономики, производящего военную продукцию для нашей армии. Мы не можем делать то же и так же, как ведущие страны в области экономики и технологии, развивать системы вооружений по тому же сценарию. Должен быть эффективный, асимметричный и достаточно дешевый ответ, опирающийся на достижения науки и высоких технологий. Говоря словами И.В. Курчатова, мы должны «обгонять, не догоняя».

Специалисты по инновационному развитию предлагают то же самое. Реальность такова: «В условиях геополитических изменений (закрытые рынки и ограничения в импорте технологий, оборудования, инвестиций) инновационная политика должна быть ориентирована на создание полноценной внутренней национальной инновационной системы, способной обеспечить разработку

необходимых для развития страны решений, при этом относительно независимой от глобальных технологических цепочек.

Для эффективной разработки и реализации инновационной политики необходимо сформировать единый центр ответственности на уровне правительства РФ. Учитывая межотраслевой характер инновационной политики, руководство его должно быть выведено на уровень председателя правительства или одного из его заместителей…

Главной задачей инновационной политики в краткосрочном периоде может стать импортозамещение… Одной из приоритетных задач инновационной политики на среднесрочную перспективу должно стать построение в России завершенной модели инновационного процесса, представляющего собой цепочку от научной разработки до продаж на рынке» [18].

Междисциплинарный характер силового противостояния и военная наука.

Профессор Военной академии Генштаба генерал-майор И.С. Даниленко так оценивал военную науку в нашем Отечестве: «Слабостью военной науки оказался преимущественно ведомственный метод её развития, малая доступность для общественности, сфокусированность её содержания на проблемах только технологии и ведения войны и слабая связь с вопросами раскрытия её природы, социального смысла и целей». Он писал, что возникло «некое сектантское положение военной науки».

Генерал армии М.А. Гареев призывал разобраться, как определить войну в современных условиях, выяснить, что такое гибридная война. Эти же проблемы рассматриваются в учебниках для магистрантов, аспирантов, докторов, адъюнктов [24]. Также вопросы обсуждаются и на многочисленных конференциях, посвященным военным проблемам, а также переход от стратегии Клаузевица к стратегии Сунь-Цзы.

Но этого явно недостаточно. Вернемся к стратегии Сунь-Цзы. Он считал, что военная сила должна согласовываться с дипломатией, с отличными шпионами в стане врага, с пониманием состояния своего войска и войска противника, а также географии и условий, в которых ведутся боевые действия. По сути, он настаивал на целостном, системном в*и*дении ситуации. О том же писал генерал-майор Е.И. Мартынов в начале XX века. Выдающийся военный

теоретик формулировал обязанности политики по отношению к стратегии. Говоря современным языком, большая стратегия страны должна согласовываться с военной стратегией. Для конкретности он приводит следующий исторический пример: «…когда французы со всеми союзниками были изгнаны из России, фельдмаршал Кутузов решительно высказался за прекращение войны. Он доказывал, что Наполеон теперь уже для России не опасен и что следует поберечь его для англичан». Того же взгляда держался и государственный канцлер граф Румянцев. Но вопреки всему этому Император Александр пожелал быть спасителем Европы… Венский конгресс показал, насколько ошибочна была политика Государя» [25].

Мир стал сложнее – у военной стратегии появилось огромное число связей не только с дипломатией, но и с другими сферами жизнедеятельности. По сути, война идет сейчас в прямом эфире. Информационные и консцинентальные (войны сознания) методы противостояния сейчас стали неотъемлемой частью военных столкновений. Скрытность, неожиданность, внезапность всегда были неотъемлемой частью военных действий. Однако дроны, авиационная и космическая разведка сделали невозможным скрытное сосредоточение больших воинских сил. Это совсем новая война… И множество других важных факторов надо оценивать в их взаимодействии и совокупности. Около тридцати лет один из ведущих американских экспертов писал: «Военная доктрина третьей волны обретает форму и возникает новое поколение «воинов знания» – интеллектуалы в мундирах и в штатском, преданные той мысли, что знание может побеждать в войне – или предотвращать её. Если посмотреть, что они делают, мы увидим постоянный прогресс от спектра узких технологических вопросов и всеобъемлющей концепции, которая когда-нибудь будет названа стратегией знания…

Возьмем приобретение – создание или покупку знаний, необходимых вооруженным силам…

Например, ясное технологическое преимущество Америки в военном деле во многом связано с тем, что министерство обороны тратит около 40 млрд долларов на исследования, связанные с обороной.

Перед отечественной военно-политической и научной мыслью стоит принципиальный вопрос – как сохранить суверенитет и территориальную целостность России в обозримой перспективе.

Начиная с XIX века, Россию представляли как медведя, имея в виду её огромное население, гигантскую территорию, громадные ресурсы. Сейчас ситуация изменилась. Население России на 2021 год составляло 146 млн человек, плотность населения 8,5 чел/кв. км., 1,85 % от общего числа людей на планете, 9 позиция по этому показателю в мире. Турция – 85 млн, 52 чел/кв. км, 1,08 %; Германия – 84 млн, 235 чел/кв. км, 1,04 %; Иран – 85 млн, 52 чел/кв. км, 1,08 %; Великобритания – 68 млн, 281 чел/кв. км, 1,06 %; Польша – 37 млн, 84 чел/кв. км, 047 % [26]. Население в странах, окружающих Россию, достаточно велико, сравнимо с числом граждан России, плотность населения является гораздо большей, чем у нас. При нынешних демографических показателях в России и в мире по прогнозу ООН к 2100 году Россия будет на 22-й позиции среди стран мира, уступая Мозамбику и опережая Мадагаскар. Наступившее столетие называют веком Африки – на этом континенте будет жить около 40 % населения мира, в Азии – 40 %, а в Европе и Америке – по 10 %. Это совсем другой мир, в котором России надо найти и сохранить своё место. Это системная проблема – несмотря на мощный ракетно-ядерный щит СССР не удалось сохранить ни страну, ни мировую систему социализма.

Поэтому в XXI веке образом России должен быть не медведь, а росомаха – сильный и опасный зверь, на которого не охотятся. Путь к этому лежит через оригинальное высокотехнологичное оружие, превосходящее то, что есть у оппонентов, форсированное развитие инновационного сектора в военной промышленности, а также формулировку и отставание своих смыслов и ценностей в отечественном и мировом пространстве.

Развитие и использование гуманитарных дисциплин и междисциплинарных подходов в военной науке.

Военные конфликты в Афганистане, Сирии, Ливии, на Украине показали, что недопонимание или непонимание гуманитарной составляющей противостояния ведет к неточностям или серьезным ошибкам в действиях вооруженных сил, сил специальных операций. Воюет не техника, а люди. Необходимы военные социологи, психологи, специалисты по средствам массовой информации, образованию, элитной разведке, культуре того региона, реальность в котором мы хотим изменить. При этом нужна целостная картина и прогноз наиболее вероятных результатов вмешательства, что требует

системных, междисциплинарных подходов. В ряде документов армий других стран эти подходы подчеркнуты. В «Оборонной доктрине» Израиля указывается, что проведение операций должно осуществляться на основе «междисциплинарной концепции» (военной, экономической, правовой, медийной, политической» и «на основе единой стратегической логики» [24].

Необходимость перевалить через «хребет стоимости». Высокотехнологичное оружие должно стоить дешево.

В вычислительной технике производительность компьютеров и число элементов на кристалле Q в последние полвека определяется законом Мура – $Q \sim 2^{(t/2года)}$, то есть в геометрической прогрессии. При этом стремительно дешевеет проведение каждой операции с плавающей запятой, измеряемое в флопсах (1 операция/секунду). Ситуация здесь как с мифом о Сизифе. Вкладывая огромные усилия, он вкатывает тяжелый камень в гору (цена высокотехнологичного оружия растет и растет). Однако потом камень срывается с горы («хребта стоимости») и летит вниз. Новые технологии позволяют делать то же самое всё дешевле и дешевле. Проследим, к примеру, цену за 1 гигафлопс (10^9флопс). Вычислительная техника играет огромную роль в системах вооружений.

1945 – $\$1{,}88 \cdot 10^{12}$; 1961 – $\$169{,}6 \cdot 10^9$; 1984 – \$48,9 $88 \cdot 10^6$; 1997 – $\$151 \cdot 10^3$; апрель 2000 – $\$1{,}6 \cdot 10^3$; август 2003 – \$121; март 2011 – \$2,19; ноябрь 2020 – \$0,04 [27].

За 10 лет цена секвенирования генома человека (одной из ключевых технологий в современной медицине и биотехнологии) уменьшилась в 20 тысяч раз.

Война показала, что всё б*о*льшую роль начинает играть дистанционное зондирование Земли из космоса. Цена запуска малых спутников уменьшилась до \$5000. Стремительно дешевеют системы с искусственным интеллектом.

После того, как в ходе прикладных исследований удается перейти «хребет стоимости» высокотехнологичное оружие становится намного дешевле. Именно в то, чтобы перейти этот хребет в ключевых технологиях, имеющих отношение к вооружениям, и должны вкладываться большие усилия.

Систематическая научная деятельность, ориентированная на создание оружия в дальней перспективе.

В 1958 году, в ответ на запуск первого искусственного спутника

Земли в США было создано Управление перспективных исследовательских проектов Министерства обороны США (Defense Advanced Research Projects Agency – DARPA). Цель этой организации – сохранение превосходства вооруженных сил США, предотвращение внезапного появления новых технических средств вооруженной борьбы, поддержка прорывных исследований, преодоление разрыва между фундаментальной наукой и решением актуальных с точки зрения обороны задач [28].

Анализ работы DARPA показывает, что эта организация успешно справляется со своими задачами [19]. В пользу этого говорит ряд «сумасшедших» проектов, достаточно быстро превратившихся в военные технологии. Ряд *открытых* конкурсов, проведенных в США, позволил найти интересные решения ряда сложных технических проблем. Известно, что излишняя секретность является серьезным тормозом для проведения фундаментальных и прикладных исследований. Большого внимания заслуживают стратегические технологические прогнозы американских военных [22].

Многолетние попытки ученых и военных СССР и России создать организацию, схожую с DARPA, в нашей стране не привели к успеху. Эти попытки не смогли преодолеть джунгли отечественной бюрократии и ведомственного феодализма. Возможно, в условиях силового противостояния с Западом, эти проблемы удастся решить.

Наличие нескольких мозговых центров, предлагающих альтернативные подходы в военной сфере.

Войны требуют большой, серьезной подготовки. В качестве примера можно привести войну в Иране (1991) или, как её называют, «первую кибервойну». Она обсуждалась и планировалась военными и гражданскими специалистами больше десяти лет [1]. Результатом этих усилий стало очень быстрое проведение операции и очень малое число погибших американцев (в десятки и сотни раз меньше, по сравнению с прогнозами «независимых экспертов», не представляющих какие технологии будут использованы.

И мы вновь возвращаемся к мудрости, высказанной Наполеоном: «Искусство войны – это наука, в которой ничто не удается, кроме того, что тщательно просчитано и тщательно продумано».

Воспитание и образование

Лучше нет солдата, чем в 15 лет!

Наполеон

Война на Украине дала очень серьезный урок всем, кто связан с образованием. Оказалось, что тридцать лет безвременья и националистическая педагогика, воспевание палачей может привить молодежи фашистскую идеологию, стремление рассматривать себя как сверхлюдей в сравнении со всеми остальными. Можно процитировать известного отечественного педагога Ю.В. Громыко: «Следует отметить, что формирование националистической фашистской идентичности у молодежи Украины в последние 8 лет осуществлялось за счет вызывания ложной жертвенности. Молодежь Украины призвали защитить националистическую государственность Украины от хищной России, «русни». Донецкий и Луганский учитель сумел защитить ценность подвига во имя России. Теперь доле за Российским учителем» [29].

Многие проблемы, которые сильные державы решают за счет слабых сейчас, в эпоху развитых СМИ и компьютерной реальности, могут быть сняты с помощью «цветных революций». Эффективность этого инструмента управления массовым сознанием часто превосходит то, что может быть достигнуто с помощью традиционных военных инструментов. Образование, адекватное мировоззрение, осознание происходящего становятся важными факторами обеспечения безопасности страны.

К сожалению, здесь не все благополучно. По данным опроса «ВЦИОМ-Спутник», проведенного в 2022 году, 35 % граждан России считают, что Солнце вращается вокруг Земли. В 2007 году таковых было 28 %, в 2011 – 32 % – ситуация ухудшается. 21 % считают, что первобытные люди жили одновременно с динозаврами, а 44 % убеждали, что продукты с ГМО вызывают рак [30]. По данным Международной программы по оценке образовательных достижений PISA (Programme for International Student Assessment), проверяющей знание средних 15-летних школьников по математике, физике и естественным наукам, а также по чтению на родном языке, российские ребята по каждой из этих дисциплин находятся в четвертом десятке. На первых позициях находятся школьники из

стран, где не на словах, а на деле осуществляется научно-технологический прорыв (Китай, Южная Корея, Сингапур, Финляндия и др.).

Советское образование считалось одним из лучших в мире. О воспитании позволяет судить победа в Великой Отечественной войне – воюет, прежде всего, молодежь.

Развал в сфере образования и воспитания в России связан с тем, что почти тридцать лет проводившиеся реформы были направлены на то, чтобы выращивать не патриотов, ответственных граждан, творцов и создателей, а «квалифицированных потребителей», созданного людьми из других, более развитых стран. Образование в нынешней реальности представляет собой важнейшую *политическую технологию.* Этот взгляд подробно обоснован в книге [31]. Что делать в этой ситуации, учитывая военные угрозы стране?

Переориентация школы России на патриотический вектор, на идеологию решения цивилизационных задач, на взлет России.

Ключевое значение приобретает этический вектор. Способность и потребность в самоорганизации. В европейских языках нет аналогов таких слов как «совесть», «воля», «образование», императива «Не в силе Бог, а в правде». А у нас они есть!

Не должно быть пустозвонства! В школах сейчас вводится урок «Разговоры о важном», на котором учителя должны обсуждать с детьми актуальные темы. Каковы они? По мысли Минобраза это «День пожилых людей», «День отца», «День матери», «День учителя», «105 лет со дня рождения К.Э. Циолковского» и т.д. [32]. Рекомендовано о политике не говорить… И это в стране, которая ведет войну, которую хочет ликвидировать Запад?! С кем вы, господа чиновники?

Вновь обратим внимание на текст Ю.В. Громыко: «Воспроизводство цивилизационной идентичности основывается на освоении новыми поколениями системы цивилизационных ценностей и достигается за счет применения недекларативных воспитательных технологий. В образовательном процессе должны быть созданы условия для самоопределения подростка по отношению к ценностям служения социальной справедливости, созидательной преобразующей деятельности и жертвенного подвига, свободы как возможности обеспечивать свою жизнь собственной

продуктивной деятельностью и творчеством» [31].

Переход к предметоцентричному образованию, к освоению знаний, умений, навыков от асмоловщины, правящей 35 лет. Мы переживаем «кадровую катастрофу», – острый дефицит специалистов. Не хватает, к примеру, пилотов, командиров, специалистов в ряде областей программирования. После отъезда десятков тысяч программистов из России с началом СВО этот дефицит стал ещё острее. В 90-95 % школ России практически нет полноценного образования, половина школьников страны пользуются услугами репетиторов. Старшие классы стоят полупустые… Развалили советскую школу под лозунгом психолога А.Г. Асмолова: «от культуры полезности к культуре достоинства», проводя преобразование советского предметоцентричного к либеральному «личностно-ориентированному» образованию. В предметоцентричном подходе учителя оценивают по знанию своего предмета, по способности научить ребят своему предмету, а школьников по знанию своих дисциплин. Советские учащиеся сдавали 8 экзаменов на аттестат зрелости: русский язык (сочинение), литература, алгебра (контрольная), геометрия, тригонометрия, физика, химия, история СССР, новая история, иностранный язык.

Это позволяло сформировать целостное мировоззрение.

В личностно-ориентированном подходе знания не очень важны, а надо, чтобы человек развивался и был доволен учебой.

Образование определяется во многом потребностями общества. И одна из ключевых потребностей сейчас – защита Отечества. Поэтому следует возродить многие важные элементы советского образования. Конечно, в школу надо вернуть начальную военную подготовку, труды, домоводство. Надо отказаться или свести к минимуму электронное образование. Нам очень важно со школьных лет отбирать элиту. Надо находить тех, кто через несколько десятилетий сможет взять на свои плечи груз забот по защите, развитию и взлету России.

Формирование единого образовательного пространства в целом и суворовских и нахимовских училищ в частности.

Мы должны иметь один отличный школьный учебник для страны и учебник повышенной сложности. Это позволяет организовать методическую работу и повысить средний уровень образования. Остальное – материал для кружков. Сейчас же в России

история XX века преподается, вопреки поручению Президента, по 86 учебникам. В некоторых из них объясняется, что Вторая мировая война была выиграна армией США при поддержке СССР… Это нетерпимо! Масса паразитического может быть выброшена из школьных программ. Учить надо меньше, но лучше.

В ранце каждого солдата должен лежать маршальский жезл. В суворовских училищах, в военных вузах должны отлично знать военную историю России, наши победы и поражения.

Многие из тех, кто предполагает стать офицером, не знают суворовских «военных добродетелей» – «Отважность для солдата, храбрость для офицера, мужество для генерала» и принципа великого полководца: «Стоянием города не берут: воюют *умением*, а не *числом*; от *умения* происходит *согласие!*» [33].

Преображение вузов, отказ от единого экзамена, отказ от болонщины и возвращение к специалитету. Единый государственный экзамен (ЕГЭ) губит школьную программу – то, что не сдается, не учится. Он лишает подростков профориентации, – «были бы баллы»… Он оголяет провинцию «В Москву, в Москву, в Москву…» ЕГЭ лишает ректораты ответственности: «Мы не можем подготовить специалистов из того, что вынуждены принимать». ЕГЭ нужно немедленно отменить!

Организация военных кафедр в большинстве вузов. Расширение военного образования. В период реформ в плане «демилитаризации», на основе подходов, выдвинутых руководством Высшей школы экономики (ВШЭ) военные кафедры были закрыты в большинстве вузов. Мы лишились огромного числа командиров. Наконец, в ряде военных специальностей не должно быть, как сейчас, монополизма, а необходима разумная конкуренция, развитие нескольких подходов. В ходе войны на Украине мы испытываем дефицит командиров, – при наличии множества военных кафедр в России этого не было.

Напомним слова Карла Клаузевица: «Война – область недостоверного; три четверти того, на чем строится действие на войне, лежит в тумане неизвестности, И, следовательно, чтобы вскрыть истину, требуется прежде всего тонкий, гибкий, проницательный ум… чтобы успешно выдержать эту непрерывную борьбу с неожиданным, необходимо обладать двумя свойствами: во-первых, *умом, способным прозреть мерцанием своего внутреннего света сгустившиеся сумерки и пощупать истину;* во-вторых,

мужеством, чтобы последовать за этим слабым указующим проблеском». Кроме того, «Но на вопрос, какого рода ум более всего соответствует военному гению, скажем, исходя из природы военной деятельности и опыта действительности, – скорее критический, чем творческий, скорее широкий, чем углубляющийся в одну сторону; горячей голове мы предпочтем холодную, и последней мы вверили бы на войне благосостояние наших братьев и детей, честь и безопасность родины»[34]. Таких людей очень немного в обществе, и военные кафедры являются отличным инструментом, чтобы найти их.

Возвращение выведенных из Москвы военных академий в столицу. У этого несколько важных смыслов. Военная элита в течение многих веков была важной частью руководства страны. Идея служения – одна из главных в нашем цивилизационном коде. Петр I присвоил себе звание бомбардира, последующие цари – полковников. Обучение в Москве дает военным совершенно иное ощущение России. Кроме того, это возможность взаимодействия таких структур и их слушателей с ведущими учеными страны, в том числе создающими оружие. Это трудно переоценить.

Литература:

1. *Тоффлер Э. Тоффлер Х.* Война и антивойна: Что такое война и как с ней бороться. Как выжить на рассвете XXI века. / Пер. с англ. М.Б. Левина. – М.: АСТ: Транзиткнига, 2005. – С. 50-52.

2. *Ленин В.И.* – Полное собрание сочинений. 5-е изд. Т. 39. – М.: Издательство политической литературы, 1970. – С. 321.

3. *Белл Д.* Грядущее постиндустриальное общество. Опыт социального прогнозирования. / Пер. с англ. «Центр исследований постиндустриального общества». Изд. 2-е.– М.: Academia, 2004. – 788 с.

4. Список стран по ожидаемой продолжительности жизни. [Электронный ресурс]. – URL: https://ru/m/wikipedia.org/wiki/список_стран_по_ожидаемой_продолжительности_жизни (дата обращения 25.10.2022).

5. *Сунь-Цзы.* Искусство войны. / Пер. с англ. М. Михайлова. – М.: Издательство АСТ, 2022. – 160 с.

6. *Малинецкий Г.Г.* Синергетика – новый стиль мышления: Предметное знание, математическое моделирование и философская рефлексия в новой реальности. – М.: URSS, 2022. – 288 с.

7. *Фурсов А.И.* De Conspiratione: Капитализм как Заговор / De Conspiratione / О Заговоре. Сборник монографий. А.И. Фурсов (сост). – М.: Товарищество научных изданий КМК, 2013. – С. 7-144.

8. «Они хотят победить». – URL: https://yandex/ru/turbo/lenta.ru/s/articles/2022/06/13/lend-lease (дата обращения 25.10.2022).

9. *Чернавский Д.С.* Синергетика и информация: Динамическая теория информации. Изд. 5-е. – М.: URSS, 2017. – 304 с.

10. *Кара-Мурза С.Г.* Потерянный разум. – М.: Алгоритм, 2005. – 704 с.

11. Торговля между Китаем и Европой демонстрирует устойчивость. – URL: https://yandex.ru/turbo/pre.today/torgovlya-mezhdu-kitaem-i-evropoj-demonstriruet-ustojchivost/ (дата обращения 25.10.2022).

12. Пояс и путь. – URL: https://ru.wikipedia.org/wiki/Один_пояс_и_один_путь (дата обращения 25.10.2022).

13. Секретарь Совбеза России нашел основания для дефолта США. – URL: https://m/lenta.ru/news/2022/22/nashe/?utm_source_yxnews&utm_medium=desktop&utm_referre=https://yandex.ru/news/story/Secretar_Sovbeza_KF_Patrushev_zayavil_chto (дата обращения 25.10.2022).

14. *Веллер М.* Остров для белых. – М.: Издательство АСТ, 2022. – 704 с.

15. *Капица С.П., Курдюмов С.П. Малинецкий Г.Г.* Синергетика и прогнозы будущего. Книга 1. Самоорганизация. История. 4-е изд. – М.: URSS, 2020 – 384 с.

16. *Иванов В.В., Малинецкий Г.Г.* Россия: XXI век. Стратегия прорыва. Технологии. Образование. Наука. – М.: URSS, 2022. – 304 с.

17. *Ваганов А.* Президент РАН Александр Сергеев: самые сложные задачи физики и научной дипломатии // В мире науки. – 2022. – №5-6. – С. 4-17.

18. *Медовников Д., Розмирович С.* 30 лет русских инноваций: почему не сложился пазл // Эксперт. – 2022. – №24. – С.48-55.

19. DARPA и наука Третьего рейха: оборонные исследования США и Германии. / Под общ. ред. А.Е. Суворова. – М.: Техносфера, 2020. – 208 с.

20. *Догерти М.* Дроны: первый иллюстрированный

путеводитель по БПЛА. / Пер. с англ. В. Бычковой, Д. Евтушенко. – М.: Издательство «Э», 2017. – 284 с.

21. О реализации государственной научно-технической политики в Российской Федерации и важнейших научных достижениях, полученных российскими учеными в 2020 году. – М.: РАН 2021. – С. 39. – URL: https://www.inr.ru/rus/2021/doclad-ran.pdf (дата обращения 25.10.2022).

22. *Альтман Ю.* Военные нанотехнологии. Возможности применения и превентивного контроля вооружений. / Пер. с англ. «Институт стратегического развития» – М.: Техносфера, 2006. – 424 с.

23. *Малинецкий Г.Г.* Развитие оборонно-промышленного комплекса России глазами математиков и инженеров // Научный вестник оборонно-промышленного комплекса России. – 2020. – Вып.3. – С. 37-49.

24. *Кокошин А.А.* Вопросы прикладной теории войны. – М.: Изд. дом Высшей школы экономики, 2018. – 227 с.

25. *Мартынов Е.И.* Обязанности политики по отношению к стратегии / «… хорошо забытое старое». / Сб. статей. – Е.И. Мартынов, А.А. Свечин, С.Ф. Ахромеев. – М.: Воениздат, 1991. – С. 67-105.

26. Численность населения стран мира: данные на 2022 год. [Электронный ресурс]. – URL: https:// migrantumir.com/naselenie-stran/ (дата обращения 15.10.2022).

27. FLOPS – Википедия. Стоимость вычислений. [Электронный ресурс]. – URL: en.m.wikipedia.org (дата обращения 15.10.2022).

28. Управление перспективных исследовательских проектов Министерства обороны США. – URL: https://ru.m.wikipedia.org/wiki/Управление_перспективных_исследовательских_проектов_Министерства_обороны_США (дата обращения 25.10.2022).

29. *Громыко Ю.В.* Основы образовательной политики 2022 г. после начала СВО // Выступление на круглом столе «Красная линия» 31.08.2022. – URL: https:// https://www.rline.tv/programs/tochka-zreniya/video-291253/?PAGEN_4=2 (дата обращения 25.10.2022).

30. Опрос «ВЦИОМ – Спутник» [Электронный ресурс] – URL: https:// www.wciom.ru (дата обращения 25.10.2022).

31. *Громыко Ю.В.* Российская система образования сегодня:

Решающий фактор развития или путь в бездну? Образование как политическая технология. – М.: Ленанд, 2019. – 368 с.

32. Разговоры о важном. Сервис для классных руководителей. [Электронный ресурс] – URL: https://apkpro.ru/razgovory-o-vazhnom/ (дата обращения 25.10.2022).

33. *Суворов А.В.* Наука побеждать. – СПб: Издательская группа «Азбука-классика», 2010. – 256 с.

34. *Клаузевиц К.* О войне: в 2 т. Т. I. – М: ООО «Издательство АСТ», СПб: Terra Fantastica, 2002. – 558 с.

DOI: 10.25728/iccss.2022.22.59.003

Цыганов В.В.

Инструменты влияния и агрессии глобального центра капитала при пределах роста

Аннотация: Рассмотрен базовый комплекс инструментов глобального центра капитала, используемых для сохранения власти при глобальных пределах роста, и включающий механизмы манипулирования желаниями и страхами граждан. Показано, что результатом такого манипулирования, при ограничениях роста, является нарастание агрессивности глобального центра капитала и его сателлитов против России. Соответственно, во избежание агрессии глобального центра капитала с использованием стран, сопредельных с Россией, нельзя допускать победу цветной революции ни в одной из этих стран.

Ключевые слова: манипулирование, желание, страх, капитал, цветная революция, агрессия

Системный подход к построению моделей и методов адаптации России к глобальным изменениям предполагает учет факторов внешней среды. В монографии [1] рассмотрены модели ключевых внешних факторов и воздействий глобальной социально-экономической системы, влияющих на долгосрочную эволюцию России. В их основе лежит нейропсихологическая модель

индивидуума, как активного элемента этой системы, с присущими ему желаниями и страхами [2].

Управление желаниями. Реакция на положительный стимул индивидуума, стремящегося к удовольствиям (гедониста), приводит, на первый взгляд, к положительным эмоциям. Однако затем возникают отрицательные эмоции. Чтобы избежать их, индивидуум стремится к новым положительным стимулам. Их последовательность формирует лестницу желаний индивидуума [2].

Реализация лестниц желаний индивидуумов, стремящихся к накоплению финансовых средств в суверенных странах, приводит к формированию локальных центров капитала [3]. При глобальной финансовой открытости (глобализации), формируется глобальный центр капитала (ГЦК), а также общество потребления в стране пребывания ГЦК (сегодня эта страна – США). Индивидуумы-гедонисты в ГЦК стремятся к все новым удовольствиям от безудержного потребления. Однако глобальные пределы роста в XXI веке ограничивают их потребление даже в стране пребывания ГЦК. Это приводит к массовому недовольству в обществе потребления, в первую очередь, в стране пребывания ГЦК.

Во избежание кризиса идеологии общества потребления, ГЦК использует инструменты, расширяющие пределы роста за счет использования дешевых ресурсов стран периферии мировой финансовой системы и захвата их рынков (что произошло, например, после развала СССР). К этим инструментам относятся цветные революции, захватнические войны и инспирированные локальные финансово-экономические кризисы в странах периферии мировой финансовой системы.

Кроме того, ГЦК манипулирует желаниями членов самого общества потребления, периодически устраняя массовое недовольство индивидуумов-потребителей материальных благ путем скачкообразного снижения потребления. В дальнейшем, по мере увеличения потребления (с пониженного уровня и до пределов роста), эти индивидуумы испытывают регулярные положительные эмоции. Это снимает проблему массового недовольства в обществе потребления. Основные инструменты, используемые ГЦК для скачкообразного снижения потребления своих граждан: мировые и локальные войны, глобальные финансово-экономические кризисы и пандемии.

Управление страхами. В условиях пределов роста и самозащиты стран периферии мировой финансовой системы, ГЦК не всегда удается использовать указанные инструменты манипулирования желаниями. Поэтому для того, чтобы обеспечить индивидууму-потребителю регулярные положительные эмоции, ГЦК использует управление страхами. Реакция напуганных ГЦК индивидуумов приводит, вначале, к отрицательным эмоциям. Однако после того, как испуг проходит, индивидуумы испытывают положительные эмоции. Со временем, однако, индивидуумы-гедонисты забывают страх и вновь стремятся увеличить потребление. А поскольку сделать это одновременно для большинства граждан ГЦК не может (из-за пределов роста), то массовое недовольство в обществе потребления возникает вновь.

Чтобы избежать этого недовольства, ГЦК должен генерировать все новые страхи. Их последовательность формирует лестницу страхов индивидуума [2]. Типичные стадии манипулирования страхами для удержания власти ГЦК связаны с:

- формированием образа внешнего врага;
- национализмом (сознанием собственной исключительности);
- нацизмом (национал-социализмом), как наиболее агрессивной формой национализма.

Таким образом, базовый комплекс инструментов ГЦК, используемых для сохранения власти при глобальных пределах роста, включает манипулирование желаниями и страхами (рисунок 1).

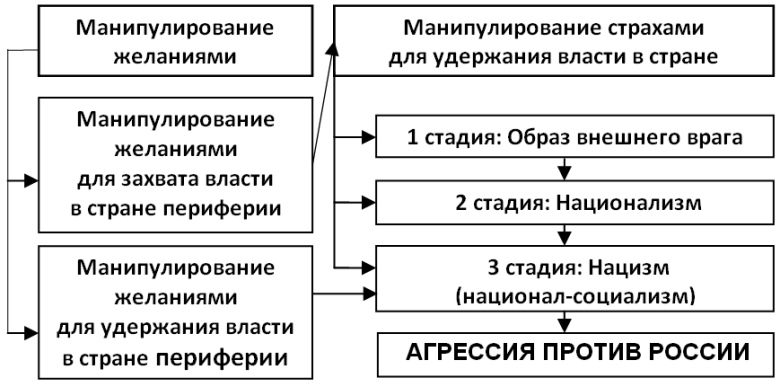


Рисунок 1 – Базовый комплекс инструментов ГЦК, используемых для сохранения власти при глобальных пределах роста

Для того, чтобы на практике использовать этот комплекс инструментов в той или иной стране периферии мировой финансовой системы, ГЦК необходимо иметь эффективные рычаги влияния на национальный капитал (например, компрадорскую буржуазию и олигархию), контролирующий средства массовой информации. Как показывает опыт Украины, чтобы получить такие рычаги, ГЦК достаточно провести цветную революцию в той или иной стране периферии мировой финансовой системы. В результате этого фактическая власть в этой стране переходит к ГЦК.

Примеры организации и результаты использования этих инструментов в беднейших странах Европы в XX и XXI веке – в Германии (в 1920-1933 гг.) и Украине (в 2014-2022 гг.) иллюстрирует рисунок 2. В обоих случаях, с моментов переворотов в Германии и Украине, и до начала войны, соответственно, с СССР (1941 г.) и Россией (2022 г.) прошло 8 лет. Таково характерное время, достаточное для изменения общественного сознания в стране периферии мировой финансовой системы, после победы в этой стране цветной революции.

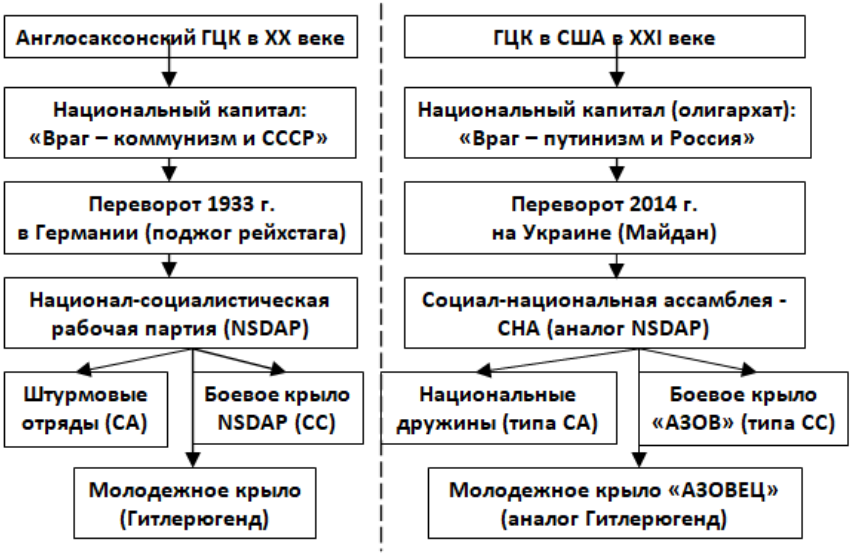


Рисунок 2 – Примеры организации и результаты использования базового комплекса инструментов ГЦК

Вывод 1. Результатом манипулирования желаниями и страхами для сохранения влияния ГЦК при пределах роста является нарастание агрессивности ГЦК и стран-сателлитов против России.

Вывод 2. Во избежание агрессии ГЦК из сопредельных стран, нельзя допускать победу цветной революции ни в одной из стран, граничащих с Россией.

Основываясь на этих выводах, в монографии [1] было спрогнозировано нарастание агрессивности ГЦК и его сателлитов против России. В результате прогнозировалось нарушение транспортного сообщения со странами Запада, в первую очередь, Европейского союза. Таким образом, в [1] было спрогнозирован поворот транспортного комплекса России на Восток. Этот вывод лег в основу долгосрочных прогнозов развития транспортной инфраструктуры Сибири, Дальнего Востока и Арктики [4]. На их основе несколько лет назад в монографии [1] были построены 3 сценария долгосрочной эволюции транспортного комплекса России – при нарастании агрессивности Запада, мобилизации и войне.

Литература:

1. Транспортный комплекс России / В книге: Стратегическое планирование устойчивого функционирования экономического комплекса Российской Федерации. Угрозы, целеполагание, прогноз, рекомендации. – М.: Изд-во РАН, 2021. – 84 с.

2. *Цыганов В.В.* Адаптивные механизмы и высокие гуманитарные технологии. Теория гуманитарных систем. – М.: Академический проект, 2012. – 346 с.

3. *Цыганов В.В., Бородин В.А., Шишкин Г.Б.* Интеллектуальное предприятие. Механизмы овладения капиталом и властью. – М.: Университетская книга, 2004. – 776 с.

4. Инфраструктура Сибири, Дальнего Востока и Арктики. Состояние и 3 этапа развития до 2050 года / В.В. Цыганов, А.К. Еналеев и др., под ред. члена-корр. РАН А.А. Макоско. – СПб.: Институт проблем транспорта им. Н.С. Соломенко РАН, 2019. – 465 с.

DOI: 10.25728/iccss.2022.26.70.004

Лещенко В.В.

О цивилизационной безопасности России

Аннотация: Изложены результаты научно-исследовательской работы по цивилизационной безопасности. Обращено внимание на актуальность темы исследований. Приведены данные по её исследованию другими авторами. Сформулировано понятие цивилизации. Описаны эпизоды цивилизационной безопасности на примере России и Китая. Использован системный подход в представлении цивилизационной безопасности в теории общих систем.

Ключевые слова: понятие цивилизации, цивилизационная безопасность, системный подход, теория общих систем, модель цивилизационной безопасности, Россия, Китай

На протяжении последнего полувека в различных странах мира произошли изменения, заставившие исследователей в очередной раз

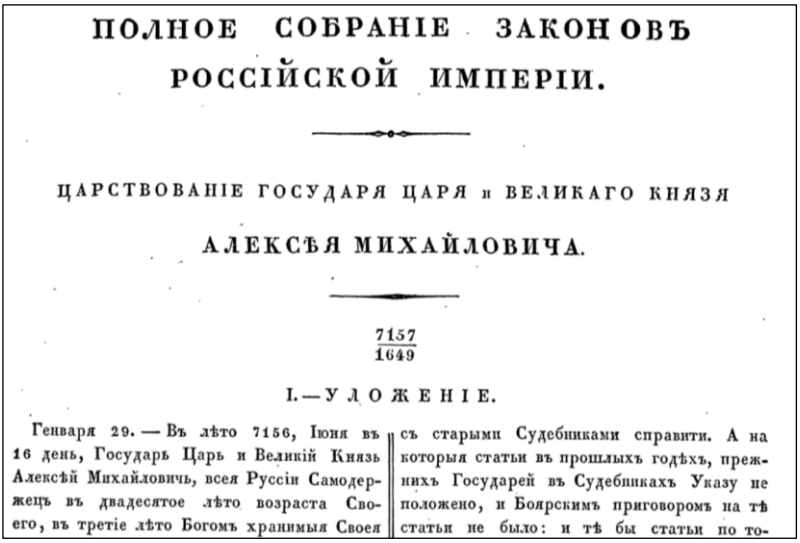
обратить внимание на процессы цивилизационного развития на нашей планете. Неотъемлемой частью этих исследований являются исследования цивилизационной безопасности.

В научной литературе появилось множество работ на эту тему. Среди них диссертация и монография [1, 2], в которых содержится обширная тематическая библиография. В Институте философии РАН был выполнен научный проект на тему цивилизационной безопасности [3].

В подавляющем большинстве упомянутых выше работ преобладает философский и политический аспект исследований и анализа цивилизационной безопасности России.

В отличие от вышеприведенных аналитических исследований цивилизационной безопасности мною избран системный подход в исследовании [4] и представлении понятия цивилизации и цивилизационной безопасности.

В настоящее время мы живем в 7530-ом году по летоисчислению Русской цивилизации. Об этом свидетельствует исторический документ [5]. Копия одной из первых его страниц представлена на рисунке 1. Как видим, дата в нём по русскому летоисчислению – 7157 лет, а по христианскому – 1649 лет.



ПОЛНОЕ СОБРАНІЕ ЗАКОНОВЪ
РОССІЙСКОЙ ИМПЕРІИ.

ЦАРСТВОВАНІЕ ГОСУДАРЯ ЦАРЯ и ВЕЛИКАГО КНЯЗЯ
АЛЕКСѢЯ МИХАЙЛОВИЧА.

7157
1649

I.—УЛОЖЕНІЕ.

Генваря 29. — Въ лѣто 7156, Іюня въ 16 день, Государь Царь и Великій Князь Алексѣй Михайловичь, всея Руссіи Самодержецъ въ двадесятое лѣто возраста Своего, въ третіе лѣто Богомъ хранимыя Своея

съ старыми Судебниками справити. А на которыя статьи въ прошлыхъ годѣхъ, прежнихъ Государей въ Судебникахъ Указу не положено, и Боярскимъ приговоромъ на тѣ статьи не было: и тѣ бы статьи по то-

Рисунок 1 – Уложение Государя Царя и Великого Князя Алексея Михайловича

Поэтому и письменность на Руси уже была 7530 лет тому назад, что является одним из основных признаков цивилизационного развития. На протяжении этого периода развитие русской цивилизации не прерывалось даже при самых неблагоприятных обстоятельствах.

Известная нам история Руси свидетельствует о выдающихся достижениях русского народа в различных сферах жизни: этнической, научной, культурной, социальной, политической, экономической, военной, демографической и ряде других сфер.

Прошлый век был исключительно богат свидетельствами фундаментальных достижений русской цивилизации в планетарных и космических масштабах развития Человечества. Использование ядерной (атомной) энергии в мирных целях. Это и открытие космической эры человечества 4 октября 1957 года. И продолжившееся в течение десятилетия стремительное развитие космических исследований, в том числе изучение планет солнечной системы. И первый в истории Человечества выход человека в космос 12 апреля 1961 года.

Но наряду с этим начался процесс агрессии против русской цивилизации с целью её уничтожения, который продолжается и по сей день.

Для анализа цивилизационной безопасности, как упоминалось выше, в работе использован системный подход в представлении модели общих систем, изображенной на рисунке 2.

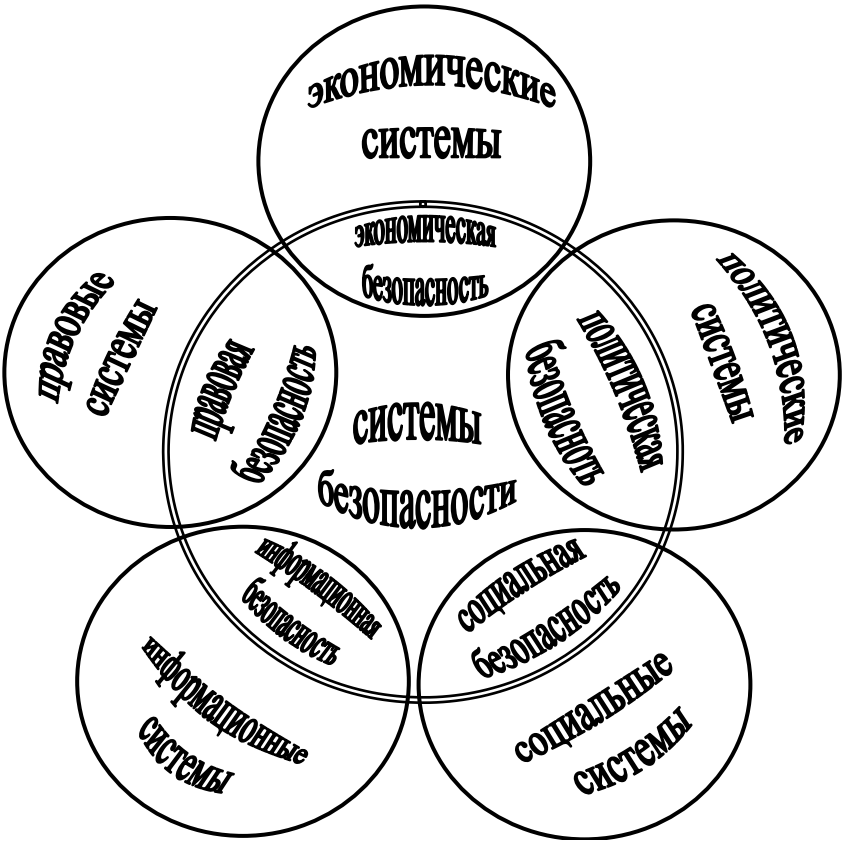


Рисунок 2 – Модель общей системы

Она отображает зависимость системы безопасности (в нашем случае цивилизационной безопасности) от других разнородных

систем: правовой, экономической, политической, социальной, информационной и ряда других, не отображенных на рисунке.

Исследования китайского ученого Линь Ифу подтверждают использование системного анализа при формировании представления развития Китая моделью общих систем.

В своей книге [6] он описывал, что Китай еще в 18 веке обладал самой развитой экономикой мира. Но затем начался период кризиса и деградации страны в период конфронтации Китая и Японии. До начала Японо-китайской войны мировое сообщество предполагало, что победителем из нее должен выйти именно Китай. На его вооружении находились закупленные у Англии и Франции новейшие английские корабли и французское вооружение. В то же время не имевшая столь объемных финансовых запасов Япония вынуждена была полагаться на малотоннажные корабли собственного производства, а ее орудия не выдерживали сравнения с теми, которыми располагал Китай.

В реформах того времени Китай делал упор на обучении использованию западных новшеств, а не на перестройку своей политической, экономической, образовательной и других систем. Поэтому значимость модернизации одного лишь вооружения без соответствующих институциональных реформ других сфер несущественна [6]. Поэтому Китай потерпел сокрушительное поражение и вынужден был выплатить Японии огромную контрибуцию и уступить остров Тайвань.

Китай потерпел сокрушительное поражение и вынужден был выплатить Японии огромную контрибуцию и передать ей остров Тайвань.

Революция в Китае и защита его Россией во второй мировой войне посредством разгрома Красной армией японской Квантунской армии позволили Китаю освободиться от японской оккупации. 9 августа 1945 года Красная армия начала наступление на миллионную Квантунскую армию и к 19 августа 1945 года разгромила её. Через 12 суток после вступления в бой Красной Армии японские войска капитулировали.

Но 30 лет тому назад Советский Союз в результате государственного переворота был расчленен на полтора десятка частей – Союза Независимых Государств. Это ознаменовало наступление решающей фазы разрушения русской цивилизации –

разрушение политической, социальной, экономической, демографической, правовой, образовательной и других разнородных систем.

Это произошло из-за декоммуникации взаимосвязи разнородных систем: социальной, политической, правовой, безопасности и некоторых других разнородных систем, при доминировании взаимосвязи их с криминальной системой.

Последние 30 лет в России развиваются процессы цивилизационного геноцида, который включает в себя:

– геноцид русского народа, о чем писал С.Ю. Глазьев [7];

– демографическое импортозамещение коренного народа;

– деградацию системы здравоохранения;

– прогрессирующая экономическая деградация страны;

– самый большой распад системы социального обеспечения в мире [8, 9];

– исчезновение в стране фундаментальной науки;

– разрушение прогрессивной системы ценностей, морали общества;

– уничтожение электронной промышленности России;

– ликвидацию авиастроения гражданского воздушного флота;

– уничтожение системы отечественного образования;

– ликвидацию ракетно-космической науки и промышленности;

– коррупцию во всех сферах государственного управления и предпринимательской деятельности;

– и ряд других тлетворных для России процессов.

С точки зрения синергетики, как одной из теорий систем, сочетание таких процессов неизбежно приведет цивилизационный процесс к точке его бифуркации, из которой может быть только два исхода: либо исчезновение цивилизации (её гибель, распад), либо революция (её переход к другой – жизнеспособной структуре).

Мировая история человечества свидетельствует об исчезнувших на нашей планете цивилизациях, артефакты которых обнаружены в результате научных исследований.

Переломный момент в современной истории России заключается в том, что останутся ли от русской цивилизации артефакты или она преодолеет кризис в своем развитии, обратившись к продолжению своей многовековой жизнеспособной

структуре развития. Это актуальный вопрос цивилизационной безопасности на кромке перед бездной ядерной войны.

Литература:

1. *Феофанов К.А.* Безопасность цивилизационного развития России в условиях глобализации: Политологический анализ: диссертация на соискание ученой степени доктора политических наук. – Москва, 2005. – 333 с.

2. *Пазюк Ю.В.* Концептуальные основы цивилизационной безопасности России в третьем тысячелетии / Федеральный исследовательский центр «Информатика и управление» Российской академии наук. – Москва: ООО «ПолиПринтСервис», 2019. – 182 с.

3. Проект «Стратегия цивилизационной безопасности России: философско-политологический анализ» (декабрь 2010 – ноябрь 2012 гг.). – URL: https://iphras.ru/page31189386.htm (дата обращения 5.10.2022).

4. *Лещенко В.В.* Теория общих систем и информационная модель мировоззрения общества / Системный подход в современной науке: (К 100-летию Людвига фон Берталанфи): [Сб. ст. / Отв. ред.: Лисеев И. К., Садовский В. Н.]. – М.: Прогресс-Традиция, 2004. – С. 309-325.

5. Полное собрание законов Российской Империи. Том 1. – Санкт-Петербург: Печатано в Типографии II Отделения Собственной Его Императорского Величества Канцелярии, 1830. – 1071 с.

6. *Ифу Л.* Демистификация китайской экономики. / Линь Ифу – перевод с китайского. – Москва: Шанс, 2017. – С. 67-68.

7. *Глазьев С.Ю.* Геноцид. – М.: Терра, 1998. – 317 с.

8. *Лещенко В.В.* Системный аспект в анализе теории и практики «устойчивого развития» на пороге третьего тысячелетия / Устойчивое развитие: актуальные проблемы и перспективы научных исследований. – М.: Экономика и информатика, 2000. – С. 73-74.

9. Нищета переходного периода? Доклад, июль 1998 г. – Б.м.: б/и. – 248 с.

DOI: 10.25728/iccss.2022.65.47.005

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

Управление процессами трансформации права в условиях цифровизации на базе сценарного подхода

Аннотация: Представлены результаты анализа комплекса проблем повышения эффективности регулирующих цифровые отношения правовых норм, а также оценки их влияния на процессы социально-экономического развития государства и общества. Для решения методологических и практических задач совершенствования системы законодательного регулирования в условиях цифровизации предложено использовать методологию сценарного анализа.

Ключевые слова: цифровизация, правовое регулирование, трансформация права, законотворчество, сценарный анализ, оценка эффективности

Введение

Цифровизация экономики неизбежно приводит к возникновению новых объектов и субъектов информационных правоотношений, существенному изменению их юридического содержания, а также появлению в этой связи новых и весьма специфических прав, обязанностей и ответственности. Это, в свою очередь, требует решения широкого комплекса задач развития системы государственного нормативно-правового регулирования и совершенствования практики правоприменения.

Конечной целью трансформации права в условиях цифровизации является создание такого правового режима, который позволит: (1) упорядочить широкомасштабное применение в системе общественных отношений современных информационных и коммуникационных технологий; (2) обеспечить необходимый уровень безопасности личности, общества и государства; (3) стимулировать интенсивное развитие высоких технологий, являющихся одной из основ интенсификации развития российского общества и государства [1].

1. Методология сценарного анализа эффективности процессов трансформации права в условиях цифровизации

Основная сложность решения проблем управления процессами трансформации права и практикой правоприменения заключается в том, что полученные результаты существенно влияют на характер и тенденции развития социально-экономической системы (СЭС) нашей страны особенно на среднесрочном и долгосрочном временных горизонтах. Проведенные исследования показали, что традиционно используемые подходы и методы математического и имитационного моделирования исследуемых политико-правовых, общественно-политических и социально-экономических процессов в рассматриваемой предметной области в своем большинстве основаны на наличии полной информации о сложной СЭС, ее окружении и взаимодействии ее сегментов (подсистем). Однако реально данные необходимой степени полноты и точности собрать практически невозможно. В данной ситуации для решения рассматриваемых задач предложено использовать методологию сценарного анализа, позволяющую в условиях неполной информации и неопределенности использовать в качестве исходных данные как качественного, так и количественного типа [2].

Сценарный подход является объектно-ориентированным методом представления и анализа информации о внутренней ситуации в обществе и государстве и состоянии внешней среды, обеспечивающим возможность прогнозирования и комплексного исследования альтернативных вариантов (сценариев) развития исследуемых ситуаций в процессах подготовки и реализации решений, направленных на повышение эффективности правового регулирования общественных отношений в информационном обществе. Данный подход базируется на структурном анализе изучаемых объектов правового регулирования, их декомпозиции на составные элементы, выявлении отношений между выделенными элементами и определении присущих им свойств с целью анализа процессов роста или уменьшения риска нарушения устойчивости развития СЭС в условиях неопределенности и при наличии внешних и внутренних возмущений или деструктивных воздействий.

Разработана формальная методология формирования и исследования моделей СЭС, основу которых составляют выделенный набор элементов, набор отношений между ними и набор определенных свойств данных отношений. Предложенная методология включает: (1) формальное описание

идентифицированных моделей СЭС; (2) описание моделей их поведения; (3) описание модели окружения СЭС; (4) формализацию моделей выбора элементов сценарной системы; (5) описание предметной области сценарного анализа; (6) выделение и способы формирования элементов сценарной системы и сценарного пространства; (7) методы определения характеристик и свойств анализируемых сценариев.

Определены основные этапы, сформированы цели, перечень задач и основные компоненты сценарной системы, получаемые в качестве результата каждого этапа.

Для решения прикладных и практических задач сценарного анализа на основе математического языка модифицированных функциональных знаковых ориентированных графов разработан программно-аналитический комплекс сценарного моделирования, методологической базой реализации функций которого являются разработанные формализованные процедуры описания управляющих воздействий и механизмов их преобразования.

2. Анализ эффективности законодательного регулирования цифровых правоотношений

Масштабная цифровизация практически всех сторон жизнедеятельности человека, неизбежно приводит к целому ряду носящих фундаментальный характер изменений, причем обусловленных не столько ростом объемов циркулирующей информации, сколько появлением новых проблем в области безопасности личности, общества и государства. Одновременно с этим сложность решения назревших и объективных проблем совершенствования законодательства заключается в том, что любые ошибки, допущенные в процессе управления трансформацией права, могут приводить к крайне тяжелым для государства и общества последствиям, а также вызывать значительный общественный резонанс.

Как следствие, оценка эффективности действия разрабатываемых законодательных актов является чрезвычайно сложной комплексной проблемой по следующим основным причинам [2]: (1) непосредственное влияние процессов нормативно-правового регулирования на развитие общественных отношений крайне трудно вычленить в силу наличия широкого спектра

описывающих процессы развития СЭС показателей; (2) достоверная статистическая оценка эффективности законодательных норм возможна только на достаточно большом временном горизонте в силу инерционности реакции СЭС на принимаемые решения; (3) высокие темпы роста вовлеченности в информационные отношения юридических и физических лиц существенно затрудняют решение задач прогнозирования возникающих в связи с этим принципиально новых угроз и возможных последствий их реализации; (4) определенные сложности вызывает и ограниченность практического опыта в решении значительной части связанных с развитием высоких технологий правовых проблем. В этих условиях возрастает актуальность задачи создания эффективных и одновременно с этим достаточно универсальных методов и механизмов опережающей сценарно-прогностической оценки эффективности разрабатываемых правовых актов.

В связи с перечисленными выше проблемами возрастает роль и значение мониторинга эффективности процессов законодательного регулирования как важнейшего источника исходной информации, на основе которой должна осуществляться комплексная оценка результативности реализации правовых актов. При этом целевые установки системы мониторинга должны быть направлены не только на формирование текущей оценки фактической результативности законодательного регулирования цифровой среды, но и на опережение возникающих проблем и новых задач с целью обеспечения возможности эффективной реакции на них системы законодательного регулирования, что, в конечном счете, определяет необходимость использования методологии сценарного анализа в качестве неотъемлемой части системы мониторинга.

В настоящее время разработаны различные подходы к оценке эффективности разрабатываемых юридических норм, которые охватывают крайне широкое множество показателей и критериев. На рисунке 1 представлена обобщенная классификация разработанных в настоящее время подходов и критериев оценки эффективности правовых норм [3-4].

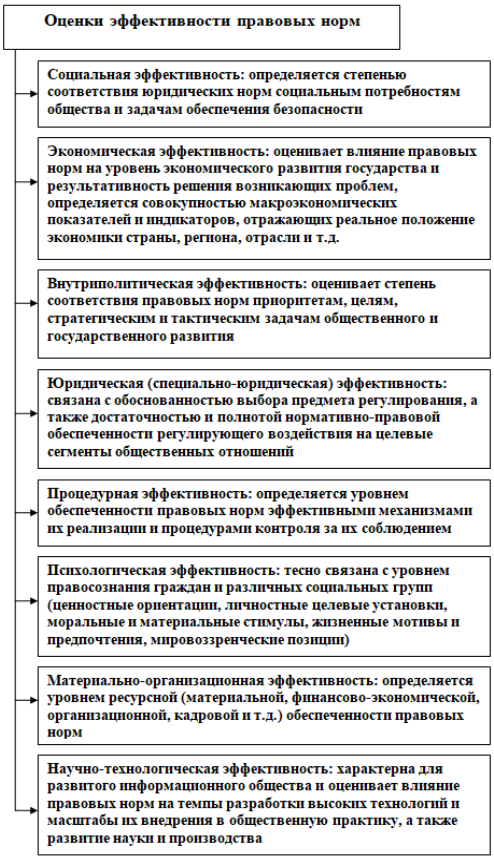


Рисунок 1 – Классификация критериев оценки правовых норм

Проведенный анализ показал, что, поскольку в настоящее время развитие законодательства идет преимущественно по пути первоочередного решения наиболее острых проблем цифровизации, в силу чего разрабатываемые правовые нормы имеют ярко выраженную целевую направленность на решение конкретных и четко очерченных задач, то для оценки эффективности правового регулирования представляется обоснованным использовать критерии и механизмы, отражающие степень достижения

поставленных в процессе законотворчества целей, в том числе на основе их сопоставления с полученными реальными результатами.

Заключение

Разработанные теоретические положения и формализованная методология сценарного анализа рассматривают процессы трансформации правового регулирования и правоприменения как неотъемлемую составную часть системы управления обществом и государством в целом, и соответственно, важнейшую основу их безопасного и устойчивого развития в условиях информационного общества. В силу этого предложенный подход обеспечивает возможность интеллектуальной поддержки и оценки качества подготовки и реализации решений в рамках управления процессами трансформации права с учетом неопределенности, а также рисков и угроз различной природы.

Полученные результаты позволили обосновать необходимость внедрения в практику правового регулирования процессов цифровизации разработанных процедур сценарно-прогнозной экспертизы законопроектов, практическое использование которых позволит повысить обоснованность системы долгосрочных и среднесрочных целей трансформации права в условиях цифровизации, а также обеспечить возможность опережающей оценки эффективности и результативности разрабатываемых нормативно-правовых актов (включая оценку эффективности практики правоприменения).

Литература:

1. *Шульц В.Л., Бочкарев С.А., Кульба В.В., Шелков А.Б., Чернов И.В., Тимошенко А.А.* Анализ проблем трансформации систем законодательного регулирования и правоприменения в условиях цифровизации и методов оценки эффективности принимаемых решений // Национальная безопасность / notabene. – 2019. – № 4. – С. 19-74.

2. *Шульц В.Л., Бочкарев С.А., Кульба В.В., Шелков А.Б., Чернов И.В., Тимошенко А.А.* Сценарное исследование проблем обеспечения общественной безопасности в условиях цифровизации. – М.: Проспект, 2020. – 240 с.

3. *Хабриева Т.Я.* Экономико-правовой анализ:

методологический подход // Журнал российского права. – 2010. – № 12. – С. 5-26.

4. Эффективность законодательства: вопросы теории и практика. / Под. ред. Ю.А. Тихомирова, В.П. Емельянцева. – М.: ИНФРА-М, 2015 – 336 с.

DOI: 10.25728/iccss.2022.66.70.006

Меденников В.И.

Цифровая платформа информационных научно-образовательных ресурсов как инструмент достижения заданного уровня информационной безопасности и надежности данных

Аннотация: В работе рассматривается эффективное решение возрастающей проблемы информационной безопасности сайтов сельскохозяйственных ВУЗов и НИИ, обусловленной не только влиянием последних громадных политических, экономических, социальных событий, усиленных пандемией COVID-19, но и ростом искаженной, недостоверной информации в интернете, резким увеличением объемов трудно перерабатываемой информации, большим объемом разнородной информации, вымыванием IT-специалистов из названных организаций, что влечет за собой падение имиджа их, снижение качества цифровой трансформации всей страны. Для решения данной проблемы предлагается осуществить формирование единой цифровой платформы информационных научно-образовательных ресурсов с одновременным решением задач, как информационной безопасности, так и надежности данных.

Ключевые слова: сельское хозяйство, информационная безопасность, сайты ВУЗов и НИИ, научно-образовательные ресурсы, цифровая трансформация

В настоящее время в результате активной цифровой трансформации сельское хозяйство и кибериндустрия становятся все более тесно взаимосвязаны с каждым годом. Чем больше

сельскохозяйственное производство становится зависимым от цифровизации, тем больше потенциальных уязвимостей возникает в неконтролируемых информационных сетях. Соответственно, с увеличением масштабов внедрения этих технологий повышаются риски кибератак на хозяйства, научные и учебные заведения. Поэтому кибербезопасность является одним из наиболее важных приложений, особенно ориентированных на предотвращение незаконных вторжений и других действий в защите данных, информации и других онлайн-ресурсов, относящихся к сельскому хозяйству. В развитых странах на основе большой практики, мнений экспертов и ИТ-специалистов как из сельского хозяйства, так и из сферы безопасности считается, что для отрасли лучше использовать наработки в сфере кибербезопасности из других отраслей экономики, адаптируя и внедряя их технологии. Но для этого необходимо сформировать реестр отраслевых словарей и классификаторов, то есть осуществить онтологическое моделирование всей предметной области. В России этот путь также представляется наиболее практичным в силу вымывания почти всех ИТ-специалистов из отрасли, в том числе, из науки и образования. Данная тенденция наблюдается также во многих НИИ и ВУЗах других отраслей. При этом они предпочитают не разрабатывать сайты с нуля, а стремятся пользоваться готовыми, в большинстве случаев примитивными, бесплатными инструментами, обладающими пропорциональным числом собственных уязвимостей.

Отток айтишников из науки и образования в бизнес привел к тому, что их место в части исследований с последующей публикационной деятельностью в области цифровой экономики (ЦЭ) заняли работники, очень далекие от информатизации, что можно объяснить требованием Минобрнауки об увеличении наукометрических показателей научных сотрудников, огромным вниманием к проблеме со стороны общества и руководителей страны. Это ожидаемо привело к росту искаженной, недостоверной информации на сайтах и в СМИ, что можно отнести также к разновидности проблемы информационной безопасности, представляющей еще большую угрозу всему инновационному будущему страны. По сути, какая разница, хакер внес на сайт

недостоверную информацию, либо недобросовестный исследователь. Последнее даже намного опасней.

Бурное развитие цифровых технологий в мире постоянно привносит в научный и бытовой обиход новую модную терминологию. Так, в данный момент резко возросло количество работ по искусственному интеллекту (ИИ), по цифровым платформам (ЦП), цифровым двойникам (ЦД), набирает популярность тема цифровых экосистем (ЦЭС). Данные понятия отличаются в работах значительным разнообразием предметной идентификации их, осложненной различным смыслом и сочетанием учитываемых при этом факторов: технологических, финансовых, биологических, экономических, человеческих, информационных и т.д. Во многих случаях идет просто переписывание ошибочных вариаций одного из первоисточников.

Так, если в исследованиях ЦЭС основоположники направления искали условия переноса законов функционирования природных экосистем на социальные, экономические, образовательные сферы, т.е. на степень способности их сохраняться или адаптироваться к изменяющимся условиям среды, то у нас Сбер, Яндекс и прочие компании навязали понимание экосистемы обществу и даже науке как отдельные разрабатываемые ими сервисы, например, по доставке еды, в целях сиюминутных интересов, обусловленных привлекательностью терминов для привлечения потенциальных пользователей к создаваемым продуктам в связи с огромным вниманием во всем мире к ЦЭ.

Под ЦД же наиболее распространено среди исследователей такое понятие: «Цифровые двойники представляют виртуальную модель реального объекта, который описывается математическими зависимостями и связан с базой данных параметров этого объекта» [1]. В [2] ЦД определяется еще более упрощенно – в виде одной базовой математической модели. Мало того, что утверждается, что у каждого предприятия есть лишь только один ЦД, так в данной работе допущена методологическая ошибка неправомерности механического переноса модели межотраслевого баланса страны на уровень предприятия, в частности, сельскохозяйственного, где под фондообразующими продуктами понимаются морковь, свекла и др. продукты. Данные понятия противоречат определению модели, представляющей

искусственный, созданный человеком объект любой природы (умозрительный или материально реализованный), который отражает наиболее существенные с точки зрения цели моделирования свойства оригинала. И самое главное, что для одного и того же объекта может быть построено множество различных моделей, отвечающих различным целям моделирования. Приведенное определение согласуется с теорией систем, которая основным предназначением любой системы считает достижение определенной цели. Лишь в одной работе по ЦД [3] данное утверждение явно выражено. Еще более запутанно выглядит ситуация с ЦП, у которых огромное количество определений. Корни же разрешения классификационных признаков ЦП лежат также в целеполагании разрабатываемых ЦП в зависимости от степени вовлеченности в разработку той или иной компоненты ИКТ, пространство функционирования которых имеет следующие три основных оси измерения: данные, иначе информационные ресурсы (ИР); алгоритмы, формализующие обработку данных, в том числе, задачи управления; инструментарий, представляющий из себя программное обеспечение (ПО) и электронные устройства. Например, IBM разрабатывает общее аппаратное и программное обеспечение, то есть инструментарий, данное Intel определение ЦП в силу рода их деятельности относится также к инструментальной оси ИКТ, многочисленные социальные сети, интернет-торговля, кадровые агентства, госуслуги и еще ряд других ориентированы лишь на две оси – на инструментальную ось и ось ИР. Отсутствие целеполагания в разрабатываемых ЦП, трактуя их как совокупность математических моделей, баз необходимых данных, определение которых настолько широко, что применимо к любому предприятию, как в прошлом веке, так и в век ЦЭ [2], еще раз ложно убеждает читателей, что ЦП должны быть свои на каждом предприятии. Такие исследования наносят огромный вред комплексности развития и внедрения цифровизации производства, дезориентируя и исполнителей программы ЦЭ, и научных сотрудников.

По истечении уже достаточного периода времени после принятия Программы цифровой экономики в стране мы видим негативные последствия такого решения. Так, в результате непонимания системности подхода к ЦЭ появляются заявления, что основным результатом выполнения программы ЦЭ должен явиться

рост числа подключений фермеров к интернету [4]. На основании такого подхода директор института аграрных проблем и информатики академик РАН Петриков А.В. даже принял решение о ненужности тематики исследований по ЦЭ АПК и закрыл ее в собственном институте. Более того, он пошел дальше и предлагает закрыть ИТ-кафедры в аграрных ВУЗах, обосновывая такое решение тем, что с цифровизацией АПК лучше справится рынок.

При отсутствии специалистов в сфере информационной безопасности в НИИ и ВУЗах указанные казусы будут только дискредитировать всю науку в глазах сообщества IT-специалистов и прочих пользователей, желающих получить надежную информацию из рук ученых.

Рассмотренные проблемы не могли не породить появление цифрового инструмента для решения их на базе одного из основополагающих принципов цифровой трансформации мирового общественного развития – создании системы управления информацией, основанной на интеграции разрозненных данных в единую систему. В качестве такого инструмента в [5, 6] предлагается создать цифровую платформу информационных научно-образовательных ресурсов (ЦПИНОР), способную выполнить триединую роль науки: поддержка научных исследований; повышение уровня образования, переподготовки для более широких слоев пользователей, а не только учащихся; возможность эффективного и быстрого трансфера знаний в экономику. При формировании ЦПИНОР можно нанять сильную команду IT-специалистов в области и информационной безопасности, поскольку расчеты показали, что при этом только на сопровождении сайтов экономия составит 1 млрд рублей.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №20-07-00836 «Научные основы формирования единой цифровой платформы (единого информационного интернет-пространства) аграрных научно-образовательных ресурсов на основе математического моделирования»

Литература:

1. *Пономарев К.С., Шутиков М.А., Феофанов А.Н.* Цифровой двойник как инструмент цифровой трансформации предприятия // Вестник МГТУ «Станкин». – 2019. – № 4(51). – С. 19-23.

2. *Сытов А.Н., Вахранев А.В., Ерешко Ф.И.* Исследование цифрового двойника предприятия / Труды четырнадцатой международной конференции «Управление развитием крупномасштабных систем MLSD'2021». – М.: ИПУ РАН, 2021. – С. 786-792.

3. *Боровков А.И., Рябов Ю.А., Кукушкин К.В., Марусева В.М., Кулемин В.Ю.* Цифровые двойники и цифровая трансформация предприятий ОПК // Оборонная техника. – 2018. – № 1. – С. 6-23.

4. *Петриков А.В.* Цифровизация АПК и совершенствование аграрной и сельской политики. – URL: http://www.viapi.ru/news/detail.php?ID=228044 (дата обращения 31.08.2022).

5. *Меденников В.И.* Математическая модель формирования цифровых платформ управления экономикой страны // Цифровая экономика. – 2019. – № 1. – С. 25-35.

6. *Зацаринный А.А.* Цифровая платформа для научных исследований / Материалы Международной научной конференции «Математическое моделирование и информационные технологии в инженерных и бизнес-приложениях». – Воронеж: Издательский дом ВГУ, 2018. – С. 104-113.

DOI: 10.25728/iccss.2022.71.94.007

Комков Н.И., Усманова Т.Х., Сутягин В.В.

Особенности развития российских нефтеперерабатывающих ТНК

Аннотация: Рассматривается роль и значение Транснациональных корпораций (ТНК) в развитии мировой экономики. Показано, что ТНК являются успешными, конкурентоспособными и инновационными компаниями. Отмечается ведущая роль ТНК в обеспечении прогресса в мировом развитии. Рассматриваются сопутствующие факторы и условия, содействующие прогрессивному

развитию. Также отмечаются недостатки и ограничения, сдерживающие возможности социально-экономического развития стран, на территории которых действуют ТНК.

Ключевые слова: глобализация, корпорация, синергия, управление, принятие решений, технология, инновации, импортозамещение

Известно, что компания – это «объединение юридических и физических лиц для проведения различных видов хозяйственной деятельности» [1]. Крупная компания – это совокупность организаций и физических лиц, успешно занимающихся хозяйственной деятельностью и имеющих высокий годовой доход (например, в США – не менее 1 млрд долл.). Транснациональная корпорация (ТНК) – это «общество с дочерними компаниями и филиалами в различных странах. Контрольный пакет акций находится у материнской компании, в свою очередь дочерние компании могут владеть контрольными пакетами акций других предприятий, организаций» [1]. Всего в мире насчитывается свыше 40 тыс. ТНК, среди которых ведущая роль принадлежит 100 корпорациям, а США принадлежит треть из них [2]. В России к 2000 году их число приблизилось к 90.

В чем причины влияния ТНК на государства, участвующих в них ТНК и достигших успехов в бизнесе, а также ограничения и недостатки в деятельности ТНК с позиций разных сторон: населения страны и государств, участвующих в ТНК?

Прежде всего – это устойчивость к мировым кризисным явлениям и надежность как финансового ответчика. Привлечение к участию в ТНК многих стран обеспечивает таким ТНК финансовую и организационно-правовую устойчивость в мировой экономической системе благодаря возможности быстрой адаптации и перемещению своих активов и коммерческих интересов в зависимости от изменения мировой конъюнктуры, включая изменение цен и спроса на продукцию ТНК на отдельных сегментах мировых рынков.

Постепенное срастание интересов, активов и потенциала финансовых кругов, банков, корпораций и правящих элит, сформировавшееся в прошлом веке, привело к переплетению множества частных и государственных интересов в сложный, взаимоподдерживающий друг друга симбиоз сторон, способных

влиять на государственное устройство в отдельных странах, включая выбор удобных для продвижения интересов ТНК государственных руководителей.

Уровень в большинстве ТНК достигнут благодаря высокой организации и методическому обеспечению процессов управления полным циклом принятия решений, начиная от прогнозов развития корпорации, формирования стратегий развития, дорожных карт, программ развития инвестиционных и инновационных проектов развития и модернизации, заканчивая операционным управлением текущими процессами и отчетами о достижении поставленных целей.

Известно, что компании могут быть успешными, конкурентоспособными, инновационными. Успешность определяется стоимостью располагаемых активов, конкурентоспособность предполагает преимущества (превосходство) поставляемой на рынок продукции, а инновационность – соответствует доле затрат на НИОКР и технологии. Подавляющее число корпораций образующих 100 лучших ТНК полностью удовлетворяют всем этим требованиям: их активы превышают 100 млрд долл., по конкурентоспособности их товаров они превосходят большинство соперничающих с ними компаний, а доля затрат на НИОКР составляет более 10 % в себестоимости продукции [3]. Многие крупные российские компании только частично соответствуют этим требованиям. Так, Компания «ОАО ГАЗПРОМ» в 2010 году заявляла себя как компания, которая имеет самую высокую рентабельность (28 %) среди мировых добывающих компаний, хотя уровень ее инновационности по затратам на НИОКР составлял всего 0,79 %. Одновременно ГАЗПРОМ позиционировал себя как высокотехнологичная компания, что не вполне соответствовало действительности. Неполный учет рисков при ориентации преимущественно на трубопроводный транспорт газа (Северный поток – 2) и отказе от технологии поставок сжиженного газа на спотовый рынок стран ЕС во многом повлияли на снижение экономических показателей ГАЗПРОМА в 2019-2022 годах.

Отличительной особенностью компаний является их стремление к развитию, реализуемое посредством слияния и поглощения производств конкурентов. При этом происходит укрупнение

компаний, наращивание капитализации их активов. В 2015 г. 500 крупнейших компаний мира дали 37,7 % мирового ВВП, а на 10 % компаний с годовым доходом более 1 млрд долл. приходится 80 % суммарной прибыли мировой экономики [3]. Увеличение активов компании позволяет тратить значительные финансовые средства на НИОКР и приобретение патентов в размере более 10 % себестоимости [3]. Наращивание капитала и активов компании является важной, что особенно проявилось в последнее время, стратегической целью компании. Многие руководители ТНК, понимая тенденцию увеличения тесной связанности современных производств, которые включают источники поставки сырья и комплектующие изделия, сосредотачивают свое внимание не столько на отдельных технологиях, сколько на возможности формирования целостных цепочек технологий, согласованно ориентированных как на рынок готовой продукции, так и на поставщиков сырья и комплектующих.

Важным достоинством организации работы ТНК, деятельность которых распределена между разными странами, расположенных на разных континентах, является высокая организация и скорость перемещения и обработки потоков информации. Для этого в рамках общей концепции цифровизации используются современные технологии передачи и обработки информации, включая высокоскоростной Интернет, Свифт, технологии Big Date, искусственный интеллект, высокоорганизованные банки технологий и др.

Важнейшим элементом управления деятельностью ТНК является управление проектами, а в качестве методической основы большинством компаний принимается Международные стандарты управления проектами [4], где определены основные практические процедуры управления проектами. Эти правила уточняются и дорабатываются с учетом направления деятельности и ориентации компании на определенные объекты. Так, компания Сахалин Энерджи, специализирующаяся на поставках сжиженного газа, вынуждена доработать механизмы принятия решений по управлению проектами [5], сочетающие проектирование, ввод в эксплуатацию новых месторождений газа и операционное управление процессами сбора, сжижения газа и заправкой газовозов [6]. Если конкурентоспособность добываемого газа

обеспечивается природным фактором, то действия газодобывающих компаний направлены на снижение себестоимости и обеспечения требуемого качества, включая очистку газа от примесей и контролирование его влажности.

Ключевым условием достижения конкурентоспособного превосходства своей продукции над продукцией конкурирующих корпораций является постоянное обновление используемых технологий на основе инновационных решений. Для этого ТНК ориентируются на прогнозы и тренды появления и освоения перспективных технологий, имеют свои информационные отделы, постоянно отслеживающие появление новых технологий, активно приобретают патенты, пользуются услугами ведущих прогнозных центров, экспертов и ученых. По числу регистрируемых патентов США превосходят остальные страны, но в последнее время существенно возросла патентная активность в Китае и Индии. К сожалению, в конкурентной борьбе многие ТНК нередко используют приемы нечестной конкуренции, запугивают и подкупают конкурентов. Для этого они содержат значительный штат консультантов и юристов.

Обозначенные ранее основные качественные характеристики ТНК (успешность, конкурентоспособность и инновационность) не всегда в полной мере отражаются в деятельности российских компаний. Также недостаточно полно учитывают возможные риски российские ТНК в своих стратегических планах, что влечет за собой экономические потери. Некоторые российские ТНК уклоняются от уплаты в полном объеме налогов в РФ, а также недостаточно поддерживают социальную сферу в регионах.

Российский нефтегазовый комплекс в настоящее время включает пять крупных компаний: ПАО «Газпром», ПАО «Роснефть», ПАО «Лукойл», ПАО «Новотек», ПАО «Сургутнефтегаз». Лидером среди них является «Газпром», который был образован на основе концерна «Газпром» в начале 90-х годов. Рассмотрим динамику за последние годы экономических показателей трех российских нефтегазовых ТНК. Географически предприятия ТНК расположены в 32 государствах, на них трудятся 69,9 миллионов человек [2]. Лучшая российская корпорация в рейтинге – это «Газпром». В таблице 1 представлены основные

показатели ПАО «Газпром» (по материалам официального сайта компании за последние три года).

Таблица 1 – Основные показатели ПАО «Газпром» за 2018-2020 годы (в млрд руб.)

№ п/п	Показатели	2020 год	2019	2018
1	2	3	4	5
1	Выручка	4061,4	4758,7	5179,5
2	Себестоимость продаж	2488,2	2657,7	2618,4
3	Приведенный EBITDA	1466,5	1859,7	2599,3
4	Валовая прибыль	1573,2	2101,1	2561,1
5	Коммерческие расходы	-1450,9	-1363,9	-1430,9
6	Управленческие расходы	111,3	108,1	106,1
7	Прибыль от продаж	11,0	629,1	1024,1
8	Доходы от участия в других организациях	311,9	316,3	367,0
9	Проценты к получению	43,2	61,3	61,2
10	Проценты к уплате	-115,3	-107,2	-100,8
11	Прочие доходы	1067,4	1060,1	1174,0
12	Прочие расходы	-2240,4	-1048,6	-1325,8
13	Прибыль до налогообложения	-922,1	910,9	1200,0
14	Налог на прибыль	227,5	-177,4	-149,9
15	Чистая прибыль	-706,9	651,1	934,4
16	налоги (кроме налога на прибыль)	1 235,8 млрд руб.	1409,2	1498,3
17	Всего налогов по итогам года	1463,3	1231,8	1348,4
17.1	Соотношение налогов к выручке стр. 1	36,0	25,9	26,0
18	Средняя численность персонала	477,6 тыс. чел		
19	Капитальные вложения	1494,2	1818,7	1795,9
20	Расходы на благотворительность	28,8	27,7	35,0
21	Прибыль, относящиеся акционерам ПАО «Газпром»	135,3	1202,9	1456,3

Продолжение таблицы 1

1	2	3	4	5
22	Результат от переоценки внеоборотных активов, не включаемых в чистую прибыль (убыток) периода	97,3	-	-
23	Налог на прибыль от прочих операций, результат которых не включаются в чистую прибыль, (убыток) периода	-170,4	-	-
24	Совокупный финансовый результат периода	-626,7	734,0	934,4

В 2020 г. налоги, начисленные Группой «Газпром» (кроме налога на прибыль), свидетельствуют об уменьшении налоговых платежей, что связано с уменьшением расходов по НДПИ, снижением контрактных цен на нефть и объемов добычи газа. Расходы от изменения курсовой разницы превысили расходы предыдущих лет почти в два раза. ТНК «Газпром» понесла существенные убытки. Подтверждаются недостатки менеджмента российского ТНК «Газпром» в условиях наднационального регулирования контрактными ценами и несовершенной бюджетно-налоговой и денежно-кредитной политики страны. Допущенные убытки во многом объясняются формальным подходом к риск-менеджменту и управлению ключевыми показателями эффективности персонала.

Аналогично «Газпрому» произошли изменения в компании «Лукойл». По итогам прошедшего года 2020 рейтинг ПАО «Лукойл» опустился с 42 на 55 место, объем выручки (по данным Fortune Global) снизился до 118,009 млрд долларов. «Лукойл» переместился с 5-й на 57-ю позицию. «Лукойл» является одной из публичных вертикально интегрированных нефтегазовых компаний в мире. На 1 января 2021 года доказанные запасы углеводородов Группы по стандартам Комиссии по ценным бумагам и биржам США составили 15,4 млрд барр.н.э. (нефть – 11,7 млрд барр., газ – 22,2 трлн куб. фут.). Запасы Группы являются преимущественно традиционными. Группа

осуществляет разведку и добычу нефти и газа в России и за рубежом. В России основными нефтедобывающими регионами являются Западная Сибирь, Тимано-Печора, Урал и Поволжье. Сегмент разведки и добычи за рубежом включает доли в СРП и в проектах в Казахстане. Азербайджане, Узбекистане, Румынии, Ираке, Египте, Гане, Норвегии, Камеруне, Нигерии, Мексике, Республике Конго и ОАЭ. Среднесуточная добыча углеводородов в 2020 г. составила 2,1 млн барр. н.э., при этом на жидкие углеводороды приходится около 78 % объема добычи».

ПАО «Лукойл», как крупная вертикально интегрированная группа, показывает ухудшение финансовых и операционных показателей из-за ограничений COVID-19.

В целом роль нефтегазового комплекса, как национального лидера в экономике России в последние годы снизилась. Этому содействует ряд как внешних, так и внутренних причин. К числу недостатков в деятельности российских нефтегазовых компаний относится:

– невысокий уровень менеджмента некоторых компаний как на тактическом, так и на стратегическом уровне;

– недостаточная поддержка государства в политике противодействия со стороны импортеров требованиям снижения контрактных цен при поставках газа, нефти и нефтепродуктов;

– в условиях санкций со стороны США и стран ЕС вполне закономерен вопрос об изменении состава учредителей, изменения дивидендной политики и распределения прибыли компаний, включая возможность национализации нефтегазовых компаний.

Литература:

1. Инновационная экономика. Энциклопедический словарь-справочник. – М.: Макс-Пресс, 2012. – 542 с.

2. ‘Superstars’: The dynamics of firms, sectors, and cities leading the global economy. – URL: https://www.mckinsey.com/featured-insights/innovation-and-growth/superstars-the-dynamics-of-firms-sectors-and-cities-leading-the-global-economy (дата обращения 15.10.2022).

3. *Пороховский А.А.* Роль и судьба корпораций. – М.: Культурная революция, 2017. – С. 157-180.

4. PMI, 2005. Practice Standard for Earned Value Management. – URL: https://www.pmi.org/ (дата обращения 15.10.2022).

5. *Дашков Р.Ю.* Приоретизация и ранжирование фаз в управлении проектами строительства производственной жизни завода. Сжижаемость природного газа // МИР (модернизация, инновации, развитие). – 2017. – Т.8. №1. – С. 88-95.

6. *Дашков Р.Ю., Комков Н.И.* Интегрированный подход к управлению крупномасштабными проектами в компании «Сахалин Энерджи» // Проблемы прогнозирования. – 2022. – № 1 (190). – С. 101-113.

7. *Usmanova T.Kh.* Projects of development of interaction of fec and hcs: problems of forecasting and management // Studies on Russian Economic Development. – 2018. – Vol. 29. № 3. – P. 274-279.

DOI: 10.25728/iccss.2022.38.67.008

Рожнов А.В.

Некоторые особенности репрезентации и правдоподобного отрицания США деятельности в космосе при интерпретации китайского и российского восприятия

Аннотация: Предложены к критическому обсуждению интересные, отчасти, аспекты «наивной» интерпретации китайского и российского восприятия и реакции на милитаристскую деятельность США в космосе по мнению коллектива авторов в рамках Программы международной политики, безопасности и обороны Исследовательского отдела национальной безопасности РЭНД (NSRD), 2022 г.

Ключевые слова: сценарный подход, информационно-аналитическое моделирование, космическая деятельность, репрезентация, правдоподобное отрицание

Сценарный подход в общих чертах, как он может пониматься подавляющей численностью подлинных специалистов с различной степенью вовлечённости в различного рода изучаемые процессы международных отношений, в наше время, по сути, осваивает новые горизонты применимости в практике стараниями прогрессивных

исследователей при его сочетании с новыми средствами, методами, методиками и т.д. *информационно-аналитического моделирования*.

В целях *повышения эффективности* мер комплексного научно-технического и экономического обоснования при формулировании новых постановок нетривиальных задач обеспечения надёжности средств управления, вычислений и связи аэрокосмической отрасли представляется необходимым учитывать преобладающие тенденции, которые отражаемы в публичных информационных ресурсах при очевидно большой зашумлённости с *правдоподобным отрицанием*.

В ходе этой работы заявлено целеполагание *репрезентации* сведений об интерпретируемых реакциях Китая и России на происходящие события при изучении некоторых представлений о военной деятельности США в космосе – коллективом авторов (*Алексис А. Бланк, Натан Бошам-Мустафага, Кристина Холинска, М. Скотт Бонд, Стивен Дж. Фланаган*) [1].

Так, в интересах совершенствования форм подготовки кадров наукоёмких специальностей аэрокосмической отрасли приводятся следующие условные вопросы исследования «*за противника*» [1, 2]:

Как со временем менялись представления Китая и России о намерениях военной деятельности Соединённых Штатов в космосе?

Какие ответы могут принимать КНР и Российская Федерация в ответ на агрессивные действия США или противодействие им?

Рассмотрим исходные положения в соответствии с отчётом [1]:

Военная деятельность и внешняя политика США в отношении космической сферы претерпели значительные изменения с 1980-х годов, а недавние события включают восстановление Космического командования США, создание Космических сил США в 2019 году, – с нарастающим оспариванием «интересов» в космической среде. Но в открытых источниках недостаточно явно освещалось китайское и российское восприятие этих событий [с проамериканских позиций]. И, для того, чтобы отчасти восполнить этот пробел, исследователи РЭНД предпринимают ряд усилий по отслеживанию различных китайских и российских источников, такие как правительственные публикации, военные журналы, академические отчёты и местные СМИ, чтобы получить более полное представление о внутреннем восприятии в Китае и в России околовоенной деятельности США, взаимоувязанной с космической / противокосмической доктринами.

При ограничении выносимого на публичное обсуждение ряда вопросов исследователи сфокусировали свои усилия в контексте репрезентативной выборки по действиям США в космической сфере: Стратегическая оборонная инициатива (1983), выход США из Договора по противоракетной обороне (2002), Операция «Бурнт Фрост» (2008), космическая политика президентов США и другие. Рассматривая каждый первоисточник для обсуждения этих событий, они предприняли попытку оценить, как развивалась с течением времени китайская и российская реакция на военную деятельность США, так или иначе в итоге связанную с космическими интересами.

Основные результаты по мнению зарубежных исследователей:

Первоисточники отражают устойчивое восприятие в КНР и в РФ того, что военная деятельность США, связанная с космосом, носит угрожающий характер и демонстрирует враждебные намерения [1].

Это восприятие частично охватывает космическую угрозу их соответствующим ядерным средствам сдерживания и опасения, соотносимые с рядом противокосмических возможностей США и способностью американских спутников скрытно приближаться к космическим объектам для их инспекции и/или сбора информации.

Состояние двусторонних отношений в конкретный момент, по-видимому, во многом формирует взгляд каждого правительства на космическую деятельность США. Тем не менее, обе страны склонны к большей «предвзятости» подтверждения, в результате чего более правдоподобные ‘агрессивные’ [прим., кавычки в исходном отчёте] действия США, как правило [1], усиливают восприятие того, что американские военные имеют враждебные намерения в космической области, тогда как «более правдоподобные» совместные инициативы США не принимаются во внимание как неискренние [см. оригинал].

Китай и Россия обычно стараются найти риторический баланс, характеризуя действия США как угрожающие, а свои собственные аналогичные действия как не угрожающие. Вашингтон, Пекин и Москва, как будто, попали в цикл «действия—реакции», который «увековечивает» аргументацию для продолжения военных действий в космосе на основе предыдущей деятельности «антагонистов» [1].

Как китайские, так и российские официальные лица утверждают, что Соединённые Штаты проложили путь к милитаризации космоса, особенно с 2001 года, что не оставило им иного выбора, кроме как принять ответные меры. Примечательно, что (по мнению авторов [1])

обе страны указывают на решение США выйти из Договора по ПРО как на ключевой и переломный момент в устремлениях США по размещению оружия в космосе, и это один из ключевых случаев, когда причинно-следственная связь устанавливается более чем явно и отчётливо между действиями США и противодействием России.

В то же время, следует отметить, что рассмотренные аргументы могут позволить сформировать предпосылки для встречного поиска компромиссов и неизбежной в будущем разрядки этих отношений.

Таким образом, дальнейшее обсуждение может быть в принципе сориентировано также при детальном рассмотрении совокупности математических моделей, методов и алгоритмов, обеспечивающих надёжность, высокую производительность информационных систем, безопасность функционирования авиационных и космических систем, а также управление ими в условиях неопределённости [2-7].

В частности, достойными внимания представляются следующие частные вопросы при уточнении их в рамках сценарного подхода [8]:

анализ надёжности, живучести, эффективности и безопасности систем сложной структуры, включая разработку методик расчёта безотказности систем на современной микроэлектронной базе;

создание взаимоувязанных моделей, методов, алгоритмического обеспечения автоматизированного анализа безопасности и надёжности информационных, авиационных и космических систем.

Комплексная работа выполняется в интересах создания научно-технического задела по новой теме «Теория надёжности и техническая диагностика в средствах управления, вычислений и связи».

Междисциплинарные исследования выполнены при частичной поддержке РФФИ, проект 20-010-00493 «Разработка методологии страт. планирования НТ-развития в условиях цифровой экономики».

Литература:

1. *Alexis A. Blanc, Nathan Beauchamp-Mustafaga, Khrystyna Holynska, M. Scott Bond, Stephen J. Flanagan.* Chinese and Russian Perceptions of and Responses to U.S. Military Activities in the Space Domain / RAND. – RR-A1835-1. – 2022.

2. *Гончаренко В.И., Рожнов А.В., Карпов В.В., Лобанов И.А.* Исследование проблемных вопросов развития автономных гетерогенных РТК и подготовки кадров наукоёмких специальностей

аэрокосмической отрасли // Труды ФГУП «НПЦАП». Системы и приборы управления. – 2018. – № 1 (43). – С. 70-76.

3. *Лычев А.В., Рожнов А.В.* Управление разработками и оценка эффективности производства изделий аэрокосмической отрасли на основе модели Free Disposal Hull / Решетневские чтения: материалы XXI Междунар. науч.-практ. конф., посвящ. памяти генерального конструктора ракетно-космических систем академика М. Ф. Решетнева (08-11 нояб. 2017, г. Красноярск): в 2 ч. / Под общ. ред. Ю. Ю. Логинова. – Красноярск: СибГУ им. М.Ф. Решетнева, 2017. – Ч. 2. – С. 447-449.

4. *Лобанов И.А., Гудов Г.Н., Рожнов А.В.* Диверсификация технологии моделирования и управления в задачах мониторинга на ретроспективном примере завершения эксплуатации авиакосмической системы / Материалы 12-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2019). – М.: ИПУ РАН, 2019. – С. 1043-1046.

5. *Рожнов А.В.* О становлении проблематики самообороны в космосе при отборе ситуационных сценариев в условиях их существенной целевой рассогласованности / Материалы 27-й Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2019. – С. 228-231.

6. *Рожнов А.В.* Оценивание критичности условий возникновения существенной целевой рассогласованности ситуаций в космическом пространстве, приводящих к гипотетическому провоцированию конфликтов / Материалы 27-й Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2019. – С. 310-315.

7. *Рожнов А.В*. Комплексные исследования интеграционных компонентов авиакосмических технологий в условиях ограничений техногенного засорения / Труды 14-й Мультиконференции по проблемам управления (МКПУ-2021): локальной научно-технической конференции «Управление в аэрокосмических системах» (УАКС-2021). – Ростов-на-Дону; Таганрог: ЮФУ, 2021. – Т. 3. – С. 99-101.

8. *Коржевский А.С., Гончаренко В.И., Рожнов А.В., Колин К.К., Копылов И.А.* и др. Прогнозируемые вызовы и угрозы национальной безопасности Российской Федерации и направления их

нейтрализации / под общей ред. А.С. Коржевского. Изд. ВА ГШ ВС РФ: ВИ (управления национальной обороной). – М.: РГГУ, 2021. – 562 с.

DOI: 10.25728/iccss.2022.39.25.009

Кононов Д.А., Тимошенко А.А., Богатырева Л.В.

Проблема неопределенности при исследовании правоохранительной системы

Аннотация. Рассмотрены основные проблемы описания неопределенности правоохранительной системы и направления исследований. Формализовано понятие неопределённости, в основание которого положены базовые положения информационной логики. Предложены цели и методология исследования. Рассмотрены источники неопределенности правоохранительной системы при разработке и практике применения законодательных и подзаконных актов, которые определяют содержание правовых отношений.

Ключевые слова: правоохранительная система РФ, направления исследования, безопасность, неопределенность, методология исследований, сценарный анализ

Введение

В предлагаемой работе рассмотрена проблематика анализа и учета неопределённости функционирования и развития правоохранительной системы РФ в условиях применения современных социальных технологий, обеспечивающих государственную безопасность. Основными направлениями исследований правоохранительной системы являются:

– разработка системы взаимосвязанных современных цифровых моделей функционирования правоохранительной системы как формальной системы с выделением наиболее важных функциональных подсистем;

– определение взаимосвязей подсистем типа «вход»–«выход», в том числе:

1) информационных взаимосвязей,

2) возможных конфигураций организационных взаимодействий,

3) возможных конфигураций управленческих связей с выделением иерархических зависимостей группового, совместного и распределенного управления;

– построение информационных моделей подсистем;

– построение общей информационно-логической модели правовой системы;

– определение системных параметров правоохранительной системы;

– выявление типов неопределенности в указанных направлениях информационных, организационных и управленческих связей;

– выявление окон и мест уязвимости в указанных направлениях информационных, организационных и управленческих связей;

– выявление существующих и потенциальных для нее рисков;

– определение требований к элементам, структуре и системным параметрам правоохранительной системы;

– разработка рекомендаций по выработке управленческих решений для оптимизации системы юстиции, трансформации законодательства и процесса его применения.

Основные цели проводимых исследований – создание инструментальных средств изучения и устранения различных типов неопределенности.

Представляется целесообразным методологию исследования составить из следующих аспектов:

– описание динамической модели объекта исследования – системы юстиции, трансформации законодательства и процесса его применения;

– информационно-логические основания правового управления, в том числе понятие неопределенности;

– описание моделей и методов сценарного исследования правового управления;

– построение сценариев управления правоохранительной системы и анализ их характеристик, в том числе характеристик неопределенности;

– методы уменьшения неопределенности.

1. Информационно-логические основания правового управления

Все общественные процессы для каждого социального объекта, прежде чем быть осуществленными, принимают информационную форму. Как научная категория «информация» составляет предмет изучения для самых различных дисциплин: информатики, кибернетики, философии, физики, метеорологии, биологии, теории связи и т.д. Несмотря на это, строгого научного определения, что же такое информация, до настоящего времени не существует, а вместо него обычно используют понятие об информации. Понятия отличаются от определений тем, что разные дисциплины в разных областях науки и техники вкладывают в него разный смысл, с тем, чтобы оно в наибольшей степени соответствовало предмету и задачам конкретной дисциплины. Имеется множество определений понятия информации от наиболее общего философского (информация есть отражение реального мира) до наиболее частного прикладного (информация есть сведения, являющиеся объектом переработки).

Большинство определений информации страдает существенным недостатком: смешиваются понятия «данные» и «информация». В работе [1] эти категории информационной логики разделены: первичным является понятие «данные», которые сводятся в определенные совокупности (наборы). «Информация» представляет ОТНОШЕНИЕ на этих наборах, создание которых существенно зависит от ОБСТОЯТЕЛЬСТВ применения (использования) «данных». Так, в трактовке Н. Винера под информацией понимают не просто сведения, а только те сведения, которые являются новыми и полезными для принятия решения, обеспечивающего достижение цели управления. Однако в данном им определении не отражено, содержанием чего является информация, каковы ее природа и материальная основа возникновения. Н. Винер дал обширную логико-функциональную трактовку регулирования (управления), назвав его кибернетикой. Базой послужила классическая теория

регулирования с обратной связью, основы которой были заложены трудами Платона, Ампера, Вышнеградского, Ляпунова и других ученых. Вместе с тем Н. Винер не дал систематического изложения идей кибернетики [2, 3]. Академику А.И. Бергу принадлежит известное определение кибернетики как науки об оптимальном управлении любыми сложными динамическими системами, основанной на теоретическом фундаменте логики и математики и применении средств автоматизации, информационно-логических машин.

Важно различать информацию как термин обыденной жизни и как правовую категорию. Так, например, в обыденной жизни информация – это просто сообщение о чем-либо, в научной сфере – это отношения между данными, которые являются объектом изучения и применения. Анализируя же информацию как предмет правоотношений, нельзя говорить о ней вообще, неконкретно. Информация и связанные с ней отношения не могут выступать в качестве объекта правового регулирования, если информация не выражена в любой объективной форме. И только по отношению к определенной форме выражения информации может быть установлен соответствующий правовой режим. Предметом рассмотрения должна быть в первую очередь информация, которая находится в гражданском, административном или ином общественном обороте и, по поводу которой или в связи с которой поэтому и возникают общественные отношения, подлежащие регулированию правом [4].

Переход от реальных объектов Природы к научно-значимым понятиям осуществляют на базе методологических положений философской теории «отражения». Сознание и объективный мир суть философские противоположности, образующие единство в рамках Общества. Основой этого единства является практика, активная чувственно-предметная деятельность людей, выражающаяся в конкретных действиях и поступках. Именно она и порождает необходимость отражения действительности в сознании людей.

В соответствии с определениями в [1] на основе наборов данных $B(O^{(NAT)},I)$ об объекте Природы $O^{(NAT)}$ полученных в определенных обстоятельствах I, посредством способов $\mathbf{Mn}(O^{(NAT)}, I))$ формируются информационные совокупности $Inf(O^{(NAT)}, \mathbf{Mn}(O^{(NAT)}, I))$.

Информационная совокупность объединяет в единый объект искусственной Природы наименование объекта Природы $O^{(NAT)}$, его образ $B(O^{(NAT)},I)$ и обстоятельства I, в которых этот образ был получен. Данные $B(O^{(NAT)},I)$, а также способы их получения **Mn**, являясь объектом искусственной Природы, в нашем формализме получают относительную независимость от прообразов, которые они отображают, т.е. могут в дальнейшем рассматриваться в качестве самостоятельных элементов искусственной Природы. Это обстоятельство может служить источником использования их для отображения других объектов Природы: одна и та же математическая модель используется для описания экономических, социальных, биологических и других процессов. В то же время информация существенно связана отношением с исходным объектом Природы и условиями получения образа. Таким образом, информационную совокупность $Inf(O^{(NAT)}, \mathbf{Mn}(O^{(NAT)}, I))$ можно классифицировать по

– объектам Природы $O^{(NAT)}$;

– обстоятельствам получения данных I;

– способам формирования информационной совокупности $\mathbf{Mn}(O^{(NAT)}, I)$.

2. Свойства информационной совокупности

Информация обладает некоторыми общими для всех ее видов свойствами. Основным свойством информации следует считать ее неразрывную связь с определенной самоорганизующейся системой. Другими важными свойствами являются структурированность и ценность. Структурированность информации – это свойство, которое позволяет рецептивной системе выделять информацию из физических процессов или объектов, воспринимать некоторые явления внешнего мира как *сигналы*. В соответствии с этим свойством в любом сигнале выделяются его структурные, идентифицирующие и информативные параметры. Структурирование информации происходит параллельно с формированием модели внешнего мира. Для самоорганизующейся системы характерно движение – стремление к цели. Все, что обеспечивает это движение, является ценным для системы. Отсюда следует, что ценными являются и вещество, и энергия, и информация. Если изолировать в информационном смысле

самоорганизующуюся систему, она прекратит свое целенаправленное движение, а возможно, и существование. Ценность информации выражается в таких понятиях, как содержательность, своевременность, полнота, достоверность, оперативность.

Наиболее распространено использование свойств (рисунок 1).

Рисунок 1 – Наиболее распространенные свойства информации

3. Неопределенность как свойство информационной совокупности

В математике и кибернетике информация является мерой устранения (снижения) неопределенности (энтропии), мерой организованности системы. Соотношение между понятиями «энтропия» и «информация» в известном смысле напоминает соотношение между физическими понятиями потенциала и разности потенциалов. Энтропия – это количественная мера неопределенности. Уничтоженная сведениями энтропия и есть информация. В этом смысле информация выступает как мера отношения, взаимосвязи между системами, явлениями, процессами, а не как показатель состояния систем. Конструктивный потенциал информации в теории информации нашел выражение в понятии «негэнтропия», которая определяется как мера порядка, упорядоченности, внутренней структуры, связанной информации.

Ключевым понятием методологии сценарного подхода к исследованию социально-экономических систем является понятие ***неопределенности***. «Неопределенность есть особая форма знания, характеризующаяся незавершенностью и неоднозначностью» [5].

Определенность – свойство отношений между элементами информационной совокупности, заключающееся в однозначном, «единообразном» отображении отношений между объектами Природы и объектами искусственной Природы при «единообразных» обстоятельствах. Неопределенность – отсутствие определенности.

Построим систему определений понятия «неопределенность» на следующих позициях.

От критерия адекватности данных $\mathbf{Cr}^{(ad)}$ требуют, чтобы соответствующее отношение обладало свойствами рефлексивности и симметричности. В то же время оно может не быть отношением эквивалентности, если не обладает свойством транзитивности. Последнее означает, что в одних и тех же обстоятельствах I получены несовпадающие адекватные отображения $B_1(O^{(NAT)},I)$ и $B_2(O^{(NAT)},I)$ объекта Природы $O^{(NAT)}$. Это, как правило, означает, что I недостаточно четко определены, в частности могут быть получены из различных источников без учета этого факта, и их следует уточнить. Критерий адекватности $\mathbf{Cr}^{(ad)}$ будем называть ***регулярным***, если для него выполнено условие: *существует не более одного элемента Природы* $B(O^{(NAT)},I)$*, адекватно отображающего объект Природы* $O^{(NAT)}$ *в условиях* I.

Пусть задана совокупность способов описания объекта Природы $O^{(NAT)}$, а также множество критериев адекватности.

Скажем, что *имеет место неопределенность данных*, если совокупность $SD(O^{(NAT)},\mathbf{Cr}^{(ad)})=\{B_\alpha(O^{(NAT)},I)\ \alpha\in A\}$ содержит более одного элемента. Это означает, что критерий адекватности и совокупность способов описания данных об объекте Природы $O^{(NAT)}$ выделяют несколько образов, отображающих его адекватно по критерию $\mathbf{Cr}^{(ad)}$. При этом заданная мера, определенная на множестве $SD(O^{(NAT)},\mathbf{Cr}^{(ad)})$, представляет собой *меру неопределенности*.

4. Источники неопределенности правоохранительной системы

Оставаясь в рамках слишком обобщенного определения неопределенности, следует осуществить переход к анализу конкретных предметных областей. С формализованной точки зрения правовое управление представляет собой процесс разработки и

практики применения совокупности законодательных и подзаконных актов, которые определяют содержание правоохранительных отношений.

Общая схема источников неопределенности заключается в структуре правовых отношений и реализации их институционных структур, определяющих системные параметры правоохранительной системы. Наиболее выпукло это видно в содержании и структуре информационного обеспечения правового управления (рисунок 2).

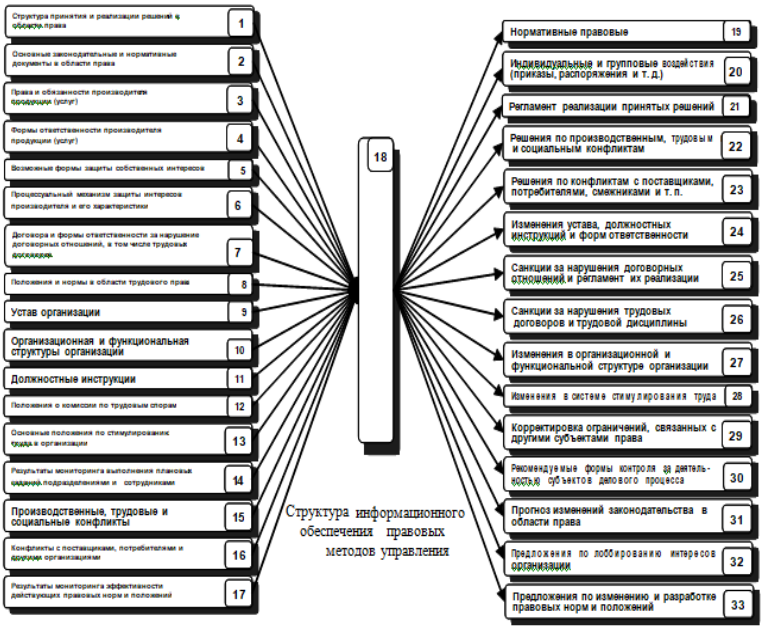


Рисунок 2 – Содержание и структура
информационного обеспечения правового управления

Заключение

При проведении исследования безопасности систем управления может использоваться широкий арсенал разнообразных методов. Они могут быть подразделены на логические (описательные), теоретическо-аналитические, эмпирические.

Перспективным методом исследования правоохранительной системы является анализ их системных параметров с последующим

сценарным анализом, применения разработанных правовых актов [6, 7].

Литература:

1. Информационное обеспечение систем организационного управления (теоретические основы). В 3-х частях. Ч. 1. Методологические основы организационного управления. / Под ред. Е.А. Микрина и В.В. Кульбы. – М.: Физматлит, 2011. – 464 с.
2. *Винер Н.* Кибернетика и общество. – М.: «Иностранная литература», 1958. – 200 с.
3. *Винер Н.* Кибернетика или Управление и связь в животном и машине. 2-е изд. – М.: Советское радио, 1968. – 201 с.
4. *Копылов В.А.* Информация как объект правового регулирования // НТИ. – Сер.1. – 1996. – № 8.
5. *Соколова О.И.* Понятие неопределенности в неклассической науке и философии: автореферат диссертации на соискание ученой степени кандидата философских наук. – Нижний Новгород, 2020. – 26 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.* Аудит информационной безопасности автоматизированных систем управления // Тренды и управление. – 2014. – № 4. – С. 319-334.

DOI: 10.25728/iccss.2022.93.75.010

Еременко В.А., Манаенкова Н.И.

К вопросу безопасности радиозондирования ионосферы мощными волновыми пучками

Аннотация: Рассмотрена задача нелинейного взаимодействия волна – ионосфера в условиях пороговой нелинейности. Приведено обоснование существования сосредоточенных волновых полей в этих условиях. Показано, что при определенном соотношении параметров возможно значительное увеличение интенсивности радиоизлучения.

Ключевые слова: распространение радиоволн; нелинейные волны; взаимодействие солитонов; пороговая нелинейность

Введение

Необходимость мониторинга ионосферной плазмы для нужд радиосвязи, радиолокации, навигации и прочих целей определяет развитие методов диагностики ионосферы, в том числе радиотехническими средствами. В современном мире процедура радиозондирования ионосферы является достаточно рутинной. При этом мощность радиоизлучения постоянно растет, что позволяет совершенствовать средства диагностики и расширяет диапазон наблюдаемых параметров. Однако увеличение мощности радиоизлучения может приводить как к положительным, так и отрицательным последствиям. Ионосферная плазма является достаточно разреженной средой. Длина свободного пробега электронов в этой среде относительно большая. В условиях электромагнитного поля электрон успевает получить значительную энергию за время одного пробега. Вследствие этого, диэлектрическая проницаемость окружающей среды становится зависимой от интенсивности волнового поля. Возникающие таким образом нелинейные возмущения ионосферной плазмы приводят к эффектам самофокусировки волнового поля. Теоретические исследования эффектов разогрева ионосферной плазмы мощным радиоизлучением начались довольно давно [1]. Экспериментальное подтверждение взаимодействия мощного радиоизлучения с ионосферной плазмой при наклонном распространении дало дополнительный импульс исследованиям по этой тематике [2, 3]. Обычно для описания нелинейных волн используется так называемая Керровская модель нелинейности, – в которой нелинейное возмущение диэлектрической проницаемости пропорционально квадрату модуля амплитуды волны. В рамках этой модели показано существование сосредоточенных волновых полей – солитонов, являющихся очень удобным инструментом зондирования окружающей среды. Но достаточно очевидны и определенные ограничения модели. В реальности нелинейные эффекты не могут возникнуть при малой мощности излучения. Только когда амплитуда волны превысит некоторое пороговое значение, происходит «пробой» среды и возникает зависимость возмущения диэлектрической проницаемости от амплитуды волнового поля.

1. Постановка задачи

Рассмотрим типичную картину распространения радиоволн в ближайшем околоземном пространстве. В области фокусировки лучей интенсивность сигнала заметно увеличивается, следовательно, возможно нелинейное взаимодействие радиоволны с ионосферой [3].

Для описания волнового поля в этой малой области, воспользуемся уравнением Гельмгольца для амплитуды волнового поля

$$\Delta u + k^2 \cdot \varepsilon \cdot u = 0, \tag{1}$$

где k – волновое число и ε – диэлектрическая проницаемость.

При высокой интенсивности излученного сигнала диэлектрическая проницаемость становится зависимой от амплитуды 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 [4].

$\frac{d^2 v}{d\eta^2} = q^2 v - (1 + \varepsilon_n(v^2))v$, где $q = \frac{d\psi}{d\xi}$ – безразмерное волновое число, $\varepsilon = 1 + \varepsilon_n(v^2)$. Первый интеграл этого уравнения имеет вид: $F(v^2) = \int_0^{v^2} \varepsilon_n(t)dt$, $\lambda^2 = q^2 - 1$. Это уравнение при $E = 0$ предполагает существование сосредоточенных волн, при

условии, что уравнение $F(t) - \lambda^2 t = 0$ имеет корни $t = 0$ и $t = t_0 > 0$ [4].

2. Пороговая нелинейность

Рассмотрим далее модель распространения волны в условиях пороговой нелинейности, считая, что нелинейные эффекты возникает только для волн, интенсивность которых превышает некоторое пороговое значение [5]. Нелинейное возмущение диэлектрической проницаемости в этом случае может быть представлено формулой

$$\varepsilon_n(v^2) = \alpha v^2 \cdot \theta\left(v^2 - A^2\right), \qquad (2)$$

где A - пороговое значение, $\theta(x)$ - функция Хэвисайда, $\theta(x) = \begin{cases} 1 & при\ x \geq 0 \\ 0 & при\ x < 0 \end{cases}$.

В этом случае функция $F(v^2)$ имеет вид

$$F(v^2) = \int_0^{v^2} \varepsilon_n(t)dt \quad = \frac{\alpha}{2}(v^4 - A^4) \cdot \theta\left(v^2 - A^2\right) \qquad (3)$$

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 - солитона. Эти локализованные волновые поля в среде с пороговой нелинейностью очень похожи на обычные керровские солитоны, но пучок – более узкий в центре и имеет «длинные хвосты». Но есть одна принципиальная особенность – зависимость эффективной ширины волнового пучка от его амплитуды. Как известно эффективная ширина «стандартного» (керровского) солитона обратно пропорциональна его амплитуде [5]. Для «порогового» солитона

(сосредоточенного волнового пучка в условиях пороговой нелинейности) ситуация принципиально другая. Зависимость эффективной ширины солитона от относительной амплитуды v / A приведена на рисунке 1. Видно, что при превышении величины v / A некоторого критического значения (порядка 5/3) характер зависимости заметно меняется.

Взаимодействие волновых пучков в средах с пороговой нелинейностью может значительно отличаться от взаимодействия стандартных солитонов в среде с керровской нелинейностью. Если «стандартные» солитоны расходятся после взаимодействия без изменения амплитуды [5], то «пороговые» солитоны, при соотношении v / A порядка 5/3, могут «слипаться» в единый конгломерат повышенной интенсивности [6]. То есть, распространение мощного радиоизлучения в ионосфере в условиях пороговой нелинейности может сопровождаться заметным увеличением амплитуды электромагнитного излучения.

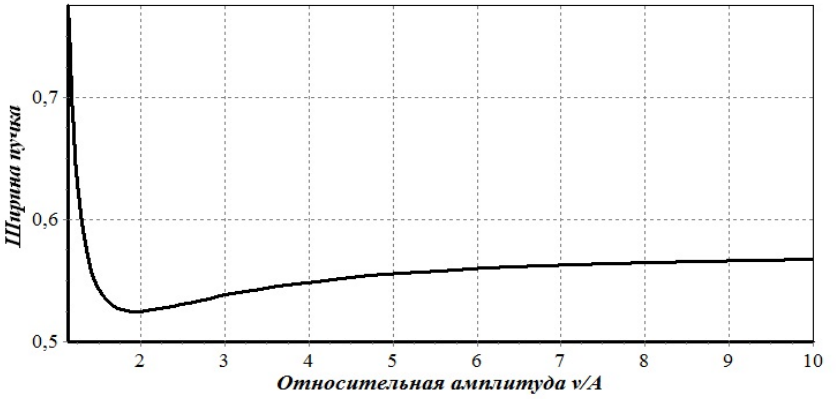


Рисунок 1 – Зависимость ширины пучка от отношения его амплитуды к величине порога нелинейности

2. Выводы

Легко видеть, что, для случая пороговой нелинейности существуют уединенные волны, – сосредоточенные решения

соответствующих волновых уравнений. Если не представляется возможным выписать аналитические выражения для этих решений, они могут быть построены путем компьютерного моделирования. Хотя эти волны подобны керровским солитонам, их взаимодействие, при определенном соотношении параметров, может принципиально отличаться от стандартного взаимодействия солитонов. Таким образом, модель пороговой нелинейности позволяет выявить в среде распространения сигнала настолько заметные изменения, которые могут оказаться опасными для широкого круга радиотехнических систем.

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. *Bochkarev G.S., Eremenko V.A., Lobachevcky L.A., Ljannoy B.E., Migulin V.V., Cherkashin Yu.N.* Non-linear interaction of decameter radio waves at close frequencies on oblique propagation // Journal of Atmospheric and Terrestrial Physics. – 1982. – V.44. № 12. – P.1137-1141.

3. *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.

4. *Еременко В.А., Манаенкова Н.И.* Влияние типа нелинейности на существование сосредоточенных волн // Успехи современной радиоэлектроники. – 2017. – №6. – С. 49-54.

5. *Ньюэлл А.* Солитоны в математике и физике. – Москва: Мир, 1989. – 323 с.

6. *Еременко В.А., Манаенкова Н.И.* О взаимодействии солитонов в средах с насыщающейся и пороговой нелинейностью / Распространение радиоволн: труды XXVI Всероссийской открытой научной конференции. В 2-х томах. Т. 2. – Казань: Изд-во Казан. ун-та, 2019. – С. 505-508.

DOI: 10.25728/iccss.2022.14.61.011

Прус М.Ю., Жубанов М.С., Лобанов И.А., Прус Ю.В.

Об объективизации экспертных оценок вероятностей редких событий

Аннотация: Обсуждается проблема объективизации экспертных оценок и предлагается способ измерения вероятностей редких событий, основанный на гипотезе о функциональной связи между результатами субъективной оценки и объективного измерения вероятностей, описываемой в соответствии с психофизическим законом Стивенса.

Ключевые слова: экспертные оценки, психофизический закон, теория измерений

Количественная оценка вероятностей редких событий и явлений предполагает, как правило, анализ достаточно большого объема статистических данных, однако достаточно часто имеющиеся выборочные совокупности данных не являются репрезентативными, либо не соответствуют требованиям, предъявляемым к организации систематического статистического учета. Следует также отметить, что в настоящее время какое-либо научное обоснование применения экспертных методов оценок вероятностей отсутствует. Поэтому обоснование экспертных методов оценки вероятностных параметров различных событий является одной из актуальных проблем в области анализа рисков и безопасности в ЧС [1].

Осознание значимости роли познающего субъекта, участвующего в процессе инструментального измерения физических величин привело к формированию понятия «эффект наблюдателя», которое имеет различную интерпретацию в различных областях физики – квантовой механике, общей и специальной теории относительности, космологии и пр. [2, 3].

Характерной особенностью экспертных методов является частичное либо полное слияние познающего субъекта и средства измерения. Исходя из общих положений теории измерений, необходимо построение общей модели экспертных методов, в качестве основных элементов которой рассматривается

совокупность: $S \leftrightarrows I \leftrightarrows O$, включающая познающего субъекта – «наблюдателя», средства измерения – «прибор» и объект с «измеряемыми свойствами». Построение подобных моделей и научное обоснование экспертных методов, по мнению авторов настоящей работы, может привести к формированию междисциплинарного научного направления, затрагивающего ряд значимых вопросов, относящихся к теории познания, нейрофизиологии, когнитивной психологии, когнитивной лингвистики, невербальной коммуникации и искусственного интеллекта.

С точки зрения математического обоснования, применение экспертных методов с процедурой перевода вербальных оценок в численные значения, как правило приводит к ошибочной интерпретации результатов [4], непосредственно представленных в ранговой шкале экспертных оценок, но фактически используемых как результаты шкалы отношений.

Разрешение указанного математического противоречия в проблеме количественной оценки вероятностей редких событий на основе экспертных методов возможно при условии введения в общую модель ряда принципиальных соображений, позволяющих установить правила однозначного перевода вербальных оценок в численные значения. Наиболее обоснованным и перспективным направлением при моделировании экспертных процедур представляется применение достижений сенсорной психофизики [5]. Психофизические или сенсометрические методы (вынужденного выбора, минимальных изменений, постоянных раздражителей, оценки, средней ошибки, центральной точки и др.) используются при построении субъективных шкал и измерении чувствительности сенсорных систем. Например, в [6] анализируется функциональная связь между объективной и субъективной вероятностями на основании эмпирических психофизических законов Фехнера и Стивенса.

Для построения модели экспертного метода измерения вероятностей редких событий, основанного на гипотезе о функциональной связи между результатами субъективной оценки и объективного измерения вероятностей, введем пространство элементарных событий, обусловленных конечным набором возможных исходов

$$\Omega = \{a_1, \ldots . . a_N\} . \quad (1)$$

Для каждого элементарного события определим объективные и субъективные вероятности

$$a_i \to p_i , \quad a_i \to q_i , \quad i\epsilon\{1, \ldots . N\}. \quad (2)$$

Законы Фехнера и Стивенса, как показано в [8], эквивалентны, но для дальнейшего решения вычислительных задач следует сделать выбор в пользу описания функциональной связи между результатами субъективной оценки и объективного измерения вероятностей в соответствии с законом Стивенса. Тогда отношение объективных вероятностей определяется (в соответствии с законом Стивенса) степенной функцией отношения субъективных вероятностей

$$\frac{p_l}{p_m} = \left(\frac{q_l}{q_m}\right)^W , \quad (3)$$

где W – некоторый параметр, значение которого при оценке редких событий существенно превышает единичное (> 1).

В современных экспертных методах для повышения точности вербальных оценок как правило применяются процедуры парных сравнений альтернатив. Метод парных сравнений основан на выводах психофизических исследований и исходит из предположения о том, что эксперты очень часто ориентируются в ситуации значительно лучше, чем они сами себе это представляют, если им предоставить комфортные условия и дать возможность сосредоточиться на рассматриваемом конкретном вопросе.

Результаты парных сравнений субъективных вероятностей для всего набора возможных исходов сводятся в квадратную матрицу

$$\boldsymbol{D} = \begin{pmatrix} d_{11} & \ldots & \ldots & \ldots & d_{1N} \\ \ldots & \ldots & d_{ij} & \ldots & \ldots \\ d_{N1} & \ldots & \ldots & \ldots & d_{NN} \end{pmatrix} \quad (4)$$

Определять численные значения элементов матрицы (4) рекомендуется на основе вербальной шкалы парных сравнений (таблица 1) для субъективных вероятностей возможных исходов.

Таблица 1 – Шкала парных сравнений вероятностей возможных исходов

Степень	Определение	Объяснение
1	Эквивалентность	Равновозможное наступления исходов
3	Слабое превышение	Некоторое преобладание возможностей наступления одного исхода над другим
5	Сильное превышение	Сильное преобладание возможностей наступления одного исхода
7	Очень сильное превышение	Практически явное преобладание возможностей наступления одного исхода
9	Абсолютное превышение	Наивысшая степень преобладания возможностей наступления одного исхода
2,4,6,8	Промежуточные значения	Компромиссное сравнение возможностей наступления исходов

Обработка матрицы парных сравнений позволяет перейти от относительных значимостей факторов к абсолютным, совокупность которых составляет компоненты главного собственного вектора обратно симметричной матрицы

$$\boldsymbol{D}\vec{X} = \lambda\vec{X}\,,$$

$$\vec{X} = \begin{pmatrix} x_1 \\ \cdots \\ x_N \end{pmatrix}, \qquad \sum_{i=1}^{N} x_i = 1\,. \tag{5}$$

Недостатки метода собственного значения связаны с невозможностью аналитического решения, при этом численное определение нормированного главного собственного вектора предполагает использование достаточно громоздкого алгоритма. Существуют достаточно простые и эффективные для близких к

согласованным обратно-симметричных матриц приближенные способы определения компонент собственного вектора, которые допускают получение аналитических решений с различной степенью точности. Наиболее точное приближение, из описанных в [7], позволяет получить реализация способа, основанного на вычислении нормированных среднегеометрических величин средних геометрических величин для расположенных в каждой строке элементов матрицы парных сравнений.

Предлагается вычисление субъективных вероятностей как нормированных среднегеометрических величин соответствующих строк матрицы (4) в соответствии с

$$q_l = \sqrt[N]{\prod_{j=1}^{N} d_{lj}} \Bigg/ \sum_{i=1}^{N} \sqrt[N]{\prod_{j=1}^{N} d_{ij}}\ , \quad l\epsilon\{1, \ldots . n\}\,. \tag{6}$$

Еще одно преимущество рассматриваемого приближенного способа проявляется при определении объективных вероятностей на основе подстановки выражений (6) в соотношение (3). Поскольку субъективные вероятности (6) пропорциональны средним геометрическим элементов соответствующих строк матрицы парных сравнений, в выражении (3) при нахождении отношения субъективных вероятностей происходит сокращение знаменателей

$$\frac{q_l}{q_m} = \sqrt[N]{\prod_{j=1}^{N} d_{lj}} \Bigg/ \sqrt[N]{\prod_{j=1}^{N} d_{mj}} \tag{7}$$

Выражение (7) имеет простой и наглядный смысл: отношение субъективных вероятностей равно отношению средних геометрических элементов соответствующих строк матрицы парных сравнений.

Принятие гипотезы о наличии функциональной связи между результатами субъективной оценки и объективного измерения вероятностей представляет, по сути, теоретическое обоснование предлагаемой ниже процедуры объективизации экспертных оценок

вероятностей редких событий. Математическая формализация данной процедуры заключается в определении правил перевода значений ранговой шкалы для экспертных оценок субъективных вероятностей в значения количественной шкалы отношений для соответствующих объективных вероятностей.

Для реализации процедуры объективизации подставляем в (3) отношения субъективных вероятностей в виде (7), а также учитываем условие нормировки вероятностей полной группы событий. В результате получаем систему соотношений, определяющую значения объективных вероятностей для всех возможных исходов

$$\begin{cases} \dfrac{p_l}{p_m} = \left(\prod_{j=1}^{N} d_{lj} \Big/ \prod_{j=1}^{N} d_{mj} \right)^{\frac{W}{N}}, \\ \sum_{i=1}^{N} p_i = 1 \quad . \end{cases} \tag{8}$$

Константа W, встречающаяся в (3) и (8) представляет собой параметр, значение которого определяет конкретный вид функциональной связи между результатами субъективной оценки и объективного измерения вероятностей. Для определения численного значения указанного параметра могут применяться как экспертные методы, так и методы, основанные на анализе имеющихся статистических данных.

Рассмотрим, например, ситуацию, в которой хотя бы для одной пары исходов возможна не только экспертная оценка отношения субъективных вероятностей, но и статистическая оценка отношения объективных вероятностей. В данном случае параметр W может быть непосредственно вычислен как показатель степенной функции для отношения субъективных вероятностей, при котором выполняется равенство (3) с отношением соответствующих объективных вероятностей.

Сформулируем основные положения предлагаемого подхода к решению проблемы объективизации экспертных оценок при оценивании вероятностей редких событий, основанного на гипотезе

о функциональной связи между результатами субъективной оценки и объективного измерения вероятностей.

1. Объективизация экспертных оценок вероятностей редких событий возможна на основе принятия гипотезы о наличии функциональной связи между результатами субъективной оценки и объективного измерения вероятностей, определенной в соответствии с психофизическом законом Стивенса (3).

2. Предложен приближенный способ вычисления субъективных вероятностей как нормированных среднегеометрических величин (6) соответствующих строк матрицы парных сравнений возможностей наступления возможных исходов.

3. Определены правила (8) перевода значений ранговой шкалы для экспертных оценок субъективных вероятностей в значения количественной шкалы отношений для соответствующих объективных вероятностей.

Литература:

1. *Орлов А.И., Савинов Ю.Г., Богданов А.Ю.* Экспертные технологии и их применение при оценивании вероятностей редких событий // Заводская лаборатория. Диагностика материалов. – 2014. – Т.80. № 3. – С.63-69.

2. *Гейзенберг В.* Физика и философия. Часть и целое. – М.: Наука, 1989. – 400 с.

3. *Бунге М.* Философия физики. – М.: Прогресс, 1975. – 348 с.

4. *Lootsma F.A.* Scale sensitivity in the multiplicative AHP and SMART // Journal Multi-Criteria Decision Analysis. – 1993. – V. 2. – P. 87-110.

5. *Терстоун Л.* Психофизиологический анализ. / В сб. Проблемы и методы психофизики. – М.: МГУ, 1984. – 296 с.

6. *Романчак В.М.* Субъективное оценивание вероятности // Информатика. – 2018. − Т. 15. № 2. – С. 74-82.

7. *Шикин Е.В., Чхартишвили А.Г.* Математические методы и модели в управлении. – М.: Дело, 2004. – 440 с.

DOI: 10.25728/iccss.2022.61.27.012

Фейзов В.Р.

Трансформация угроз обществу

Аннотация: Работа посвящена исследованию возможных способов деструктивного влияния на государство, общество и граждан. Рассматриваются некоторые виды угроз населению приводящие к продолжительному эффекту депривации. Вопросы, изучаемые в работе, заинтересуют исследователей обеспечения безопасности социально-экономических систем.

Ключевые слова: общество, угрозы, депривация, потребности, моделирование, социум, безопасность, аномия

Долгий путь развития от традиционного до постиндустриального общества вызвал изменение не только в быту и технологиях, но в потребностях населения. Значительные изменения в обществе особенно повлияли на стиль жизни граждан, а технологический прогресс, разделение труда, высокая мобильность и развитие гражданского общества позволили в значительной степени обеспечить базовые потребности граждан. Следует отметить, что потребность – это переживаемая человеком нужда в чем-либо для поддержания жизнедеятельности организма. Более того, корректное функционирование и развитие личности невозможно без удовлетворения соответствующих потребностей.

С увеличением продолжительности и качества жизни постепенно образовывались и новые потребности. Если на более ранних этапах развития человечества достаточным уровнем для жизни являлись базовые потребности совместно с потребностями в безопасности, то со временем помимо основных потребностей образовались творческие, а также духовные. Потребности относятся к статусу гражданина, его ощущению и чувствам, потребность можно связать и с необходимость в каком-либо ресурсе.

С момента перехода к доиндустриальному обществу ускоренное развитие предпринимательского ресурса и человеческого капитала сформировало большое количество социальных конструктов и институтов, одним из таких социальных институтов является семья,

являющаяся основной ячейкой общества. Особую значимость такого рода социального института как основу общества подчеркивают и известные философы того времени: «Индивид порождает индивида, семья порождает семью, а из семьи вырастает гражданское общество» [1]. Из семей формируются слои общества, при реализации угроз к которым, существует возможность разрушения социальных структур.

В соответствии с классической моделью потребностей человека, составленной А. Маслоу [2], существуют 7 классов потребностей. Каждый из классов представлен в текстовом формате в первом столбце таблице 1.

Таблица 1 – Модель угроз обществу в соответствии с потребностями слоев населения

Потребности	Основные угрозы	Наиболее подверженные слои населения	Депривация
Физиологичес-кие	Преступность	Низший	Экономическая /Политическая
Связанные с безопасностью	Преступность	Низший	Политическая
Социальные	Слабый уровень доверия к социальным институтам и между гражданами	Средний	Социальная
Связанные с местом в обществе	Социальное и экономическое неравенство	Высший	Социальная/ Экономическая
Творческие	Доступность образования и слабо развитая сфера развлечений	Средний/Высший	Социальная/ Экономическая

Эстетические	Проблемы института семьи, преступность	Средний/Высший	Социальная
Духовные	Социальное и экономическое неравенство	Средний/Высший	Социальная

Депривация в психологии является психическим состоянием, возникновение которого обусловлено жизнедеятельностью личности в условиях продолжительного лишения или существенного ограничения возможностей удовлетворения жизненно важных потребностей. Тем не менее, депривация относится не только к психологическому состоянию гражданина, но также и к политическому или экономическому [3], ведь в соответствии с реалиями современного общества граждане, которые обделены в удовлетворении каких-либо потребностей, могут быть недовольны своим уровнем жизни.

Выбор политического лидера страны, который может являться президентом или премьер-министром (в зависимости от полномочий), является своего рода социально-политическим договором между населением, которое определит направление развития страны, ее экономической и социальной сферы на годы вперед. Продолжительное недовольство больших слоев населения в связи с ощущением депривации, может вызвать самые негативные последствия, такие как аномия.

Аномия – понятие, выражающее состояние общества, при котором отсутствие или неустойчивость социальных и моральных императивов и правил, регулирующих отношения между индивидами и обществом, приводит к тому, что значительная часть населения оказывается «вне» общества, вступает в конфронтацию с его нормативными предписаниями [4].

Аномия проявляется в виде следующих нарушений:

1) расплывчатость, неустойчивость и противоречивость ценностно-нормативных предписаний и ориентаций, в частности, расхождение между нормами, определяющими цели деятельности, и нормами, регулирующими средства их достижения;

2) низкая степень воздействия социальных норм на индивидов

и их слабая эффективность в качестве средства нормативной регуляции поведения;

3) частичное или полное отсутствие нормативного регулирования в кризисных, переходных ситуациях, когда прежняя система ценностей разрушена, а новая не сложилась или не утвердилась как общепринятая;

4) аномия проявляется в различных сферах жизни общества. В настоящее время проводятся исследования проявлений аномии в экономике, политике, семейных отношениях, религии.

Литература:

1. *Сапрыкин Д.Л.* Значение и смысл понятия «образование» (на примере немецкой философии конца XVIII-начала XIX в.) // Вестник Московского университета. Серия 7. Философия. – 2008. – №. 1. – С. 19-42.

2. *Коротаева Е., Царегородцева Е.* Пирамида потребностей по А. Маслоу // Дошкольное воспитание. – 2008. – №. 5. – С. 36-41.

3. *Смольянов Г.И.* Социальная депривация как фактор политического неравенства // Государственное и муниципальное управление. Ученые записки СКАГС. – 2015. – № 4. – С. 255-258.

4. *Мертон Р.К.* Социальная структура и аномия // Социология власти. – 2010. – № 4. – С. 212-223.

II. Проблемы обеспечения экономической и социально-политической безопасности

DOI: 10.25728/iccss.2022.83.26.013

Дашков Р.Ю., Комков Н.И., Лазарев А.А.

Формирование целевых проектов развития

Аннотация: Рассматривается механизм формирования проектов развития социально-экономических систем (СЭС). Основой механизма является выделение обязательных составляющих компонент проекта, а цель проекта задается последовательным приближением к ее содержанию путем формирования внешних требований в полезности использования ожидаемого результата ее достижения для дальнейшего развития рассматриваемой СЭС и смежных с ней. Далее внешние требования к ожидаемому результату достижения цели. Поэтапность перехода из принимаемого за исходное состояние последующее предполагает выбор из множества возможных состояний такое, которое обладает наибольшей синергией с точки зрения достижения конечной цели проекта. Далее процесс повторяется до достижения конечной цели.

Ключевые слова: целевой проект, компоненты, способ, синергия, проектное управление

Одним из обязательных условий согласованности взаимодействующих систем и объектов разной сложности и назначения является получение дополнительной синергии, удерживающей эти системы и объекты при взаимодействии между собой.

Условия полезного взаимодействия разных систем и их составных частей наглядно иллюстрирует теория целевых систем [1, 2], где эффективность сконструированных сложных объектов из

разных составных частей подтверждается наличием предпочтительного, а в некоторых случаях и единственного порядка согласованного конструирования сложных объектов из разных составных частей (компонент).

Одна из основных проблем неэффективного использования проектного управления состоит в нарушении логической последовательности определения обязательных компонент формирования и управления проектами. Наиболее часто такие нарушения допускают эксперты, разрабатывающие проекты. Так, при разработке целевых проектов главным остается формирование привлекательной цели проекта (программы). После этого намечается стоимость проекта, а затем формируется состав участников проекта, включая компании, в том числе и с государственным участием. Когда удается достичь компромисса между предполагаемыми участниками, формируется удобный для них состав целевых нормативов, которые необходимо достичь. Далее формируется паспорт проекта. Выбор исполнителей проекта, качество выполнения проекта, возможности управления проектом и другие параметры рассматриваются как второстепенные. При таком подходе доля полезных и своевременно завершенных проектов остается низкой.

В состав обязательных компонент целевого проекта развития в соответствии с порядком построения информационно-логических моделей, а также с учетом регламента входит: внешняя потребность, цель, требование к цели, исходное состояние, способ достижения цели, стоимость, длительность (качество), риск.

Если известно назначение каждой компоненты целевого проекта, включая цель проекта, то основной задачей является установление порядка формирования информации о содержании всех остальных компонент, приближающей проект к достижению цели. При этом содержание каждой новой компоненты служит основой для выбора порядка предпочтительного определения последующей. Если известны свойства каждой компоненты, то их использование позволяет исключить полный перебор всех возможных вариантов, количество которых равно (n-1)!, а для целевого проекта при n=8 получим: 8!=40320. Рассмотрим схематически выбор на 2-м шаге (рисунок 1). Если рассматривается возможность достижения цели, то на следующем шаге

предпочтительно выбрать внешние требования к цели, т.е. C_R^v (рисунок 2).

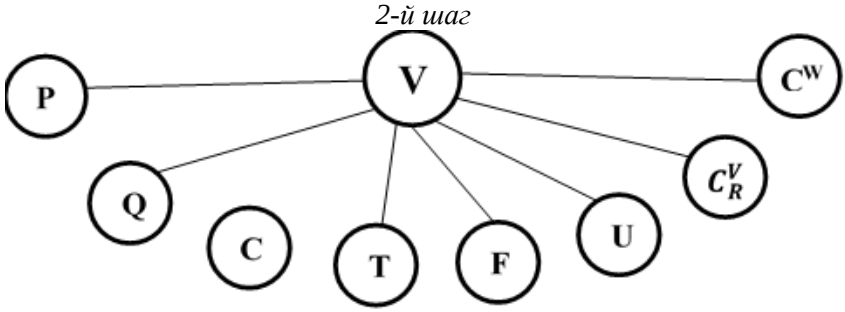


Рисунок 1 – Выбор потребности в цели

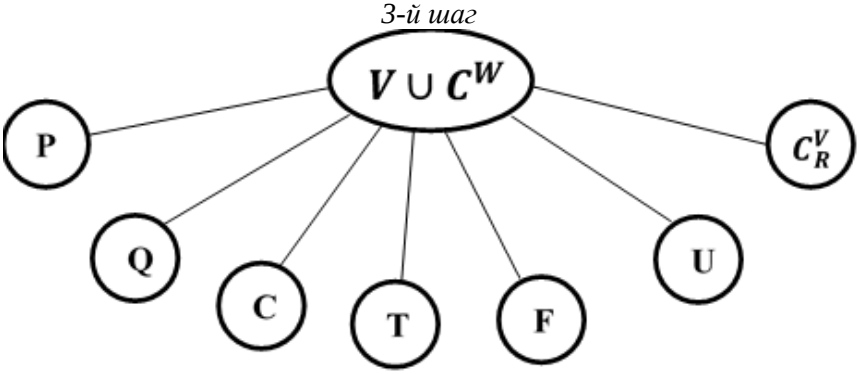


Рисунок 2 – Выбор требований к цели

После того, как известны C^w, V, то на 3-м шаге логично выбрать требование к полученному результату, т.е. C_R^v . На четвертом шаге рассматривается принимаемое исходное состояние U и наиболее близкий к достижению V после выбора U является выбор способа F достижения V с учетом C^w и C_R^v . (рисунок 3).

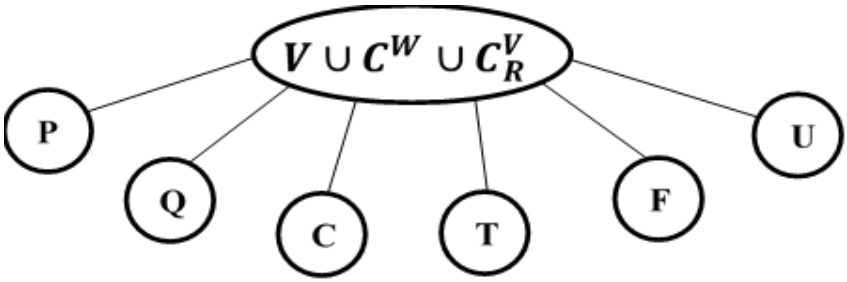


Рисунок 3 – Выбор исходного состояния для достижения способа реализации проекта

Выбор *F* на пятом шаге позволяет определить структуру проекта как совокупность взаимосвязанных работ, позволяющих приблизиться *U* с помощью *F* к цели *V*, ориентированной из *U* на C^w с учетом C_R^v .

Необходимо подчеркнуть, что *F* соответствует общей технологии проекта, но его отдельные работы могут выполняться известными способами, что упрощает содержание *F*.

Выбор *F* задает требования к численности и составу исполнителей определенной специализации и квалификации, задаваемых *F* . Следующий шаг дает возможность определить состав коллектива исполнителей проекта с учетом *V*, C^w, C_R^v ,*U*, *F* (рисунок 4). Для этого обозначим численность как *n*, а его составляющие как $\{n_{iq}^s\}$, где n_{iq}^s означает количество специалистов s -й специализации, и количество специалистов q-й квалификации.

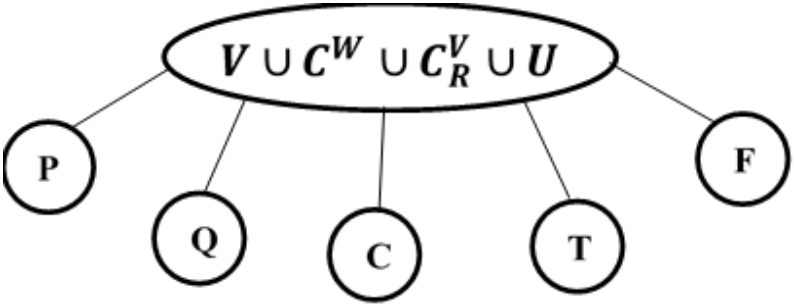


Рисунок 4 – Выбор способа реализации проекта

Анализ и выбор интенсивности выполнения проекта возможен при помощи двухуровневой системы моделей [2]. В данном случае излагается упрощенный подход к первоначальному анализу и выбору интенсивности проекта, основанный на возможности поэтапного сокращения стоимости проекта при условии соблюдения заданной его продолжительности и уровня качества.

Каждая $i \in R$ работа, где R множество работ выполняется определенной группой исполнителей за определенное время Δt_i и требует нужного качества и определенных затрат ресурсов стоимостью равной C_i. Возможность выполнения каждой работы разными коллективами с разной интенсивностью позволяет рассмотреть, по крайней мере, три варианта: максимально интенсивный, средний и минимально интенсивный. При этом

$$t_{cp} = \frac{t_{min} + t_{max}}{2}, t_{min}, t_{max}. \quad (1)$$

При t_{min} интенсивность выполнения работы будет самая высокая, а при t_{max} - наоборот самая низкая. Интегральные оценки выполнения всех работ проекта с разной интенсивностью находятся как

$$T_{min}^{кр} = \{t_{min}\}, \quad (2)$$

$T_{min}^{\text{кр}}$ – длительность критического пути при минимальной интенсивности выполнения работ

$$T_{cp}^{кр} = \{t_{cp}\}, \quad (3)$$

$T_{\text{ср}}^{\text{кр}}$– длительность критического пути при средней интенсивности; $T_{max}^{\text{кр}}$ - длительность при наименее интенсивном выполнении работ

$$T_{max}^{кр} = \{t_{max}\} \quad (4)$$

Разработка проекта состоит из двух связанных частей: создаваемого объекта и проекта его использования. Создаваемый

проект имеет свою конструкцию, а сам проект представляет собой процесс эксплуатации объекта, отвечающего определенному назначению и обладающему необходимыми свойствами, обеспечивающими его функционирование (выпуск продукции, оказание услуг) и отвечающими определенным требованиям, включая требования к качеству продукции (оказываемых услуг).

Архитектура, т.е. устройство, конструкция создаваемого объекта при подготовке проекта входит в состав технико-экономического обоснования проекта (ТЭО), представляющего содержательное описание создаваемого объекта, дополненное необходимыми оценками эффективности, ресурсами и графиками. В работе [2] представлен алгоритм поэтапного конструирования ТЭО проекта с учетом возможности достижения синергии на каждом шаге.

Определение состава работ и их взаимосвязей позволяет рассматривать экономические показатели проекта. Это возможно с учетом опыта обмена «стоимости на длительность» и выбора различной интенсивности выполнения работ и проекта в целом. Первоначально следует определить стоимостные показатели проекта, указав предельно допустимую стоимость проекта, которую обозначили как C^{max}. Далее выберем предпочтительную из (1)-(3) интенсивность и распределим величину C^{max} между всеми работами проекта, обозначив их длительность как t_i, $i \in R$. Затем определим продолжительность критического пути проекта при условии найденной длительности каждой работы, которую обозначим его как $T_0^{кр}$. При этом вполне возможно уменьшить стоимость отдельных работ, не лежащих на критическом пути, а сделать все пути равными критическому. Для этого, используя метод последовательных приближений, можно получить оценки стоимости работ, не лежащих на критическом пути, на основе следующего правила: стоимость каждой работы, не лежащей на критическом пути, уменьшается на одинаковую величину ΔC^1, до уровня, позволяющего выполнить проект с найденной длительностью $T_0^{кр}$. Если это невозможно, а $T_1^{кр} > T_0^{кр}$, то следует ΔC^1 скорректировать, т.е. уменьшить $\Delta C^2 > \Delta C^1$ для сокращения стоимости работ, не лежащих на критическом пути.

Также возможно, не меняя C_{max} определить возможные варианты интенсивности каждой работы, а затем уточнить интегральные оценки С и $T^{кр}$.

Стоимость проекта при максимальной интенсивности его выполнения равна

$$C_{max} = \sum_{i \in R} C_i^{max} \tag{5}$$

Аналогично определяется стоимость выполнения со средней интенсивностью

$$C_{cp} = \sum_{i \in R} C_i^{cp} \tag{6}$$

и с наименьшей интенсивностью

$$C_{min} = \sum_{i \in R} C_i^{min}. \tag{7}$$

Выбор какого-либо варианта из (4)-(6) зависит от его соответствия требуемому уровню качества проекта. При соблюдении требуемого качества следует отдать предпочтение более дешевому варианту выполнения проекта.

Целевой инвестиционный проект – это совокупность обязательных компонент информационной модели проекта, последовательность определения содержания которых, с одной стороны ориентирована на достижение цели проекта, а с другой стороны – на максимально полное использование содержания каждой компоненты при переходе от исходного состояния проекта к цели проекта. Степень полноты и полезности найденного содержания каждой компоненты оценивается с точки зрения увеличения синергии целевого проекта при выборе варианта для каждой из оставшихся не рассмотренных компонент целевого проекта.

Завершающий шаг – это оценка риска невыполнения проекта при установленных условиях его реализации (рисунок 5). Если известна потенциальная эффективность проекта на основе оценки NPV, то в качестве величины риска может использоваться условная вероятность PV успешного завершения проекта, формируемая

независимым экспертом. Тогда можно использовать формулу вычисления математического ожидания успешного завершения проекта

$$M(NPV) = NPV \cdot P + NPV(1 - P) \quad (8)$$

Следовательно, величина *NPV(1 - P)* может рассматриваться как необходимый размер страхового фонда, расходуемого в случае возникновения проблем с реализацией проекта.

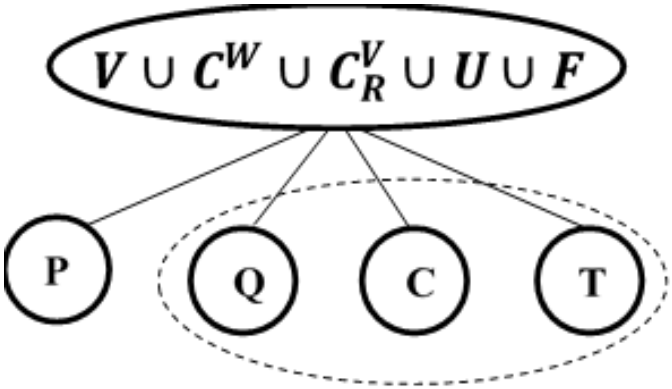


Рисунок 5 – Выбор интенсивности выполнения проекта

Если известны все параметры проекта C^w, C_R^v, *V ,U, F C, T, Q, P,* то могут быть вычислены финансовые потоки и экономические параметры проекта, включая ожидаемый чистый дисконтированный доход, ожидаемую прибыль, срок окупаемости, доходность на вложенный капитал и др. Для этого могут быть использованы продукты ТЭО-инвест, Project-expert. Представленная в п.4 информационная технология подготовки инвестиционных проектов позволяет получать более обоснованные экономические оценки инвестиционных проектов, что повышает их достоверность и реализуемость.

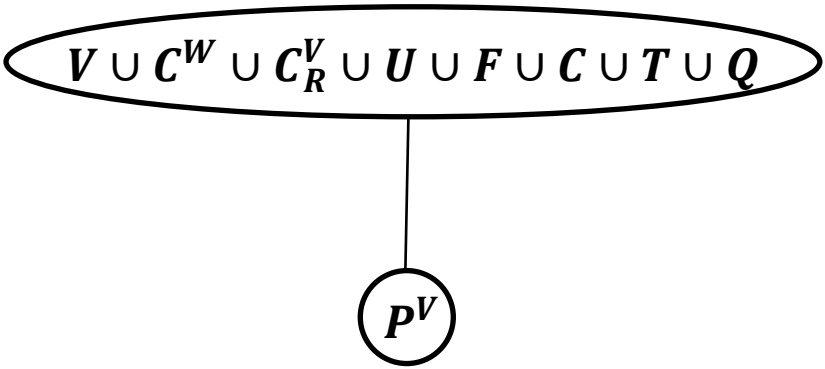


Рисунок 6 – Оценка степени риска

Пошаговое рассмотрение всех компонент целевого проекта позволяет алгоритмизировать процесс формирования технико-экономического обоснования проекта и проводить его построение в диалоговом режиме «Эксперт-ЭВМ».

Литература:

1. *Месарович М., Такахара Я.* Общая теория систем. / Пер. с англ. Э.Л. Наппельбаума, под ред. С.В. Емельянова. – М.: МИР, 1978. – 312 с.

2. *Комков Н.И., Бондарева Н.Н., Романцов С.Н., Диденко Н.И., Скрыпнюк Д.Ф.* Методические и организационные основы управления развитием компаний. – М.: Наука, 2015. – 520 с.

DOI: 10.25728/iccss.2022.68.42.014

Комков Н.И., Лантер Н.Н.

Анализ и оценка уровня критичности отраслевых и корпоративных сбоев в условиях санкционной экономики РФ

Аннотация: Исследование ставит целью поиск путей достижения РФ технологического суверенитета и роста экономики, с учетом анализа причин и масштаба отраслевых сбоев после ухода иностранного бизнеса в условиях санкций. Разработан методологический инструмент на

основе информационно-логической модели (ИЛМ) импортозамещения в рамках цикла полного инновационного воспроизводственного цикла (ПИВЦ) для усиления потенциала конкурентоспособности РФ.

Методика исследования. Методической основой исследования стали сравнительный анализ статистических и открытых аналитических данных, информационно-логические модели (ИЛМ), математические модели принятия решений, полный жизненный цикл технологической цепи инновационного воспроизводства.

Ключевые слова: информационно-логическая модель, полный инновационный воспроизводственный цикл, многопараметричность, технологический суверенитет, отраслевой, логистический сбой, уход иностранного бизнеса, технологические звенья, точки непреодолимой зависимости, утрата критических компетенций, вторичные санкции

Сложные условия внешней среды трансформировали отраслевые рынки, вызвали технологические сбои и дисбаланс после ухода из РФ иностранных компаний (806 компаний из списка Йельской школы менеджмента). Эти компании длительно встраивали РФ в глобальную систему рыночных отношений через создание СП (48 тыс. компаний в 2021 году), трансфер технологий, открытую логистику, доступ к глобальному капиталу и вывод фондового рынка РФ на мировые биржи.

Ушедшие из РФ компании из 70 стран мира представляли компетенции в 55 различных отраслях. Суммарно из экономики РФ выпал огромный пласт технологических компетенций и логистических наработок, в результате чего изменилось качество ввозимых и производимых товаров и услуг, нанесен ущерб национальному интеллектуальному капиталу, усилился отток специалистов за рубеж. При выходе из СП иностранные компании пользовались услугами консалтинговых фирм для минимизации своих потерь, без учета интересов РФ, что создавало серьезные отраслевые угрозы и вызовы.

Отметим, что задачи РФ в области комплексного замещения технологий, восстановления компетенций и усиления потенциала

роста экономики реализуются с учетом прогнозируемых рыночных трендов: роста адаптивности оставшегося бизнеса; активных слияний и поглощений; ускоренного замещения ряда звеньев технологий; вынужденного временного упрощения потребительских характеристик товаров; выхода на рынок новых иностранных брендов; трансформации потребностей общества и государства через снижение ожиданий качества и ассортимента товаров и услуг; трансформации инвестиционного, кредитного и потребительского поведения.

Ряд экономических секторов с затруднением восстанавливают полный жизненный цикл импортозамещения (ПЖЦИ) из-за запретов на импорт технологий, включая гражданские, отставания/отсутствия технологических заделов пятого уклада (турбины, микросхемы, 6G–технологии, биотехнологии, медроботы, др.). В итоге нарастания санкционного давления до критического уровня возможен запуск инерционного сценария технологического развития ряда отраслей РФ. Тем не менее*, потенциал импортозамещения* как инструмента разрешения «узких мест» (например, в формате онлайн бирж по импортозамещению) остается значительным, что показала адаптации МСБ в РФ [1]. Выпавшие звенья технологий успешно замещаются на российские или доступные иностранные аналоги, идет поиск новых торговых и технологических партнеров. Для крупных проектов этот вариант имеет существенные *ограничения по времени и затратам. Достижение технологического* суверенитета РФ на долговременную перспективу должно стать основной задачей при принятии решений на всех уровнях управления, включая мобилизацию ресурсов, развитие союзов и партнерств.

Анализ новых нарастающих рисков для РФ в условиях санкционной экономики позволяет выявить следующие: 1) риск утраты традиционных рынков сбыта; 2) риск роста внутренних цен на товары и услуги, удорожания национальных проектов; 3) ограниченный доступ к новым мировым технологиям в ключевых отраслях; 4) риски наложения вторичных санкций; 5) ограничение доступа к мировому капиталу и разделению труда; 6) риски ограничения участия РФ в глобальном энергопереходе; 7) закрытие ряда компаний из-за недозагрузки мощностей и невозможности заменить выпадающие технологические звенья; 8) риски длительного технического «каннибализма»; 9) переход на

неэффективные аналоги из-за отсутствия комплектующих для сложных машин и механизмов; 10) вывод значительного объема средств производства из оборота; 11) сокращение присутствия РФ в ранее занятых кооперационных, торговых, гуманитарных и научно-исследовательских нишах; 12) нарушение имущественных и нематериальных прав граждан РФ и других стран; 13) снижение качества зарубежной продукции в рамках параллельного импорта и импортозамещения; 14) риски утраты доверия со стороны зарубежных партнеров на долгосрочную перспективу; 15) риск утраты технологического суверенитета (включая лекарственный); 16) риски остановки и закрытия проектов, предприятий и кризиса моногородов; 17) риски утраты фондового рынка РФ и части международных финансовых операций; 18) снижение качества национальных товаров и услуг из-за снижения конкуренции и др.

Отметим комплексный, системный характер рисков, что обусловлено ростом *числа «болевых точек» первого и второго уровня (точек непреодоленной и непреодолимой зависимости*) РФ от технологий, расходных и запасных материалов и интеллектуальной компетенции стран, наложивших санкции.

Авторы проанализировали масштаб, глубину и последствия разрыва международных связей РФ в разных отраслях экономики (на примере 39 секторов). Так, уход с рынка РФ компаний «Airbus», «Boeing», «Airbus», «Dassault Aviation», «AerCap» привел к отзыву сертификатов летной годности лайнеров, запрету поставок комплектующих, сокращению пилотов, дефициту летного парка. Уход «Rolls-Royce» остановил поставки двигателей и запчастей для автомобилей и самолетов «Аэрофлота», Компания «Boeing» отказалась от техподдержки на территории РФ. Прекращение производства на 30 заводах автопрома иностранных марок в РФ стало результатом разрыва логистических связей. Компании «Eli Lilly», «AbbVie», «Merck &Co.Inc.», «Bayer», «Pfizer», «Gilead» частично или полностью приостановили инвестиции. Фирма «Novartis AG» (Швейцария) остановила научные мероприятия в РФ, оставив только сокращенные инвестиции и гуманитарные поставки. Это приводит к росту дженериков, поскольку 85 % контрактов подписано в валюте и трудно заменимо. Нефте-сервисные корпорации «Baker Hughes», «ExxonMobil» (США), «TotalEnergies» (Франция), «Eni» (Италия), «Shell» (UK, Нидерланды), «Equinor»

(Норвегия), «OMV» (Австрия), «BP» (UK), концерн «Siemens» (Германия) прекращают обслуживание российских СПГ-проектов. Отмечена трудность импортозамещения газовых турбин и ноу-хау. Также выявлен сбой в доставках продукции, отмечается дефицит судов и контейнеров вследствие ухода ряда иностранных компаний («DHL Express», «MSC», «CGM», «Hapag-Lloyd», «Samskip», «Moeller-Maersk», «Nurminen Logistics», «HMM», «FedEx», «UPS», «DHL», «Cyprus Post», «CMA Shipco», «Ocean Network Express», «Yang Ming»). Отмечен рост цен на лифты на 40 %, снижение объемов производства, дефицит запчастей как результат ухода с российского рынка компаний «OTIS Elevator Company» (США) и «Kone Oy» (Финляндия). Трудности выявлены в строительной отрасли после ухода таких компаний, как «Kingspan» (Ирландия), «Holcim» (Швейцария), «Velux», «Aarsleff» (Дания). Производство 11 из 26 видов стройматериалов в РФ зависит полностью от импортного оборудования. Данные для анализа взяты из открытых источников, не включают СП в банковском, страховом бизнесе, образовании, медицине, торговле.

Отметим, что уход части иностранных компаний был юридически оформлен через передачу активов российскому оператору, менеджменту, продажу, временную приостановку инвестиций и торговых операций и другие формы взаимодействия. Многие западные компании, продолжившие операции в РФ, отметили рост конкурентоспособности и объема продаж после включения их компаний в новые схемы импортозамещения и подписание новых торговых и логистических контрактов вместо ушедших с рынка отраслевых конкурентов.

Полагаем, что выявленные дисбалансы и вызовы в ряде отраслей российской экономики могут быть трансформированы в статус проектов, открывающих новые возможности для *импортозамещения* и создания *аналогов превосходящего качества*, на которые существует сложившийся в ходе *локализации* иностранных производств национальный и мировой рыночный спрос. Комплексность задач состоит в оперативном закрытии выпавших ниш, звеньев, «узких мест» и сбоев в технологических и управленческих процессах, логистике и НИОКР. При этом профилактика возможных рисков и минимизации всех текущих рисков после трансформации рынков приобретает особое значение,

Значительные объемы компетенций для заполнения ниш в сфере импортозамещения требуют инновационного подхода, новых законов, мобилизации ресурсов, кадров и опыта в целях сохранения технологической устойчивости России в условиях нарастания санкций.

Отметим, что причины технологической уязвимости РФ связаны с сокращением численности исследователей (в 1992-2020 гг. с 800 тыс. до 325 тыс. чел.), игнорированием ресурсодобывающим сектором отечественных НИИ, многолетним импортом «под ключ» западных технологий, ликвидацией Центра управления НТР в формате ГКНТ, отказом от формирования национальной научно-технологической политики, «утечкой мозгов».

Важно отметить, что анализ масштаба отраслевых и корпоративных сбоев и ожидаемых рыночных деформаций может быть рассчитан с учетом «узких мест» в каждой отрасли и синергетического эффекта (прямого и опосредованного) отраслевых дисбалансов на экономику РФ в целом. Данный подход позволит с определенной периодичностью отслеживать процесс формирования проектов импортозамещения и степень разрешения отраслевых проблем, динамику сбоев (рост/сокращение), уровень адаптации государства, бизнеса, общества к вызовам, восстановление потенциала отраслей через информационно-логической модели инновационного воспроизводственного цикла (ИЛМИВЦ).

Необходимость замены бывшего ранее инновационного продукта на рынке устаревших продуктов на новые лучшие продукты соответствует понятию смысла цикла и определяется конкуренцией за лучший продукт, технологию. Кроме оценки конкурентных преимуществ технологии в формате «цена и качество», учитывается длительность ПЖЦ цикла ряда продуктов, стоимость текущих и капитальных затрат для создания ПЖЦ. Полное преимущество по всем параметрам, учитывающим как векторность (многопараметричность) показателей качества, так и значения всех затрат, необходимых для поддержания потребительских свойств продукта в работоспособном состоянии в течение ПЖЦ, соответствует термину «превосходства» либо «тотального превосходства». Если превосходство утрачено, но сохраняются лучшие значения хотя бы по одному показателю, то это означает «преимущество» продукта. При сравнении продуктов, имеющих

только локальное преимущество по каким-либо параметрам, лучший продукт определяется на основе сравнения векторов либо их скалярных оценок.

Согласно правилам ранжирования целевых проектов их конструирование начинается с определения содержания главной компотенты – *цели проекта*. Основные потребители инновационных технологий – компании, реализующие инновационные технологии и, создаваемые на их основе, продукты и услуги. ПИВЦ включает производителя конечной инновационной продукции – компанию, которая реализует и серийно выпускает инновационный продукт. Поиск заказчика, формирующего потребность в импортозамещении импортируемого продукта, сосредотачивается на установлении компании в РФ, использовавшей данный продукт ранее, знакомой с аналогами и потенциальными покупателями заменяемого импортного аналога. Предварительная оценка объема рынка отечественного аналога импортного продукта – основание для поиска возможных объектов производства аналога, замещающего импорт. Далее осуществляется поиск отечественной технологии, способной выпускать аналог замещаемого импортного продукта. Возможны следующие варианты:

1) отечественная технология требует существенной доработки до уровня конкурентоспособности выпускаемого продукта-аналога;

2) необходим поиск инновационных идей и решений, способных скоординировать отечественную инновационную технологию для производства отечественного аналога;

3) отсутствуют необходимые компетенции для проведения НИР по поиску замены импортных технологий и продуктов требуемого качества;

4) возможна замена импортного продукта отечественным аналогом худшего качества.

В случае п.1. и п.2 готовятся договор, обоснование к нему и предложение по включению намеченных работ в Программу импортозамещения федерального уровня. Поиск решения в случае п.3. требует подготовки и переподготовки кадров либо приглашения специалистов из-за рубежа. В случае п.4. проводится исследование возможных потерь при замене импортируемого продукта аналогом худшего качества. Смысл содержания ПИВЦ – включение в его состав не только начальных этапов фундаментальных исследований,

но и последующих этапов последовательного преобразования результатов фундаментальных исследований в инновационные идеи и решения, прикладные НИОКР. Для проекта ПИВЦ проводятся поиск и идентификация компании, заинтересованной в импортозамещении продукта отечественным аналогом в соответствии с правилами подготовки целевых проектов и максимизации синергии при переходе к достижению конечной цели проекта.

Комплексная технология включает четыре основные части: 1) собственно технологию как способ создания импортного продукта; 2) необходимое оборудование, машины и механизмы для реализации технологии; 3) регламент для трудового потенциала сотрудников, обслуживающих технологию и технику; 4) нормативы и порядок работы управляющего персонала технологией, машинами и оборудованием, трудового коллектива для реализации комплексной технологии в целом. Определение потенциала конкурентоспособности сформированного варианта технологии включает оценку качества, технического уровня, экономических показателей, соблюдения экологических требований (таблица 1).

Таблица 1 – Импортозамещение технологий и продуктов, а также устранение сбоев в условиях санкционной экономики (разработано авторами)

Баллы	Уровень сложности задач для решения проблемы	Прогноз срока разрешения проблемы	Вероятность разрешения в указанные сроки
1	Восстановление торговых, партнерских отношений, альтернативная замена поставщиков/потребителей продукции	В течение 3-12 месяцев	0,7-0,9
2	Восстановление торговых, партнерских отношений, альтернативная замена поставщиков/потребителей продукции	В течение 3-12 месяцев	0,3-0,8
3	Импортозамещение	В течение	0,6-0,8

	одного/нескольких *второстепенных, некритических* звеньев технологии/логистических цепочек	1-3 года	
4	Импортозамещение одного/ нескольких *второстепенных, некритических* звеньев технологии/логистических цепочек	В течение 3-7 лет	0,4-0,7
5	Импортозамещение одного/ нескольких *критических, ключевых* технологических звеньев	В течение 1-3 года	0,5-0,8
6	Импортозамещение одного или нескольких *критических, ключевых* технологических звеньев	В течение 3-7 лет	0,4-0,7
7	Ограниченная совместимость со сторонними решениями, необходимость комплексного перехода на другие доступные технологии и диверсификацию бизнеса.	В течение 1-3 года	0,5-0,8
8	Совместимость со сторонними решениями, необходимость разработки отечественных альтернативных технологий	В течение 3-7 лет	0,3-0,7
9	Безуспешный поиск альтернатив по импортозамещению продукции или услуг, поиску поставщика/ рынка сбыта. Потеря рынка сбыта и/или поставок. Выход из бизнеса.	В течение 1- 5 лет	0,4-0,6
10	Безуспешный поиск альтернатив по импортозамещению продукции или услуги, поиску поставщика/ рынка сбыта. Потеря рынка сбыта и/или поставок. Выход из бизнеса.	В течение более 5 лет	0,4

При максимальном уроне дисбаланса и критичности сбоев разрешимость в указанное время разрешения проблемы может достигать оцениваемой экспертами субъективной вероятности в пределах от 0 до 1,0.

Таким образом, предложенные методологические подходы позволят учитывать причины, масштаб и пути преодоления

отраслевых сбоев после ухода иностранного бизнеса в условиях санкций, принимать эффективные решения по достижению РФ технологического суверенитета и роста экономики на базе цикла полного инновационного воспроизводства. Комплексные программы по достижению РФ технологического суверенитета следует рассматривать как большие системы, мобилизующие все ресурсы для роста экономики в условиях текущих и будущих вызовов.

Литература:

1. *Комков Н.И., Бондарева Н.Н.* Импортозамещающая стратегия РФ как фактор развития в условиях глобальных вызовов 2017-2019 гг. // МИР (Модернизация. Инновации. Развитие). – 2017. – Т. 8. № 4 (s). – С. 640-656.

DOI: 10.25728/iccss.2022.99.32.015

Байрамов О.Б.о.

О тенденциях развития микрофинансирования в России

Аннотация: Подчеркивается роль процесса микрофинансирования для различных слоев населения стран мира и России. Рассматриваются основные проблемы в секторе российского микрофинансирования, подчеркивается стабилизирующая роль государственных структур, обсуждается взаимоотношение со страховыми компаниями.

Ключевые слова: микрофинансирование, заемщик, микрофинансовые организации, страховая компания, процентные ставки

Микрофинансирование возникло в 1970-х годах и оправдало свое первоначальное предназначение – показало возможность создания необходимых условий для малоимущих людей заниматься предпринимательской деятельностью в разных странах мира, что, в свою очередь, снимает социальную напряженность в беднейших странах мира, в определенной степени содействует борьбе с нищетой и преступностью и, наконец, позволяет конкретному человеку

проявить свои предпринимательские качества, открывает в его жизненном пути новые возможности.

Наибольшего успеха в реализации программ микрофинансирования добились в странах с наибольшей долей бедного населения, для которого практически недоступно финансово-кредитное обслуживание, а также уровень развития экономики находится на низком уровне. Наиболее выраженно социальная направленность микрофинансирования проявляется в развивающихся странах, в которых деятельность микрофинансовых структур восполняет неполноту и несовершенство традиционного финансового рынка [1]. Микрофинансовые программы как средство борьбы с нищетой и безработицей на начальном этапе наиболее широко были представлены и реализованы в странах третьего мира, но уже к началу 1990-х годов стало очевидным, что они могут применяться как в слаборазвитых, так и в развивающихся и развитых странах. При этом микрофинансирование в индустриально развитых странах выполняет несколько иные функции.

Микрофинансирование за рубежом

Микрофинансирование в таких странах, как Индия, Бразилия, Аргентина и др. так называемых странах с переходной экономикой носит не только социальный, но и политический характер, так как способствует формированию класса собственников посредством поддержки развития малого предпринимательства. Программы микрофинансирования в этих странах не столь масштабны и своей главной целью считают не столько преодоление крайней нищеты, сколько финансовую поддержку предпринимательских инициатив, проявляемых экономически активными слоями населения. Так же аналогичные микрофинансовые программы, приспособленные к национальным особенностям, развиваются во многих странах Юго-Восточной Азии и Африки [1].

В последние годы микрофинансовые программы успешно реализуются во многих странах центральной и восточной Европы. После распада СЭВ и других социалистических структур, когда банковский сектор перестал удовлетворять растущие потребности населения в финансовых услугах, микрофинансирование заполнило этот пробел, предоставив гражданам финансовую поддержку для поддержания жизненного уровня. В большинстве этих стран

микрофинансовые программы поддерживаются различными фондами и государственными структурами.

В странах СНГ микрофинансирование стало осуществляться относительно недавно и темпы распространения отличаются. Но в целом структуры микрофинансирования находятся в стадии становления и накопления опыта разработки и реализации собственных моделей микрокредитования с целью поддержки предпринимательской инициативы и обеспечения занятости населения.

В США и странах Западной Европы, в других индустриально развитых странах рынок микрофинансирования используется для решения таких социальных задач, как снижение уровня безработицы, оказание финансовой поддержки социально неустроенным категориям граждан, обеспечение безболезненной интеграции в общество мигрантов и переселенцев. Микрофинансирование в этих странах осуществляется как неправительственными организациями, так и специализированными государственными и полугосударственными учреждениями. В Западной Европе наибольшее распространение микрофинансирование получило во Франции, которое с 2005 года стало одним из приоритетов правительства. В США и др. странах используются стимулирующие механизмы, способствующие распространению розничных банковских услуг на микрофинансовые рынки нижележащего уровня. В России действует аналогичная модель в рамках программы микрокредитования, которая реализуется Европейским банком реконструкции и развития через сеть коммерческих банков. В данном случае предоставленные уполномоченным банкам на льготных условиях финансовые ресурсы стимулируют их экспансию в микрофинансовый сектор.

Микрофинансирование в России

Развитие микрофинансирования и его институтов в России имеет ряд схожих черт с аналогичными явлениями за рубежом, одновременно имеет ряд отличительных особенностей, основные из которых приводятся в [1]: а) разрыв между спросом и предложением на рынке микрофинансовых услуг. б) микрофинансирование имеет некоммерческую ориентацию-прибыль не и является основной целью деятельности, условия микрокредитования ориентируются на

обеспечение самоокупаемости и жизнедеятельности организации. в) высокая доля неформального сектора на рынке предоставления микрофинансовых услуг, г) практически полное отсутствие собственных микрофинансовых программ и низкая мотивация в их разработке и реализации у российских банков, д) отсутствие льготных условий для развития рынка микрофинансовых услуг, е) отсутствие четкого структурного разделения рынка на «классическое» микрофинансирование, включающее потребительское кредитование и кредитование малого и среднего бизнеса (МСБ) и сегмент микрофинансовой деятельности, специализирующийся на выдаче «займов до зарплаты». Тем не менее, анализ состояния отечественного микрофинансового рынка свидетельствует о том, что вступил в период интенсивного развития, а темпы роста отрасли имеют ярко выраженную положительную динамику. По темпам роста микрофинансовый сектор сравнялся с динамикой необеспеченного кредитования физлиц и заметно опережает кредитование МСБ. Таким образом, микрофинансирование постепенно становится неотъемлемой частью всей финансово-кредитной системы страны, дополняющей традиционный банковский сегмент, расширяя доступ к заемным средствам той категории бизнеса и населения, которая не отвечает традиционным банковским стандартам.

В [2] подробно рассматриваются основные проблемы в секторе российского микрофинансирования. Подчеркивается, что на международном уровне существует единое понимание микрофинансирования как инструмента социальной политики, предназначенного для обслуживания предприятий, которые коммерчески не привлекательны для основных представителей финансирования, но, тем не менее, играют значительную социальную роль для страны. Кроме того, микрофинансирование воспринимается многими зарубежными странами в качестве важного государственного инструмента, с помощью которого можно бороться с социальным и финансовым неравенством, стимулировать самозанятость населения. В России сложилась исключительно ростовщическая модель МФО, одновременно пытающаяся пользоваться регуляторным арбитражем наравне с кредитными организациями. Имеет место высокая степень закредитованности населения страны со стороны МФО. Долгое время на

законодательном уровне не применялось эффективных мер по регламентированию величины процентной ставки по кредитам, выдаваемым МФО физическим лицам, в связи с чем этот показатель в МФО в среднем может достигать 600-1000 % годовых. Финансовая неграмотность населения при заключении договора микрофинансирования не позволяет потребителям в достаточной степени оценить возможные риски. Для решения имеющихся проблем необходимо проводить работу по планомерному регулированию отрасти микрофинансирования в России на законодательном уровне с учетом положительного опыта регулирования сектора микрофинансирования в зарубежных странах, а также исходя из приоритета социальной составляющей деятельности МФО. Отсутствие государственной политики по регулированию сектора микрофинансирования приведет к росту имеющихся проблем. Среди основных проблем российского рынка микрофинансирования выделяются: несоблюдение МФО принципов ответственного кредитования; информационная непрозрачность деятельности МФО; агрессивная реклама, которая используется МФО в различных каналах СМИ; подчас незаконные действия коллекторов по взиманию с должников просроченной задолженности; игнорирование МФО стандартов деятельности, прописанных, в частности, в Базовом стандарте защиты прав и интересов физических и юридических лиц-получателей финансовых услуг, утвержденном Банком России в 2017 г. Новые регуляторные ограничения, которые будут действовать на российском микрофинансовом рынке в соответствии с Базовым стандартом, устанавливают единые условия для PDL-займов (займов «до зарплаты») и коэффициентов предельного размера долговых обязательств заемщика. Другая проблема для МФО-регуляторный риск-риск несоблюдения требований регулятора. Регуляторный риск означает угрозу потерь из-за невыполнения в повседневной работе юридических норм, стандартов, установленных регулятором, неправительственными организациями, а также внутренних правил. При этом МФО в статусе банков могут регулироваться одним органом, а небанковские МФО-другим. Требования регуляторов могут различаться, что порождает регуляторный арбитраж: собственники МФО стремятся выйти на рынок через менее регулируемый сегмент.

Основной вывод из приведенного заключается в следующем – более активное участие государства в поддержке процесса микрофинансирования и деятельности МФО придаст стабильность рынку микрофинансирования в России. МФО могут рассчитывать на доступ к более выгодным источникам финансирования и структурам страхования. В свою очередь, к услугам страховых компаний могут обращаться заемщики МФО и сами МФО. Здесь коротко рассмотрим случай обращения МФО в страховую компанию.

Пусть МФО планирует осуществить свою деятельность в интервале времени $[0,T]$, пользуясь финансовым ресурсом R. Обращаясь в страховую компанию, МФО обязуется выплатить страховой взнос S страховой компании за текущий период своей деятельности. При работе со страховой компанией МФО для согласования размера страхового взноса S может пользоваться историей работы с заемщиками за предыдущий период деятельности. Пусть по результатам обработки статистической и др. информации стало известно, что процент непогашения займа клиентами МФО составлял P процентов, $0<P<100$. Тогда МФО может ограничиться страхованием определенной части R, а именно, $R \cdot P/100$. Таким образов, размер взноса для страховой компании составит $R \cdot P/100 \cdot S$.

В дальнейшем при определении процентных ставок q_i, $0<q_i<Q$, где Q – период (количество дней) займа, например, $Q \leq T \leq 365$, $I=1,\ldots,n$, n – число заемщиков, МФО будет ориентироваться на получение средств после завершения своей деятельности в размере не меньше $R \cdot (1+P/100 \cdot S)$. Определение значений S и q_i, $i=1,\ldots,n$ для МФО имеет важное значение и является предметом отдельного рассмотрения.

Заключение

Рассмотрение особенности процесса микрофинансирования в России подсказывает более активное участие государственных структур в нем, а исследование поведения некоторых участников этого процесса приводит к созданию соответствующей математической модели и изучению взаимоотношений между ними.

Литература:

1. *Цхададзе Н.В.* Микрофинансирование за рубежом: опыт решения социальных задач // За рубежом 2017. – №1. – С. 101-109.

2. *Уткин В.С., Юрьева А.А.* Анализ основных проблем российского рынка микрофинансирования // Финансовый журнал. – 2018. – №5. – С. 97-107.

DOI: 10.25728/iccss.2022.54.67.016

Фомичев А.Н.

Концепция энергетической псевдобезопасности как генезис мирового экономического кризиса

Аннотация: Текущее состояние как мировой экономической системы в целом, так и являющихся её неотъемлемыми элементами, национальных экономик отдельных государств и регионов Земного шара, как никогда остро ставит вопрос обеспечения энергетической безопасности как сферы промышленного и сельскохозяйственного производства, так и сферы бытового обеспечения потребностей населения.

Вышеизложенное обусловливает необходимость поиска, разработки и внедрения альтернативных источников энергоснабжения. Решением данного вопроса активно и занимаются ведущие умы мирового научного сообщества.

В рамках проведенного исследования автором сделана попытка подтвердить, либо опровергнуть положения о экономической целесообразности, экологичности и социальной значимости «зеленой энергетики». При этом ключевое внимание уделено, в первую очередь, проблематике энергообеспечения автомобильного транспорта, причем как в пассажирской, так и в грузовой сфере его функционирования.

Ключевые слова: энергетическая безопасность, «зеленая энергетика», система транспортных коммуникаций, автомобильный транспорт

Текущее состояние как мировой экономической системы в целом, так и являющихся её неотъемлемыми элементами, национальных экономик отдельных государств и регионов Земного шара, как никогда остро ставит вопрос обеспечения энергетической безопасности как сферы промышленного и сельскохозяйственного производства, так и сферы бытового обеспечения потребностей населения.

Вышеизложенное обусловливает необходимость поиска, разработки и внедрения альтернативных источников энергоснабжения. Решением данного вопроса активно и занимаются ведущие умы мирового научного сообщества. Попытаемся проанализировать, насколько успешно продвигаются фундаментальные и прикладные исследования в указанном направлении.

В современной, как научной, так и популярной литературе красной нитью проходит мысль о необходимости развития так называемой «зеленой энергетики». На первый взгляд предложенная концепция представляется вполне своевременной, перспективной и в полной мере отвечающей насущным требованиям мировой экономической системы. По мнению её авторов, максимально возможно широкое проектирование и прикладное использование альтернативных источников энергии позволит улучшить экологическую обстановку, снизить издержки производителей на энергоносители, составляющие львиную долю в себестоимости продукции как промышленного, так и сельскохозяйственного сектора экономики. И, что, наверное, самое главное, применение рассматриваемой концепции должно снизить зависимость мировой экономики от невозобновляемых источников энергии.

В рамках проведенного исследования автором сделана попытка подтвердить, либо опровергнуть положения об экономической целесообразности, экологичности и социальной значимости «зеленой энергетики». Для этого целесообразно обратить внимание, в первую очередь, на проблематику энергообеспечения автомобильного транспорта, причем как в пассажирской, так и в грузовой сфере его функционирования.

На сегодняшний день не только довольно активно идет разработка автомобилей с электрическим двигателем, но и осуществляются многочисленные попытки максимально возможной

популяризации их практического применения. Причем речь идет не только, да и не столько, о широко нашумевшей и дорогостоящей программе «Tesla», но и о целом ряде более скромных проектов, реализуемых такими лидерами мирового автопрома, как «Chevrolet», «Nissan», «Audi», «BMW», «FISKER» и др., а также представителями отечественной автомобильной отрасли, как то концерн «АвтоВАЗ», инжиниринговая компания «ZETTA», автоконцерн «Монарх», концерн «Калашников».

В современной, как научной, так и популярной литературе красной нитью проходит мысль о необходимости развития так называемой «зеленой энергетики». На первый взгляд предложенная концепция представляется вполне своевременной, перспективной и в полной мере отвечающей насущным требованиям мировой экономической системы. По мнению её авторов, максимально возможно широкое проектирование и прикладное использование альтернативных источников энергии позволит улучшить экологическую обстановку, снизить издержки производителей на энергоносители, составляющие львиную долю в себестоимости продукции как промышленного, так и сельскохозяйственного сектора экономики. И, что, наверное, самое главное, применение рассматриваемой концепции должно снизить зависимость мировой экономики от невозобновляемых источников энергии [1].

В рамках проведенного исследования автором сделана попытка подтвердить, либо опровергнуть положения об экономической целесообразности, экологичности и социальной значимости «зеленой энергетики». Для этого целесообразно обратить внимание, в первую очередь, на проблематику энергообеспечения автомобильного транспорта, причем как в пассажирской, так и в грузовой сфере его функционирования.

На сегодняшний день не только довольно активно идет разработка автомобилей с электрическим двигателем, но и осуществляются многочисленные попытки максимально возможной популяризации их практического применения. Причем речь идет не только, да и не столько, о широко нашумевшей и дорогостоящей программе «Tesla», но и о целом ряде более скромных проектов, реализуемых такими лидерами мирового автопрома, как «Chevrolet», «Nissan», «Audi», «BMW», «FISKER» и др., а также представителями отечественной автомобильной отрасли, как то концерн «АвтоВАЗ»,

инжиниринговая компания «ZETTA», автоконцерн «Монарх», концерн «Калашников» [2].

Примечательно и то, что совсем недавно на Восточном экономическом форуме о разработке собственного электрокара под отечественным брендом «Лада», а конкретно электрической Lada Largus, заявил глава одного из крупнейших отечественных автомобильных предприятий концерна АвтоВАЗ, Максим Соколов [3]. Как отметил господин Соколов, производство электрической Lada Largus может начаться в 2023 году, будет выпущена «небольшая серия».

На первый взгляд подобные разработки, при условии их широкого практического внедрения, во-первых, будут способствовать улучшению экологической обстановки, как в отдельных регионах Земного Шара, так и во всем мире, во-вторых, приведут к существенному снижению зависимости экономики от нефти и газа.

Но при всем при этом, по не вполне понятным причинам, электрокары, так и не смогли занять сколь-нибудь значимую долю мирового автомобильного рынка [4]. Постараемся разобраться в этом вопросе, сразу де отбросив конспирологические теории, типа мирового заговора нефте- и газодобывающих компаний.

Причины, ограничивающие распространение электромобилей на мировом авторынке, кроются в структуре источников необходимой им электроэнергии. Так, если мы обратимся к статистическим данным по энергетическому рынку Евросоюза, то увидим, что большая часть электроэнергии здесь вырабатывается за счет использования невозобновляемых энергоресурсов. Согласно данным Евростата, 26 % электроэнергии производится на атомных электростанциях, ровно столько же за счет использования угля, 17 % за счет сжигания природного газа и 2 % – на основе нефтепродуктов. В сумме получаем 71 % экологически «грязной» электроэнергетики [5].

При этом не трудно подсчитать, что на, так называемые экологически чистые и возобновляемые источники электроэнергии приходится всего 29 %, в числе которых 3 % солнечная энергия, 5 %энергия, получаемая за счет переработки биомассы, 0,2 % геотермальная энергия, 11 % водная и 10 % ветряная энергия.

В России преобладают электростанции на газовом топливе (около 50 %). Существенную часть составляют АЭС (порядка 16 %) и гидрогенерация (порядка 18 %). На долю угля приходится около 15 %. Доля произведенной электроэнергии из нефти и возобновляемых источников очень невелика [6].

Что же касается энергетического рынка США, то в основном электричество вырабатывается ТЭС (70 %, из которых 56 % дают угольные ТЭС), ГЭС (10 %) и АЭС (17 %). Таким образом, в энергобалансе страны преобладает выработка тепловой энергии. Наиболее крупными энергетическими объектами в США (по видам) являются: ГЭС «Гранд-Кули» (установленная мощность – 6 809 МВт), АЭС «Уинтерсберг» (3 942 МВт), ТЭС «Навахо» (2 250 МВт), ВЭС «Альта Винд Энерджи Центр» (1 020 МВт) [7].

Таким образом, становится очевидным, что большая часть электроэнергии в мировой экономике вырабатывается за счет использования невозобновляемых источников энергии. Причем низкая доля возобновляемых источников обусловлена вовсе не нежеланием властей или представителей бизнеса развивать зеленую энергетику, а, в первую очередь, техническими и климатически-природными естественными ограничениями, преодолеть которые в обозримой перспективе возможным не представляется.

В создавшихся условиях, интенсификация развития рынка электромобилей не только не решит имеющихся экономических и экологических проблем, но напротив существенно усугубит их. Ведь растущее число электрокаров приведет к значительному росту потребления объемов электроэнергии, компенсировать который придется за счет повышения доли использования невозобновляемых и неэкологичных источников.

Наряду с вышеизложенным следует отметить, что проблемы развития рынка электромобилей не ограничиваются энергетической сферой. Существенное значение имеют как юридические, так и социальные аспекты.

Так, например, и в нашей стране, и за рубежом, законодатель уделяет первоочередное внимание стимулированию продаж электрокаров, посредством предоставления широкого спектра налоговых и иных льгот их владельцам. В то же самое время, вопросы безопасности эксплуатации автомобилей данной категории остаются за пределами правового поля. Между тем, несмотря на все

плюсы использования электрокаров, имеются и существенные факторы риска. Так, общеизвестно, что электродвигатель, особенно в сравнении с двигателем внутреннего сгорания, работает практически бесшумно. Данный факт в значительной степени увеличивает риск наезда электромобилей на пешеходов. Указанная особенность требует не только соответствующих законодательных инициатив, но и вызывает необходимость развития культуры использования индивидуальным электротранспортом.

Таким образом, прежде, чем интенсифицировать темы развития рынка автомобилей с электрическими двигателями, целесообразно обеспечить создание жизненно необходимо для данной отрасли инфраструктуры, законодательной базы и этических норм.

На основании всего вышеизложенного и с учетом новейших достижений теории и практики дальнейшего развития энергетического сектора, как отдельно рассматриваемых национальных экономик независимых государств, так и мировой хозяйственной системы в целом, в целях повышения эффективности процессов электрификации автомобильного транспорта представляется целесообразной разработка и реализация следующих безотлагательных мероприятий.

1. Всемерно стимулировать развитие рынка возобновляемых источников энергии.

2. Решить вопрос создания широкой сети заряжающих станций и центром технического обслуживания электромобилей.

3. Разработать соответствующую национальную и международную законодательную базу, регламентирующую развитие «зелёной» энергетики, а также особенности эксплуатации и обслуживания электрокаров.

4. Принять превентивные меры по развитию культуры использования электрического автотранспорта физическими лицами.

Реализация на практике предложенных выше мероприятий позволит создать необходимые условия и предпосылки для развития рынка электромобилей, как в Российской Федерации, так и за ее пределами.

Литература:

1. *Фомичев А.Н.* Проблемные аспекты диагностики и

конструктивизации управленческих дисфункций в условиях глобальной цифровизации мировой экономики / Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы: Сборник научных трудов, Челябинск, 31 января 2022 года. – Челябинск: Челябинский филиал РАНХиГС, 2022. – С. 134-138.

2. *Фомичев А.Н.* Оптимизация стратегического управления деятельностью организации // Экономические системы. – 2022. – Т. 15. – № 1. – С. 129-135. – DOI: 10.29030/2309-2076-2022-15-1-129-135.

3. *Костерева М.* Глава АвтоВАЗа считает, что в 2023 году компания сможет восстановить почти всю модельную линейку / Газета «Коммерсантъ». 06.09.2022. – URL: https://www.kommersant.ru/doc/5547631 (дата обращения 02.09.2022).

4. *Фомичев А.Н.* Управление коммуникативными дисфункциями в условиях глобализации информационных процессов // Проблемы теории и практики управления. – 2022. – № 1. – С. 51-61. – DOI: 10.46486/0234-4505-2022-01-51-61.

5. *Фомичев А.А.* Внедрение компьютерных технологий в систему управления таможенными органами / Компьютерные технологии в моделировании, управлении и экономике: Сборник материалов XIV студенческой всероссийской научно-практической конференции с международным участием, Орел, 17 марта 2022 года. / Под общей редакцией А.В. Полянина. – Орел: Среднерусский институт управления – филиал РАНХиГС, 2022. – С. 88-91.

6. *Карпов К.* Как устроен рынок электроэнергии в России / БКС Экспресс. 18 февраля 2019. – URL: https://bcs-express.ru/novosti-i-analitika/kak-ustroen-rynok-elektroenergii-v-rossii (дата обращения 02.09.2022).

7. *Фомичев А.А.* Адаптация системы обучения персонала организации к социально-экономическим условиям развития современной экономики / Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы: Сборник научных трудов, Челябинск, 31 января 2022 года. – Челябинск: Челябинский филиал РАНХиГС, 2022. – С. 130-134.

III. Проблемы обеспечения информационной безопасности

DOI: 10.25728/iccss.2022.75.12.017

Курако Е.А.

К вопросу безопасности отечественного программного обеспечения

Аннотация: Рассмотрена разработка программного обеспечения для отечественных операционных систем общего назначения с использованием документации и примеров, расположенных на сайтах операционных систем. Поднят вопрос о качественном подборе материалов для создания безопасного программного обеспечения.

Ключевые слова: программное обеспечение, документация, разработка, операционная система, безопасность

Количество задач, возникающих в области создания программного обеспечения, достаточно велико. Основными проблемами являются возрастающая сложность кода и архитектуры приложений, и, как следствие, высокий начальный порог вхождения в эту область. Непрерывное совершенствование и исследование новых методов разработки безопасности программного обеспечения [1] и обработки данных добавляет значительный объем необходимой для изучения информации. В то же время, в рамках импортозамещения [2], возникает срочная потребность в разнообразных программах для отечественных операционных систем (ОС) общего назначения. Процесс обучения в учебных заведениях, как правило, направлен на получение базовых фундаментальных знаний и не успевает за быстроменяющимися тенденциями.

Известно, что операционная система, сама по себе, без прикладных программ не интересна пользователям. И для развития ее окружения необходимо создание (адаптация) большого количества приложений. Как пример, можно рассмотреть мобильную операционную систему HarmonyOS, когда Huawei

провела огромную компанию по привлечению разработчиков на свою платформу [3].

Безопасность системы определяется самым слабым звеном. Таким образом, сторонние приложения должны советовать уровню операционной системы. Сторонний разработчик должен оперативно разобраться в организованной системе безопасности ОС для создания надежного программного продукта. Ввиду постоянного совершенствования ОС, основным источником сведений о ней и ее механизмах является официальный веб-сайт.

Рассмотрим раздел официальных сайтов основных отечественных операционных систем, посвященный разработке приложений и механизмам защиты.

Альт Линукс СПТ (Разработчики: ООО «Свободные программы и технологии», «Базальт СПО»)

На сайте присутствует раздел с документацией и есть описание некоторых особенностей при разработке программ для системы. К сожалению, раздел, посвященный разработке безопасных приложений, отсутствует. Хотя стоит отметить, что сообщество разработчиков приглашает вступить в их ряды, где новичку организуют помощь на начальном этапе. Так же есть раздел с книгами и тезисами докладов, посвящённый разработке ПО.

Astra Linux (НПО «Русские базовые информационные технологии»)

Портал Astra Linux достаточно объемный по содержанию, сложно структурирован, но в нем есть информация для разработки приложений интегрирующихся с механизмами безопасности системы, например, «Руководящие указания по конструированию прикладного программного обеспечения для операционной системы общего назначения Astra Linux Common Edition». На сайте есть форум и раздел с бюллетенями, содержащие обновляющиеся методики и обновления программного обеспечения для нейтрализации угроз уязвимостей в информационных системах.

Ред ОС и GosLinux (Разработчик: компания «Ред Софт»)

На сайтах этих систем никакой информации не представлено. Есть документация для пользователя и для администратора.

ROSA Linux (Разработчик: ООО «НТЦ ИТ РОСА»)

Сайт имеет ярко выраженную рекламную направленность. На главной странице присутствует ссылка на раздел «Разработчикам», где можно перейти на форум или на википедию, посвященную Rosa Linux. Дополнительно новичкам создали группу на сайте vk.com, где обещают помощь. Но раздела, повещённого методикам безопасного программирования, нет.

Эльбрус (Разработчик: АО «МЦСТ»)

Сайт операционной системы «Эльбрус» для разработчика лаконичен. Ему предлагается приобрести «Набор разработчика «Эльбрус Линукс» (PDK)», в котором есть примеры, документы и даже исходники компонентов системы. Для приобретения набора необходимо прислать официальный запрос в отдел продаж.

В целом можно сделать вывод о слабом распространении методик и результатов исследований, направленных на создание защищённого программного обеспечения. С одной стороны, идет исследование новых и усовершенствование существующих моделей, методов, алгоритмов, эти результаты отражаются в обновляющихся нормативных документах. С другой стороны, есть запрос разработчиков (как начинающих, так и переквалифицирующихся) на актуальную документацию, позволяющую вести разработку приложений для отечественных операционных систем с современными механизмами защиты. В то же время, разработчики отечественных систем, как правило, не спешат делиться наработанным опытом.

Литература:

1. *Девянин П.Н., Тележников В.Ю., Хорошилов А.В.* Формирование методологии разработки безопасного системного программного обеспечения на примере операционных систем // Труды ИСП РАН. – 2021. – Том 33. Вып. 5. – С. 25-40.

2. *Курако Е.А., Орлов В.Л.* К вопросу перевода информационных систем на отечественное программное обеспечение / Материалы 28-й Международной научной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС'2020, Москва). – М.: ИПУ РАН, 2020. – С. 246-249.

3. Huawei привлекает разработчиков в свой магазин

приложений. – URL: https://new-science.ru/huawei-privlekaet-razrabotchikov-v-svoj-magazin-prilozhenij/ (дата обращения 01.10.2022).

DOI: 10.25728/iccss.2022.52.24.018

Курако Е.А., Орлов В.Л.

Принципы обеспечения безопасности при использовании сервис-браузерной технологии

Аннотация: Рассматриваются вопросы защиты информации при использовании сервис-браузерной технологии. Выделяются уровни обеспечения безопасности. Определяется возможность использования сервис-браузера для защиты информационных систем.

Ключевые слова: сервис-браузер, клиент, сервер, средства защиты, безопасность, хранилище, аутентификация, авторизация

В качестве клиентов для информационных систем могут использоваться сервис браузеры [1, 2]. Сервис-браузер, в отличие от обычного браузера, имеет компонент, выполняющийся на клиенте (клиент браузера), и компонент (сервис браузера), выполняющийся на сервере (рисунок 1). Кроме того, на сервере (может быть отдельном) размещается хранилище данных браузера.

Причем каждый компонент включает три фрагмента.

- Фрагмент загрузки и обновления.
- Фрагмент обеспечения безопасности.
- Фрагмент организации запуска и завершения модулей.

В настоящей работе рассматривается фрагмент обеспечения безопасности, поэтому сосредоточимся на описании основных принципов, на которых базируется его разработка.

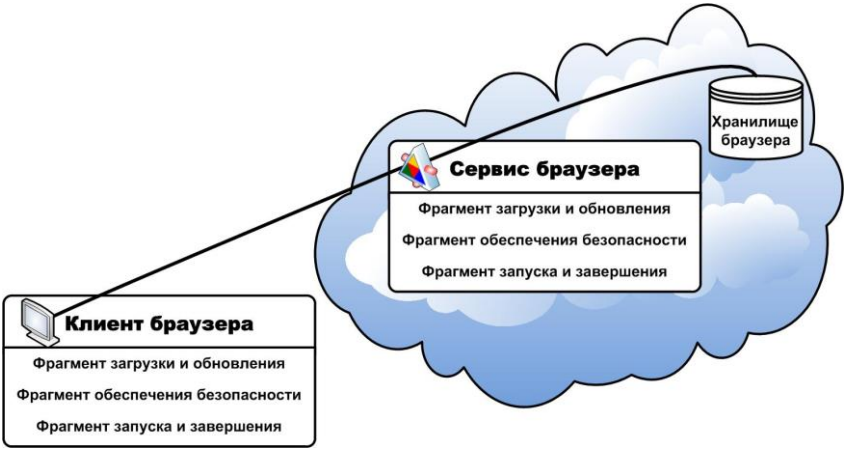


Рисунок 1 – Структура сервис-браузера

Ниже (рисунок 2) представлен краткий перечень базовых средств, использующихся при организации защиты информации в сервис-браузере.

Средства защиты клиента	Средства защиты сервера	Защита хранилища
Идентификация сеансов Авторизация Аутентификация HTTPS	Идентификация сеансов Авторизация Аутентификация HTTPS	Средства защиты БД

Рисунок 2 – Базовые средства защиты сервис-браузера

Так как фрагмент обеспечения безопасности присутствует как в клиентской, так и в серверной части, и более того, на клиенте и сервере существуют сопрягаемые средства, то для таких средств допускается различная реализация программного обеспечения. То есть, например, авторизация для различных сервис-браузеров может быть реализована по-разному, важно лишь то, что клиентские и серверные компоненты выполняют свои функции и хорошо сопрягаются друг с другом.

На нижнем уровне рекомендуется использовать HTTPS, так как существующие средства реализации протокола хорошо отлажены и обеспечивают высокий уровень защиты.

На следующем уровне проводится аутентификация, по существу, представляющая надежное определение пользователя. Обычно пользователь проверяется либо по сертификату, либо по паре «логин-пароль».

Если используется сертификат (чаще всего размещаемый на отдельном носителе), то обычно от сервиса получают случайную последовательность, подписывают ее электронной подписью и проверяют на сервисе. Если подпись верна, то из сертификата выбираются данные пользователя. Пользователь обычно имеет доступ к одной или нескольким информационным системам. Система может быть выбрана оператором из списка возможных.

Если на клиенте используется сочетание «логин-пароль» (вместе с идентификатором информационной системы), то эти данные следует проверить на сервисе. Для этого используется механизм хеширования. Как правило, на клиенте вычисляется хеш первого уровня, который определяется по значению строки, содержащей логин, пароль, константу. Затем формируется хеш второго уровня, где перед вычислением к хешу первого уровня добавляется значение текущего времени, и после вычисления – идентификатор информационной системы. Для передачи на сервер полученное значение обычно шифруется с использованием симметричного алгоритма.

На сервере путем расшифрования извлекается хеш. Из хранилища браузера также извлекается хеш первого уровня. Вычисляется хеш второго уровня с учетом времени и проводится сравнение хешей. Если сравнение прошло успешно, то по идентификатору системы определяется адрес системы. Таким образом, мы понимаем, какой пользователь к нам обратился, с какой информационной системой он хочет работать, и где располагается его система и пользовательская база данных этой системы.

То есть аутентификация завершена. Мы все, что необходимо, знаем о пользователе и его информационной системе.

Далее – авторизация. Мы на основании данных хранилища можем определить, какие пользовательские модули доступны обратившемуся к системе пользователю, какие действия он может

выполнять с использованием данных модулей. Таким образом, мы можем определить права данного пользователя относительно каждого приложения.

И наконец, очень важно, чтобы осуществленная аутентификация, проведенная авторизация действовали в течение определенного времени – сеанса пользователя. Отметим, что в рамках одного сеанса могут многократно вызываться сервисы, размещенные в серверной части. Если сеанс завершился, то для организации нового необходимо повторение процедур аутентификации и авторизации. И не только потому, что права пользователя за это время могли измениться. А главным образом потому, что каждое подключение к системе должно быть уникальным и санкционированным. То есть идентификатор сеанса должен формироваться с использованием криптосредств так, чтобы практически исключить возможность его вычисления со стороны злоумышленника. Идентификатор сеанса определяется в процессе проведении процедур аутентификации и авторизации и отменяется только при завершении сеанса.

Заметим, что для интеграции информационной системы с методами обеспечения безопасности сервис-браузера к каждому прикладному модулю должна подключаться клиентская библиотека, обеспечивающая взаимодействие со средствами защиты (получение параметров аутентифицированного пользователя, функции шифрования, дешифрования, обеспечения подписи). В каждом сервисе также происходит подключение к сервисной библиотеке, которая помимо обычных защитных функций обеспечивает строку подключения к хранилищу сервера, которое обычно реализуется как база данных.

Таким образом, сервис-браузер в процессе своей работы обеспечивает защиту информации для различных систем. Разработчики модулей таких систем не проектируют средства защиты, а только получают параметры при развертывании модуля для выполнения функций обеспечения безопасности и подключают соответствующие библиотеки сервис-браузера.

Литература:

1. *Курако Е.А., Орлов В.Л.* Сервис-браузеры для информационных систем // Программная инженерия. – 2017. – Том 8. №9. – С. 413-421.

2. *Курако Е.А., Орлов В.Л.* Организация защиты информации в системах, использующих сервис-браузеры / Материалы 26-й Международной научной конференции «Проблемы управления безопасностью сложных систем» (Москва, 2018). – М.: ИПУ РАН, 2018. – С. 109-112.

DOI: 10.25728/iccss.2022.61.68.019

Исхаков А.Ю.

Анализ запросов в протоколах прикладного уровня при реализации усиленной проверки подлинности субъектов доступа

Аннотация: При реализации эшелонированной защиты для критически важных объектов особое внимание уделяется снижению коэффициентов ложноположительных срабатываний средств защиты информации. В этой связи эффективным решением является разработка адаптивных многофакторных алгоритмов проверки подлинности, учитывающих особенности индикаторов компрометации и векторов предполагаемых атак в том числе в ходе инспектирования протоколов прикладного уровня. В рамках данного исследования рассматриваются признаки, доступные в ходе проведения инспекции HTTP-запросов при реализации усиленной проверки подлинности субъектов доступа.

Ключевые слова: протокол прикладного уровня, анализ запросов, индикатор компрометации, усиленная проверка подлинности, кибератака

В настоящее время в ходе инструментального анализа кибербезопасности различных объектов критической инфраструктуры исследователи продолжают фиксировать большое количество уязвимостей, связанных с интерфейсами доступа,

функционирующих на прикладном уровне. Так, на рисунке 1 представлена выдержка из ежегодно публикуемого общедоступного отчета компании Positive Technologies [1].

В этой связи, при построении защищенного периметра необходимо особое внимание уделять обеспечению защиты веб-сервисов, а также других интерфейсов взаимодействия прикладного уровня [2].

Сервис	Высокий риск, эксплойт	Высокий риск	Средний риск, эксплойт	Средний риск	Низкий риск
Веб-сервисы	24	609	344	3659	1507
Удаленный доступ	110	192	234	452	441
Служба доменных имен	36	183	21	227	15
Электронная почта	—	10	102	598	437
VPN-сервисы	—	—	12	30	24
Файловые службы	—	—	4	49	19
Другие	—	7	14	72	51

Рисунок 1 – Распределение уязвимостей по сервисам и уровням риска

При разработке алгоритмического обеспечения для усиленной проверки подлинности субъектов актуальной является задача реализации адаптивного подбора дополнительно проверяемых факторов. Для реализации механизмов, осуществляющих адаптацию набора, типа факторов, а также подбора безопасных для конкретной операции технологии транспорта данных необходимо осуществлять автоматизированную оценку риска угрозы при нетипичном поведении субъекта в режиме времени, близком к реальному.

В ходе проведения данного исследования был проведен обзор возможных индикаторов компрометации, применяемых для решения данной задачи. Под индикаторами компрометации понимаются исключительно технические категории IOC [3], т.е. цифровые артефакты, явно указывающие на потенциальную вредоносность

описываемого запроса и/или факт компрометации защищаемого объекта. При этом, в качестве ограничения выступает соответствие протоколам прикладного уровня. В ходе инспекции предлагается осуществлять анализ всех запросов, поступающих от субъектов доступа, с целью проверки фактов:

– обращения к не содержащимся в WL (white list) списке доступа URL/URI, использование нелегитимных значений host и т.д.;

– несоответствия используемых токенов безопасности;

– наличия артефактов Slowloris атак [5];

– ограничений на список используемых методов HTTP;

– фактов превышения пороговых значений на длину HTTP-запроса;

– превышение общей длины всех HTTP-заголовков;

– время подготовки ответа по заголовкам и телу запроса.

Не менее важным является проведение глубокого анализа тела запроса, включая поиск индикаторов по наличию хеш-значений из TI-платформ, анализ по преднастроенным шаблонам регулярных выражений, выявление различных инъекций и т.д.

Использование вышеуказанных индикаторов в ходе анализа запросов в протоколах прикладного уровня позволяет реализовывать эффективные механизмы усиленной проверки подлинности субъектов доступа за счет обогащения анализируемых индикаторов в произвольном теле запроса с помощью автоматизированных проверок других его составных элементов.

Исследование выполнено при финансовой поддержке РНФ (проект №21-71-00125)

Литература:

1. Уязвимости периметра корпоративных сетей Результаты инструментального анализа защищенности. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/vulnerabilities-corporate-networks-2020-rus.pdf (дата обращения 15.10.2022).

2. *Баранова Е.М.* Анализ современных систем защиты Web-сервисов // Известия ТулГУ. Технические науки. – 2018. – №10. – С. 93-100.

3. *Дрянных Ю.Ю., Жуков В.Г.* Автоматизация сбора, проверки и загрузки индикаторов компрометации в платформу Threat

Intelligence / Актуальные проблемы авиации и космонавтики: Сборник материалов V Международной научно-практической конференции, посвященной Дню космонавтики. В 3-х томах. Том 2. – Красноярск: Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, 2019. – С. 225-227.

4. *Исхаков А.Ю., Мещеряков Р.В., Исхаков С.Ю.* Проблемы применения индикаторов компрометации для проактивного поиска угроз в работе робототехнических комплексов / Управление развитием крупномасштабных систем (MLSD'2021): Труды Четырнадцатой международной конференции (Москва, 27-29 сентября 2021 года) / Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2021. – С. 1340-1347.

5. *Силаков Н.В*. Метод обнаружения аномальных вторжений в компьютерной сети, использующий критерий Фишера // Научно-образовательный журнал преподавателей и студентов «StudNet». – 2020. – № 10. – С. 1-13.

DOI: 10.25728/iccss.2022.17.30.020

Жарко Е.Ф.

Управление требованиями, верификация и валидация программного обеспечения АСУ ТП АЭС

Аннотация: Верификация и валидация важных этапов обеспечения безопасности и надежности программного обеспечения. Управление требованиями играет важную роль в рамках всех этапов верификации и валидации. В работе представлена схема управления требованиями для программного обеспечения систем, важных для безопасности АЭС, а также связь этого процесса с верификацией и валидацией.

Ключевые слова: программное обеспечение, верификация, валидация, управление требованиями, АСУ ТП АЭС

Системы верхнего уровня (СВУ) являются важной составляющей АСУ ТП АЭС. Верификация и валидация (V&V) [1] являются необходимыми этапами в обеспечении качества

программного обеспечения [2]. Безопасность и надежность программного обеспечения, применяемого в СВУ, должны быть продемонстрированы и подтверждены в процессе верификации и валидации.

Управление требованиями – это систематический подход к получению, организации и документированию системных требований, а также процесс, позволяющий заказчикам и разработчикам достигать и согласовывать меняющиеся системные требования. Наряду с этим, управление требованиями является важной составляющей обеспечения качества при разработке систем важных для безопасности АЭС в целом. Управление требованиями включает в себя управление изменениями требований, управление версиями требований отслеживанием требований, которые предоставляют собой повторно используемые и отслеживаемые доказательства для верификации программного обеспечения.

В соответствии со стандартами [3-5] построим модель B&B на основе B&B проекта в сочетании с текущей ситуацией с требованиями к программному обеспечению и процесса проектирования систем для АЭС. На рисунке 1 представлена взаимосвязь процессов верификации и валидации применительно к любому этапу.

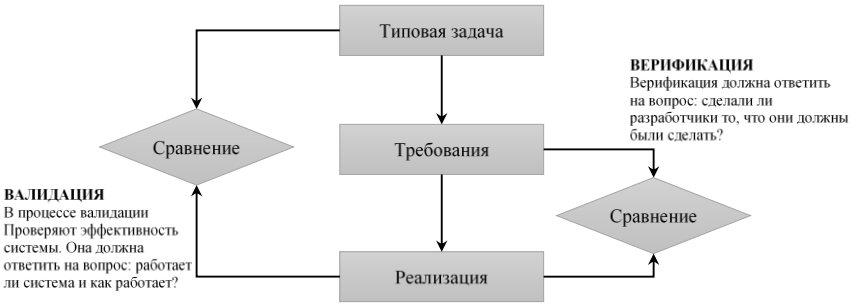


Рисунок 1 – Взаимосвязь верификации и валидации

На рисунке 2 показано, как в соответствии с разработкой и реализацией системных требований и требований к программному обеспечению подсистем АСУ ТП, формальная модель верификации и верификации делит процесс B&B на 5 этапов, включая B&B концепции, B&B требований, B&B проекта, B&B реализации и

испытания (тестирование). На каждом этапе проверяют входные и выходные данные, присущие специфике этапа. Этап испытания (тестирование) включает в себя интеграционные испытания, подтверждающие требования к программному обеспечению, и приемочные испытаний, подтверждающие системные требования.

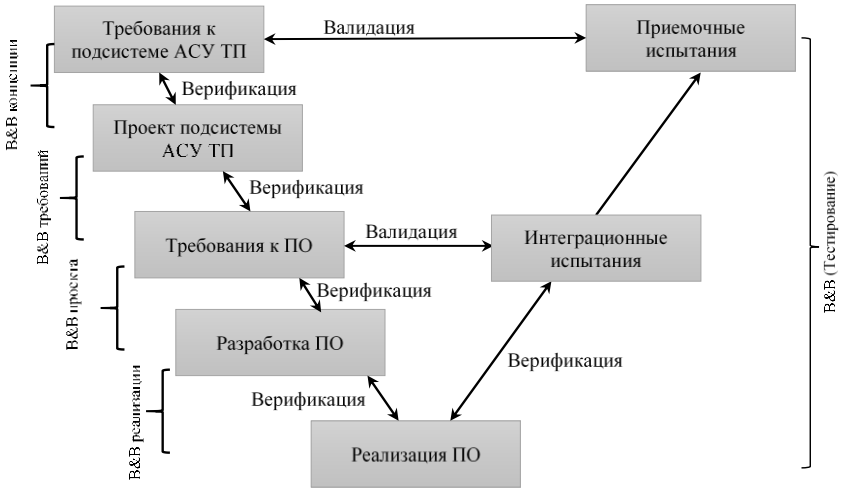


Рисунок 2 – Формализованная модель B&B

В соответствии с взаимосвязями входных и выходных данных строится модель управления требованиями на основе трех аспектов: управление версиями требований, управление изменениями требований и управление отслеживанием требований. Отслеживание требований является основным содержанием управления требованиями. Модель (рисунок 3) устанавливает базовую линию для каждой совокупности требований в части управления версией, выполняет отслеживание требований на каждом этапе. При изменении требований базовый уровень должен быть обновлен, а процесс управления требованиями после обновления необходимо повторить и убедиться, что изменение требований в исходной совокупности было повторно реализовано в исходной совокупности с сохранением согласованности и прослеживаемости.

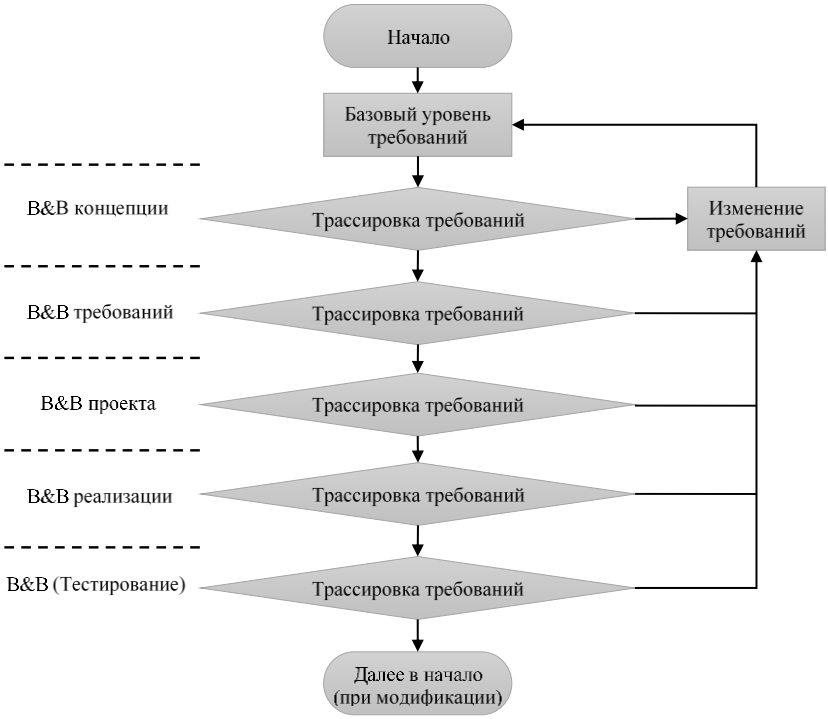


Рисунок 3 – Модель B&B и управление требованиями

Представленные модели B&B и управления требованиями повышают эффективность прослеживаемости, повышают качество разработки программного обеспечения систем, а также предоставляют методическое обеспечение для программы управления требованиями для систем, важных для безопасности АЭС.

Литература:

1. ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. – М.: Стандартинформ, 2011. – 106 с.

2. *Жарко Е.Ф.* Оценка качества программного обеспечения для систем, важных для безопасности АЭС // Информационные технологии и вычислительные системы. – 2011. – № 3. – С. 38-44.

3. ГОСТ Р МЭК 60880-2010. Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А. – М.: Стандартинформ, 2011. – 90 с.

4. ГОСТ Р МЭК 62138-2021. Атомные электростанции. Программное обеспечение систем контроля и управления атомной станции, выполняющих функции безопасности категорий В и С. Общие требования. – М.: Российский институт стандартизации, 2022. – 46 с.

5. IEEE Std 1012-2016. IEEE Standard for System, Software, and Hardware Verification and Validation. – IEEE, 2017. – 260 p.

DOI: 10.25728/iccss.2022.22.70.021

Тимиршаяхова Ю.В., Шагин Н.А.

Преимущества и недостатки классических методов нахождения лиц

Аннотация. В настоящее время вопросы информационной безопасности стали главной задачей для всего мира. Чтобы решить такую задачу создаются биометрические системы. В статье рассмотрены классические методы нахождения лиц по изображению. Проведен анализ достоинств и недостатков рассмотренных методов. Предлагается постановка задачи исследования выявления лиц по классическим методам.

Ключевые слова: алгоритмы нахождения лиц, метод главных компонент, Eigenfaces, линейный дискриминантный алгоритм, Fisherfaces, метод Виолы-Джонса

Во всех методах распознавания лиц основной задачей является нахождение лица на изображении. Популярные методы нахождения лиц делятся на два основных класса: классические (метод главных компонент, линейный дискриминантный алгоритм, метод Виолы-

Джонса,) и нейросетевые (использование искусственных нейронных сетей).

Работая с изображениями высокого разрешения, приходится сталкиваться со слишком большой размерностью векторного пространства. Если учесть, что, решая задачу распознавания лиц зачастую приходится работать с десятками, а иногда и с сотнями тысяч изображений в различных форматах, то большая размерность исследуемых данных может затруднить целевые вычисления. Данная проблема хорошо решается методом главных компонент (Principal Component Analysis – далее PCA) – один из основных способов уменьшить размерность данных, потеряв наименьшее количество информации.

В 1988 году Майкл Кирби и Лоуренс Сирович применили подход «собственных лиц» (Eigenfaces) с использованием линейной алгебры для анализа изображений [1]. Для разметки лиц они применяли менее 100 различных значений, доказав, что этого достаточно для точного кодирования изображения лица. Через три года технология Eigenfaces была усовершенствована использованием некоторых факторов окружающей среды, что в свою очередь помогло автоматизировать процесс распознавания. Перейдем к рассмотрению классического метода, в основе которого лежит вышеупомянутый PCA.

Математическое описание алгоритма Eigenfaces:

Пусть $X = \{x_1, x_2, \dots, x_n\}$ вектор признаков $x_i \in \mathbb{R}^d$.

1. Вычисление среднего и ковариационной матрицы

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{1}$$

$$S = \frac{1}{n}\sum_{i=1}^{n} (x_i - \mu)(x_i - \mu)^T \tag{2}$$

2. Вычисление собственных чисел λ_i и собственных векторов v_i матрицы S

$$Sv_i = \lambda_i v_i, i = 1,2,\dots,n \tag{3}$$

3. Упорядочивание собственных векторов по убыванию собственных значений т.е. k главных компонент – собственные векторы, соответствующие k наибольшим собственным значениям.

4. k главных компонент вектора x задаются формулой

$$y = W^T(x - \mu), \tag{4}$$

где $W = (v_1, v_2, \dots, v_3)$.

Исходя из PCA базиса находим

$$x = Wy + \mu \tag{5}$$

Другими словами, метод Eigenfaces выполняет распознавание лиц с помощью:

1) проецирования всей обучающей выборки в подпространство PCA по формуле (4).

2) проецирования целевого изображения в подпространство PCA по формуле (5).

3) поиска ближайшего соседа между проецируемыми изображениями, взятыми для обучения и целевым проецируемым изображением, взятым для распознавания.

На рисунке 1 приведены результаты по построению Eigenfaces на основе изображений из AT&T Facedatabase. Была использована палитра Jet для наглядности распределения значений оттенков серого внутри каждого собственного лица. Исходя из этого рисунка можно видеть, что каждый из Eigenfaces содержит в себе не только характерные признаки лица, но и информацию об освещенности. Это отчетливо видно на левой части #4 и правой части #5 лица.

Таким образом, основное преимущество алгоритма – это наличие возможности хранения и поиска изображения в больших базах данных. Недостатком является его чувствительность к внешним факторам. Если присутствуют значительные изменения в условиях входных данных, то эффективность Eigenfaces падает в связи с тем, что не учитывается классовое разделение, и поэтому при удалении некоторых компонент возможна потеря дискриминантной информации. Метод требует идеальных условий, таких как освещенность, ракурс, отсутствие растительности на лице, маски и

тому подобное. Например, во время пандемии эффективность применения данного метода была низкой, поскольку все ходили в масках, а метод выбирает подпространство так, чтобы предельно приблизить входной набор данных, а не разделять изображения на классы. Это может послужить причиной плохих результатов, в особенности, когда дело доходит до решения задачи классификации. Для решения этой причины используется линейный дискриминантный анализ (от англ. Linear discriminant analysis).

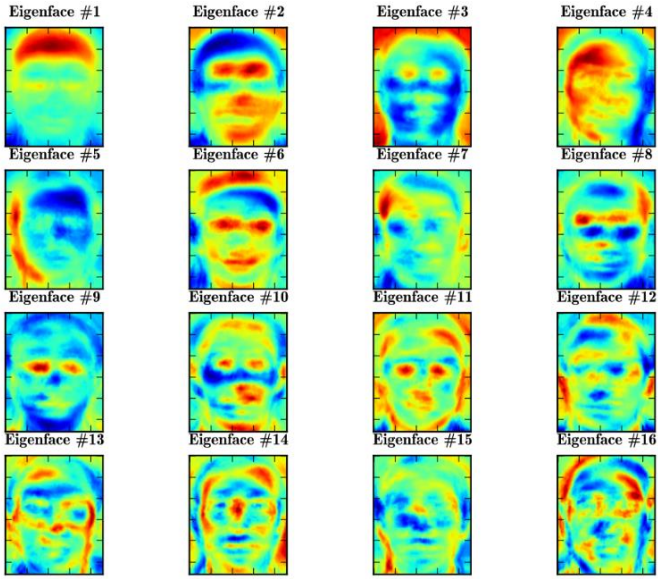


Рисунок 1 – Собственные лица в палитре Jet из AT&T database

Линейный дискриминантный алгоритм был создан в 1936 году Рональдом Фишером [2]. Идея линейного дискриминантного алгоритма в том, что необходимо найти линейную комбинацию признаков наилучшим образом, разделяющих два или более класса объектов или событий. Полученная комбинация используется в качестве линейного классификатора или для сокращения размерности пространства признаков перед последующей классификацией. Найденные линейные комбинации, полученные с помощью линейного дискриминанта Фишера, называют «Фишеровскими лицами» (от англ. Fisherfaces). Вкратце выбирается

проекция пространства изображения на пространство признаков таким образом, чтобы минимизировать внутриклассовое и максимизировать межклассовое расстояние в пространстве признаков. Смысл в том, что одни и те же классы должны плотно группироваться вместе [3, 4].

Математическое описание алгоритма Fisherfaces.

Пусть X – вектор выборок для с классов

$$X = \{X_1, X_2, \dots, X_c\}$$
$$X_i = \{x_1, x_2, \dots, x_n\}$$

Вычисляются следующие матрицы рассеивания

$$S_B = \sum_{i=1}^{c} N_i(\mu_i - \mu)(\mu_i - \mu)^T \quad (6)$$

$$S_W = \sum_{i=1}^{c} \sum_{x_j \in X_i} (x_j - \mu_i)(x_j - \mu_i)^T \quad (7)$$

$$\mu_i = \frac{1}{|X_i|} \sum_{x_j \in X_i}^{n} x_j - \text{среднее внутри класса}, i \in \{1, \dots, c\} \quad (8)$$

Геометрическая интерпретация матриц S_B и S_W для задачи с тремя классами (c=3) приведена на рисунке 2.

Классический алгоритм Фишера ищет проекцию W, которая максимизирует критерий разделения классов

$$W_{opt} = argmax_W \frac{|W^T S_B W|}{|W^T S_W W|} \quad (9)$$

Решение оптимизационной задачи получается из решения следующего базового уравнения линейной алгебры

$$S_B v_i = \lambda_i S_W v_i \quad (10)$$
$$S_W^{-1} S_B v_i = \lambda_i v_i \quad (11)$$

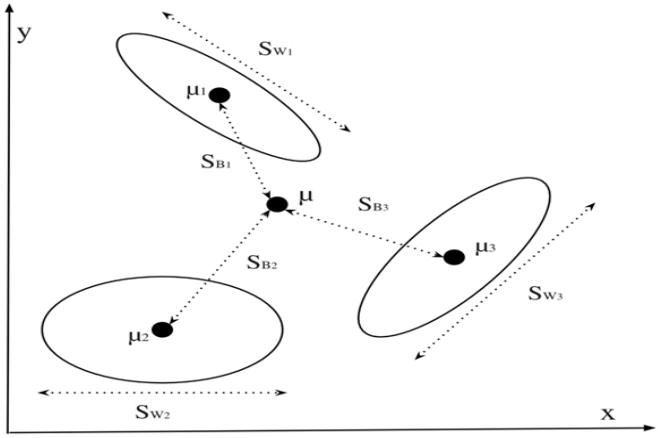


Рисунок 2 – Матрицы S_B и S_W для задачи с тремя классами (c=3)

Поскольку Fisherfaces предполагает наличие множества фотографий при разных условиях освещенности у каждого человека в базе данных, то преимуществом данного метода и является устойчивость к изменениям условиям освещенности (продемонстрировано на рисунке 3).

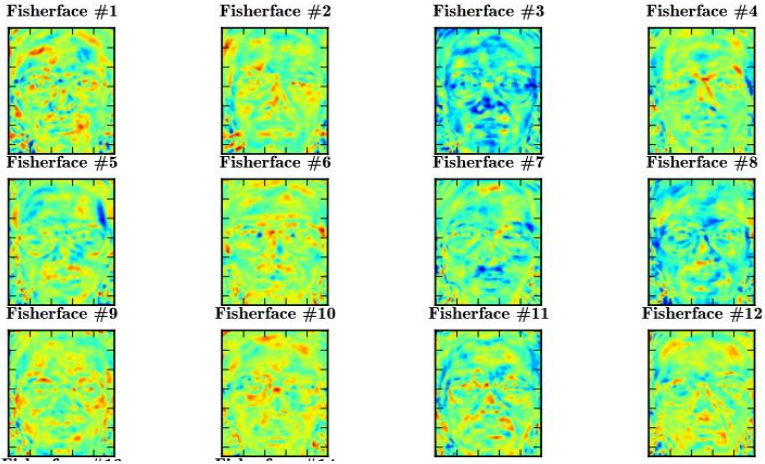


Рисунок 3 – 12 Fisherfaces на основе изображений из AT&T database

Дискриминантный анализ по определению помогает сфокусироваться только на основных лицевых признаках для решения классификационной задачи. Однако стоит отметить, что классический метод также чувствителен к входным данным. Например, если обучать алгоритм на освещенных объектах, а тестировать на слабоосвещенных, то в данном случае с высокой вероятностью метод будет выдавать ошибочные результаты при распознавании лиц.

Метод Виолы-Джонса был разработан Полом Виолой и Майклом Джонсоном в 2001 году. Данный метод получил широкое применение в силу своей скорости и минимальным ложным срабатыванием [5]. Идея алгоритма заключается в выделении локальных признаков изображения. То есть перед началом распознавания алгоритм обучения на базе изображений обучает классификатор, состоящий из значений определённых признаков. Затем алгоритм распознавания ищет объекты на разных масштабах изображения, основываясь на обученном классификаторе. На выходе алгоритма выдаётся большое число обнаруженных объектов на разных масштабах. Алгоритм Виолы-Джонса использует принципы: признаки Хаара; AdaBoost.

Как было описано выше, алгоритм выделяет признаки изображения. Признаки, которые использовали П. Виола и М. Джонсон базируются на каскадах признаков Хаара. Данные признаки использовали, чтобы уйти от пиксельного представления с сохранением скорости вычисления признака. Признаки Хаара представляют собой прямоугольные области, которые составлены из нескольких соседних прямоугольных областей, отмеченных как светлая или темная. Каждый признак способен продемонстрировать наличие или отсутствие того или иного свойства изображения. Например, признак из двух смежных прямоугольных областей способен продемонстрировать в каком месте расположена граница между темным и светлым, легко сможет отразить темнее область глаз и светлее область носа. Наклонные признаки позволяют определить наличие края под углом 45 градусов.

AdaBoost – алгоритм машинного обучения, предложенный Йоавом Фройндом и Робертом Шапиром [5]. AdaBoost во время обучения строит каскад из базовых алгоритмов обучения с целью

улучшить эффективность, то есть каждый следующий алгоритм строится так, чтобы компенсировать недостатки предыдущих.

Преимущества алгоритма в легкости реализации, в наличии навыка к обобщению (алгоритм дополняет точность обучения, превосходя по качеству базовые алгоритмы). Также имеются и недостатки алгоритма: чтобы обучить алгоритм необходимо давать большое количество выборок; алгоритм иногда строит большие каскады из базовых алгоритмов в следствие чего повышается время обучения и затраты на память для хранения каскадов.

Из выше сказанного метод Виолы-Джонса имеет ряд преимуществ такие как: способность распознавать любые объекты, следует только обучить каскад-классификаторов; высокая точность распознавания; подходит для распознавания в реальном времени. Так же, как и у всех алгоритмов у метода Виолы-Джонса имеются недостатки: длительное время на обучение каскадов классификаторов, при угле наклона больше 30° вероятность обнаружения лица резко падает [6].

Заключение

Рассмотренные в статье классические методы нахождения лиц имеют достоинства и недостатки. В дальнейшем планируется рассмотреть популярные архитектуры нейронных сетей, выделить их преимущества и недостатки и определить алгоритмы, которые не имеют приведенные недостатки.

Литература:

1. *Kirby M., Sirovich L.* Application of the Karhunen-Loeve procedure for the characterization of human faces // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1990. – Vol. 12. № 1. – P. 103-108. DOI: 10.1109/34.41390

2. Линейный дискриминантный анализ. – URL: https://ru.wikipedia.org/wiki/Линейный_дискриминантный_анализ (дата обращения 08.08.2022).

3. *Левчук С.А., Якименко А.А.* Исследование характеристик алгоритмов распознавания лиц // Сборник научных трудов НГТУ. – 2018. – № 3-4 (93). – С. 40-58.

4. *Исаев А.Л., Газаров Д.А., Евсеев С.Д.* Распознавание лиц по изображениям // Символ науки: международный научный журнал. – 2017. – Т. 2. № 4. – С. 70-76.

5. *Тымчук А.И.* Метод Виолы-Джонса для распознавания объектов на изображении // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2017. – №6. – С. 63-68.

6. *Мищенкова Е.С.* Сравнительный анализ алгоритмов распознавания лиц // Вестник Волгоградского государственного университета. Серия 9. Исследования молодых ученых. – 2013. – № 11. – С. 74-76.

DOI: 10.25728/iccss.2022.52.62.022

Козлов А.Д., Нога Н.Л.

Метод усредненных коэффициентов влияния для формирования нечеткой базы знаний при оценке рисков информационной безопасности

Аннотация: Предложен метод, позволяющий сократить трудозатраты для формирования продукционных правил (нечеткой базы знаний) при определении рисков информационной безопасности с использованием методов нечеткой логики.

Ключевые слова: риски, информационная безопасность, нечеткая логика, продукционные правила, коэффициенты влияния

Широкое внедрение цифровизации в экономику связано с появлением новых вызовов и угроз. Особенно важно учитывать эти вызовы и угрозы в условиях жестких санкций. При эксплуатации информационных систем, особенно КИИ, требуется постоянно мониторить и оценивать риск информационной и кибербезопасности.

Принципы руководства и технологии обеспечения менеджмента риска определены нормативными документами [1, 2].

Методов оценки риска существует достаточно много. Все они имеют свои плюсы и минусы. У большинства из них присутствует существенный недостаток – они плохо работают в условиях неопределенности. В работе [3] предложена методика оценки риска с использованием методов нечеткой логики. Данная методика

позволяет осуществлять оценки поиска информационной безопасности по множеству параметров в условиях неочевидности взаимосвязи между параметрами.

Указанная методика подразумевает построение нечеткой базы знаний (совокупности продукционных правил). При оценке риска по шести и более параметрам количество этих правил может достигать нескольких тысяч. Что в свою очередь вызывает определенные трудности при расчетах рисков.

В дальнейшем данная база знаний может быть использована как для оценки риска средствами пакета Matlab [4], так и для последующей обработки методами регрессионного анализа [5] для определения наиболее критичных для оценки риска показателей.

Чтобы облегчить задачу создания нечеткой базы знаний на первичном этапе оценки риска авторы предлагают использовать метод усредненных коэффициентов влияния.

В общем виде риск можно представить как некоторую функцию R из (1), зависимую от N параметров.

$$R = R\,(y_1, \ldots, y_i, \ldots, y_N) \qquad (1)$$

Каждый параметр, включая риск, можно охарактеризовать как качественно, так и количественно. Количественное значение для удобства сравнения различных параметров лучше нормировать, т.е. чтобы их значения изменялись в пределах от 0 до 1. При этом в определенных границах терма качественное значение (значение лингвистической переменной) будет постоянным.

Значения лингвистической переменной могут быть разными, но они должны характеризовать переменную в пределах указанного терма. Например, лингвистическая переменная – уровень затрат может принимать значения: *низкий, средний, высокий, значительный.* Или лингвистическая переменная – уровень износа оборудования может принимать значения: *незначительный, низкий, средний, высокий, критический*.

Количество термов для разных переменных может быть различным. Чем их больше, тем точнее получается конечный результат, но усложняются вычисления. Будем считать в нашем примере количество нечетких переменных в терм-множестве для всех лингвистических переменных равным T. Пример терм-

множества для лингвистических переменных приведен в таблице 1, где Ly_{lt} представляет собой нечеткую переменную для y_i-й лингвистической переменной, а $[y'_{it}; y''_{it}]$ – границы значений терма.

Следует обратить внимание, что при использовании метода усредненных коэффициентов влияний необходимо, чтобы все параметры, по которым оценивается риск информационной безопасности, были однонаправленными, т.е. при увеличении уровня любого из параметров риск либо увеличивался, либо уменьшался.

Практически всегда любому параметру можно найти соответствующий антипод, при котором риск бы увеличивался с ростом уровня, а не уменьшался. Например, для лингвистической переменной *импортозамещение* (процент использования отечественного ПО) антиподом будет *использование зарубежного ПО*.

Таблица 1 – Терм-множество для лингвистических переменных

Лингвистические переменные	Нечеткие переменные	Границы терма
Риск, R	LR_1	$[R'_1; R''_1]$
	…	
	LR_t	$[R'_t; R''_t]$
	…	
	LR_T	$[R'_T; R''_T]$
y_1	Ly_{11}	$[y'_{11}; y''_{11}]$
	…	
	Ly_{1t}	$[y'_{1t}; y''_{1t}]$
	…	
	Ly_{1T}	$[y'_{1T}; y''_{1T}]$
…		
y_i	Ly_{i1}	$[y'_{i1}; y''_{i1}]$
	…	
	Ly_{it}	$[y'_{it}; y''_{it}]$
	…	
	Ly_{iT}	$[y'_{iT}; y''_{iT}]$
…		
y_N	Ly_{N1}	$[y'_{N1}; y''_{N1}]$

Лингвистические переменные	Нечеткие переменные	Границы терма
	…	
	Ly_{Nt}	$[y'_{Nt}; y''_{Nt}]$
	…	
	Ly_{NT}	$[y'_{NT}; y''_{NT}]$

На основе значений переменных в таблице 1 можно создать нечеткую базу (таблица 2), представляющую некоторую матрицу размерностью $M \times (N+1)$, где N – число показателей (лингвистических переменных), по которым рассчитывается риск, а M – количество строк в матрице, равное количеству вводимых продукционных правил.

Последний столбец представляет собой уровень риска.

Таблица 2 – Нечеткая база знаний, продукционные правила

y_1	…	y_i	…	y_N	R
Ly_{11}	…	Ly_{i1}	…	Ly_{N1}	LR_1
…					
Ly_{1T}	…	Ly_{iM}	…	Ly_{NM}	LR_M

Как правило, уровень риска в нечеткой базе определяется экспертным путем по каждой строке. Когда переменных много, а строк несколько тысяч, то такая работа становится очень трудоемкой, а подчас и совсем невыполнимой.

Авторами предложено провести экспертную оценку для каждой нечеткой переменной и указать усредненный коэффициент влияния K_{it} для каждого интервала значений (терма) (таблица 3).

Проведенные авторами исследования показали, что вполне достаточно, чтобы значения этих коэффициентов лежали в интервале от 0 до 10. Это позволяет получить значение уровня риска с приемлемой точностью.

Таблица 3 – Соответствие нечетких переменных усредненным коэффициентам влияния (для i-ой лингвистичекой переменной)

Лингвистическая переменная	Нечеткая переменная	Границы терма	Коэффициент влияния
y_i	Ly_{i1}	$[y'_{i1}; y''_{i1}]$	K_{i1}
	…		
	Ly_{it}	$[y'_{it}; y''_{it}]$	K_{it}
	…		
	Ly_{iT}	$[y'_{iT}; y''_{iT}]$	K_{iT}

Далее в таблице 2 заменим значения нечетких переменных на соответствующие значения коэффициентов влияния (таблица 4).

Таблица 4 – Нечеткая база знаний с коэффициентами влияния

	y_1	…	y_i	…	y_N	$\sum K$	Уровень риска, R
1	K_{11}	…	K_{i1}	…	K_{N1}	$\sum_{i=1}^{N} K_{i1}$	R_1
…	…						
M	K_{1M}	…	K_{iM}	…	K_{NM}	$\sum_{i=1}^{N} K_{iM}$	R_M

По каждой строке определяем суммарный коэффициент влияния $\sum K$ и находим максимум из этих сумм равный $\max\limits_{1 \le m \le M} \sum\limits_{i=1}^{N} K_{im}$.

Считаем, что этому максимуму соответствует и максимальное значение риска. Нечеткая переменная риска по каждой строке m ($1 \le m \le M$) будет определяться по формуле (2).

$$LR_m = \begin{cases} LR_T, & \text{если } \dfrac{\sum\limits_{i=1}^{N} K_{im}}{\max\limits_{1\le m\le M}\sum\limits_{i=1}^{N} K_{im}} > \dfrac{R'_T}{R''_T}; \\ LR_{T-1}, & \text{если } \dfrac{R'_T}{R''_T} \ge \dfrac{\sum\limits_{i=1}^{N} K_{im}}{\max\limits_{1\le m\le M}\sum\limits_{i=1}^{N} K_{im}} > \dfrac{R'_{T-1}}{R''_T}; \\ \ldots & \\ LR_1, & \text{если } \dfrac{R'_2}{R''_T} \ge \dfrac{\sum\limits_{i=1}^{N} K_{im}}{\max\limits_{1\le m\le M}\sum\limits_{i=1}^{N} K_{im}}. \end{cases} \quad (2)$$

Вывод

Предлагаемый метод позволяет существенно снизить трудоемкость по созданию нечеткой базы знаний при оценке рисков информационной или кибербезопасности, а соответственно сделать процедуру оценки рисков с использованием методов нечеткой логики более доступной.

Метод также легко реализуется в системах электронных таблиц (например, MS Excel) и пригоден для первичной оценки риска в различных информационных системах, включая сетевые структуры.

Литература:

1. ГОСТ Р ИСО 31000-2019 Менеджмент риска. Принципы и руководство. – М.: Стандартинформ, 2020. – 14 с.

2. ГОСТ Р 58771-2019 Менеджмент риска. Технологии оценки риска. – М.: Стандартинформ, 2020. – 86 с.

3. *Козлов А.Д., Нога Н.Л.* Риски информационной безопасности корпоративных информационных систем при использовании облачных технологий // Управление риском. – 2019. – № 3. – С. 31-46.

4. *Штовба С.Д.* Проектирование нечетких систем средствами MATLAB. – М.: Горячая линия-Телеком, 2007. – 288 с.

5. *Kozlov A., Noga N.* Applying the Methods of Regression Analysis and Fuzzy Logic for Assessing the Information Security Risk of Complex Systems / Proceedings of the 14th International Conference "Management of Large-Scale System Development" (MLSD). – M.: IEEE, 2021. – URL: https://ieeexplore.ieee.org/document/9600245 (дата обращения 10.10.2022).

DOI: 10.25728/iccss.2022.48.34.023

Абдулова Е.А.

Оценка критической информационной инфраструктуры: киберцели и оценка критичности

Аннотация: В работе рассмотрены кибер-цели и их характеристики, приведено сопоставление целей в физическом и кибер-пространствах и принципы их преобразования, рассмотрены уровни кибер-целей, показана разница в методологических подходах к оценке критичности и риска.

Ключевые слова: критическая информационная инфраструктура, киберсистема, кибер-цели, оценка риска, оценка критичности

Современное общество – это общество, основанное на знаниях, которое в значительной степени полагается на технологии для выполнения или поддержки выполнения задач или функций. В результате современное общество гораздо более уязвимо даже по сравнению с началом века.

Масштабы уязвимости обусловлены тем, что очень много выполняемых операций в какой-то момент поддерживается вводом, хранением и поиском данных и информации во взаимосвязанной сети жестких дисков и серверов данных. Более того, в каждом из этих моментов существует возможность кражи информации, обхода защит, манипулирования или диверсии. При этом не учитывается риск, связанный с непреднамеренными инцидентами, связанными с человеческим фактором, системными сбоями, несовместимостью или другими неожиданными проблемами, а также «стихийными бедствиями». Все больше и больше экспертов по безопасности

заявляют, что защита киберсистем и данных является более серьезной проблемой, чем терроризм, учитывая масштаб угрозы (относительно кибератак) и фактический ущерб, который ежегодно наносится (а также возможные последствия в случае компрометации определенных систем и структур) [1].

Приоритетной целью на сегодняшний день является обеспечение информационной безопасности объектов критической информационной инфраструктуры (КИИ), так и КИИ в целом [2]. Для успешной реализации мероприятий по обеспечению безопасности объектов КИИ и КИИ в целом необходимо решение целого ряда сложных научно-технических задач, из которых задача оценки текущего уровня безопасности объектов КИИ и КИИ в целом и прогнозирования его изменения является одной из ключевых [3].

Оценка критичности, наряду с оценками рисков, критической инфраструктуры, в том числе и КИИ, является важной задачей в комплексе задач по обеспечению защиты критической инфраструктуры. В 2014 году в США была разработана национальная система кибербезопасности, а в основу которой заложен подход, базирующийся на оценке риска, который помогает при столкновении с угрозами кибербезопасности, систематически рассматривать, что они собой представляют (люди, информация, объекты и т. д.), и каковы возможные последствия этих угроз, что можно сделать для устранения этих угроз, как отреагировать на угрозы, и что можно сделать, чтобы обеспечить быстрое восстановление [1].

Кибер-цели в критической инфраструктуре можно оценивать и классифицировать по целевым характеристикам. Каждая цель имеет определенные характеристики, которые составляют основу для обнаружения, определения местоположения, идентификации и классификации цели для последующего наблюдения, анализа, нападения и оценки. Можно выделить четыре категории характеристик, на основе которых можно определить обычные цели: физические, функциональные, когнитивные, экологические [4].

Основными характеристиками цели являются физические особенности: форма, внешний вид, количество и природа элементов, отражательная способность, структурный состав, степень упрочнения, электромагнитное излучение, местоположение, размер и дисперсия. Примером характеристик окружающей среды являются

особенности местности. К когнитивным функциям относятся, например, способ обработки информации целью, информация, которая требуется цели для функционирования, также сюда относятся процессы, которые выполняет цель, количество информации, которую может обрабатывать цель и как цель или система хранит информацию. Функциональные особенности – к ним относятся, например, какие материалы или ресурсы требуются цели для функционирования.

Преобразование физических и экологических характеристик в киберпространство может быть осуществлено путем преобразования их в виртуальные характеристики и функции информационной инфраструктуры. Физические характеристики будут преобразованы в виртуальные характеристики кибер-цели, такие как операционная система, необходимая эффективность процессора, необходимый объем памяти и форматы файлов или данных. Кибер-цель также может иметь интерфейс к физическому пространству, что позволяет злоумышленнику проникнуть в систему кибер-цели через физическое соединение. Характеристики среды будут учитывать характеристики сети, такие как сетевые протоколы, уровни, серверные операционные системы и базы данных, т.е. характеристики информационной инфраструктуры.

Функциональные характеристики учитывают, что выполняет кибер-цель. Например, такими характеристиками могут быть мобильность цели, способность ее защищаться и восстанавливаться. Эти характеристики у кибер- и обычной целей очень похожи. Когнитивные особенности кибер-цели – это, например, способы обработки информации, обработки ввода и вывода и способы хранения информации.

Общие физические и экологические характеристики должны быть преобразованы в виртуальные характеристики, а функциональные и когнитивные характеристики очень похожи в физическом и киберпространствах. Аналогия между физическими и кибер-характеристиками целей показана на рисунке 1.

Кибер-цель может быть разделена на разные категории в зависимости от уровня цели. Высшим уровнем концепции кибер-цели будет система кибер-цели, которая формируется из подсистем и является основной целью атаки. Это может быть, например, SCADA или система управления объектом критической

инфраструктуры. Кибер-целями будут отдельные функции и подсистемы, необходимые для функционирования всей системы.

Рисунок 1 – Аналогия между характеристиками обычных и кибер-целей

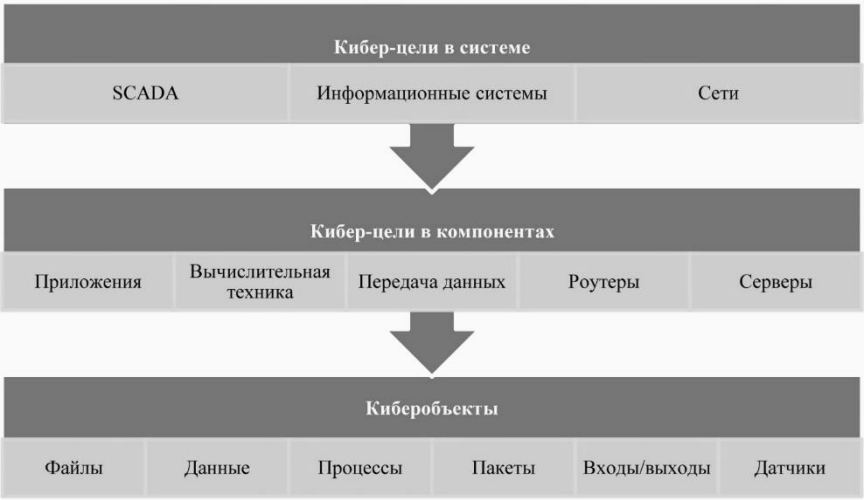


Рисунок 2 – Уровни кибер-целей

Объект кибер-цели — это часть кибер-цели, которая может быть уничтожена по отдельности, но необходима для работы целевой системы. Объектом кибер-цели может быть один процесс, файл, датчик или одна функция. Объекты кибер-цели автономны, соединяются вместе и формируют услугу. Уровни кибер-цели представлены на рисунке 2.

На уровне кибер-целей системы к целям можно отнести SCADA или другие информационные системы, сети и сетевые коммуникации или информационно-телекоммуникационная инфраструктура организаций, содержащая, например, хранилища данных, офисное программное обеспечение и системы обработки сертификатов безопасности. Сложная и распределенная структура этого уровня создает против нее несколько векторов атак.

Кибер-цель в системе также может быть гибридной, существующей как в киберпространстве, так и в физическом пространстве. В такой системе можно оказывать влияние на конечного пользователя через систему, даже если пользователь не существует в киберпространстве или целью может быть физическое устройство.

При оценке критичности критической инфраструктуры, включая КИИ, важно понимать разницу в методологических подходах к оценке критичности и риска (или рискового потенциала [5]). При оценке критичности объекта инфраструктуры в первую очередь учитывают оценку негативного воздействия инфраструктуры на население, общество, окружающую среду, экономику государства, национальную безопасность и т.д. То есть важно оценить ущерб, который был бы вызван, если бы объект перестал функционировать или был бы уничтожен. Вероятность инцидента считается равной единице. При анализе рисков сначала анализируют угрозу активам объекта и оценивают ущерб, который будет нанесен самому объекту. В этом принципиальное различие между подходами к оценке критичности и оценке риска.

Основными критериями, возникающими при оценке критичности объекта критической инфраструктуры, являются: воздействие на общество; экономический эффект; воздействие на окружающую среду; политическое влияние; влияние на национальную безопасность; оценка взаимозависимости, т.е. влияния на функционирование другой критической

инфраструктуры. При оценке также учитываются: масштаб воздействия (каскадные эффекты, географический масштаб и др.), временные характеристики – скорость проявления негативного воздействия, продолжительность воздействия, время восстановления безопасного состояния. Общий уровень критичности оценивается на основе анализа обобщенной нормативной оценки (сумма всех баллов по всем критериям) с последующим применением универсальной шкалы Харингтона [6].

Литература:

1. *Bullock J.A., Haddow G.D., Coppola D.P.* Cybersecurity and critical infrastructure protection (in book Introduction to Homeland Security Principles of All-Hazards Risk Management). – Elsevier, 2021. – P. 425-497

2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

3. *Калашников А.О.* Управление информационными рисками организационных систем: механизмы комплексного оценивания // Информация и безопасность. – 2016. – Т. 19. № 3. – С. 315-322.

4. Air Force Doctrine Publication 3-60, Targeting, U.S. Air Force, 2021. – URL: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf (дата обращения 25.10.2022).

5. *Абдулова Е.А., Калашников А.О.* К вопросу управления рисками критической информационной инфраструктуры / Труды 14-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD-2021). – М.: ИПУ РАН, 2021. – С. 1275-1282.

6. *Harrington E.C.* The Desirability Function // Industrial Quality Control. – 1965. – Vol. 21. № 10. – P. 494-498.

DOI: 10.25728/iccss.2022.61.95.024

Авдеева З.К., Коврига С.В.

Обнаружение изменений в социально-экономических ситуациях на основе разнородной информации

Аннотация: В работе представлены особенности процедуры ситуационного мониторинга на основе разнородной информации. Данный подход предполагает совместное использование методов обнаружения и обработки значимой качественной и количественной информации о наблюдаемой ситуации для формирования сигналов, предназначенных для решения целевых задач анализа, прогнозирования и управления.

Ключевые слова: социально-экономическая ситуация, неопределенность, мониторинг, когнитивная карта, сценарный анализ и моделирование

Введение

Мониторинг играет связующую роль в цикле управления, начиная с этапа целеполагания и прогнозирования развития управляемого объекта вплоть до этапа контроля исполнения планов и коррекции. Объектами мониторинга могут быть технические объекты и системы, а также геополитические, политические, социально-экономические и другие ситуации, в которых протекающие процессы и явления взаимосвязаны через регулярное влияние факторов внешней среды. В таких ситуациях нередко динамика процессов непредсказуема, прежде всего из-за неожиданных событий и (или) резких или множественных изменений в параметрах внешней среды, например, в случаях: 1) резкого перехода из одного состояния в другое, обусловленного событием, которое вызывает резкое изменение значений процесса; 2) нарушения или слабой выраженности сезонности в процессах при переходе от стабильного состояния к кризисному.

В зависимости от доступности и полноты информации по наблюдаемой ситуации применяются различные методы обработки обнаруженной мониторинговой информации – качественной и\или количественной. Традиционно в хорошо определенных ситуациях в

бóльшей степени используются модели и методы работы с количественными данными. По мере нарастания неопределенности развития наблюдаемой ситуации, ее усложнения из-за разнородности протекающих процессов (как правило, нестационарных) возрастает потребность в экспертной информации и применении методов на ее основе.

При мониторинге процессов количественными методами, преимуществом которых является возможность с определенной точностью обнаруживать структурные сдвиги, возникает задача объяснения обнаруженных изменений с одной стороны, а с другой по обнаруженным сигналам об изменении на основе качественной информации о ситуации выдавать сигналы о подтверждении изменений на уровне количественных данных. С одной стороны, при цифровом мониторинге нестационарных процессов необходимо снизить количество «ложных» сигналов об изменениях и соответственно при использовании процедур в задачах прогнозирования, планирования и управления не принимать их во внимание без подтверждения и объяснения в происходящих событиях, а с другой стороны необходимо повысить качество сигналов об изменениях, обнаруживаемых на основе качественной информации о ситуации и событиях. Другой проблемой мониторинга является неоднородность информационных массивов, характеризующих факторы ситуации.

В работе представлен подход к мониторингу на основе разнородной информации в зависимости от степени неопределенности параметров ситуации, где отслеживаются изменения наблюдаемого процесса и связанных с ним процессов. Данный подход предполагает совместное использование методов обнаружения и обработки значимой качественной и количественной информации о наблюдаемой ситуации для формирования сигналов, предназначенных для решения целевых задач в цикле управления. Количественная информация накапливается в виде временных рядов, отражающих закономерности поведения исследуемых процессов в ситуации. Качественная информация структурируется и формализуется в виде когнитивной карты ситуации (ККС) – формализованной модели экспертных представлений о причинно-следственных влияниях между факторами ситуации. Эти факторы отражают взаимосвязанность наблюдаемых процессов,

характеризующих объект управления, и его окружением – внешней средой.

Подход к мониторингу на основе разнородной информации. Общая характеристика

Укрупненная схема совместного мониторинга на основе разнородной информации приведена на рисунке 1.

Рисунок 1 – Укрупненная схема мониторинга (на примере использования количественных методов анализа временных рядов)

Согласно предложенному подходу, мониторинг социально-экономических ситуаций организуется в виде трех связанных компонент наблюдения, анализа и моделирования:

– традиционный мониторинг цифровых показателей наблюдаемых объектов, процессов в социально-экономических

ситуациях, представленных временными рядами;

– ситуационный мониторинг, основанный на обработке экспертной информации, формализуемой в виде ККС;

– управление взаимодействием обоих видов мониторинга и обработка сигналов от них.

Последний компонент предназначен для управления информационным обменом между цифровым и ситуационным мониторингом, агрегирования и передачи сформированных сигналов в систему решения целевых задач в цикле управления.

Цифровой мониторинг направлен на идентификацию структурных сдвигов следующего вида: изменение тренда, изменение уровня, изменение дисперсии [1]. Для такого вида цифрового мониторинга предлагается применять методы, основанные на алгоритмах последовательного анализа, адаптированных для мониторинга нестационарных процессов [2].

В цикле управления процедуры мониторинга обеспечивают решение задачи обнаружения изменений значимых параметров, к изменениям которых чувствительны целевые параметры системы, для 1) классификации неопределенности условий по критериям количества факторов, подверженным изменениям, и оценке периодичности, частоты и силы изменений; 2) определения характеристики текущих условий по оценке значимости влияния на изменение целевых параметров; 3) детектирования сигналов об изменении тренда целевого параметра и вклада факторов-причин в его изменения в процедурах совместного обнаружения изменений в нестационарных процессах по цифровым данным. Соответственно при настройке процедур мониторинга структурно-целевой анализ причинно-следственных моделей ситуаций должен обеспечить классификацию возможных сочетаний изменений факторов внешней среды в их негативном влиянии на целевые параметры системы. Условия меняются неожиданно или ожидаемо по некоторому возможному сценарию, что приводит к систематическим отклонениям по целям при заданных управлениях. Известные методы построения причинно-следственных моделей для описания развития системы под влиянием внешней среды с использованием доступной качественной и количественной информации по разным периодам позволяют построить верифицированные модели сложных ситуаций с включением факторов, обуславливающих изменение

факторов, которые определяют систему. С одной стороны, эта модель избыточная, так как некоторый рассматриваемый период определяется срезом графа, ассоциированного с моделью, по активным вершинам, с другой может не включать значимые факторы для нового периода. Тем не менее, включение в процедуры мониторинга изменений ситуации таких моделей для обработки доступной информации и данных, связанных с факторами, позволяет формировать разные сценарии обработки информации по наборам ключевых слов, оценивать наблюдаемые события и значимость изменений, регулировать процедуры цифрового мониторинга запросами на ранних стадиях о подтверждении изменений в режиме реального (календарного) времени.

Соответственно в блок ситуационного мониторинга поступают данные об изменении ситуации по факторам в некоторый момент времени (с периодичностью), и соответственно генерируются сигналы об изменении тренда целевого параметра, у,: Signal_1– изменение тренда, Signal_2 – измененные веса значимости изменений в системообразующих факторах, которые группируются при построении модели (связанных с реальными или еще не произошедшими экспертно значимыми событиями во внешней среде). Реализация базируется на методах структурного анализа и моделирования на ККС [3, 4], методологии сценарного моделирования развития социально-экономических систем [5].

Заключение

В работе предложен подход к мониторингу на основе разнородной информации, который расширяет возможности традиционного цифрового мониторинга благодаря предоставлению дополнительной информации от ситуационного мониторинга.

Работоспособность представленного подхода проверена на анализе рынка вторичного сырья за 2019 год, где центральным процессом наблюдения являлось формирование закупочных цен на черный лом [1]. Эксперимент подтвердил, что совместный мониторинг повышает качество обнаружения структурных сдвигов в наблюдаемых процессах цифровым мониторингом благодаря информации от ситуационного мониторинга.

Ограничения предложенного подхода связаны с его реализацией в части ситуационного мониторинга, предполагающего работу с

большими объемами текстового контента при выявлении информации о событиях и явлениях, значимых по влиянию на развитие наблюдаемого процесса.

Направления дальнейших исследований мы связываем с:

– адаптацией предложенного подхода к совместному мониторингу применительно к другим методам анализа и обработки количественной информации в части цифрового мониторинга;

– расширением состава сигналов о возможном изменении развития социально-экономических ситуации на основе совместного учета качественных и количественных данных;

– разработкой формализованной модели организации ситуационного мониторинга, объединяющую: 1) когнитивную карту ситуации в качестве основы для выявления и фильтрации информационно-поисковых параметров, и 2) современные подходы (методы) настройки поиска и интеллектуального анализа текстового контента.

Литература:

1. *Авдеева З.К., Гребенюк Е.А., Коврига С.В.* Комбинированный мониторинг разнородной информации для прогнозирования динамики нестационарных процессов / Материалы 15-ой Мультиконференции по проблемам управления (МКПУ-2022), 4-6 октября 2022 г. – СПб: Государственный НЦ РФ АО «Концерн «ЦНИИ «Электроприбор», 2022 (в печати).

2. *Grebenyuk E.A.* Monitoring and identification of structural shifts in processes with a unit root / Proc. of the 13th Inter. Conf. MLSD'2020. – URL: https://ieeexplore.ieee.org/document/9247829 (дата обращения 10.10.2022).

3. *Avdeeva Z., Kovriga S., Makarenko D.* On the statement of a system development control problem with use of SWOT-analysis on the cognitive model of a situation // IFAC PapersOnLine. – 2016. – V. 49 (12). – P. 1838-1843.

4. *Авдеева З.К., Коврига С.В.* О постановке задач управления ситуацией со многими активными субъектами с использованием когнитивных карт // Управление Большими Системами. – 2017. – Выпуск 68. – С. 74-99.

5. Модели и методы анализа и синтеза сценариев развития социально-экономических систем: в 2-х кн. / Под ред. В.Л. Шульца и В.В. Кульбы. – М.: Наука, 2012. Кн. 1. – 304 с., кн. 2. – 358 с.

DOI: 10.25728/iccss.2022.53.89.025

Ходнев Н.Д., Краснов А.Е.

Хранение документов, аспекты информационной безопасности

Аннотация: Ценность и объем информации вырос. Организации всё чаще сталкиваются с проблемой хранения и доступности информации. Целью данной работы является анализ специфики хранения данных.

Ключевые слова: хранение данных, хранения данных в облаке, хранение данных на локальном сервере, информационная безопасность

Дистанционный формат обмена документами представляет значительный интерес, как для компаний, так и для образовательных учреждений. Он служит поддержке осуществляемых бизнес-процессов в масштабе реального времени. Помимо этого, с каждый годом увеличивается общий объем информации и ее ценность. Рабочие документы необходимо хранить и иметь к ним оперативный доступ для пополнения и использования. Также немаловажным требованием является безопасность обрабатываемых данных.

Цель данной статьи связана с анализом специфики хранения данных в облаке и на собственном сервере при использовании дистанционного формата взаимодействия.

Основной задачей работы является сравнение:

- соответствий международным стандартам;
- стоимости хранения данных;
- конфиденциальности доступа;
- надежности и целостности данных;
- масштабируемости системы.

В случае локального хранения данных сервер приобретается самой организацией и встраивается в общую инфраструктуру. Во многих случаях это физический носитель. Все данные на сервере контролирует, обслуживает и поддерживает все аппаратное и

программное обеспечение организация (непосредственно IT-отдел) или привлеченные извне эксперты. Такие сервера, как правило, закрыты для внешнего доступа и функционируют только внутри локальной сети.

При использовании облачного хранения данных, всю информацию размещают у сторонних поставщиков услуг, например Yandex. Поставщик облачных технологий сам заботится о приобретении, поддержке и т.д. аппаратного и программного оборудования, а также о всех издержках вспомогательной инфраструктуры для сопровождения этого решения. Организация управляет своими данными через учетную запись в интернете с помощью веб-браузера.

Оба этих решения сравниваются по следующим ключевым позициям: соответствие международным стандартам, стоимости хранения данных, конфиденциальность доступа, надежность и целостность данных, масштабируемость системы.

Соответствие международным и локальным требованиям. Если организация нацелена на внутренний рынок Российской Федерации, она должна соответствовать требования основополагающих документов, например, таких как: ФЗ № 149 «Об информации, информационных технологиях и о защите информации»; ФЗ № 152 «О персональных данных»; ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» и других. При выходе на внешний рынок, организация должна соответствовать международным стандартам, например, регламенту GDPR и т.п.

При разворачивании собственной инфраструктуры, для соответствий всем требованиям придется нанимать эксперта в этой области и затратить много ресурсов и времени на реализацию. При обращении к поставщику облачных услуг, вы можете убедиться, что их решение имеет сертификат о подтверждении соответствия во всех ключевых областях, которые вам необходимы.

Стоимость. Локальное размещение сервера в краткосрочной перспективе требует вложения множества средств в оборудование, оплату лицензий, содержание IT-отдела, обслуживающего сервер и отдел (служба), обеспечивающий информационную безопасность. Помимо этого, после завершения всех циклов установки и настройки аппаратного и программного обеспечения придется содержать в

штате IT-отдела специалиста для поддержки работоспособности сервера и реагирования на инциденты. Стоимость обслуживания должна быть заложена в бюджет организации, так как аппаратное обеспечение может выйти из строя по разнообразным причинам.

Облачное решение имеет значительное преимущество над локальным размещением – отсутствие первоначальных капиталовложений. Организация оплачивает только ежемесячную или ежегодную подписку. Актуальность, безопасность, обслуживание и поддержка аппаратного и программного обеспечения находится в зоне ответственности поставщика облачных решений. Зачастую расходы на облачные технологии меньше, чем сумма, которая необходима на поддержание собственной инфраструктуры. Однако стоит отметить, что облачные технологии не являются панацеей и оправданность перехода на этот тип хранения данных необходимо рассматривать отдельно в каждом частном случае.

Конфиденциальность доступа. С точки зрения безопасности, размещение своих данных локально не снимает ответственности за разработку средств защиты информации. Даже несмотря на то, что локальные сервера, как правило, недоступны снаружи, необходимо разграничивать доступ ко всем данным. Это требует высокого уровня знаний в области информационной безопасности [1].

При использовании облачных решений, все ваши данные находятся в сети интернет. Эта технология обеспечивает наиболее высокий уровень защиты и избавляет организацию от лишних затрат на информационную безопасность. Облачные решения, как правило, поддерживает большая команда экспертов по кибербезопасности. Все накладные расходы на это выделяются за счет поставщика облачных решений. По оценке Gartner, облачные решения на 60 % меньше подвержены инцидентам, связанным с информационной безопасностью, чем размещение данных на собственных серверах.

Надежность и целостность данных. Часть организаций размещают ресурсы локально, так как штатным сотрудникам не требуется подключение к интернету, чтобы получить доступ к данным. Однако может случиться форс-мажор, например пандемия, впоследствии которого придется организовывать удаленный доступ и обеспечить защищенное подключение. Кроме того, для функционирования локального сервера требуется резервное питание

(например, генератор) для бесперебойной работы [2]. И создать систему резервного копирования данных, сохранность которых должна обеспечивать организации.

Для взаимодействия с облачным хранилищем необходимо быстрое и стабильное подключение к интернету. При отсутствии интернета нет возможности получить доступ к данным. Сбой подключения во время работы может привести к снижению продуктивности и частичной потере данных. Резервное копирование данных и бесперебойный доступ при хранении в облаке гарантирует поставщик облачного решения.

Масштабируемость. Если ваша локальная инфраструктура перестает справляться с рабочей нагрузкой [3], организации необходимо масштабировать свои вычислительные возможности, добавляя новое программное и аппаратное обеспечение. Для этого необходимо выделять бюджет и время. В случае если такой прирост нагрузки вносит временные рамки, то расходы могут оказаться неэффективными и неоправданными.

Облачные технологии позволяют автоматизировать эти издержки. Организация может масштабировать свои ресурсы путем повышения тарифного плана. Это экономит время на установку и введение в эксплуатацию аппаратного обеспечения. Также все эти изменения могут быть отменены в любой момент времени.

Каждый из двух подходов имеет свои плюсы и минусы и должны быть отдельно рассмотрены для каждого конкретного случая. Средний и малый бизнес всё чаще используют облачные решения для разворачивания своей инфраструктуры, так как это помогает сократить время на начальных этапах развития. Но в долгосрочной перспективе это может оказать негативные последствия. Облачные технологии не лишены изъянов, и очередное минорное обновление базы данных может сильно увеличить нагрузку и послужить причиной отказы от обслуживания со стороны базы данных.

Литература:

1. *Краснов А.Е., Мосолов А.С., Феоктистова Н.А.* Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность

информационных технологий. – 2021. – Т. 28 (1). – С. 106-120. DOI: 10.26583/bit.2021.1.09

2. *Кононов А.А., Котельников А.П., Черныш К.В.* Оценка защищенности критически важных объектов на основе построения моделей событий рисков // Труды ИСА РАН. – 2012. — Т. 62. Вып. 4. – С. 69-75. – URL: http://www.isa.ru/proceedings/images/documents/2012-62-4/t-4-12_69-75.pdf (дата обращения 10.10.2022).

3. *Краснов А.Е., Надеждин Е.Н., Никольский Д.Н., Калачев А.А.* Нейросетевой подход к проблеме оценивания эффективности функционирования организации на основе агрегирования показателей ее деятельности // Информатизация образования и науки. – 2017. – № 1 (33). – С. 141-154. – URL: https://informika.ru/pechatnye-izdaniya/zhurnal-informatizaciya-obrazovaniya-i-nauki/arhiv-vypuskov/2017/vypusk-n33/ (дата обращения 10.10.2022).

DOI: 10.25728/iccss.2022.54.97.026

Сомов С.К.

Влияние использования архивов магнитных носителей на некоторые показатели надежности распределенных систем обработки данных

Аннотация: В работе представлены результаты анализа влияния использования восстановительного резерва в виде архива магнитных носителей на показатели надежности работы распределенных систем обработки данных. Анализировались такие показатели надежности работы систем, как среднее время работы системы до отказа, вероятность отказа и вероятность безотказной работы системы заданных интервалах времени.

Ключевые слова: распределенные системы, оперативное и восстановительное резервирование данных, показатели надежности работы распределенных систем

В распределенных системах обработки данных (РСОД) различного назначения для обеспечения высокого уровня

сохранности данных часто используется информационная избыточность в виде идентичных копий оперативного резерва (ОР) [1]. Оперативный резерв представляет собой некоторое количество идентичных копий массива данных. Несколько копий ОР размещаются оптимальным образом в различных узлах системы. Копии массивов данных оперативного резерва поочередно используются при обработке запросов к данным согласно одной из трех стратегий оперативного резервирования [2, 3]. Использование нескольких копий для обработки запросов повышает вероятность их успешной обработки в узле с оперативным резервом. Однако существует ненулевая вероятность разрушения всех копий ОР в узле системы в результате чего этот узел становится неработоспособным. В этом случае запросы, ранее обрабатываемые в данном узле, перераспределяются для обработки в другие работоспособные узлы системы. Это приводит к потере эффективности и надежности всей системы в целом.

Для восстановления работоспособности отказавшего узла используется восстановительный резерв в виде архива магнитных носителей (АМН), размещенного в узле системы, ближайшем к отказавшему узлу. АМН – это некоторое множество множества копий массивов данных. В узлах системы могут быть размещены несколько идентичных копий АМН. АМН используется для восстановления разрушенного ОР в узлах сети. Для этого в узле с АМН создается необходимое количество копий массива данных, которые пересылаются по каналам связи в отказавший узел.

В данной работе проводится анализ показателей надежности РСОД, использующий представленный выше метод восстановления разрушенных данных в неработоспособных узлах системы.

Предположим, что АМН ненадежны, и при обработке в узле с АМН запроса на восстановление разрушенного ОР может произойти отказ самого узла с АМН. Тогда под отказом всей РСОД будем понимать ситуацию, когда в состояние отказа перешли все узлы с ОР и все узлы с АМН.

Функционирование такой РСОД можно рассматривать как процесс случайных переходов системы во множестве допустимых состояний. Переходы РСОД между различными состояниями происходят в результате отказов и восстановления узлов системы.

Сделаем несколько предположений о работе РСОД: 1) запросы, поступающие в отказавший узел с ОР, не переадресуются и не обрабатываются до восстановления узла; 2) при отказе узла с АМН узел не восстанавливается; 3) все запросы, ранее поступающие в отказавший узел с АМН, переадресуются в работоспособные узлы с АМН.

Работу рассматриваемой РСОД опишем при помощи однородной поглощающей цепи Маркова с дискретным временем [4,5]. Предположим, что вероятность одновременного отказа более одного узла с ОР или более одного АМН за единичный интервал времени стремится к нулю.

Обозначим как H множество состояний РСОД $H = \{H_{m,n}\},\ m = \overline{0,M}, n = \overline{0,N}$. Система находится в состоянии $H_{m,n}$, если в системе отказало m узлов с АМН и n узлов с ОР. Множество H преобразуем во множество

$$S = \{S_i\}, i = \overline{1,K}, K = M + N - 1, \quad (1)$$

где $S: S = \{S_i,\ (i = \overline{1,K}, k = M + N - 1)\}$.

Предположим, что за единичный интервал времени в каждый из N узлов с ОР поступает λ запросов. При обработке одного запроса узел с ОР может отказать с вероятностью $Q = 1 - P$. Каждый узел с АМН при обработке запроса на восстановление узла с ОР может отказать с вероятностью $Q_A = 1 - P_A$.

Если предположить, что РСОД находится в состоянии S_i $(i = \overline{1, M-1})$, то в каждый узел с АМН за единицу времени поступает μ_i запросов на восстановление ОР

$$\mu_i = \mu_0 + i\mu_0(M-i)^{-1} = \mu_0 M(M-i)^{-1} \quad (2)$$

Если система находится в состоянии S_i, то узел с АМН за единичный интервал времени может отказать с вероятностью φ_i: $\varphi_i = 1 - P_A^{\mu_i}$. Узел с АМН с вероятностью $\Psi_i = 1 - \varphi_i$ может успешно обработать запрос на восстановление разрушенного ОР. Тогда переход системы из состояния S_i в состояние S_{i+1} $(i = \overline{1 = M-1})$ происходит с вероятностью $p_{i,i+1}$

$$p_{i,i+1} = 1 - \Psi_i^{M-i} = 1 - P_A^{\mu_0 M} = 1 - P_A^{\lambda QN};$$
$$p_{ii} = 1 - p_{i,i+1} = P_A^{\mu_0 M} \tag{3}$$

Следовательно, вероятность $p_{i,i+1}$ при $i = \overline{M,(K-1)}$ равна

$$p_{i,i+1} = 1 - p^{\lambda N}; \quad p_{ii} = p^{\lambda N} \tag{4}$$

Определим показатели надежности функционирования рассматриваемой РСОД. Так как узлы системы с АМН могут стать неработоспособны, то РСОД можно считать невосстанавливаемым объектом.

Вначале функционирования РСОД находится в начальном состоянии S_0. Тогда очевидно, что среднее время T_1 работы РСОД до отказа будет равно среднему времени пребывания РСОД во множестве невозвратных состояний $S^1 = \{S_0, \dots, S_{K-1}\}$. Тогда значение T_1 рассчитывается по формуле

$$T_1 = \sum_{j=0}^{M-1} \left[1 - P_A^{\lambda QN}\right]^{-1} + \sum_{j=0}^{K-1} \left(1 - P^{\lambda N}\right)^{-1} \tag{5}$$

Вероятность $P(t_0)$ безотказной работы РСОД и вероятность $Q(t_0)$ отказа РСОД на интервале времени $[0, t_0]$ равны соответственно

$$P(t_0) = 1 - \sum_{n=K}^{t_0} p_{0,K}(n) = 1 - p_{0,K}(K) \sum_{m=0}^{t_0-K} B^m$$
$$p_{0,K}(K) = \prod_{i=0}^{K-1} p_{i,i+1} = \left[1 - P_A^{\mu_0 M}\right]^M \left[1 - P^{\lambda N}\right]^{(N-1)} \tag{6}$$
$$B = \sum_{i=0}^{K-1} p_{ii} = M P_A^{\mu_0 M} + (N-1) P^{\lambda N}$$
$$Q(t_0) = 1 - P(t_0) \tag{7}$$

Аналогичные вероятности на интервале времени $[t, t + t_0]$ будут равны

$$P(t, t + t_0) = P(t + t_0)/P(t) \quad (8)$$
$$Q(t, t + t_0) = 1 - P(t, t + t_0) \quad (9)$$

Заключение

В работе представлена формальная модель распределенной системы обработки данных, в которой оперативный резерв из копий массивов данных используется для повышения надежности обработки запросов к данным в узлах системы. Если в процессе обработки запроса оперативный резерв разрушается, то узел становится неработоспособным. Работоспособность узла восстанавливается с помощью ближайшего узла с архивом магнитных носителей. Узел с архивом в свою очередь также может потерять работоспособность. Процесс функционирования такой РСОД формально описана в работе с помощью поглощающей цепи Маркова с дискретным временем. Это позволило получить аналитические выражения для расчета значений показателей надежности функционирования рассмотренной РСОД.

Полученные результаты целесообразно использовать для анализа показателей надежности функционирования РСОД, после того как для системы было определено оптимальное размещение в узлах системы оперативного резерва и архивов магнитных носителей.

Литература:

1. *Кульба В.В., Сомов С.К., Шелков А.Б.* Анализ влияния использования информационной избыточности на показатели надежности распределенных информационных систем // Надежность. – 2022. – Том 22. № 1. – С. 4-12.

2. *Сомов С.К.* Сохранность информации в распределенных системах обработки данных. – М.: ИПУ РАН, 2019. – 254 с.

3. *Микрин Е.А, Сомов С.К.* Анализ эффективности стратегий восстановления информации в распределенных системах обработки данных // Информационные технологии и вычислительные системы – 2016. – №3. – С. 5-19.

4. *Розанов Ю.А.* Введение в теорию случайных процессов. – М.: Наука, 1982. – 128 с.

5. *Кемени Д., Снелл Д.* Конечные цепи Маркова. – М.: Мир, 1970. – 271 с.

DOI: 10.25728/iccss.2022.96.68.027

Мистров Л.Е.

Метод обоснования задач информационной безопасности организационно-технических систем

Аннотация: Предлагается на основе применения методов ветвей и границ метод обоснования приоритетных задач информационной безопасности в структуре организационно-технических систем.

Ключевые слова: организационно-техническая система, информационная безопасность, критерий эффективности, метод ветвей и границ, оптимизация

В современных условиях выполнение задач различного предназначения и структурной сложности организационно-технических систем (ОТС) осуществляется во взаимодействии с другими системами. Появление конкуренции обусловило возникновение формы конфликта типа «соперничество», представляющего угрозу устойчивому развитию ОТС, актуализируя решения задачи информационной безопасности (ИБ) на основе применения различного уровня эффективности мероприятий и средств ИБ.

Особенность обоснования задач ИБ, вследствие структурной сложности ОТС, обусловлена необходимостью их определения на нескольких $j=1,\ldots,J$ иерархических уровнях системы. Эффективность (целевая функция) R_j определения задач ИБ на j -ом уровне ОТС представляется в виде

$$R_j = \sum_{i \in Z_j} \lambda_{ij} \sum_k P_j(i \mid H_{ij}^k) P(H_{ij}^k), \qquad (1)$$

где λ_{ij} – коэффициент важности решения i -й, $i=1,\ldots,I$ задачи ИБ на j -ом уровне ОТС; $P_j(i \mid H_{ij}^k)$ – вероятность решения i -й задачи ИБ на j -ом уровне ОТС при H_{ij}^k гипотезе об эффективности мероприятий и средств ИБ; $P(H_{ij}^k)$ – вероятность гипотезы H_{ij}^k об уровне эффективности мероприятий и средств ИБ для решению i -й задачи ИБ на j -ом на уровне ОТС; k – количество гипотез об эффективности мероприятий и средств ИБ, $\sum_k P(H_{ij}^k)=1$; Z_j – множество задач ИБ, подлежащих решению на j -ом уровне ОТС.

Постановка задачи по обоснованию задач ИБ состоит в нахождении оптимального решения – максимальной суммарной эффективности решения задач ИБ на всех уровнях ОТС за $T_з$ ограниченное время

$$R^*(V_o)=\max\sum_{j=1}^{J}R_j(Z_j); \qquad T^*=\min\sum_{j=1}^{J}\sum_{i\in Z_j}T_{ij}(Z_j); \quad T^*\le T_з, \tag{2}$$

где R^* – суммарная эффективность решения задач ИБ на всех уровнях ОТС; V_o – множество допустимых вариантов решений задач ИБ; T^* – суммарное время решения задач ИБ на всех уровнях ОТС; T_{ij} – время решения i -й задачи ИБ на j -ом уровне ОТС; $T_з$ – директивное время решения задач ИБ в структуре ОТС.

Рассматриваемая задача, как задача оптимального управления, относится к классу задач дискретной оптимизации, для решения которой предлагается использовать метод ветвей и границ. Метод реализует последовательный алгоритм определения оптимального решения на основе ветвления (построения дерева решений) всего множества решений на подмножества $V_в$ в соответствии с выбранным показателем и определения нижних (верхних) оценок или границы на каждом шаге ветвления. Под множеством решений $V_в \subset V_o$ понимается множество допустимых вариантов задач ИБ с учетом взаимного влияния результатов на предшествующих уровнях структуры ОТС.

В общем случае решение задачи основывается на нахождении R целевой функции на множестве V_o допустимых вариантов решения i -й задачи ИБ на j -ом уровне ОТС, удовлетворяющей верхней

оценке целевой функции $R^{\max}(V_д)$ с учетом ограничений, определяющих область решения задачи. При этом верхняя оценка целевой функции для всех допустимых вариантов решений $V_д$ должна отвечать условию

$$R^{\max}(V_д) \geq R(V_в); \qquad V_в \subset V_{д,} \tag{3}$$

то есть оценка по множеству допустимых решений должна быть не хуже оценки по любому входящему в него подмножеству.

Вследствие иерархичности построения структуры ОТС решение задачи (3) осуществляется разбиением исходного множества $V_д$=V_0 решений поиска в соответствии с выбранным признаком на подмножества $V_0 = \bigcup V_{i,1}$, $V_{i,1} = \bigcup V_{i,2}$,… . При этом на первом шаге выбирается решение r_1 и образуется подмножество $V_{r_1,1}$; на втором производится ветвление подмножества $V_{r_1,1}$ и вычисляются оценки на подмножествах $V_{r_1;i,2}$. Далее выбирается решение r_2. Процесс ветвления продолжается до тех пор, пока полностью не будет определено решение $R^*(V_д)$, соответствующее условию оптимальности (3); в этом случае выделенное подмножество решений включает в себя только один вариант $R^*(V_д)$.

Для решения задачи предположим, что $V_д$ множество допустимых вариантов решений формируется при условии, что каждая задача ИБ решается на всех уровнях ОТС только один раз. Принимаем также в выражении (1) k=1 и $P(H_{ij}^k) = 1$. Тогда оптимизация решения задачи обоснования задач ИБ при ограничении на общее время T^* представляется в виде

$$R^*(V_д) = \max \sum_{j=1}^{J} \sum_{i=1}^{I} \lambda_{ij} P_{ij}(V_д), \tag{4}$$

при

$$T^* = \min \sum_{j=1}^{J} \sum_{i=1}^{I} T_{ij}(V_д); \quad T^* \leq T_з, \qquad P_{ij}(V_д) = [0;1]. \tag{5}$$

Такое представление задачи позволяет осуществить поиск ее решения на основе дерева ветвления. С этой целью подмножества первого уровня разбиения формируются путем фиксирования на этом уровне одной из задач ($V_{1,1}, V_{2,1}, ..., V_{i,1}, ..., V_{I,1}$). Например, множество $V_{2,1} = V_{r_1,1}$ включает в себя все варианты, где вторая задача решается на первом уровне структуры РЭО, а разбиение остальных задач по уровням $\overline{2, J}$ произвольное. Аналогично, множество второго уровня формируется фиксированием на этом уровне одной из задач, оставшихся незакреплёнными после выбора задачи r_1=2, решаемой на первом уровне. Так, множество $V_{r_1;\, i,\, 2}$ включает в себя варианты решений, где на первом уровне решается задача r_1, на втором уровне любая задача $i = \overline{1, I}$, кроме r_1 ($i \neq r_1$), а остальные задачи имеют произвольное распределение по оставшимся уровням $\overline{3, J}$ и т.д. Для каждого из подмножеств (вершин дерева) строится верхняя оценка целевой функции и нижняя оценка ограничения. Общее выражение верхней оценки целевой функции $R(V_s)$ для множества вариантов V_o на уровне s с учетом [1, 2] строится в виде

$$R(V_s) = \sum_{j=1}^{s} \lambda_{r_j,j} \cdot P_{r_j,j}(V_{r_j}) + \sum_{j=s+1}^{J} \max_{i, i \neq r_1, \ldots r_s} \lambda_{ij} P_{ij}(V_o), \qquad (6)$$

а общее выражение для нижней оценки ограничения

$$T(V_s) = \sum_{j=1}^{s} T_{r_j,j}(V_{r_j}) + \sum_{j=s+1}^{J} \min_{i, i \neq r_1, \ldots r_s} T_{i,j}(V_o), \qquad (7)$$

где r_j – номер внутренней задачи на уровне $j < s$.

Оценка для функции ограничения (7) необходима для исключения из процесса распределения множества заранее не подходящих вариантов решения с учетом ограничения на общее время решения задачи обоснования задач ИБ.

Оценку обоснования задач ИБ в структуре ОТС рассмотрим применительно к следующему примеру. Пусть определены матрицы вероятностей P и временных затрат T на определение задач ИБ и установлены значения важности λ_{ij} решения I=5 задач ИБ на $J = 5$ уровнях ОТС:

$$P = \begin{bmatrix} 0{,}7 & 0{,}4 & 0{,}3 & 0{,}5 & 0{,}4 \\ 0{,}6 & 0{,}5 & 0{,}6 & 0{,}5 & 0{,}3 \\ 0{,}8 & 0{,}7 & 0{,}6 & 0{,}5 & 0{,}3 \\ 0{,}9 & 0{,}8 & 0{,}7 & 0{,}3 & 0{,}8 \\ 1{,}0 & 0{,}5 & 0{,}4 & 0{,}4 & 0{,}6 \end{bmatrix}^{\mathrm{T}}, \quad T = \begin{bmatrix} 1 & 3 & 5 & 9 & 7 \\ 8 & 7 & 6 & 9 & 10 \\ 5 & 3 & 6 & 11 & 6 \\ 6 & 7 & 5 & 12 & 8 \\ 5 & 6 & 7 & 4 & 5 \end{bmatrix}^{\mathrm{T}},$$

$\lambda_{i,j=1} = 5;\ \lambda_{i,j=2} = 4;\ \lambda_{i,j=3} = 3;\ \lambda_{i,j=4} = 2;\ \lambda_{i,j=5} = 1.$

Тогда $$\lambda_{ij} P_{ij} = \begin{bmatrix} 3{,}5 & 2{,}0 & 1{,}5 & 2{,}5 & 2{,}0 \\ 2{,}4 & 2{,}0 & 2{,}4 & 2 & 1{,}2 \\ 2{,}4 & 2{,}1 & 1{,}8 & 1{,}5 & 0{,}9 \\ 1{,}8 & 1{,}6 & 1{,}4 & 0{,}6 & 1{,}6 \\ 1{,}0 & 0{,}5 & 0{,}4 & 0{,}4 & 0{,}6 \end{bmatrix}^{\mathrm{T}}.$$

Решение задачи состоит в нахождении максимального значения $R^*(V_o)$ – оптимального пути на дереве задач ИБ в структуре ОТС при общем времени решения задачи, не превышающем $T_з = 23$ мин, т.е. $T^* \le 23$ мин.

Так как каждая задача ИБ на множестве допустимых вариантов решается только один раз, то возможно упростить матрицы $\lambda_{ij} P_{ij}$ и T, исключив варианты, для которых не выполняется ограничение на $T_з$ общее время решения задачи

$$\sum_{k=1}^{i-1} \min_{\substack{r=1,..5 \\ r \ne j}} T_{kr} + T_{ij} + \sum_{k=i+1}^{5} \min_{\substack{r=1,...5 \\ r \ne j}} T_{kr} > T_з, \quad i = \overline{1,5};\ \ j = \overline{1,5};\ \ r \ne j. \qquad (8)$$

Используя условие (9) и учитывая ограничение по времени, можно из матриц $\lambda_{ij} P_{ij}$ и T исключить варианты решений (элементы), которые не влияют на выбор оптимального пути поиска задач ИБ. После проведения такого преобразования матрицы $\lambda_{ij} P_{ij}$ и T будут иметь вид

$$\lambda_{ij}P_{ij} = \begin{bmatrix} 3{,}5 & 2{,}0 & – & – & – \\ 2{,}4 & 2{,}0 & 2{,}4 & 2{,}0 & 1{,}2 \\ 2{,}4 & 2{,}1 & – & – & 0{,}9 \\ 1{,}8 & 1{,}6 & 1{,}4 & – & 1{,}6 \\ 1{,}0 & 0{,}5 & – & 0{,}4 & 0{,}6 \end{bmatrix}^{\mathrm{T}}; \quad T = \begin{bmatrix} 1 & 3 & – & – & – \\ 8 & 7 & 6 & 9 & 10 \\ 5 & 3 & – & – & 6 \\ 6 & 7 & 5 & – & 8 \\ 5 & 6 & – & 4 & 5 \end{bmatrix}^{\mathrm{T}}.$$

из которых видно, что исходные матрицы упростились.

Теперь, исходя из полученных в результате преобразований матриц, осуществим непосредственное решение задачи. Дерево решений задач ИБ в структуре ОТС на пяти уровнях элементов с учетом построенных оценок (6) и (7) приведено на рисунке 1.

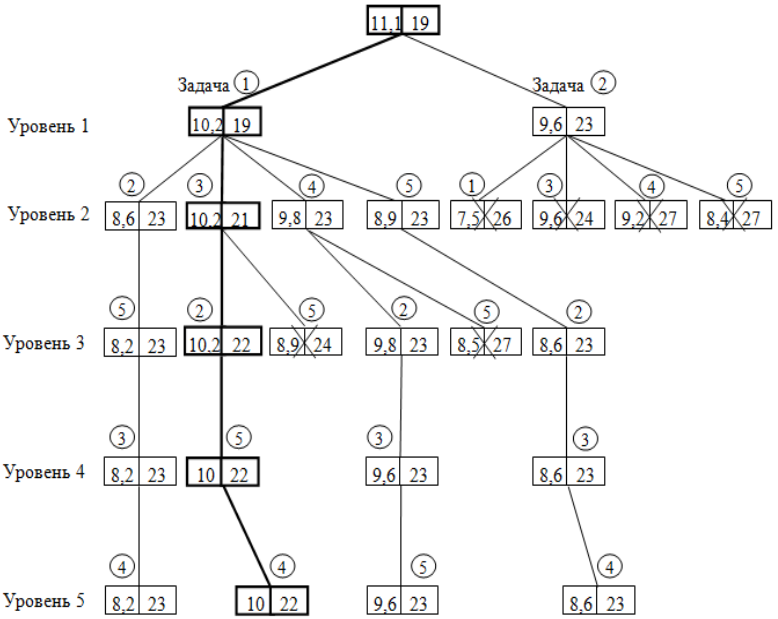


Рисунок 1 – Оптимальный путь распределения задач ИБ по задачам и уровням принятия решений в структуре ОТС

На нем в корневой вершине дерева приведены предельная верхняя граница функции цели $R^{\max}(V_0)$=11,1 и предельная нижняя

граница времени поиска $T^{min}(V_0)$=19 мин. В левой части остальных вершин для каждого уровня указаны текущая верхняя граница значения функции цели $R(V_s)$, в правой части – нижняя граница общего времени $T(V_s)$. Жирными линиями выделен путь поиска оптимального решения на множестве $V_д$ допустимых вариантов. Результаты обоснования задач ИБ ОТС состоят в распределении ресурса средств ИБ: на 1-ом уровне решается задача №1; на 2-ом – №3; на 3-ем – №2; на 4-ом – №5 и на 5-ом – №4.

Результаты проведенных расчетов задач ИБ ОТС показали, что оптимальное значение целевой функции составляет $R^*(V_д) = 10$ при $T^*(V_д) = 22$ мин, не превышающем Тз=23 мин.

Предложенный метод обеспечивает решение задачи обоснования задач ИБ для различной типа и структурной сложности ОТС на основе оптимального распределения временного ресурса средств ИБ на иерархических уровнях системы.

Литература:

1. *Мистров Л.Е.* Метод выбора и распределения ресурсов в обеспечивающих организационно-технических системах // Автоматизация и современные технологии. – 2006. – №11. – С. 24-29.

2. *Денисов А.А., Колесников Д.Н.* Теория больших систем. – Л.: Энергоиздат, 1982. – 287 с.

DOI: 10.25728/iccss.2022.83.42.028

Саломатин А.А.

Анализ характеристик аппаратного обеспечения для задач информационной безопасности

Аннотация: В работе авторами проводится исследование характеристик аппаратного обеспечения для решения задач информационной безопасности. Выделяют наиболее значимые задачи, среди которых основное внимание в работе уделено задачам аутентификации и идентификации пользователей. Рассматриваются статические и динамические характеристики основных аппаратных

платформ, применимых в данных задачах. Описанные особенности характеристик и процесса их вычисления позволяют выбирать конкретные характеристики аппаратного обеспечения для обеспечения более высокого уровня информационной безопасности в задачах.

Ключевые слова: кибербезопасность, информационная безопасность, аппаратное обеспечение, аутентификация, идентификация, цифровой след

В настоящее время растущей становится проблема кибербезопасности сетей и критически важных элементов инфраструктуры. Необходима поддержка высокого уровня информационной безопасности, при котором информация обладает достаточной степенью конфиденциальности, целостности и доступности на различных уровнях использования.

Эффективными становятся средства защиты, позволяющие детектировать атаки на системы ещё на ранних этапах [1, 2]. Однако, разработка таких мер является сложной комплексной задачей, поскольку предметная область должна учитывать большой объём данных, связанных с пользовательским программным и аппаратным обеспечением.

Задачи аутентификации и идентификации пользователей сетей выступают в центре внимания исследователей. Современные подходы к решению представленных задач постоянно обновляются, поскольку совместно с разработкой методов аутентификации создаются способы обхода защиты, что может привести к серьёзным негативным последствиям для системы и её пользователей [3, 4].

Исследование данного направления показало, что перспективным является проведение аутентификации пользователя на основе его уникального многокритериального цифрового следа [5]. Цифровой след содержит данные о различных статических и поведенческих характеристиках профиля субъекта доступа. Например, данные браузера, операционной системы и аппаратного обеспечения, данные, связанные с запросами, и т.д.

Более жёсткую связь пользователя с устройствами и более слабую подверженность успешным кибератакам даёт цифровой след на основе характеристик аппаратного обеспечения.

В [6] для формирования цифрового следа рассматриваются характеристики статического и динамического характера ПО компьютера, полученные с помощью Диспетчера устройств, «Информации системы» и AIDA64 Engineer v. 6.33.5700.

Характеристики первого типа являются неизменными для устройства. Их число большое и зависит от конкретных используемых аппаратных платформ. Вычисляют названия подключенных устройств и составляющих компонент, определяются текущие аудиовходы и аудиовыходы, вычисляют показатели работы батареи, характеристики монитора, материнской платы, батареи, оперативной памяти и др.

Характеристики второго типа связаны с изучением работы компонент системы по истечению определённого временного промежутка. Проводятся тесты различных типов: чтение из памяти, запись в память, копирование в память, CPU Queen, CPU PhotoWorxx, CPU ZLib, CPU AES, FPU Julia, FPU Mandel и др.

В результате исследования определян оптимальный набор тестов, позволяющих наиболее успешно проводить аутентификацию пользователя.

Похожие исследования были проведены также в [7], где для определения динамических характеристик каждого устройства проведены тесты 4 типов с помощью собственных написанных программ. Результаты эксперимента показывают, что вычисленные результаты тестов могут помочь в формировании цифрового следа с высокой уникальностью и стабильностью при его формировании и использовании.

В другой работе [8] для вычисления статических характеристик пользователя авторы используют JavaScript и HTML5 API. В качестве вычисляемых характеристик выступают некоторые показатели монитора, батерии, подключенные устройства в виде камеры и микрофона и др. Также в работе вычисляются браузерные отпечатки, которые хоть и не являются характеристикам аппаратного обеспечения, но могут составлять будущий цифровой след.

Стоит отметить, что класс устройств может быть расширен и дополнен другими мобильными устройствами, для которых возможно выделить классы данных аппаратного обеспечения, на основе которых проводится аутентификация. В отмеченных группах

данных присутствуют как статические, так и динамические показатели.

- Датчики (магнитометр, показатели ориентации, показатели света, вектор ротации, показатели температуры, CAP_PROX, RPC, показатели цветодатчика, линейное ускорение и др.).
- Центральный процессор (SoC модель, архитектура ядра, технологический процесс, наборы инструкций, число ядер, частотные характеристики, поддержка стандартов хеширования, шифрования).
- Отображение (разрешение экрана, технология, размер экрана, диагональ экрана, плотность пикселей, производитель, рендерер, версия графического процессора).
- Сеть (сетевой оператор, состояние передачи данных, активность данных, Wi-Fi, тип сети и др.).

Выбор количества и типа данных для любой аппаратной платформы зависит от конкретной ситуации и цели. Универсальная методика пока не разработана. Использование большего числа статических, нежели динамических, параметров позволяет избежать лишних временных задержек при решении задач информационной безопасности. В свою очередь, использование динамических характеристик отдельно или совместно со статическими характеристиками позволяет точнее проводить аутентификацию в связи с анализом большего объёма данных как из-за их динамики, так и из-за их количества и уникальности определения для пользователей.

Исследование выполнено при финансовой поддержке гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук МК-3172.2021.1.6

Литература:

1. *Хозяинова Т.В,, Шечева И.А., Кобзев Д.А., Бенгарт З.С., Кутлубаева Е.Г.* Организация процесса мониторинга уязвимостей программного обеспечения и оборудования АСУТП // Наука и технологии трубопроводного транспорта нефти и нефтепродуктов. – 2019. – № 9. – С. 458-466.

2. *Avizienis A., Laprie J.-C., Randell B.* Fundamental concepts of dependability // Research Report. – 2001. – Vol. 1145. – P. 1-6.

3. *Бабаев Д.И., Полетыкин А.Г., Промыслов В.Г., Тимофеев*

М.Ю. Управление архитектурой кибербезопасности АСУТП атомных электростанций // Проблемы управления. – 2018. – № 3. – С. 47-55.

4. *Cherdantseva Y., Burnap P., Blyth A., Elden P., Jones K., Soulsby H., Stoddart K.* A review of cyber security risk assessment methods for SCADA systems // Computers & security. – 2016. – Vol. 56. – P. 1-27.

5. Струков А.В., Ветлугин К.А. О методах количественного анализа кибербезопасности технических систем на основе логико-вероятностного подхода // Интернет-журнал «Науковедение». – 2017. – Том 9. №4. – URL: http://naukovedenie.ru/PDF/01TVN417.pdf (дата обращения 15.10.2022).

6. *Salomatin A.A., Iskhakov A.Yu., Meshcheryakov R.V.* Formation of a Digital Footprint Based on the Characteristics of Computer Hardware to Identity APCS Users / Proceedings International Russian Automation Conference (RusAutoCon). – Sochi, Russia: IEEE, 2021. – P. 314-320.

7. *Dong S., Farha F., Cui S., Ning H., Ma J.* CPG-FS: A CPU perfomance graph based device fingerprint scheme for devices identification and authentication / Proc. of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing. – IEEE, 2019. – P. 266-270.

8. *Takasu K., Saito T., Yamada T., Ishikawa T.* A survey of hardware features in modern browsers: 2015 Edition / Proc. of the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. – IEEE, 2015. – P. 520-524.

DOI: 10.25728/iccss.2022.72.91.029

Сомов С.К.

Показатели надежности распределенной системы с невосстанавливаемыми узлами

Аннотация: В работе выполнен анализ показателей надежности функционирования распределенных систем обработки данных, использующих оперативный резерв из нескольких копий массивов данных для повышения надежности обработки в узлах запросов к системе. Рассматривается ситуация, при которой система не восстанавливает оперативный резерв в случае его

разрушения. Для рассматриваемой ситуации получены аналитические выражения для некоторых показателей надежности работы распределенных систем.

Ключевые слова: распределенные системы, оперативное резервирование данных, показатели надежности работы распределенных систем

Для обеспечения высокой степени сохранности данных в распределенных системах обработки данных (РСОД), широко используется информационная избыточность в виде идентичных копий оперативного резерва, размещенных в узлах системы [1]. Оперативный резерв (ОР) представляет собой некоторое количество копий массивов данных, которые используются для повышения надежности обработки запросов к данным [2]. Использование ОР в узлах системы значительно снижает вероятность разрушения данных, но не исключает ее полностью. В результате разрушения ОР в некотором узле системы этот узел становится неработоспособным. Для восстановления работоспособности такого узла можно использовать один из методов восстановительного резервирования [3].

В данной работе рассматриваются показатели надежности функционирования РСОД, которая не использует восстановительное резервирование.

В данном случае в РСОД используется ОР, копии которого размещены в нескольких узлах системы. Причем при отказе узла он не восстанавливается, и будет находиться в неработоспособном состоянии. Функционирование такой РСОД можно рассматривать как процесс случайных переходов системы из одного состояния в другое. Такие переходы происходят при возникновении случайного события – потери работоспособности узла системы по причине разрушения ОР данного узла в процессе обработки запроса к данным. После отказа узла запросы к данным, ранее поступавшие для обработки в этот узел, равномерно распределяются между оставшимися в работоспособном состоянии узлами системы с оперативным резервом. При отказе всех узлов с ОР система переходит в состояние отказа и перестает обрабатывать поступающие запросы.

Предположим, что в M узлах РСОД размещен ОР. Множество всех состояний системы обозначим через H

$$H = \{H_0, H_1, \dots, H_N, H_{1,2}, \dots, H_{1,2,\dots,N}\} \quad (1)$$

Состоянию $H_{1,2},..n$ множества H соответствует такое состояние системы, при котором неработоспособны n узлов с ОР.

Последовательно пронумеровав элементы из H, получим множество S

$$H = S = \{S_0, S_1, \dots, S_N, S_{N+1}, \dots, S_M\}, \;\; M = 2^N \quad (2)$$

Рассматриваемый случайный процесс переходов РСОД между состояниями множества S является однородным процессом, т.к. состояние РСОД в будущем не зависит от истории предыдущих переходов системы, а зависит только от текущего состояния системы [4, 5].

Тогда справедливо, что условная вероятность $P\left\{\xi(t) = \frac{S_j}{\xi(u)} = = S_i\right\}$ того, что в момент времени t РСОД находится в состоянии S_j при условии, что в момент времени u, система находилась в состоянии S_i, будет равна

$$\begin{aligned} P\left\{\xi(t) = \frac{S_j}{\xi(t_1)} = S_{i_1}, \dots, \xi(t_n) = S_{i_n}, \xi(t_u) = S_i\right\} = \\ = \left\{\xi(t) = \frac{S_j}{\xi(t_u)} = S_i\right\} = p_{ij}(t-u) \end{aligned} \quad (3)$$

при этом: $u > t_n > \cdots > t_1; \quad t > u; \;\; i, j \in \{0,1, \dots, N\}$.

Величины переходных вероятностей p_{ij} случайного процесса переходов РСОД определяются в соответствии с формулой

$$p_{ij} = \begin{cases} 0 \text{ при } (i < j) \text{ или } \xi(t) = S_j \neq S_i = \xi(t-1) \text{ и} \\ |I_0(t)| = |I_0(t-1)| \\ \prod\limits_{n \in R} \tau_n(S_i) \left[\prod\limits_{n \in R} \beta_n(S_i) \right]^{-1} \prod\limits_{n \in I_p(S_i)} \beta_n S_i \\ -\text{в остальных случаях} \end{cases} \quad (4)$$

В этой формуле используются обозначения:

$I_0(t)$ – множество номеров узлов, отказавших ко времени t. $I_p(S_i)$ – множество работоспособных узлов РСОД, которая находится в состоянии S_i. $\tau_n(S_i)$ – вероятность отказа за единицу времени узла n системы, которая находится в состоянии S_i. $R = \left[I_0(S_i) - I_0(S_j)\right]$ – множество узлов, отказавших за один шаг перехода РСОД между двумя состояниями. $I_p(S_i)$ – множество номеров работоспособных узлов системы, находящейся в состоянии S_i. $\beta_n(S_i) = \tau_n(S_i)$.

Так как в РСОД отказавшие узлы не восстанавливаются, то такую систему можно рассматривать как невосстанавливаемый объект. Данный объект имеет конечное множество работоспособных состояний и единственное состояние отказа всей системы. Такой процесс переходов системы между несколькими возможными состояниями можно трактовать как поглощающая цепь Маркова с дискретным временем.

Ниже на рисунке 1 показан граф переходов для системы, соответствующей сделанным предположениям.

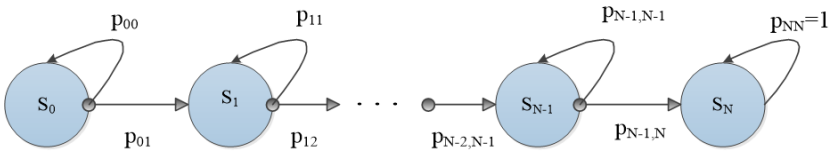


Рисунок 1 – Граф случайного процесса переходов системы во множестве состояний S

С учетом сделанных предположений о характере переходов РСОД между различными состояниями получены выражения для оценки следующих показателей надежности функционирования рассмотренной системы: T_1 – среднее время работы РСОД до отказа; $Q(t_0)$ и $Q(t, t+t_0)$ – вероятность отказа системы в интервалах времени $[0, t_0]$ и $[t, t+t_0]$; $P(t_0)$ и $P(t, t+t_0)$ – вероятность безотказной работы системы в интервалах времени $[0, t_0]$ и $[t, t+t_0]$.

Обозначим через $p_{ij}(n)$ вероятность перехода системы из состояния S_i в состояние S_j за n шагов. Тогда, используя формулу полной вероятности, получим, что эта вероятность будет вычисляться по формуле

$$p_{ij}(n) = \sum_{S_m \in S^1} p_{im} p_{mj}(n-1); \quad p_{mj}(0) = \delta_{mj} \tag{5}$$

Здесь S^1 множество невозвратных состояний системы, а $\delta_{ij} = 1$ при $i = j$ и 0 при $i \neq j$.

Так система за единичный интервал времени выполнит один шаг процесса переходов, то на интервале $[0, t_0]$ система выполнит t_0 шагов. Тогда, учитывая, что $p_{0N}(n) = 0$ при $n < N$, получим, что вероятность $P(t_0)$ безотказной работы системы и вероятность $Q(t_0)$ отказа системы в интервале времени $[0, t_0]$ равны

$$P(t_0) = 1 - \sum_{n=N}^{t_0} p_{0N}(n); \qquad Q(t_0) = \sum_{n=N}^{t_0} p_{0N}(n) \tag{6}$$

Вероятность $P(t, t+t_0)$ безотказной работы системы на интервале от t до $[t, t+t_0]$ в соответствии с формулой условной вероятности равна

$$P(t+t_0) = P(t+t_0)/P(t) \tag{7}$$

Тогда вероятность $Q(t+t_0)$ противоположного события – отказа системы на интервале времени $[t, t+t_0]$ равна

$$Q(t + t_0) = 1 - P(t + t_0)/P(t) \quad (8)$$

Предположив, что единичный интервал времени и параметры системы таковы, что вероятность одновременного отказа двух и более узлов системы равна нулю, получим, что, среднее время T_1 работы системы до отказа равно

$$T_1 = \sum_{j=0}^{N-1} p_{j,j+1}^{-1} = \sum_{j=0}^{N-1} \left(1 - p_{jj}\right)^{-1} \quad (9)$$

Заключение

В работе представлена модель распределенной системы, которая использует оперативное резервирование для повышения надежности обработки запросов к данным. В случае разрушения оперативного резерва в узле он не восстанавливается, а узел остается неработоспособным. На основе данной модели получены аналитические выражения для расчета значений важных показателей надежности функционирования распределенных систем обработки данных. Полученные результаты целесообразно использовать при анализе эффективности размещения копий оперативного резерва по узлам распределенной системы.

Литература:

1. *Кульба В.В., Сомов С.К., Шелков А.Б.* Анализ влияния использования информационной избыточности на показатели надежности распределенных информационных систем // Надежность. – 2022. –Том 22. № 1. – С. 40-12.

2. *Сомов С.К.* Сохранность информации в распределенных системах обработки данных. – М.: ИПУ РАН, 2019. – 254 с.

3. *Микрин Е.А., Сомов С.К.* Анализ эффективности стратегий восстановления информации в распределенных системах обработки данных // Информационные технологии и вычислительные системы – 2016. – №3. – С. 5-19.

4. *Розанов Ю.А.* Введение в теорию случайных процессов. – М.: Наука, 1982. – 128 с.

5. *Кемени Д., Снелл Д.* Конечные цепи Маркова. – М.: Мир, 1970. – 271 с.

DOI: 10.25728/iccss.2022.91.86.030

Синюк А.Д., Тарасов А.А.

Принципы открытого сетевого многоключевого согласования

Аннотация: Одной из сложных организационно-технических задач обеспечения информационной безопасности функционирования закрытых сетей связи, использующих криптографические методы, является оперативное восстановление скомпрометированного нарушителем общего ключа. Решение возможно на основе формирования сетевого ключа по открытым каналам связи. Частые повторные компрометации сетевого ключа вызывают существенное увеличение времени его восстановления. Предлагаются принципы открытого сетевого многоключевого согласования, определяющие условия построения конструктивных протоколов формирования увеличенной криптосвязности корреспондентов сети связи, которая обеспечит оперативное восстановление сетевого ключа.

Ключевые слова: закрытая сеть связи, сетевой ключ, групповой ключ, парные ключи, нарушитель, протокол открытого сетевого многоключевого согласования

Обмен информацией между корреспондентами сети связи (СС), закрытый на сетевом ключе, имеет ряд преимуществ. Однако компрометация сетевого ключа нарушителем влечет за собой полную потерю криптографической связности одновременно всех корреспондентов закрытой СС [1].

Доставка нового сетевого ключа по защищенному каналу связи не всегда представляется возможной, целесообразной и требует достаточно больших организационных, материальных и временных затрат [1, 2]. Альтернативой служат методы формирования сетевого ключа по открытым каналам связи [3]. Проблема восстановления сетевой криптосвязности усугубляется в условиях частых повторных компрометаций уже вновь восстановленных сетевых ключей, когда закрытый информационный обмен корреспондентов в сети связи останавливается вовсе [1, 2].

Актуализируется поиск путей построения конструктивных протоколов формирования сетевого ключа по открытым каналам связи, для которых время ключевого согласования существенно минимизируется. Решение возможно на основе подхода открытого сетевого многоключевого согласования [4], когда в ходе реализации протокола одновременно формируются вместе с сетевым (групповым) ключом еще несколько ключей между различными парами корреспондентов. Это позволит после выявления компрометации сетевого ключа быстро его восстановить с использованием оставшихся нескомпрометированных парных криптосвязностей (ключей) корреспондентов сети связи [4]. Разрабатываются принципы открытого сетевого многоключевого согласования, позволяющие синтезировать искомые протоколы.

Реализация протокола открытого сетевого многоключевого согласования (ПОСМС) в СС включающей трех корреспондентов *A, C* и *B*, возможна путем осуществления обмена данными конечной длины между ними по каналам связи (КС), доступным нарушителю (НРЛ) *E*. При этом требуется обеспечить оперативное и одновременное формирование как сетевого ключа (СК) так и парных ключей (ПК) с требуемыми вероятностью попарного совпадения СК и ПК, достоверностью, вероятностью совпадения с соответствующим ключом НРЛ.

Обмен информации в СС описывается моделью передачи информации (МПИ), в которой каналы описываются моделями двоичных симметричных КС без памяти (ДСК) [5]. Канал 1 — КС от корреспондента *A* к корреспонденту *B* с вероятностью ошибки p_y, а Канал 2 —от корреспондента *A* к корреспонденту *C* – p_m. Совокупность Канала 1 (КС1) и Канала 2 (КС2) описывается моделью двоичного широковещательного канала без памяти (ДШК) [5]. Передача сигналов по ДШК определяется составляющими КС1 (СК1) и КС2 (СК2) с алфавитами входным *X*, выходными *Y* и *M*. На вход ДШК двоичный источник информации без памяти (ДИИБП) с равномерным выходом [6] корреспондент *A* подает в виде последовательности $\bar{x} \in X^N$, где X^N – декартова *N*-я степень *X* [5, 6], корреспондент *B* принимает на выходе КС1 последовательность $\bar{y} \in Y^N$ и корреспондент *C* на выходе КС2 - $\bar{m} \in M^N$.

Каналом перехвата (КП) НРЛ определяется КС от корреспондента *A* к *E*, который описывается моделью ДСК с

вероятностью p_w с входным алфавитом X и выходным алфавитом Z. E принимает на выходе КП последовательность $\bar{z} \in Z^N$.

В МПИ имеются каналы без ошибок (p=0), которые позволяют сформировать между корреспондентами группу каналов обратной связи (КОС) [5]: первый КОС от корреспондента A к корреспонденту B (КОС-1), второй КОС от корреспондента B к корреспонденту A (КОС-2), третий КОС от корреспондента A к корреспонденту C (КОС-3), четвертый канал КОС от корреспондента C к корреспонденту A (КОС-4), 5-й КОС от корреспондента B к корреспонденту C (КОС-5), 6-й КОС от корреспондента C к корреспонденту B (КОС-6). НРЛ контролирует каждый КОС соответствующим идеальным КП обратной связи (КПОС).

Принципы одновременного формирования СК и двух ПК в МПИ заключаются в реализации задач четырех последовательно выполняемых этапов. Первый определяет задачу создания условий, при которых из исходных ДШК и КП, создаются «виртуальные» ДШК и КП, для которых качество первого улучшается по отношению к качеству второго (генерирование начальных данных (НД) корреспондента A последовательности символов $\bar{x}$ и получение НД корреспондентами B и C: последовательностей $\bar{y}$ и $\bar{m}$ на выходах СК1 и СК 2).

Второй этап – формирование начальных данных для одновременного синтеза сетевого и парных ключей: последовательности $\bar{x}$, $\bar{y}$ и $\bar{m}$ выбираются корреспондентами как исходный материал для одновременного формирования ключей. Наличие ошибок в КС1 и КС2 позволяет создать условия для одновременного формирования различающихся СК и ПК [4].

Третий этап предназначен для обеспечения формирования ключей с высокой достоверностью, которая достигается устранением ошибок передачи НД. Для формирования СК исправление производится в НД корреспондентов B и C относительно НД корреспондента A на основе использования дополнительной информации (ДИ). Она передается от A к B и C по КОС. В результате корреспонденты формируют ключевые последовательности (КлП) для формирования СК. Подобным образом для формирования ПК между A и B коррекция производится в НД корреспондента A относительно НД корреспондента B на основе использования ДИ [7]. Она передается от B к A по КОС. В

результате корреспонденты *A* и *B* формируют КлП для формирования ПК. Одновременно для формирования ПК между *A* и *C* исправление производится в НД корреспондента *A* относительно НД корреспондента *C* на основе использования ДИ. Она передается от *C* к *A* по КОС. В результате корреспонденты *A* и *C* формируют КлП для формирования ПК.

Предполагается, что НРЛ перехватывает всю информацию, передаваемую по КПОС и использует для устранения ошибок в НД нарушителя (НДН).

Четвертый этап предназначен для обеспечения формирования ключей с малой вероятностью совпадения с соответствующим ключом НРЛ *E* путем сжатия соответствующих КлП [3].

Предполагается, что модель пассивного НРЛ *E* [3] описывается условиями, когда в ходе реализации первого этапа нарушитель получает по КП НДН $\bar{z}$, а для последующих этапов реализации протокола НРЛ знает полное описание порядка действий корреспондентов и обработки доступной ему информации.

Подводя итог, отметим, что в работе предлагаются принципы открытого сетевого многоключевого согласования, которые позволяют создать условия при реализации в ПОСМС для одновременного формирования различающихся СК и ПК, отвечающим требованиям достоверности и безопасности. Это существенно увеличивает криптосвязность корреспондентов СС и создает условия для быстрого восстановления закрытого информационного обмена в СС в случае компрометации СК (ПК) НРЛ.

Литература:

1. *Menezes A.J., Oorschot P.C., Vanstone S.A.* Handbook of applied cryptography. – CRC Press, N.Y., 1996. – 780 p.

2. *Фергюсон Нильс, Шнайер Брюс.* Практическая криптография: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 424 с.

3. *Синюк А.Д., Остроумов О.А.* Протокол открытого формирования трехстороннего ключа // Наукоемкие технологии в космических исследованиях Земли. – 2014. – Т. 6. № 2. – С. 48-52.

4. *Синюк А.Д., Тарасов А.А.* Информационные базисы открытого сетевого многоключевого согласования // Известия

Института инженерной физики. – 2022. – № 1 (63). – С. 36-42.

5. *Bernard Sklar*. Digital Communications: Fundamentals and Applications. – University of California. Los Angeles, 2007. – 1104 p.

6. *Вентцель Е.С.* Теория вероятностей: Учеб. для вузов. – 9-е изд. стер. – М.: Издательский центр «Академия», 2003. – 576 с.

7. *Берлекэмп Э.* Алгебраическая теория кодирования. – М.: Мир, 1971. – 139 с.

DOI: 10.25728/iccss.2022.68.92.031

Чеканов И.Р., Краснов А.Е.

Анализ семантических элементов базы данных экспертной системы для работы с законодательными и нормативными документами в области информационной безопасности

Аннотация: Текущее положение и острая необходимость развития области информационной безопасности, а также регламентирующих данную сферу документов отражают повышенную актуальность для любой организации и в особенности объектов критических информационных инфраструктур, в обеспечении полного понимания и ориентирования в обширном объеме нормативной базы, необходимой для ведения бизнес-процессов руководителю предприятия. Такая ситуация подчеркивает наличие спроса на использование особой экспертной системы, способной структурным образом предоставить топ-менеджеру сведения рассматриваемой области, в соответствии с поставленным им запросом, помочь в принятии управленческого решения. Важной задачей данной работы является анализ подготовленной базы данных, состоящей из выбранных нормативных и законодательных документов, имеющих наибольшую ценность в области информационной безопасности для организаций и выделение наиболее важных, примечательных закономерных особенностей и свойств, способных помочь в разработке экспертной системы

Ключевые слова: база данных, информационная безопасность, законодательные и нормативные документы, семантические элементы, экспертная система

Особую актуальность в настоящее время имеет вопрос информационной безопасности (ИБ) страны. Большую роль в обеспечении защищенности государства и высокой квалификации сотрудников занимает ориентирование в необходимом объеме нормативных и законодательных документов в области ИБ.

Путем анализа научных работ по заданной тематике [1] было выявлено особое значение в создании базы данных нормативных и законодательных документов, которые будут использованы для построения экспертной системы помощи специалистам на основе разрабатываемой архитектуры и функционала.

Для такой объемной и многоэтапной работы необходимо начать с обозначения фундаментального объема основных документов, на которые можно опираться в систематизации. Благодаря поиску ресурсов, справочников и перечней документов ИБ [2], удалось собрать 383 документа в области информационной безопасности, способный к полноценному применению в работе отделов ИБ организаций с небольшой корректировкой в соответствии с нуждами специфики предприятия.

Основными юридическими группами, в которые вошли собранные документы по ИБ, имеющие различную юридическую силу, были выделены:

- международные нормативные правовые акты (НПА) – 2 шт.;
- федеральные законы – 55 шт.;
- указы Президента – 13 шт.;
- постановления Правительства – 74 шт.;
- акты министерств и ведомств – 90 шт.;
- стандарты – 38 шт.;
- законы субъектов РФ – 3 шт.;
- НПА Банка России – 35 шт.;
- стандарты Банка – 15 шт.;
- документы, носящие рекомендательный характер – 57 шт.;
- судебная практика – 3 шт.

Процесс исследования заключается в анализе ключевых семантических элементов базы данных, которые отбирались

вручную студентами области информационной безопасности в процессе детального изучения каждого из документов.

Ручной отбор семантических элементов представляет собой опору на вводные ключевые слова, указанные, как правило, в начале документа, а также смысловую нагрузку в процессе детального изучения текста целиком. Данной практической частью исследования были заняты студенты РГСУ, обучающиеся по специальности «Безопасность информационных технологий в правоохранительной сфере», в рамках учебной практики.

Общее число ключевых элементов базы составило примерно 30 тыс., что в среднем на документ приходится 78 слов.

Последующая обработка носила автоматизированный характер, с помощью Интернет-ресурса ADVEGO [3]. Подготовленный список всевозможных терминов, обобщений и конкретных смысловых значений для каждого из документов, был скопирован в поле анализа текста.

Выявленные наиболее часто встречающиеся слова представлены на гистограмме (рисунок 1), где вертикальная ось представляет собой количество встречающихся повторяемых слов, а горизонтальная ось – сами семантические элементы, слова.

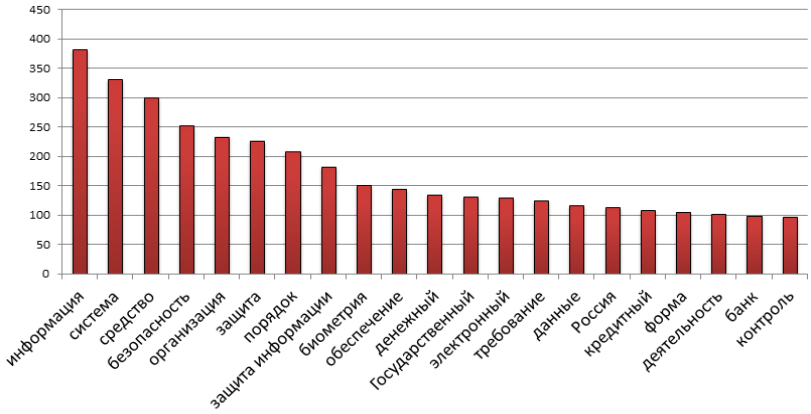


Рисунок 1 – Гистограмма часто встречающихся ключевых слов

Как видно из гистограммы, многие слова носят более общий характер. Можно объединить и просуммировать выявленные

элементы в небольшие подгруппы, позволяющие сделать определенный вывод об анализируемой базе.

Выделенными группами, характеризующие определенные составляющие являются:

– информационная безопасность (информация, безопасность, защита, защита информации, деятельность, контроль), общее количество слов группы – 1242;

– программные и аппаратные средства защиты (система, Средство, биометрия, обеспечение, электронный), общее количество слов – 1059;

– организационные аспекты (организация, государственный, Россия), общее количество слов – 478;

– финансовые аспекты (денежный, кредитный, банк), общее количество слов – 340;

Бухгалтерские аспекты (порядок, требование, данные, форма), общее количество слов – 439.

Вычисляем процентное соотношение каждой группы от общего числа (3558 слов):

ИБ = $\frac{1242}{3558} * 100\% \approx 35\%$;

программные и аппаратные средства защиты = $\frac{1059}{3558} * 100\% \approx 30\%$;

организационные аспекты = $\frac{478}{3558} * 100\% \approx 13\%$;

финансовые аспекты = $\frac{340}{3558} * 100\% \approx 10\%$;

бухгалтерские аспекты = $\frac{439}{3558} * 100\% \approx 12\%$.

Соотношение указано на диаграмме (рисунок 2).

Таким образом, из анализа следует, что наибольшее внимание в подготовленной базе данных занимают общие вопросы ИБ, компоненты программной и аппаратной защиты, а также организационные, финансо и бухгалтерские аспекты, которые наиболее важны в деятельности любой организации. Данное исследование позволяет определить основные освещаемые стороны собранной базы данных, определить векторы построения базы знаний и основного функционала разрабатываемой экспертной системы.

Рисунок 2 – Диаграмма соотношения обобщенных ключевых групп

Литература:

1. *Чеканов И.Р., Краснов А.Е.* К вопросу построения архитектуры законодательных и нормативных документов в области информационной безопасности / Цифровизация в условиях пандемии: миссия социального университета будущего: Сборник материалов XXI международного социального конгресса. Москва, 25-26 ноября 2021 года. – Москва: Издательство Российского государственного социального университета, 2022. – С. 344-347.

2. Справочник законодательства РФ в области информационной безопасности (версия от 13.10.2022) [Электронный ресурс]. – URL: https://habr.com/ru/post/432466/ (дата обращения 13.10.2022).

3. ADVERGO [Электронный ресурс]. – URL: https://advego.com/ (дата обращения 01.10.2021).

IV. Кибербезопасность. Особенности обеспечения безопасности в социальных сетях

DOI: 10.25728/iccss.2022.57.97.032

Промыслов В.Г., Семенков К.В.

Проблема обеспечения кибербезопасности критических объектов в недоверенной среде

Аннотация: В работе рассматривается проблема синхронизации жизненного цикла кибербезопасности с жизненным циклом объекта в промышленных системах. Отмечается, что несоответствие в жизненных циклах может привести к невозможности обеспечить основные свойства монитора безопасности в системе. Для противодействия данной угрозе, предлагается использовать глубокоэшелонированную защиту основных компонентов системы от информационных угроз.

Ключевые слова: кибербезопасность, глубокоэшелонированная защита, жизненный цикл, доверенная среда

Введение

Концепция обеспечения информационной безопасности по умолчанию всегда строилась на концепции доверия [1]. В рамках этой концепции основным являлось понятие доверенной среды и наличия монитора обращений, в рамках которого реализовывалась политика безопасности. Причем предполагалось, что монитор обладает свойствами, препятствующими попыткам его обмануть или скомпрометировать, постоянной готовностью и простотой.

Концепция доверия, несмотря на некоторые сложности в ее реализации, в целом выполнялась и выполняется для большинства цифровых систем общего назначения, ориентированных в основном на конфиденциальность. Однако реализация данной концепции столкнулась с трудностями, когда встала проблема обеспечения информационной безопасности, для промышленных объектов с

цифровыми системами управления ориентированной на сохранение доступности и целостности. Информационную безопасность в контексте промышленных объектов, часто определяют как кибербезопасность, чтобы подчеркнуть различие в приоритетах целей безопасности. Проблема обеспечения кибербезопасности промышленных систем является комплексной, связанной с обеспечением общепромышленной безопасности. Для критических объектов безопасность может быть также связана с энергетической, транспортной, ядерной и иными аспектами безопасности [2].

Трудности в реализации механизма монитора обращений и всей доверенной среды для промышленных систем управления состоят в том, что жизненный цикл системы кибербезопасности не соответствует жизненному циклу объекта, что приводит к невозможности обеспечить основные свойства безопасности монитора обращений.

В работе рассмотрены проблема соотнесения жизненного цикла кибербезопасности с жизненным циклом защищаемой системы и предложены решения, смягчающие несоответствия в жизненных циклах.

Жизненный цикл обеспечения кибербезопасности

Возможный жизненный цикл работ по обеспечению кибербезопасности программируемой цифровой АСУ ТП для атомной электростанции (АЭС) и его соотнесение с жизненным циклом самой АСУ ТП приведен на рисунке 1.

Можно видеть, что по составу этапов жизненные циклы защищаемой системы (левая часть рисунка) и системы кибербезопасности (правая часть) принципиально не отличаются. Проблема возникает в случае наличия переходов между этапами вверх на каждом из жизненных циклов. Такие переходы могут возникать при устранении несоответствий в выполненных ранее работах на объекте, повышения эффективности его функционирования, а для системы кибербезопасности, например, при выявлении новых угроз для системы или уязвимостей в компонентах.

Временные рамки таких переходов и их частота, как показала практика, не сопоставима для обоих жизненных циклов. Для примера приведем характерные значения для АСУ ТП АЭС (таблица 1).

Рисунок 1 – Жизненный цикл работ по обеспечению кибербезопасности АСУ ТП АЭС

Таблица 1 – Параметры жизненного цикла. Данные параметры являются субъективными оценками авторами, основанными на опыте работы для проектов АСУ ТП АЭС с реакторами типа ВВР-1000

Параметр	Система кибербезопасности АСУ ТП АЭС	АСУ ТП АЭС
Частота необходимостей изменений в год	Еженедельно	Менее 5 раз в год
Частота уязвимостей/несоответствий	Около 200 в месяц	Менее 5 в год
Фактическая длительность внесения изменения на объекте	Менее 1 дня	От одного дня до нескольких недель
Время на подготовку изменения	Около 1 месяца	Не менее 1 месяца

Как мы видим, число выявленных несоответствий и интервал их устранения значительно отличаются для ситемы кибербезопасности и собственно объекта защиты. Оценка частоты выявления уязвимостей сделана по базе данных уязвимостей CVE [3]. За 2021 год выявлено чуть более 20000 новых уязвимостей, с учётом того, что значения охватывают все наиболее известные ОС и прикладные пакеты, то для конкретной АСУ ТП доля уязвимостей, относящихся к ней, по нашим оценкам будет составлять около 10 процентов. Следовательно, за год в системе будет открыто приблизительно 2000 уязвимостей, часть которых будет носить критический характер.

Остальные значения, оценивающие трудоемкость внесения изменений сравнимы. Необходимо также учесть, что некоторые обновления программных пакетов, требуемые для кибербезопасности, конфликтуют с прикладным ПО (программным обеспечением АСУ ТП), и для их установки требуется переработка прикладного ПО. Таким образом, если жизненный цикл объекта превалирует над жизненным циклом его системы кибербезопасности, то это приводит к тому, что основную часть времени система находится в недоверенном с точки зрения кибербезопасности состоянии.

Очевидным способом обеспечения кибербезопасности в этом случае является внедрение административных и организационных мер защиты или применения, если это возможно, стратегии по переносе риска кибербезопасности от объекта на третью сторону. Однако перенос риска, являясь предпочтительным, невозможен для многих объектов критической инфраструктуры т.к. риск для них может быть неприемлемым ни в какой форме, а административные и организационные меры сами по себе не могут обеспечить кибербезопасность системы. Одним из способов обеспечения кибербезопасности в частично недоверенной среде является реализация на уровне архитектуры системы концепции глубоко эшелонированной защиты кибербезопасности ГЭЗК [4].

Архитектура кибербезопасности для работы в недоверенной среде

Глубокоэшелонированная защита от компрометации активов по кибербезопасности включает в себя обеспечение нескольких последовательных мер защиты, которые необходимо обойти для

того, чтобы кибератака прогрессировала и повлияла на компонент АСУ ТП и на выполняемые системой критические функции.

Последовательность преодоления мер защиты, на пути атаки обеспечивается делением системы на уровни и зоны кибербезопасности (рисунок 2).

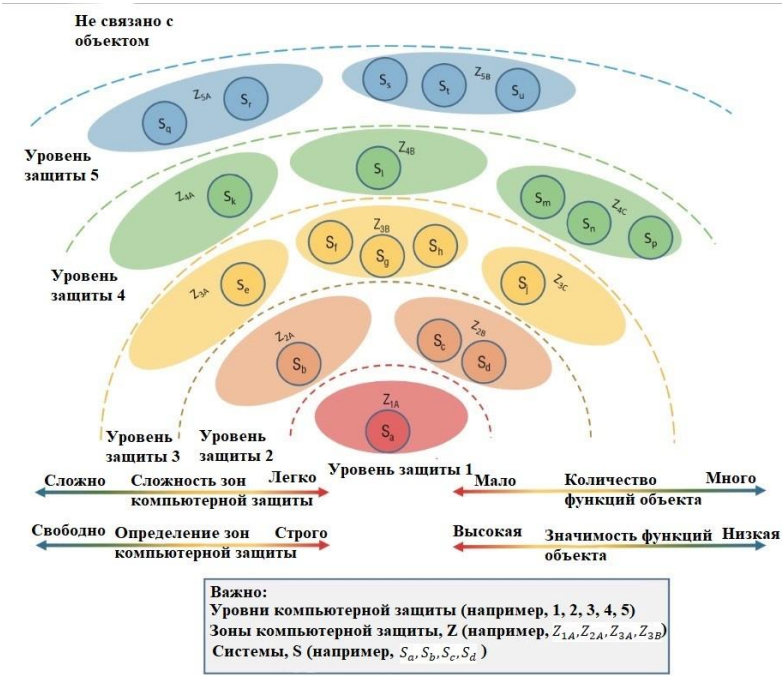


Рисунок 2 – Концептуальная модель уровней и зон кибербезопасности в рамках ГЭЗК [2]

Для кибербезопасности важно не только наличие последовательных мер защиты, но и их разнообразие. Разнообразие в реализации мер защиты потенциально увеличивает возможную размерность вектора атаки. Это происходит из-за большего набора механизмов защиты, которые может атаковать злоумышленник, но это же и обеспечивает независимость мер защиты в последовательной цепочке барьеров, преодолеваемых злоумышленником.

Общий подход в обеспечении ГЭЗК включает в себя пункты, необходимые для обеспечения кибербезопасности с использованием комбинации независимых и разнообразных мер. Данные меры должны быть преодолены нарушителем для достижения целей атаки путем компрометации актива [5]. Разработчики подсистем при выборе компенсирующих мер защиты должны учитывать воздействие конкретной меры защиты на определенную угрозу.

Заключение

В современном мире обеспечение кибербезопасности промышленных объектов, например АЭС, транспортной и энергетической инфраструктуры является актуальной задачей. Однако, ее трудно решить, оставаясь в рамках классической парадигмы, когда уязвимости, по крайней мере связанные с критическими компонентами системы, устраняются фактически сразу после их появления. Практика показывает, что из-за несоответствия временных рамок жизненного цикла объекта защиты и системы обеспечения кибербезопасности основную часть времени в системе нельзя выделить доверенную часть. Это верно не только для этапа эксплуатации, но и для более ранних этапов жизненного цикла: проектирования и разработки.

Задачу обеспечения кибербезопасности в этом случае необходимо трактовать как комплексную задачу, с приоритетом административных, организационных и физических мер защиты.

Как одна из возможных мер, обеспечивающих выполнение системой кибербезопасности своих функций, предлагается использовать концепцию глубокоэшелонированной защиты, реализуемую на уровне архитектуры защищаемого объекта.

Литература:

1. Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD Supersedes CSC-STD-00l-83, dtd l5 Aug 83. Library №. S225,7ll. – URL: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf (дата обращения 12.10.2022).

2. IAEA 17-T INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear

Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021). – URL: https://www.iaea.org/publications/14729/computer-security-techniques-for-nuclear-facilities (дата обращения 12.10.2022).

3. CVE [Электронный ресурс]. – URL: https://cve.mitre.org (дата обращения 12.10.2022).

4. *Промыслов В.Г., Семенков К.В., Шумов А.С.* Синтез архитектуры кибербезопасности для систем управления атомных электростанций // Проблемы управления. – 2019. – № 3. – С. 61-71.

5. *Chris Moschovitis.* "Controls," in Privacy, Regulations, and Cybersecurity: The Essential Business Guide. – John Wiley & Sons, 2021. – P. 301-320. DOI: 10.1002/9781119660156.ch18

DOI: 10.25728/iccss.2022.60.22.033

Степанцов М.Е.

Моделирование сценария информационного противоборства с асимметричным влиянием на малые группы

Аннотация: В работе рассматривается сценарий бинарного информационного противоборства, в котором одна из сторон имеет большую степень влияния на общество в целом, а вторая – на малые группы. Для математического моделирования используется ранее предложенная автором клеточно-автоматная модификация модели информационного противоборства, основанной на нейрологической схеме Рашевского. Вычислительные эксперименты, проведенные при помощи имитационной системы, построенной на основе данной модели, показывают, что в достаточно широком диапазоне параметров описанная ситуация приводит к «атомизации» общества.

Ключевые слова: математическое моделирование, имитационное моделирование, клеточные автоматы, информационное противоборство, малые группы

В рамках исследования различных сценариев информационного противоборства представляется уместным рассмотреть ситуацию, в которой информационное воздействие с двух сторон происходит

асимметричным образом. В частности, в данной работе будет рассмотрен случай, когда одна из альтернатив более интенсивно влияет на позицию индивида, будучи представленной в качестве поддерживаемой обществом в целом, а вторая – через малые группы.

Для анализа упомянутого сценария воспользуемся дискретной модификацией модели информационного противоборства [1], основанной на нейрологической схеме Рашевского [2]. Исходная непрерывная модель рассматривает простейший случай информационной кампании, в которой индивиды осуществляют выбор одной из двух позиций – L или R – по некоторому вопросу. При этом у одних индивидов существует априорное мнение по этому вопросу, а у других оно изначально не определено.

Данная модель имеет вид интегро-дифференциального уравнения

$$\frac{d\psi}{dt} = A\left(C\left(2\int\limits_{-\psi(t)}^{+\infty} N(\varphi)\,d\varphi - N_0\right) + b_R - b_L\right) - a\psi \qquad (1)$$

с начальным условием

$$L(0) = \int\limits_{-\infty}^{-\psi(0)} N(\varphi)\,d\varphi. \qquad (2)$$

Функция $\psi(t)$ определяет сдвиг предпочтений индивидов под влиянием пропаганды. Параметры b_R, b_L, C, A и a характеризуют соответственно, интенсивность влияния пропаганды альтернатив R и L, общественного мнения, способность индивидов менять свое мнение и «затухание» таких изменений.

Однако анализ влияния малых групп на позицию индивида удобнее проводить при помощи аналогичной дискретной модели [3], представляющей собой двумерный клеточный автомат на классической ортогональной решетке с клетками, имеющими три возможных состояния (поддержка альтернативы L (-1), поддержка альтернативы R (1) и не определившиеся взгляды (0)), и параметр u,

принимающий одно из этих же значений и задающий априорное состояние взглядов индивида.

В работе [3] было доказано, что последовательное применение на каждом шаге по времени к каждой клетке трех алгоритмов, приводимых ниже, приводит при правильном подборе коэффициентов к такой же макродинамике, какая порождается исходной непрерывной моделью.

Алгоритм А (прямое влияние пропаганды)

if Δ > 0 then
if Center = 0 and r < Δ then Center = 1
if Center = -1 and r < Δ then Center = 0
end if
if Δ < 0 then
if Center = 0 and r < -Δ then Center = -1
if Center = 1 and r < -Δ then Center = 0
end if

Здесь $\Delta = A^*(b_R - b_L)$ – интегральное влияние пропаганды в пользу каждой из альтернатив, $r \in [0;1]$ – случайное число, *Center* – традиционное обозначение состояния рассматриваемой клетки поля клеточного автомата. Все коэффициенты, обозначенные звездочкой, имеют тот же смысл, что и в непрерывной модели, но не обязательно совпадают с ними численно.

Алгоритм Б (затухание изменений точки зрения, вызванных пропагандой)

if not u = Center then
if r < a^* then
if Center > u then Center = Center – 1
if Center < u then Center = Center + 1
end if
end if

Алгоритм В (влияние общественного мнения и малых групп)

S=North+NorthWest+West+SouthWest+South+SouthEast+East+NorthEast

if $\psi^* > 0$ then
if Center < 1 and r < c ψ^* then Center = Center + 1*
end if

if $\psi^* < 0$ *then*
if Center > -1 and r < -c ψ* then Center = Center – 1*
end if
if S > 0 then
if Center < 1 and r < d S then Center = Center + 1*
end if
if S < 0 then
if Center > -1 and r < -d S then Center = Center – 1*
end if

Здесь *d** – коэффициент, характеризующий влияние на мнение индивида его ближайшего окружения, в качестве модели которого может взята окрестность Мура [4] (переменные *North*, *NorthWest*, *West*, *SouthWest*, *South*, *SouthEast*, *East* и *NorthEast* представляют собой состояния восьми клеток-соседей данной). Интериоризация общественного мнения и мнения малых групп, также рассматривавшаяся в [3], не использовалась в данном исследовании, поэтому вторая часть алгоритма B, приведенного в [3], здесь отсутствует.

В рамках данного исследования рассматривалась ситуация, при которой пропаганда альтернативы R позиционируется как общественно приемлемая и оказывает большее влияние на мнение индивида со стороны общества в целом, а альтернативы L – влияет преимущественно через малые группы. Для реализации этого предположения в алгоритме B были использованы две пары различных коэффициентов *c**и *d** для описания влияния общественного мнения и мнения малой группы в пользу той или иной альтернативы. Таким образом, алгоритм принял вид:

Алгоритм B1 (асимметричное влияние общественного мнения и малых групп, интериоризация)

S=North+NorthWest+West+SouthWest+South+SouthEast+East+NorthEast

if $\psi^* > 0$ *then*
if Center < 1 and r < $c_R^* \psi^*$ *then Center = Center + 1*
end if
if $\psi^* < 0$ *then*
if Center > -1 and r < $-c_L^* \psi^*$ *then Center = Center – 1*

end if
if S > 0 then
if Center < 1 and r < $d_R^* S$ then Center = Center + 1
end if
if S < 0 then
if Center > -1 and r < $-d_L^* S$ then Center = Center – 1
end if

При этом значения коэффициентов выбирались так, чтобы $c_L^* < c_R^*$ и $d_L^* > d_R^*$.

При помощи такой модифицированной модели были проведены вычислительные эксперименты. Для достаточно широкого набора значений параметров при равной интенсивности пропаганды с обеих сторон была изучена динамика модели на протяжении 100 шагов по времени. При этом исследовались случаи симметричного (с использованием алгоритма B) и асимметричного (B1) влияния пропаганды двух альтернатив. Во втором случае устойчиво наблюдалась картина, при которой поле клеточного автомата распадается на небольшие участки, в которых клетки находятся в одинаковом состоянии.

Типичные примеры распределения состояний клеток по полю клеточного автомата приведены на рисунке 1.

Для численной оценки различия распределений рассмотрим на поле клеточного автомата окрестности Марголуса [4] (все возможные квадраты 2x2). В каждом эксперименте были вычислены доли тех из них, состояния клеток в которых оказались одинаковыми. По результатам 80 пар экспериментов средняя доля для симметричного влияния оказалась равной 0,0166, а для асимметричного – 0,0942. Уровень значимости различий при этом оказывается равным 0,008, то есть различия в долях практически достоверны.

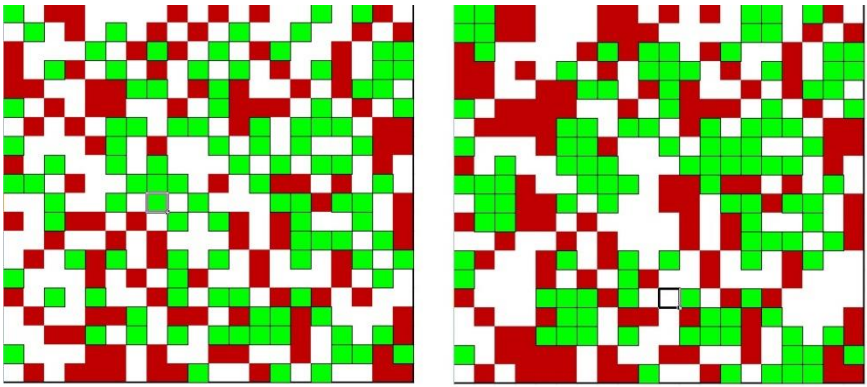


Рисунок 1 – Распределение клеток, изображающих мнения индивидов в случаях симметричного (слева) и асимметричного (справа) влияния пропаганды

Если предположить, что рассматриваемые альтернативы являются значимыми для индивидов (то есть, если это, например, не сорта предпочтительных напитков, а важные вопросы жизни общества и базовых ценностей), то данное явление социологи предлагают интерпретировать как атомизацию общества [5], при которой последнее распадается на отдельные группы, социальные связи между которыми слабеют и/или становятся чисто формальными. Эта крайне вредная для развития и угрожающая самому существованию общества ситуация, как мы видим, может возникать или усиливаться благодаря тому, что альтернативы, из которых обществу предстоит делать выбор, ставятся в неравное положение.

Литература:

1. *Петров А.П., Маслов А.И., Цаплин Н.А.* Моделирование выбора позиций индивидами при информационном противоборстве в социуме // Математическое моделирование. – 2015. – Т.27. №12. – С. 137-148.

2. *Rashevsky N.* Mathematical biophysics: physicomathematical foundations of biology. − Univ. of Chicago, Chicago Press, 1938. – 340 p.

3. *Степанцов М.Е.* Моделирование некоторых сценариев информационного противоборства при помощи клеточного автомата / Проектирование будущего. Проблемы цифровой реальности: труды 5-й Международной конференции (3-4 февраля 2022 г., г. Москва). – М.: ИПМ им. М.В. Келдыша, 2022. – С. 205-214.

4. *Тоффоли Т., Марголус Н.* Машины клеточных автоматов. – М: Мир, 1991. – 283 с.

5. *Новиков А.С.* Атомизация общества и её роль в становлении «общества масс» // Теория и история. – 2009. – № 2. – С. 192-197.

DOI: 10.25728/iccss.2022.76.66.034

Исхакова А.О.

Детектирование разнородных проявлений кибератак на примерах анализа веб-ресурсов

Аннотация: В работе авторами поднимается вопрос анализа электронного текстового и медиаконтента с целью выявления кибератак. Рассматривается пласт кибератак, характеризующийся использованием виртуальной среды, сети Интернет, различных онлайн-инструментов для осуществления неправомерных действий. Обозначено направление обработки и анализа перечисленных средств для детектирования проявлений кибератак на основе эмоционального воздействия на пользователя.

Ключевые слова: кибератака, Интернет, веб-ресурс, виртуальная среда, анализ данных, эмоциональное воздействие, Интернет-контент

В последние годы влияние виртуальной среды на человека выросло в разы. На это повлияли многократный рост ресурсов, вовлеченность всех сфер жизни, бизнеса, социальных институтов в онлайн формат, привлекательность создаваемого контента. Вместе с масштабом Интернет-среды выросла и его значимость для человека – его потребителя [1, 2]. Веб-ресурсы, а также ресурсы на основе популярных мессенджеров, на сегодняшний день, являются основным методом как информирования населения, так и воздействия на него. Возможность сокрытия авторства, отсутствие

строгих канонов представления информации, доступность как с точки зрения формирования контента, так и с точки зрения потребления, – факторы, которые позволяют говорить о высоком потенциале виртуальной среды как средства воздействия на человека, манипуляции и обмана.

Многими специалистами используется достаточно радикальное определение совокупности описанных процессов – «информационная война» [3, 4]. Если говорить о формах воздействия в Интернете, то нельзя назвать их жестокими и бесчеловечными (как подразумевает упомянутое определение). Однако присущие в данном случае массовость, сложность детектирования и блокирования, разнообразие реализаций позволяют сегодня констатировать в этой связи серьезную угрозу для государства.

Исследование данного направления показало, что перспективными являются несколько направлений детектирования проявлений угроз через воздействие на пользователей в виртуальной среде:

1) оценка процессов функционирования сообществ социальных сетей;

2) оценка эмоциональной составляющей содержимого виртуального контента;

3) оценка воздействия конкретных проявлений контента (цвет, частота звука, шрифт и т.д.);

4) экспертное формирование перечня рубрик, с использованием которых воздействие наиболее вероятно.

Например, цикл работ [5-7] по созданию динамической системы функционирования сообществ социальной сети показал, что ресурсу присуще характерное изменение выделенных показателей в разные периоды. Например, размещение нового контента закономерно порождает всплеск ответных действий пользователей. Но при этом факты искусственной активизации и «раскрутки» заданной темы показывают характерные изменения графиков поведения аудитории.

В работе [8] представлен результат оценки воздействия звуковых частот на оператора (слушателя) с целью выявления возможных реакций. Сравнительная таблица оценок информативности рассмотренных время-частотных преобразований для анализа паттернов пользовательских показателей показала, что определенные частоты заставляют чувствовать пользователя

усталость или наоборот бодрость. Однако сложность оценки биомедицинских сигналов не позволяет повсеместно применять такой подход в исследуемой задаче.

Подход на основе оценки эмоциональной составляющей Интернет-контента предоставил наибольший потенциал в части автоматизации процесса детектирования исследуемых кибератак. В связи с гетерогенностью электронных материалов следует исследовать каждый из них, но сначала по отдельности, а в дальнейшем объединять результаты. Применение методов машинного обучения, в частности нейронных сетей, позволяет сегодня говорить о возможности достаточно эффективной классификации медиафайлов по признаку наличия эмоции. Например, при исследовании изображений с целью выявления деструктивного Интернет-контента по одному кадру [9] удалось показать точность классификации не ниже 80 %, по всем классам при тестировании на заранее размеченной коллекции. В работе [10] показаны идентичные исследования по голосовому (аудио) материалу.

Задача классификации разнородного контента, распространяемого в сети, во многом является слабоформализованной. Процессы в сообществах социальных сетей зачастую зависят от множества неоцениваемых факторов. Разбиение на классы субъективно. Проявление эмоций или форм воздействия можно оценить как многоликое и сложно учитываемое. Все эти факторы объясняют наличие множества направлений исследований для решения задачи выявления кибератак в контенте социальных сетей, а также трудоемкость их компоновки. При этом применение методов машинного обучения позволило достичь высоких результатов классификации медиаконтента – обнаружения материалов агрессивного содержания – до 80 %, что говорит о перспективности данного подхода.

Исследование выполнено при финансовой поддержке гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук МК-3172.2021.1.6

Литература:

1. *Казарин О.В., Скиба В.Ю., Шаряпов Р.А.* Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. – 2016. – № 1(3). – С. 54-72.

2. *Власенко М.С.* Обеспечение информационной безопасности несовершеннолетних в сети интернет: современное состояние и совершенствование правового регулирования // Вестник Волжского университета им. В.Н. Татищева. – 2019. – Т. 1. № 3. – С. 98-105.

3. *Губанов Д.А., Новиков Д.А., Чхартишвили А.Г.* Информационные войны и социальные сети // Информационные войны. – 2010. – № 3 (15). – С. 44-53.

4. *Фролов Н.В.* Социальные сети как инструмент ведения информационных войн // Социодинамика. – 2018. – № 8. – С. 1-6.

5. *Охапкина Е.П., Охапкин В.П., Мещеряков Р.В., Исхакова А.О., Исхаков А.Ю.* Динамическая система функционирования сообществ социальной сети // Известия Кабардино-Балкарского научного центра РАН. – 2022. – № 2 (106). – С. 41-71.

6. *Охапкина Е.П., Мещеряков Р.В., Исхакова А.О., Исхаков А.Ю.* К вопросу устойчивости динамической системы функционирования сообществ социальной сети // Вестник КРАУНЦ. Физико-математические науки. – 2022. – Т. 38. № 1. – С. 106-130.

7. *Охапкина Е.П., Роганов А.А.* Управляющие воздействия в социальных сетях: аспекты выявления / Комплексная защита информации. Материалы XXVI научно-практической конференции. Ответственный за выпуск Касанин С.Н. – Минск: И.Сивчиков, 2021. – С. 192-195.

8. *Iskhakova A.O., Alekhin M.D., Bogomolov A.V.* Time-frequency transforms in analysis of non-stationary quasiperiodic biomedical signal patterns for acoustic anomaly detection // Информационно-управляющие системы. – 2020. – № 1. – С. 15-23.

9. *Русаков К.Д., Исхакова А.О., Мещеряков Р.В.* Распознавание деструктивного мультимедиаконтента в социокиберфизической системе мониторинга сети интернет по одному кадру // Нейрокомпьютеры: разработка, применение. – 2022. – Т. 24. № 3. – С. 5-17.

10. *Iskhakova A.O., Wolf D.A., Galin R.R., Mamchenko M.V.* 1-D

convolutional neural network based on the inner ear principle to automatically assess human's emotional state // E3S Web of Conferences. – 2020. – Vol. 224. – P. 1-10.

DOI: 10.25728/iccss.2022.95.50.035

Асратян Р.Э.

Подход к созданию защищенных сетевых туннелей в распределенных системах на основе Cryptographic Message Syntax (CMS)

Аннотация: Рассмотрен новый подход к построению защищенных каналов (туннелей) через общедоступную сеть, основанный на использовании технологии Cryptographic Message Syntax (CMS) для инкапсуляции информационных запросов в структуру т.н. «защищенного сообщения». Показано, что, в отличие от известных подходов, предложенная организация защищенного туннеля позволяет ему гибко настраиваться на работу с любой криптосистемой, поддерживающей стандарт CMS, прямо в ходе работы без какой-либо доработки и/или конфигурирования.

Ключевые слова: распределенные системы, VPN, информационная безопасность, web-сервисы, разграничение прав доступа, маршрутизация запросов

Так как почти все современные территориально-распределенные информационные системы используют Интернет для организации взаимодействия удаленных друг от друга рабочих станций и серверов, задача защиты данных в общедоступной сети уже давно находится в центре внимания разработчиков [1, 2]. Разумеется, возможно интегрировать крипто-средства и защищенные сетевые протоколы непосредственно в клиентские и сервисные компоненты системы. Однако такое решение весьма трудоемко, а цена ошибки в данной области может быть высока. Поэтому, обычный способ решения этой задачи заключается в использовании технологии VPN (Virtual Private Network), в качестве готового решения, позволяющего реализовать защищенный «туннель» через общедоступную сеть [3, 4]. Так как средства криптозащиты

подключаются в VPN на нижнем уровне иерархии протоколов OSI (на «сетевом» или «транспортном»), эта технология отличается высокой универсальностью: «выгодополучателями» оказываются все сетевые службы и протоколы уровня приложения – от WWW и электронной почты до Удаленного рабочего стола.

Тем не менее, разработчики распределенных систем до сих пор сталкиваются с серьезными сложностями в области информационной безопасности. Это в основном связано с дефицитом готовых технических решений для таких задач, как разграничение прав доступа к информационным ресурсам, аутентификация информационных запросов и проверка подлинности серверов, организация доступа к серверам, «спрятанным» в т.н. частных локальных сетях предприятий. Это приводит разработчиков к необходимости создавать множество «частных решений» этих задач, приспособленных к особенностям конкретных проектов, что увеличивает трудозатраты и риск появления «пробелов» в информационной защите.

В данной работе рассматривается новый подход к организации безопасных взаимодействий в распределенных системах, основанный на построении защищенных сетевых туннелей с помощью технологии CMS [5]. В отличие от традиционных, данный подход является строго специализированным: он ориентирован на поддержку систем, использующих технологию web-сервисов [6, 7] для обслуживания информационных запросов. Именно эта специализация позволяет дольше продвинуться в сторону готовых технических решений по сравнению с универсальными технологиями.

Описываемый подход опирается на соединение двух сетевых технологий: CMS и технологии прокси-серверов. В основу CMS заложено понятие (и соответственный программный класс) «подписанного сообщения» (SignedCms), представляющее собой своего рода защищенный контейнер для хранения информации и обеспечения ее аутентичности и конфиденциальности. С этой целью класс SignedCms оснащен необходимыми функциями-членами для загрузки в него произвольных данных, формирования и проверки электронных подписей, шифрования и расшифровки данных. Важным свойством CMS является его способность использовать любую криптосистему, поддерживающую этот стандарт (выбор

криптосистемы осуществляется динамически и целиком определяется используемым сертификатом открытого ключа). Защищенный туннель, опирающийся на CMS, в полной мере «наследует» эту гибкость в выборе крипто-средств (рисунок 1).

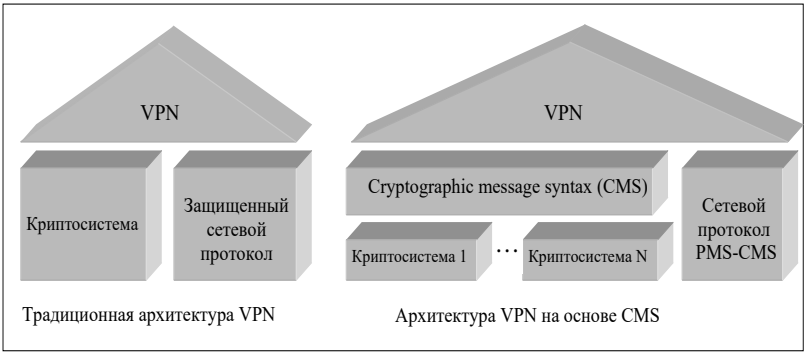


Рисунок 1 – Архитектурные решения для реализации VPN

Структура защищенного туннеля приведена на рисунке 2. Как видно из рисунка, его основу составляют два шлюза: клиентский (CG) и серверный (SG). Каждый шлюз представляет собой постоянно активную программу, размещенную или на рабочей станции, или на выделенном сервере. Основное назначение клиентского шлюза включает выполнение следующих функций:

- «перехват» исходящих от клиента HTTP/SOAP-запросов в режиме прокси-сервера,
- анализ заголовков запросов и выбор удаленного SG на основе имени адресуемого web-сервера (высокоуровневая маршрутизация запросов),
- установка защищенного соединения с выбранным SG и проверка подлинности серверного шлюза на основе сертификата открытого ключа,
- инкапсуляция информационного запроса в объект SignedCms, формирование электронной подписи CG, шифрование его открытым кличем SG, передача объекта серверному шлюзу и получение от него другого объекта SignedCms, содержащего результат обработки запроса,

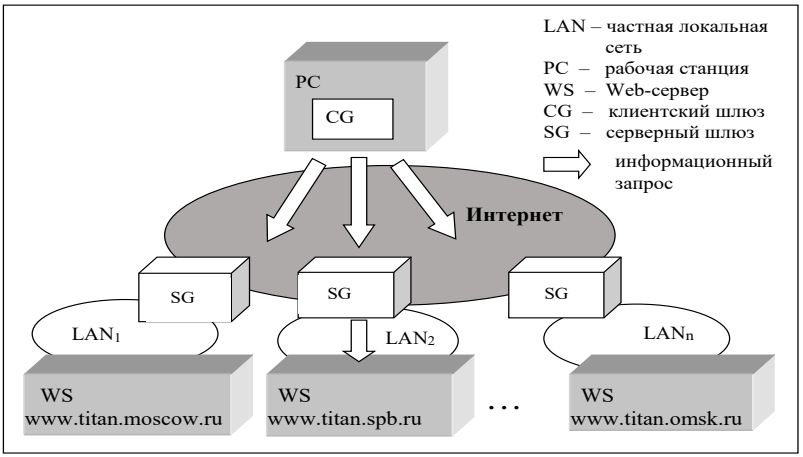


Рисунок 2 – Высокоуровневая маршрутизация запросов в туннеле

- расшифровка, проверка электронной подписи SG в полученном объекте, извлечение из него результата обработки запроса и передача последнего клиенту.

Основное назначение серверного шлюза включает выполнение следующих функций:

- установление защищенного соединения с клиентским шлюзом по его запросу и передача ему сертификата открытого ключа,
- получение объекта SignedCms, содержащего информационный запрос, от клиентского шлюза,
- расшифровка, проверка электронной подписи CG в полученном объекте и извлечение из него информационного запроса,
- проверка права клиента на доступ к адресуемому web-сервису или к отдельной сервисной функции на основе сертификата открытого ключа, полученного от клиентского шлюза,
- установление открытого сетевого соединения с web-сервисом и передача ему полученного информационного запроса,
- получение результата обработки запроса от web-сервиса по открытому соединению,
- инкапсуляция результата обработки запроса в объект SignedCms, формирование электронной подписи SG, шифрование

его открытым кличем CG и передача объекта клиентскому шлюзу и передача его клиентскому шлюзу по защищенному соединению.

Важно отметить, что конверсия имени адресуемого web-сервера в IP-адрес осуществляется лишь после доставки запроса в SG. Поэтому, сложная ситуация, в которой web-серверы в различных частных локальных сетях имеют одинаковые «серые» адреса, не вызывает никаких проблем.

Проверка прав доступа к web-сервисам или отдельным функциям-членам осуществляется на основе сопоставления реквизитов владельца клиентского сертификата открытого ключа с контрольными значениями реквизитов, указанными в конфигурационном файле серверного шлюза.

Литература:

1. *Салимова Ш.А.* Кибербезопасность в России: актуальные угрозы и пути обеспечения в современных условиях / Достижения вузовской науки 2021: Сборник статей XVII Международного научно-исследовательского конкурса, Пенза, 20 января 2021 года. – Пенза: «Наука и Просвещение», 2021. – С. 207-214.

2. *Жаранова А.О.*, *Птицына Л.К.* Анализ влияния распределенности на качество функционирования комплексных систем защиты информации / Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020): Сборник научных статей IX Международной научно-технической и научно-методической конференции. – СПб: СПБГУТ, 2020. – С. 324-327.

3. *Акушуев Р.Т.* Принцип работы VPN и его особенности // Modern Science. – 2020. – № 7. – С. 312-314.

4. *Хант К.* TCP/IP. Сетевое администрирование. – СПб.: Питер, 2007. – 816 с.

5. Request for Comments: 5652. Cryptographic Message Syntax, 2009. – URL: https://datatracker.ietf.org/doc/html/rfc5652 (дата обращения 10.10.2022).

6. *Шапошников И.В.* Web-сервисы Microsoft .NET. – СПб: БХВ-Петербург, 2002. – 336 с.

7. *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.

DOI: 10.25728/iccss.2022.86.51.036

Зорин В.А., Ненашева Ю.А.

Анализ уязвимостей RFID-меток СКУД на объектах КИИ

Аннотация: Рассмотрены уязвимости RFID-меток, используемые в системах контроля и управления доступом. Приведены предложения для снижения возможности успешных атак.

Ключевые слова: RFID, анализ уязвимостей, объекты КИИ, СКУД

Рост цен на микросхемы и чипы иностранного производства влечёт за собой рост стоимости систем контроля и управления доступом (СКУД). Организации стремятся снизить затраты на инфраструктуру, в связи с чем ищут наиболее доступные решения, закрывающие основные потребности. На объектах критической информационной инфраструктуры (КИИ) ситуация аналогична, поскольку существующие регламентирующие документы [1, 2] не категорируют СКУД. В большинстве случаев СКУД рассматривается как самостоятельный блок, отделённый от производственных процессов.

Целью настоящей работы является рассмотрение уязвимостей RFID-меток, используемых в системах контроля и управления доступом, и атак на них (рисунок 1).

В качестве реализации угроз рассмотрены модели атак на RFID-метку. В работе [3] представлена модель с определением типов и уровней атакующего киберфизическую систему на примере СКУД. Однако приведённая типология не удовлетворяет поставленной в работе задаче, и для этих целей введён дополнительный тип атакующего: «Тип 5. Наличие у атакующего доступа к RFID-меткам, без доступа к системе СКУД. (С применением методов социальной инженерии)».

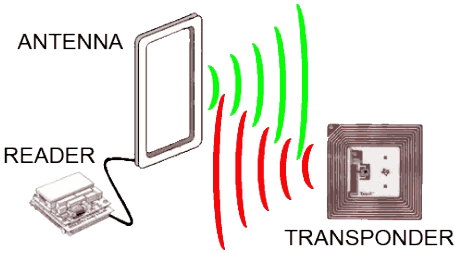


Рисунок 1 – Пример обмена данными RFID-меток в СКУД

Уровень атакующего по модели [3] определён от 1 до 3. Из которых наибольший интерес представляет уровень 2: «Наличие у атакующего специальных знаний о блоках или сети СКУД. Атакующий может использовать специализированные инструменты и эксплуатировать уязвимости нулевого дня (примеры атакующих действий: атаки типа «человек-посередине», отказ в обслуживании, переполнение буфера)».

Существующие уязвимости использования карт доступа.

1. Незащищенность данных. UID хранится в открытом виде и не защищён от считывания, что делает карту доступа и всю систему уязвимой, позволяя злоумышленникам получить не только доступ к объекту, но и информацию о владельце карты. Проблема частично решается применением алгоритмов шифрования. Стандартизированные Международной организацией по стандартизации (ISO) в рамках стандарта радиоинтерфейса RFID-шифры по состоянию на октябрь 2018 г. были успешно подвергнуты криптоанализу [4] с использованием метода Раддума-Семаева.

2. Повторное воспроизведение. При каждом чтении карты передается одна и та же информация, которую можно перехватить, записать и повторно воспроизвести для получения доступа. Защитой от повторного воспроизведения служит взаимная аутентификация карты доступа и считывателя.

Рассмотрен частный случай атаки на RFID-метку с целью компрометации уникального идентификационного номера (UID), в бесконтактных картах доступа ISO 14443, по типу Mifare, каждая RFID-метка Mifare оснащена UID и памятью с возможностью перезаписи. UID не является секретным и не подлежит защите,

соответственно не относится к зашифрованной информации. Считывание данных из карты памяти и запись информации на нее осуществляется исключительно при наличии специальных кодов доступа. Данные, которые передаются между ключом и считывателем, зашифрованы. Считыватели одновременно распознают как UID, так и информацию, расположенную в зашифрованной памяти. Наиболее распространенные системы контроля и управления доступом не обладают такой возможностью и считывают только UID. Системы СКУД, которые поддерживают работу с двумя способами идентификации одновременно – с памятью и UID стоят дороже и на практике встречаются редко.

Для атаки на RFID-метку используется дубликатор, например, SMKey [5], позволяющий получить криптоключ для чтения Mifare непосредственно от самого считывателя, что дает возможность изготовить копию метки даже со всеми закрытыми секторами (рисунок 2). Дубликатор имеет память на 18 ячеек (ключей). Скопированный UID в дальнейшем записывается на заготовки MF Zero и MF OTP, либо используется дубликатором в режиме эмуляции для получения несанкционированного доступа.

Рисунок 2 – Пример дубликатора RFID-меток

Способы защиты от атак.

1. Взаимная аутентификация. При наличии алгоритма взаимной аутентификации, карта доступа, попадая в зону считывания, предоставляет считывателю свой уникальный номер CSN и

сгенерированный 16-битный случайный номер. В ответ считыватель, используя Hash-алгоритм, создает диверсификационный ключ, который должен совпасть с ключом, записанным на карте. При совпадении – карта и считыватель обмениваются 32-битными откликами, после чего считыватель «принимает» решение о валидности карты. Таким образом, осуществляется защита от повторного воспроизведения информации. Однако в большинстве систем взаимная аутентификация не используется.

2. Диверсификация ключа. С помощью программного обеспечения настраивается разграничение доступа для повышения надежности СКУД на следующих уровнях:

А) «Дверь» – доступ в помещения разграничен в соответствии со служебными обязанностями и полномочиями. Однако, данный способ не защитит, в случае компрометации карты сотрудника, имеющего повышенный уровень доступа;

Б) «Время» – после окончания рабочего дня, а также в выходные и праздничные дни доступ может быть ограничен;

В) «Запрет повторного прохода» – разграничение запрещает проход злоумышленника с клоном карты присутствующего на рабочем месте сотрудника, а также запрещает работникам пропускать по своей карте посторонних.

В работе [6] отмечается актуальность и перспективность использования комбинированных СКУД в задачах цифровизации, однако критериев рациональности использования таких систем в условиях высокой стоимости комплектующих не приведено.

В результате анализа уязвимостей RFID-меток в системе контроля и управления доступом на объектах критической информационной инфраструктуры следует учесть возможность компрометации карт доступа, использующих RFID. Предусмотреть комбинированный способ разграничения доступа и одновременное считывание данных UID и информации в зашифрованной области памяти RDIF-меток.

Литература:

1. Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

3. *Левшун Д.С., Чечулин А.А., Котенко И.В.* Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи. – 2019. – Т. 5. № 4. – С. 114-123.

4. *Куценко А.В., Атутова Н.Д., Зюбина Д.А., Маро Е.А., Филиппов С.Д.* «Алгебраический криптоанализ низкоресурсных шифров Simon и Speck» // ПДМ. Приложение. – 2021. – № 14. – С. 84-91.

5. iKey – Всё для копирования ключей [Электронный ресурс]. – URL: https://ikey.ru/smkey/ (дата обращения 14.10.2022).

6. *Горохов А.В., Гаврин В.А., Мартынов В.А.* Обеспечение информационной безопасности посредством построения комбинированных систем контроля и управления доступом // Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2022. – Т.5. №4. – Порядковый номер: 26.

DOI: 10.25728/iccss.2022.61.81.037

Логинова Л.Н., Королев А.Д.

Принципы обеспечения информационной безопасности в социальных сетях

Аннотация: В работе показаны особенности обеспечения информационной безопасности в социальных сетях, проведен анализ существующих способов защиты, даны рекомендации по защите информации и персональных данных.

Ключевые слова: информационная безопасность, утечка данных, защита информации, социальные сети, аутентификация

В настоящее время пользовательские данные представляют высокую ценность для злоумышленников. Так, например, в 2016 году данные более 100 млн пользователей социальной сети «Вконтакте» были выставлены на продажу за 1 биткойн [1]. Данные, которые были утеряны, содержали конфиденциальную информацию, а именно, логины и пароли от социальной сети, имена, номера телефонов.

Важно отметить, что в настоящее время грань между разнообразными интернет-сервисами размылась, сложно произвести категоризацию сервисов, поскольку функционал часто дублируется. Сервисы позволяют общаться, проводить поиск профилей, отправлять и просматривать файлы, заполнять информацию о себе и т.д. Так, например, некоторые мессенджеры полностью повторяют функционал социальных сетей, а настройки безопасности и конфиденциальности идентичны.

Целью работы является проведение анализа обеспечения информационной безопасности (ИБ) социальных сетей, который, в свою очередь, является основой функционирования цифрового пространства современного общества, а также формирования рекомендаций по защите информации и персональных данных пользователям.

Каждый второй человек имеет аккаунт в социальной сети. По данным [2], более 4 миллиардов человек пользуются социальными сетями. Ценность каждого аккаунта зависит от информации, которая в нем содержится, а, в случае массовой утечки, ценность составляет совокупность различных актуальных аккаунтов.

В социальных сетях особо важным объектом является передаваемая информация, поскольку человек по неосторожности может отправить некоторые секретные данные не по зашифрованным каналам связи, а через социальную сеть или мессенджер, а получение злоумышленником доступа к таким данным может иметь весьма серьезные последствия. Так, например, злоумышленник может использовать данные с целью вымогательства, шантажа, получения доступа к финансовым активам.

К сожалению, массовая утечка данных аккаунтов не редкость в текущей мировой ситуации [3]. Под угрозой атаки могут быть и определённые социальные сети, серверы которых базируются в

разных странах и содержат данные большого количества пользователей.

Пользователи социальных сетей не застрахованы от подобных массовых утечек данных, в таком случае вся ответственность ложится на компанию, которая хранит и обрабатывает пользовательские данные, но существуют также и точечные атаки, когда целью злоумышленника является конкретная персона, пользователь, аккаунт, и в таком случае весь риск лежит на конкретном владельце аккаунта.

Точечную атаку стоит расценивать как более опасную для самого пользователя, потому что при такой атаке злоумышленнику необходимо получить доступ к определенному аккаунту с конкретной целью. Цели, как при массовой утечке, так и при точечной атаке, могут быть идентичны, например, получение корпоративных данных, являющихся поводом для шантажа. При защите аккаунта понятия «безопасности» и «приватность» часто не разделяют. Настройки приватности в социальной сети служат для скрытия профиля или отдельных его элементов на площадке и в сети интернет от посторонних глаз. Можно утверждать, что строгие настройки приватности косвенно повышают безопасность аккаунта, но не исключают взлом. В свою очередь, безопасность позволяет предотвратить возможный взлом аккаунта путем более сложной и строгой настройки аутентификации и других параметров доступа к аккаунту.

Обеспечение ИБ в социальных сетях – актуальная проблематика для большого количества компаний, обладающих ценной коммерческой информацией, находящейся в поле поиска злоумышленников.

В исследовании *Verison* [4] указано, что 80 % инцидентов ИБ связано с аутентификацией, методы которой являются средствами обеспечения ИБ в социальных сетях:

- аутентификация по СМС;
- аутентификация только по паролю;
- двухфакторная аутентификация.

Аутентификация по СМС – один из наиболее слабых методов контроля доступа. Аутентификация происходит путем отправки СМС сообщения на указанный мобильный номер с кодом доступа к аккаунту. Уязвимость кроется в возможности перехвата самого

сообщения, а также в системах сотовых операторов, когда, например, можно воссоздать дубликат сим-карты и незаметно перехватывать сообщения. Рекомендуется отказаться от такого способа аутентификации, а в случае невозможности не заводить аккаунт или минимизировать обмен любыми данными.

Аутентификация по паролю – это наиболее распространённый способ получения доступа к аккаунту, требующий особого внимания к стойкости пароля и его сохранности. Многие пользователи социальных сетей используют крайне слабые пароли. По данным [5], самыми часто встречающимися паролями стали:

1. «password»;
2. «123456»;
3. «123456789».

Для создания сложного пароля следует использовать случайную комбинацию чисел, заглавных и прописных букв, специальные символы. В работе [6] рекомендуется использовать сложные, уникальные пароли длиной больше 8 символов. Важно, чтобы пароль был уникальным и не использовался в других сервисах, т.к. в случае утечки общего пароля от одной социальной сети под угрозой находятся данные в других социальных сетях. Стоит отметить, что использование совершенно разных паролей затруднительно – возникает сложность в запоминании огромного количества случайных паролей. Для облегчения ведения и запоминания пароля от каждой социальной сети можно использовать случайно сгенерированный шаблон пароля с индивидуальным алгоритмом его модификации. Некоторые онлайн-сервисы и социальные сети жестко ограничивают максимальную длину пароля и\или запрещают использовать те или иные специальные символы – это сомнительный подход к обеспечению ИБ платформы, что является причиной задуматься об отказе регистрации в подобных сервисах.

В работах [6, 7] показано, что безопасным и стойким способом аутентификации на сегодняшний день является двухфакторная аутентификация. Двухфакторная аутентификация позволяет избежать несанкционированный взлом системы или аккаунта, снизить риск утечки персональных данных и другой важной информации в корпоративных сетях, а также обезопасить пользователя от ошибочных транзакций в интернет-магазинах, социальных сетях и т.д. [7].

Большинство современных социальных сетей позволяют следить за входами и попытками входа в аккаунт, а также просматривать, на каких устройствах, с каких IP-адресов выполнен вход, уничтожать текущие сессии. Следует отметить, что неизвестная попытка входа в аккаунт является весомым поводом сменить пароль, проверить личные онлайн-сервисы. В случае, если личный аккаунт в социальной сети не нужен, то рекомендуется удалить всю личную информацию и аккаунт.

Важным аспектом ИБ в социальных сетях являются настройки приватности, рекомендуется использовать максимально строгие правила: ограничивать видимость номера телефона, подробной информации о личности, фотографиях и другой информации, которой может воспользоваться злоумышленник. Рекомендуется регулярно проверять настройки приватности, с осторожностью относиться к любым сообщениям от незнакомых людей, не открывать подозрительные файлы.

В последнее время появилась возможность использовать аккаунт в социальной сети для входа в другие сервисы в интернете, однако стоит учесть, что это небезопасный метод входа, т.к. предоставляется сторонним сервисам информация об аккаунте и его владельце, а в случае взлома аккаунта в социальной сети злоумышленник получит доступ ко всем сервисам, где была выполнена аутентификация.

Проведенный анализ методов и способов защиты информации и персональных данных в социальных сетях позволяет сформулировать следующие рекомендации: не следует оставлять социальные страницы в сетях заброшенными, и в случае их неиспользования – важно удалять профиль и личные данные аккаунта; не следует принимать заявки от неизвестных аккаунтов, поскольку те могут быть использованы для кражи личных данных пользователя; рекомендуется использование сложных паролей; рекомендуется настроить двухфакторную аутентификацию при входе на страницу в социальной сети; не следует делиться конфиденциальной информацией и важно ознакомиться со всеми пунктами пользовательского соглашения, поскольку многие социальные сети, как владельцы аккаунтов, имеют право продавать личные данные третьим лицам-сторонам.

В настоящее время, когда утечка данных, паролей и другой конфиденциальной информации не редкость, следует максимально

ответственно подходить к ИБ в социальных сетях, использовать двухфакторную аутентификацию, а также регулярно изменять пароли, интересоваться новостями в сфере безопасности, а при выявлении утечки заранее обновлять пароли и доступы к социальным сетям.

Литература:

1. Данные более 100 млн аккаунтов «Вконтакте» продаются в сети за 1 биткоин. – URL: https://habr.com/ru/company/bitrix/blog/305704/ (дата обращения 03.10.2022).

2. Статистика социальных сетей на 2021 год. – URL: https://logotip.online/blog/statistika-socialnyh-setej/ (дата обращения 03.10.2022).

3. Безопасность в социальных сетях. – URL: https://vc.ru/social/81702-bezopasnost-v-socialnyh-setyah (дата обращения 03.10.2022).

4. Двухфакторная аутентификация. Уже пора? – URL: https://www.securitylab.ru/blog/personal/sborisov/347776.php (дата обращения 04.10.2022).

5. Анализ паролей из утечек 2020-2021 года по версии LeakCheck. – URL://www.securitylab.ru/blog/company/leakcheck/351426.php (дата обращения 05.10.2022).

6. *Лим В.Б.* Создание надежных паролей // Проблемы науки. – 2021. – №3 (62). – URL: https://cyberleninka.ru/article/n/sozdanie-nadezhnyh-paroley (дата обращения 11.09.2022).

7. *Замолоцких В.С., Сидоренко В.Г.* Разработка методики восстановления данных на запоминающих // Надежность. – 2022. – Т. 22. № 1. – С. 56-62. DOI: 10.21683/1729-2646-2022-22-1-56-62

DOI: 10.25728/iccss.2022.37.91.038

Волгина О.А.

Анализ возможности применения некоторых графовых моделей к имитационному моделированию социальных сетей

Аннотация: В работе описана роль теории графов в области исследования социальных сетей, рассмотрены некоторые графовые модели, широко используемые для решения различных задач, связанных с моделированием и анализом структуры сети. Показано, что выбор графовой модели во многом зависит от исходных данных, используемых для построения, и цели исследования.

Ключевые слова: социальные сети, имитационное моделирование, графовые модели, стохастические блоковые модели, вероятностные модели, байесовские модели

Процесс изучения закономерностей распространения информации в реальных социальных сетях – трудная задача, так как сеть постоянно растет из-за появления новых пользователей и на образование каждой связи влияет большое количество параметров. В таком случае, наиболее приемлемым вариантом становится использование моделей. В научной литературе описано значительное количество теоретических и численных методов, показывающих, что имитационные модели позволяют моделировать и оценивать комплекс наиболее значимых и релевантных социально-психологических феноменов динамики мнений в сетях.

Каждую социальную сеть математически можно представить в виде графа с множеством вершин и множеством ребер. Вершины такого графа являются участниками сети, ребра отражают наличие отношений между участниками. Теория графов является подходящим инструментом для исследований различных процессов и явлений в области социальных сетей так как: обладает наглядностью, как и геометрия; проста в изучении и применении, имеет сложные нерешённые задачи, как и теория чисел; не имеет громоздкого математического аппарата; имеет выраженный прикладной характер.

В графовых моделях основными данными для изучения выступают матрицы, содержащие информацию о наличии или отсутствии связи между вершинами, а также характер этой связи.

Стохастические блоковые модели задаются квадратной матрицей, в которой количество строк равно количеству столбцов и отражает число выделенных групп участников сети. Элементы матрицы задают плотность связи между участниками двух групп, на пересечении номеров которых находится значение. В графах стохастических моделей нет вершин или ребер, которые отражают связи участников внутри одной группы. Авторы статьи [1] утверждают, что стохастические графы, в которых веса связей являются случайными величинами, могут быть основой для построения модели, имитирующей социальную сеть. Однако, на сегодняшний день использование моделей стохастических графов для сетей ограничено тремя несвязанными факторами: относительная сложность реализации данной модели, недостаточное количество имитационных исследований и сложность в понимании свойств методов вывода.

Вероятностные графовые модели обеспечивают статистически точные и гибкие средства построения моделей, непосредственно применимых при изучении процесса распространения активности в социальных сетях. Модели вероятностных графов также позволяют создавать механистические модели, которые являются ключевыми элементами при проверке гипотез. Данный тип моделей представляют собой союз между теорией графов и теорией вероятностей, который предлагает гибкие парадигмы моделирования с хорошей интерпретируемостью. Графическое представление состоит из узлов, соединенных ребрами, которые могут быть направленными или ненаправленными. Отношения между узлами в графе можно интерпретировать с точки зрения условной независимости. Вероятностные графовые модели задаются квадратной матрицей, в которой количество строк и столбцов равно и соответствует количеству участников сети. Элементы матрицы отражают вероятность наличия связи участника с номером столбца и участника с номером строки в некоторый промежуток времени [2].

Байесовская сеть является вероятностной графической моделью, которая представляет собой набор переменных и их условных зависимостей через ориентированный ациклический граф.

Байесовские сети идеально подходят для анализа произошедшего события и прогнозирования вероятности того, что любая из нескольких возможных известных причин была способствующим фактором. Использование простых байесовских моделей для отслеживания попарных связей всех узлов в графе с целью оценки нормальности поведения показало удовлетворительные результаты. Байесовская сеть также часто используется для реализации функционирования рекомендательных систем социальных сетей. Показано, что предлагаемая рекомендация, основанная на байесовском выводе, лучше, чем существующие рекомендации, основанные на доверии, и сопоставима с рекомендацией по совместной фильтрации [3]. Данный тип моделей обладает большой гибкостью и производительностью, что дает возможность решать широкий круг задач и делает перспективным его использование при построении информационно-аналитических систем.

Для графовых моделей социальных сетей характерны количественные оценки полученных результатов [4]. Наиболее ценными являются коэффициент плотности, средняя длина пути, количество путей заданной длины, а также минимальное число ребер, удалив которые можно разбить граф на несколько отдельных частей.

Коэффициент плотности определятся отношением числа ребер в анализируемом графе к числу ребер в полном графе с тем же числом вершин. Средняя длина пути определяется среднее количество шагов по кратчайшим путям для всех возможных пар сетевых узлов. Это показатель эффективности передачи информации в сети. Показатель центральности или близости к центру в теории графов и анализе сетей определяет наиболее важные вершины графа.

Таким образом, графовые модели социальных сетей используются для моделирования различного рода связей между участниками сети, для аналитической оценки процессов распространения информации, а также для выделения сообществ и связанных подгрупп, на которые можно разбить всю социальную сеть. Данная группа моделей дает количественные оценки, позволяющие выявлять основные свойства полученных сетей. Выбор конкретной графой модели зависит от конечной цели исследования и выбранного метода исследования.

Литература:

1. *Rezvanian A., Meybodi M.R.* Stochastic graph as a model for social networks // Computers in Human Behavior. – 2016. – Volume 64. – P. 621-640.

2. *Farasat A.* et al. Probabilistic graphical models in modern social network analysis // Social Network Analysis and Mining. – 2015. – Volume 5. Issue 1. – Article: 62. DOI: 10.1007/s13278-015-0289-6

3. *Yang X., Guo Y., Liu Y.* Bayesian-inference-based recommendation in online social networks // IEEE Transactions on Parallel and Distributed Systems. – 2013. – Volume 24. Issue: 4. – P. 642-651. DOI: 10.1109 / TPDS.2012.192

4. *Kadushin C.* Understanding social networks: Theories, concepts, and findings. – New York, NY: Oxford University Press, 2012. – 264 p.

V. Экологическая и техногенная безопасность

DOI: 10.25728/iccss.2022.39.49.039

Баранов Л.А., Бестемьянов П.Ф., Балакина Е.П., Пудовиков О.Е.

Методика выбора длины виртуальной сцепки по требованиям безопасности в интеллектуальных системах управления движением поездов

Аннотация: Рассматривается использование соединения двух поездов для повышения проводной и пропускной способности железнодорожных линий с помощью виртуальной сцепки. Расстояние между «головой» сзади идущего поезда и «хвостом» впереди идущего называется «длиной виртуальной сцепки», зависящей от режимов движения поездов. Методика расчёта безопасной длины виртуальной сцепки в реальном времени представлена в данной работе.

Ключевые слова: виртуальная сцепка, длина виртуальной сцепки, экстренное торможение, служебное торможение, погрешности измерения координат и скоростей, верхние оценки, условия безопасности

В настоящее время для увеличения провозной и пропускной способности железнодорожных линий, как одно из возможных направлений, рассматривается использование так называемой «виртуальной сцепки». При этом по радиоканалу впереди идущим (первым) поездом передается сзади идущему (второму) поезду информацию о своей координате и скорости. Второй поезд выбирает режим движения таким образом, чтобы при экстренном торможении первого поезда не произошло аварийного столкновения. Расстояние между «хвостом» первого и «головой» второго будем называть «длиной виртуальной сцепки». Используемая терминология «виртуальная сцепка» связана с известной ранее технологией

вождения соединённых поездов, имеющих физическую сцепку локомотива второго поезда с последним вагоном первого. В технологии виртуальной сцепки отсутствует необходимость в разъединения поездов перед их входом на станцию, где длина станционных путей меньше длины соединённого поезда.

При виртуальной сцепке система управления, имея результаты измерения координаты и скорости второго поезда и получая по радиоканалу результаты измерения координаты и скорости первого поезда, должна вычислять допустимую по условиям безопасности длину виртуальной сцепки и автоматически выбирать управление вторым поездом, обеспечивающее реализацию этой длины. Очевидно, что при минимальной длине виртуальной сцепки в том случае, когда выполняются требования безопасности движения, можно получить максимальную провозную способность рассматриваемого участка железнодорожной линии при условии выполнения технических и технологических ограничений [1-4].

1. Задача определения длины виртуальной сцепки

Условие обеспечения безопасности движения виртуального сцепления поездов выполняется, если

$$L\,(t) = S_1(t) - S_2(t) - l \geq S_{2слторм}[V_2(t)] - S_{1эторм}[V_1(t)], \quad (1)$$

где t – текущее время,

L – длина виртуальной сцепки,

l – длина первого поезда,

$S_1(t)$ – координата «головы» первого поезда в момент времени t,

$S_2(t)$ – координата «головы» второго поезда в момент времени t,

$S_{1\text{эторм}}(V_1)$ – путь экстренного торможения первого поезда, движущегося в момент времени t со скоростью V_1,

$S_{2\text{слторм}}(V_2)$ – путь служебного торможения второго поезда, движущегося в момент времени t со скоростью V_2.

Очевидно, что неравенство (1) записано для идеальных условий отсутствия методических и инструментальных погрешностей измерения координат и скоростей движения поездов, отсутствия погрешностей от запаздывания, вызванных конечным временем передачи информации о координате и скорости первого локомотива,

отсутствия разброса путей служебного и экстренного торможения, погрешности в заданной длины l первого поезда.

Для учёта перечисленных погрешностей при формализации задачи определения длины виртуальной сцепки перейдем к дискретному времени, обозначив $t = (m + \varepsilon)T$ для первого поезда, $t = (n + \varepsilon)T$ для второго поезда, где $m = 0,1,2,\ldots, 0 \le \varepsilon \le 1$, T – шаг временной дискретизации, определяемый временем необходимым для передачи информации о координате и скорости первого поезда второму. В течение времени T происходит цифровое измерение координат поездов и их скорости. В частности, величина T для передачи 24 байт информации составляет 140 мс для радиоканала 160 мГц, 70 мс для радиоканала 2130 мГц. Время цифрового измерения скоростей и координат поездов соответствует этому шагу временной дискретизации. Наличие двух переменных m и n при обозначении текущего времени вызвано тем, что цифровое измерение координаты и скоростей для первого и второго поезда не синхронизировано.

Информация, полученная вторым поездом в момент mT соответствует информации, передаваемой первым поездом в момент $(m - 1)$, и используется для вычисления T на втором локомотиве при $t = nT$.

Тогда погрешность, вносимая запаздыванием, составляет

$$\Delta S_1[nT] = S_1[nT] - S_1[(n - 2 + \varepsilon_1)T] \qquad (2)$$

Выражение (2) получено при условии, что при передаче по радиоканалу случай отказа приемником от декодирования полученной информации при обнаружении ошибок отсутствуют и трансформация кодовых комбинаций невозможна. Использование современных методов избыточного кодирования позволяет получить вероятность трансформации порядка 10^{-14}. Вероятность отказа от декодирования значительно выше и это следует учитывать при расчёте погрешности от запаздывания. При отказе от декодирования k подряд кодовых серий погрешность от запаздывания составляет

$$\Delta S_1[nT] = S_1[nT] - S_1[(n - 2 - k + \varepsilon_1)T] \qquad (3)$$

Максимальная величина погрешности от запаздывания достигается при $\varepsilon_1 = 0$ и $k = k_{max}$, где k_{max} выбирается из

нормированной, согласно SIL4, допускаемой вероятности отказа от декодирования k подряд кодовых серий, что может привести к опасным последствиям. Пусть P - вероятность отказа от декодирования одной кодовой серии, события отказа от декодирования кодовых серий статистически независимы. Тогда вероятность того, что при приёме первых подряд k кодовых серий приёмник откажется от декодирования, после чего будет достоверно принята кодовая серия при условии, что вероятность трансформации пренебрежимо мала, составит $P^k(1-P)$, Если $P_н$ – нормированная допустимая вероятность подряд не принятых кодовых серий, то k_{max} вычисляется из выражения $P_н = P^{k_{max}}(1-P)$.

Аналогично выражению (3) погрешность от запаздывания результатов измерения скорости определяется следующей формулой

$$\Delta V_1[nT] = V_1[nT] - V_1[(n-2-k+\varepsilon_1)T] \quad (4)$$

Соответствующие максимальные значения погрешностей от запаздывания, связанные с передачей информации по радиоканалу составляют

$$\Delta S_{1,k}^{max}[nT] = S_1[nT] - S_1[(n-2-k_{max})T] \quad (5)$$
$$\Delta V_{1,k}^{max}[nT] = V_1[nT] - V_1[(n-2-k_{max})T] \quad (6)$$

Обозначим максимальные значения модуля инструментальной погрешности измеренных координат поездов как ΔS_{1a}^{max} и ΔS_{2a}^{max}.

Тогда максимальные значения погрешностей измерения координат соответственно первого и второго поездов, определяются выражениями

$$\Delta S_{1\,max} = \Delta S_{1a}^{max} + \Delta S_1^{max}[nT] \quad (7)$$
$$\Delta S_{2\,max} = \Delta S_{2a}^{max} \quad (8)$$

При цифровом измерении скорости поездов по частоте вращения колёсной пары локомотива имеют место методические и инструментальные погрешности. Методические погрешности определяются квантованием по уровню при цифровом измерении и погрешностью от запаздывания на $\frac{T_v}{2}$, где $T_v \le T$ – время измерения

скорости. Обозначим сумму инструментальных и методических погрешностей измерения скоростей соответственно первого и второго поездов как ΔV_{1a}^{max} и ΔV_{1a}^{max}.

Тогда максимальные значения погрешностей измерения скоростей соответственно первого и второго поездов определяются выражением

$$\Delta V_{1\,max} = \Delta V_{1a}^{max} + \Delta V_{1}^{max}[nT], \quad (9)$$

$$\Delta V_{2\,max} = \Delta V_{2a}^{max}. \quad (10)$$

Оценим далее сверху величины погрешностей от запаздывания $\Delta S_1^{max}[nT]$ и $\Delta V_1^{max}[nT]$.

За время запаздывания информации о координате первого поезда $nT - (n - 2 - k_{max})T = (k_{max} + 2)T$ путь пройденным первым поездом при $V_1 = V_{max}$ составляет $(k_{max} + 2)TV_{1\,max}$,что является верхней оценкой погрешности $\Delta S_1^{max}[nT]$. Эта погрешность не приводит к уменьшению допустимой по условиям безопасности длины виртуальной сцепки – L. Вместе с тем за время $(k_{max} + 2)T$ скорость первого поезда уменьшаться, что в свою очередь приводит к уменьшению пути экстренного торможения первого поезда, непосредственно влияющего на выбор L. Худшей с точки зрения выполнения условий безопасности будет ситуация, когда за время $(k_{max} + 2)T$ скорость первого поезда уменьшается с замедлением g_{max}, которое можно принять равным замедлению экстренного торможения $g_э$. Тогда путь экстренного торможения первого поезда при известном в момент nT второму поезду измеренном значении скорости первого поезда в момент $(n - 2 + k_{max})T$ можно оценить как

$$S_{эторм1}\{V_{изм}[n] - \Delta V_{1a}^{max} - (2 + k_{max})Tg_э\} = \frac{\{V_{изм}[n] - \Delta V_{1a}^{max} - (2 + k_{max})Tg_э\}}{2\,g_э} \quad (11)$$

Таким способом оценивается влияние максимального значения погрешности $\Delta V_1^{max}[nT] = (k + 2)Tg_э$ от запаздывания при передаче информации скорости движения первого поезда.

2. Оценка длины виртуальной сцепки

В момент времени $t = nT$ вычислитель второго поезда определяет допустимую по условиям безопасности длину виртуальной сцепки как разность путей служебного торможения второго поезда и экстренного торможения первого поезда с учётом заданной погрешности Δl длины первого поезда и погрешностей измерения координат поездов. Путь служебного торможения второго поезда, движущегося со скоростью $V_{2\text{изм}}[n] + \Delta V_{2a}^{max}$ можно оценить, как

$$S_{торм\ сл\ 2}\{V_{2изм}[nT] + \Delta V_{2a}^{max}\} = \frac{\{V_{изм}[nT] + \Delta V_{2a}^{max}\}^2}{2\ g_{сл}} \qquad (12)$$

Путь экстренного торможения первого поезда, вычисляемый в момент времени nT с учётом возможного уменьшения скорости за время $(k+2)T$ можно оценить по формуле (11).

Допустимая по условиям безопасности длина виртуальной сцепки определяется как

$$L[nT] = \frac{(V_{2изм}[nT] + \Delta V_{2a}^{max})^2}{2g_{сл}} + \Delta S_{1a}^{max} + \Delta S_{2a}^{max} + \Delta l - -\frac{[V_{1изм}[nT] - \Delta V_{1a}^{max} - g_э(k+2)T]^2}{2g_э} \qquad (13)$$

Это выражение преобразуем к виду

$$L[nT] = \frac{V_{2max}^2[nT]}{2g_{сл}} - \frac{V_{1max}^2[nT]}{2g_э} + L_0 + L_1, \qquad (14)$$

где $L_0 = +\Delta S_{1a}^{max} + \Delta S_{2a}^{max} + \Delta l + \frac{(\Delta V_{2a}^{max})^2}{2g_{сл}}$;

$$L_1[nT] = V_{2\text{изм}}[nT]\frac{\Delta V_{2a}^{max}}{2g_{\text{сл}}} + V_{1\text{изм}}[nT]\frac{\Delta V_{1a}^{max} + g_э(k+2)T}{2g_э}$$

Величину $L_1[nT]$ можно оценить сверху как L_1^*, приняв $V_{2\text{изм}}[nT] = V_{2max}$; $V_{1\text{изм}}[nT] = V_{1max}$, где V_{1max} и V_{2max} – максимально допустимые скорости движения соответственно первого и второго поездов

$$L_1^* = \frac{V_{2max}\Delta V_{2a}^{max}}{2g_{сл}} + \frac{V_{1max}[\Delta V_{1a}^{max} + g_э(k+2)T]}{2g_э} \qquad (15)$$

Тогда оценка длины виртуальной сцепки $L[nT]$ по условиям безопасности

$$L[nT] = \frac{V_{2изм}^2[nT]}{2g_{сл}} - \frac{V_{1изм}^2[nT]}{2g_э} + L_0 + L_1^* \qquad (16)$$

Благодарности. Исследование выполнено при финансовой поддержке РФФИ, НТУ «Сириус», ОАО «РЖД» и Образовательного Фонда «Талант и успех» в рамках научного проекта № 20-37-51001

Acknowledgments. The reported study was funded by RFBR, Sirius University of Science and Technology, JSC Russian Railways and Educational Fund «Talent and success», project number 20-37-51001

Литература:

1. *Бушуев С.В., Гундырев К..В., Голочалов Н.С.* Повышение пропускной способности участка железной дороги с применением технологии виртуальной сцепки // Автоматика на транспорте. – 2021. – №1. – С. 7-20.

2. *Flammini F., Marrone S., Nardone R., Petrillo A., Santini S., Vittorini V.* Towards Railway Virtual Coupling. – International Conference of Electrical Systems for Aircraft, Raiway, Ship Propulsion and Road Vehicles and International Transportation Electrification Conference, 2018. – P. 1-6. DOI: 10.1109/ESARS-ITEC.2018.860752

3. *Mitchell I., Goddard E., Montes F., Stanley P., Muttram R., Coenraad W., Pore J., Andrews S., Lochman L.* ERTMS Level 4, Train Convoys or Virtual Coupling. – Institution of railway signal engineers, IRSE news issue 219. – 2016.

4. *Goikoetxea J.* Roadmap Towards the Wireless Virtual Coupling of Trains / Part of the Lecture Notes in Computer Science book series (LNCCN, volume 9669). – Springer International Publishing Switzerland, 2016. – P. 3-9.

DOI: 10.25728/iccss.2022.78.22.040

Чернов К.В.

Сциентное взаимодействие в системе управления техносферной безопасностью

Аннотация: Раскрывается содержание отношений в системе управления техносферной безопасностью, охватывающей руководителей, специалистов, рабочих, при использовании понятий и положений разновидности системного подхода, именуемой системнологией.

Ключевые слова: системный подход, системнология, сопринадлежность, сциенция, техносферная безопасность

«Системный подход – направление методологии научного познания и общественной практики, в основе которого лежит исследование объектов как систем …». При этом, «система – множество элементов, находящихся в отношениях и связях друг с другом, образующих определенную целостность, единство, подчиненных достижению цели» [1]. В системнологии [2] как разновидности системного подхода прогрессируются основные и вводятся дополнительные понятия и положения.

Система в системнологии есть осознаваемое при кодорефлексии отображение части Универсума, обособленной в соответствии целью и разделяемой на компоненты, которые посредством отношений объединяются в целое, связанное с внешней средой. Кодовая рефлексия, или кодорефлексия, при категориальном выражении есть способность живого посредством субстанции воспроизводить, т.е. имитировать, существующее, представленное составляющими Универсума, его формообразованиями, их внешним окружением и взаимовлиянием, включая самоимитацию и воплощение имитируемого при преобразованиях [3]. В системнологическом определении сходятся два аспекта: имитируемое существует, а существующее имитируется. Сознание всегда оперирует с имитацией существующего, называемой также его моделью.

Цель кодорефлексируемой части Универсума, перенесённая на систему, становится её функцией. Компонент в соответствии с

положением о сопринадлежности входит в состав системы и обладает определённой функцией, обусловленной системной функцией. Сопринадлежность может быть многоуровневой, при которой система исходного уровня разделяется на компоненты, принимаемые системами, которые имеют в своём составе компоненты последующего уровня и т.д., включая системы крайнего уровня. Компоненты крайнего уровня сопринадлежности становятся элементами системы. Сопринадлежность функционирования системы и компонентов может быть соподчинённой

Отношения компонентов в системе создаются связями взаимодействия и связями наследования. Взаимодействие является связью между компонентами в данный момент. Последствия, возникающие в компонентах, именуются эффектами взаимодействия. Наследование относительно компонента представляет собой связь между его состояниями, поддерживающую сохранность его свойств во времени. Связи наследования, как правило, эквивалентируются процессами. Процесс в системнологии есть изменение компонента или взаимодействия компонентов во времени.

Внешняя среда – внешний компонент системы исходного уровня сопринадлежности, предстающий системой последующего уровня, которая имеет бесконечное количество компонентов, но включает в свой состав лишь компоненты, взаимодействующие с внутренними компонентами исходной системы.

Ключевая особенность системнологии состоит во введении, определении и использовании понятий, способствующих раскрытию содержания компонентов, отношений и эффектов.

Система, отображающая осознаваемую при кодорефлексии косную часть Универсума, является абиогенной. Абиогенная система исходного уровня имеет в своём составе абиотические компоненты и внешнюю среду. Многоуровневая декомпозиция абиотических систем приводит к выделению систем переходного и последующих уровней сопринадлежности, компоненты которых предстают частицами, начиная с молекулярных. Содержание молекулярных и внутримолекулярных частиц является вещественно-энергетическим. Вещество в системнологии – это слагаемое компонента, которое проявляется массой, предстает его структурой и служит носителем энергии. Слагаемое компонента, которое

проявляется посредством силы, поддерживает его структуру, придаёт ему активность и может создавать поле дальнодействия, именуется энергией. Абиотические компоненты, процессы и взаимодействия в абиотической системе вследствие вещественно-энергетического содержания частиц описываются свойствами вещества и энергии.

Система, отображающая осознаваемую при кодорефлексии живую часть Универсума, является биогенной. Биогенная система исходного уровня имеет в своём составе биотические и абиотические компоненты и внешнюю среду. Многоуровневая декомпозиция биотических систем приводит к выделению систем переходного и предыдущих уровней сопринадлежности, компоненты которых предстают организмами, начиная с внутриклеточных супрамолекулярных и макромолекулярных частиц. Компоненты последующих уровней являются абиотическими. Абиотический компонент биогенной системы переходного уровня в сравнении с компонентом абиогенной системы содержит более сложное вещество и энергию, соответствующую сложности этого вещества. Более сложные вещество и энергия имеют дополнительные свойства, обусловливающие кодорефлексию, которая при переходе от категориального подхода к системному предстаёт транскодингом.

Транскодинг, или транскодированное представление компонентов, отношений и внешней среды биогенной системы внутри биотического компонента системы исходного и последующих уровней сопринадлежности, осуществляется посредством знаков, создаваемых веществом и энергией этого компонента. Совокупности вещественно-энергетических знаков транскодинга биотических компонентов являются сциенцией. Знаками сциенции являются знаки, обладающие потенциалами самодействия, которые обусловливают аутоактантность биотических компонентов. Посредством сциенции биотические компоненты биогенной системы исполняют транскодинг, вследствие чего обеспечивается их организованность. Биотические компоненты систем предыдущих уровней сопринадлежности относительно переходной и отношения между ними характеризуются вещественными, энергетическими и сциентными свойствами. Отношения и эффекты в системе имеют вещественно-энергетическое и сциентное содержание.

Система управления техносферной безопасностью (УТБ) в РФ разделяется на составляющие в зависимости от законодательно регулируемых областей, например области с названием «охрана труда». Система УТБ в области охраны труда имеет три уровня сопринадлежности: федеральный, региональный (республиканский, краевой, областной), уровень организации.

Система УТБ в области охраны труда федерального уровня сопринадлежности имеет в своём составе системы, компоненты и элементы со следующими названиями:

/0/ – система УТБ федерального уровня;

/1.0/ – система УТБ федерального уровня в области охраны труда;

/2.0/ – внешняя среда;

/1.1.0/ – Председатель правительства РФ и его заместитель, ответственный за государственную политику в сфере трудовых отношений;

/2.1.0/ – Минтруд России;

/3.1.0/ – федеральные министерства, службы, агентства и внебюджетные фонды;

/4.1.0/ – Российская трёхсторонняя комиссия по регулированию социально-трудовых отношений;

/1.2.0/ – органы президентской власти;

/2.2.0/ – органы прокуратуры;

/3.2.0/ – органы судебной власти;

/4.2.0/ – система УТБ в области охраны труда уровня сопринадлежности регионов;

/5.2.0/ – система УТБ в области охраны труда уровня сопринадлежности организации;

/1.2.1.0/ – федеральная служба по труду и занятости (Роструд);

/2.2.1.0/ – департамент оплаты труда, трудовых отношений и социального партнерства Минтруда России;

/3.2.1.0/ – департамент условий и охраны труда Минтруда России;

/4.2.1.0/ – департамент правовой, законопроектной и международной деятельности Минтруда России;

/1.3.1.0/ – департамент бюджетной политики в сфере труда и социальной защиты Минфина России;

/2.3.1.0/ – департамент, управление или отдел охраны труда министерства, службы, агентства, например отдел охраны труда департамента государственной службы и кадров Минобрнауки;

/3.3.1.0/ – государственный внебюджетный «Социальный фонд России»;

/1.1.2.1.0/ – главный государственный инспектор труда РФ;

/2.1.2.1.0/ – подразделение с названием «Управление осуществления федерального надзора в сфере труда Роструда России»;

/3.1.2.1.0/ – подразделение с названием «Управление делами и контроля Роструда России».

Система УТБ является антропогенной, имеющей в своём составе антропные системы с антропными компонентами, которыми являются руководители, специалисты, рабочие, и внешнюю среду с такими же антропными компонентами.

Функция антропных систем при управлении техносферной безопасностью определяется Конституцией РФ, федеральными конституционными законами, федеральными законами, актами Президента РФ и Правительства РФ, а также нормативными правовыми актами (НПА), принимаемыми для их исполнения. Сопринадлежность функционирования в системе УТБ является комплексной с преобладанием иерархичности.

Отношения в антропогенной системе, образованной антропными системами и компонентами, имеют сциентный характер. Работник пригоден к деятельности, если степень развития его сциентной системы [3] соответствует сложности задач, решение которых должно быть приемлемо правильным и достаточно точным.

Сциентная система работника готова к правильному и точному взаимодействию в процессе деятельности при выполнении комплекса условий, в том числе следующих: восприятие световых фотонов, отражённых от знаков текста актуального, требующего исполнения, положения НПА, должно сопровождаться транскодированием сциенции и приводить к активации секвентных и рацемусных гностических групп (СГГ и РГГ) нейронов, вокализующих и имажирующих зрительную сциенцию в троксии и во внутренний образ актуального положения, который вызывает воспитанное ранее чувство ответственности; активность РГГ, имажирующих зрительную сциенцию, должна представать

аутоактантными паттернами чувства ответственности; аутоактантность паттерна чувства ответственности должна приводить к активации темплатных рацемусно-бихевиоральных групп (РБГ) нейронов, которые должны вызывать необходимые действия; транскодирование зрительной сциенции с активацией СГГ нейронов вокализует троксии в модусе думаемых или произносимых мыслей; когерентная взаимная аутоактантность РГГ и СГГ, обусловленная транскодированием сциенции и определяющая мышление, приводит к правильному пониманию воспринимаемого, на основе которого должны приниматься правильные решения.

Сциентная система работника при восприятии звуковых фононов, возникающих при прослушивании текстов, должна реагировать похожим образом.

Вывод

Глубокое раскрытие содержания отношений в системе управления техносферной безопасностью, охватывающей руководителей, специалистов, рабочих, становится возможным при использовании понятий и положений разновидности системного подхода, именуемой системнологией.

Литература:

1. *Новиков Д.А.* Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития. – М.: Ленанд, 2016. – 160 с

2. *Чернов К.В.* Системнология безопасности. – Иваново: ГОУВПО «Ивановский государственный энергетический университет им. В.И. Ленина», 2011. – 196 с.

3. *Чернов К.В.* Кодорефлексия и когнификация безопасности техногенной деятельности: монография. – М.: Русайнс, 2022. – 188 с.

DOI: 10.25728/iccss.2022.89.26.041

Мусаев В.К.

Математическое моделирование ударного воздействия (переходной процесс) на десятиэтажное здание с подвалом

Аннотация: Приводится информация о компьютерном моделировании нестационарного сосредоточенного ударного воздействия на десятиэтажное здание с подвалом. Решена задача о компьютерном (цифровом) моделировании нестационарных волн при сосредоточенном ударном воздействии на десятиэтажное здание с подвалом.

Ключевые слова: механика быстропротекающих процессов, ударные воздействия, подвальный этаж, десятиэтажное здание, импульс в виде трапеции, комплекс программ Мусаева В.К.

Рассматриваемая научная работа являются продолжением ранее полученных результатов. Такой подход к исследованию новых задач, которые опираются на предыдущие результаты, могут быть выполнены, если изначально была принята постановка и реализация задач с использований методов фундаментальной науки.

В основе этих исследований заложены методы вычислительной механики деформируемых тел с возможностями языков программирования и вычислительных машин.

В работе приводится цифровое (численное) решение задачи о моделировании нестационарных волн (ударное воздействие) в подвале десятиэтажного здания с упругой полуплоскостью.

Переходные процессы очень важны для оценки безопасности сложных технических систем при чрезвычайных ситуациях природного, техногенного и антропогенного характера.

Исследования выполнялись с помощью уравнений нестационарной волновой теории упругости.

Волновые нестационарные процессы проходят очень быстро, поэтому материал исследуемого деформируемого тела не успевает перейти за пределы упругости и тем самым в нем возникают трещины и отколы.

Основное напряженное состояние в исследуемом объекте формируется при переходном процессе, то есть нестационарном волновом.

Применение рассматриваемого численного метода, алгоритма и комплекса программ для решения нестационарных волновых задач в деформируемых телах сложной (различной) формы приведено в работах [1-6].

Оценка точности и достоверности (верификация) рассматриваемого численного метода, алгоритма и комплекса программ приведена в следующих работах [1, 5-6].

Приводится численное решение задачи о моделировании нестационарных волн при сосредоточенном ударном воздействии на десятиэтажное здание с подвалом.

Приближенное значение уравнения движения в теории упругости приведено в следующих работах [1-6].

В работах приведена информация о явной двухслойной схеме [1-6].

Шаг по времени для устойчивости явной двухслойной схемы для внутренних и граничных узловых точек на квазирегулярных сетках приведен в следующих работах [1-6].

С помощью метода конечных элементов (цифровое моделирование), линейную задачу с начальными и граничными условиями привели к линейной задаче Коши.

Задание различных физических свойств, для каждого конечного элемента, позволяет с помощью метода конечных элементов решать динамические задачи теории упругости для областей сложной (различной) формы [1-6].

На основе метода конечных элементов разработана методика, разработан алгоритм и составлен комплекс программ для решения двумерных волновых задач динамической теории упругости [1-6].

Расчеты проводились при следующих единицах измерения: килограмм-сила (кгс); сантиметр (см); секунда (с).

Рассматривается задача о моделировании напряженного состояния в десятиэтажном здании с подвальным этажом (рисунок 1) при сосредоточенном ударном воздействии (рисунок 2).

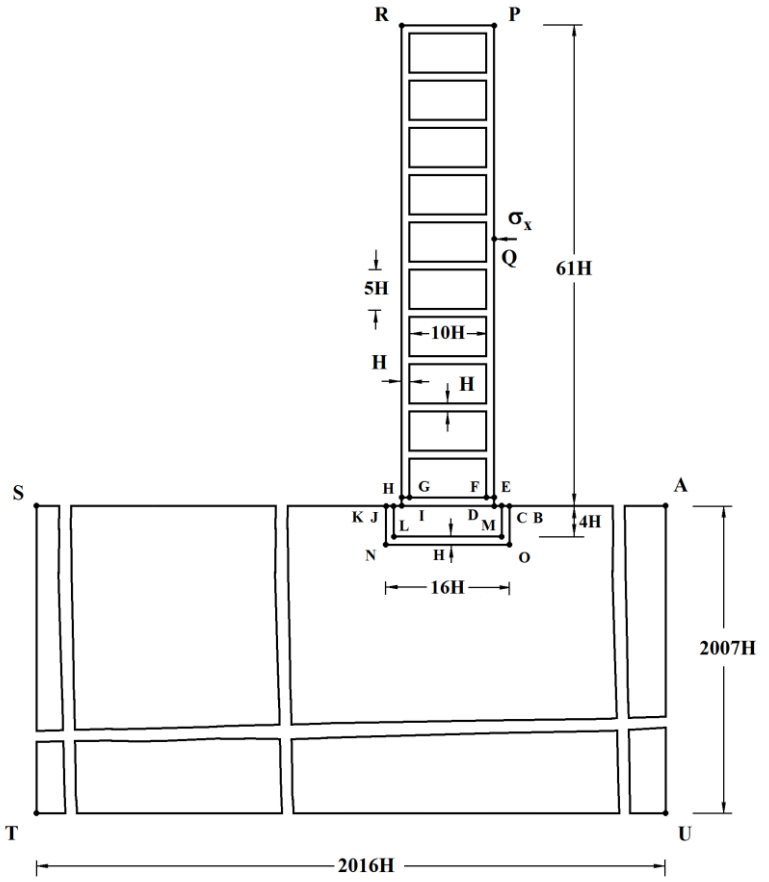


Рисунок 1 – Постановка задачи для десятиэтажного здания с упругим основанием в виде полуплоскости при сосредоточенном ударном воздействии. Схема Мусаева В.К.

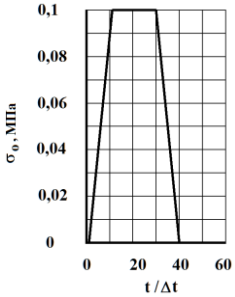


Рисунок 2 – Ударное воздействие в виде трапеции.
График Мусаева В.К.

Исследуемая задача впервые решена Мусаевым В.К. с помощью разработанной методики, алгоритма и комплекса программ [1-6].

Начальные условия приняты нулевыми. В точке Q приложено нормальное напряжение σ_x, которое при $0 \le n \le 11$ ($n = t/\Delta t$) изменяется от 0 до P, а при $11 \le n \le 30$ равно P и при $31 \le n \le 40$ изменяется от P до 0 ($P = \sigma_0$, σ_0 = -0,1 МПа (-1 кгс /см^2)). Граничные условия для контура $STUA$ при $t > 0$ $u = v = \dot{u} = \dot{v} = 0$.

Отраженные волны от контура $STUA$ не доходят до исследуемых точек при $0 \le n \le 500$.

При расчетах приняты следующие исходные данные: $H = \Delta x = \Delta y$; $\Delta t = 2{,}788 \cdot 10^{-6}$ с; $E = 3{,}15 \cdot 10^4$ МПа ($3{,}15 \cdot 10^5$ кгс/см^2); $\nu = 0{,}2$; $\rho = 0{,}255 \cdot 10^4$ кг/м^3 ($0{,}255 \cdot 10^{-5}$ кгс с^2/см^4); $C_p = 3587$ м/с; $C_s = 2269$ м/с.

Решается система уравнений из 16202276 неизвестных. Контурное напряжение $\overline{\sigma}_k$ получено в точках $A1$-$A10$ (рисунок 3).

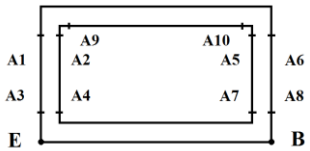


Рисунок 3 – Точки, в которых получены упругие напряжения во времени. Схема Мусаева В.К.

В точках *А*1 и *А*6 (рисунки 4, 5) показано изменение контурного напряжения $\overline{\sigma}_k$ в десятиэтажном здании с подвальным этажом во времени $t/\Delta t$.

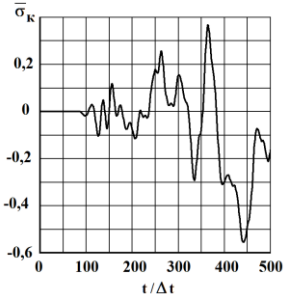


Рисунок 4 – Изменение упругого контурного напряжения $\overline{\sigma}_k$ в точке А1 на контуре десятиэтажного здания во времени $t/\Delta t$. График В.К. Мусаева

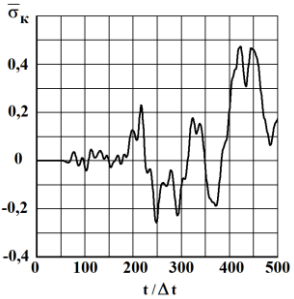


Рисунок 5 – Изменение упругого контурного напряжения $\overline{\sigma}_k$ в точке А6 на контуре десятиэтажного здания во времени $t/\Delta t$. График В.К. Мусаева

Выводы

1. Исследования в рассматриваемой научной работе являются продолжением ранее полученных результатов. Такой подход к исследованию новых задач, которые опираются на предыдущие научные результаты, могут быть выполнены, если изначально была принята постановка и реализация задач с использований методов фундаментальной науки. Этот выбор можно было сделать благодаря

применению методов вычислительной (компьютерной) механики деформируемых тел с возможностями языков программирования и вычислительным машин.

2. Составлен комплекс программ для решения нестационарной динамической задачи теории упругости для областей разной (сложной) формы.

3. Десятиэтажное здание с подвальным этажом и упругим основанием моделируется с помощью метода конечных элементов (математическое моделирование). Ударное воздействие моделируется в виде трапеции. Решается система уравнений из 16202276 неизвестных.

4. В характерных точках получены контурные напряжения.

Литература:

1. *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.

2. *Musayev V.K.* Mathematical modeling of non-stationary elastic waves stresses under a concentrated vertical exposure in the form of delta functions on the surface of the half-plane (Lamb problem) // International Journal for Computational Civil and Structural Engineering. – 2019. – Volume 15. Issue 2. – P. 111-124.

3. *Мусаев В.К.* Математическое моделирование нестационарных упругих волн напряжений (переходной процесс) при воздействии (вертикальное сосредоточенное в виде треугольного импульса) на поверхность полуплоскости (задача Лэмба) // Геология и геофизика Юга России. – 2020. – № 4. – С. 164-174.

4. *Мусаев В.К.* Математическое моделирование волн напряжений при сосредоточенном вертикальном воздействии в виде треугольного импульса: задача Лэмба // Строительная механика инженерных конструкций и сооружений. – 2021. – № 2. – С. 112-120.

5. *Мусаев В.К.* Математическое моделирование нестационарных волн напряжений в деформируемых телах при ударных, взрывных и сейсмических воздействиях. – М.: Российский университет транспорта, 2021. – 629 с.

6. *Мусаев В.К.* Защита нарушенного авторского права (плагиат) в Пушкинском городском, Московском областном и Верховном Судах Российской Федерации. – М.: Российский университет транспорта, 2021. – 874 с.

DOI: 10.25728/iccss.2022.50.37.042

Кацко Д.И., Кацко А.И.

К вопросу о повышении безопасности проектирования природно-технических систем

Аннотация: При строительстве сооружений гидротехнического, гражданского, промышленного назначений, автомобильных и железных дорог возникает задача вероятностного анализа опасностей и их учета при проектировании. В работе показано, что использование экстремальных законов распределения (Вейбулла, Гамма и др.) при оценке устойчивости откосов и склонов может лучше соответствовать эмпирическому распределению, полученному в результате имитационного эксперимента.

Ключевые слова: безопасность, метод Монте-Карло; оползень, откос, закон распределения, метод Феллениуса

Для расчета устойчивости склона в геотехнических программах есть возможность задания законов распределения входных параметров: сцепления, угла внутреннего трения и др., однако остается не понятным, каким законам распределения в таком случае будет подчиняться коэффициент устойчивости [1]. Для ответа на этот вопрос была разработана методика вероятностной оценки устойчивости склона, основанная на имитационном моделировании (метод Монте-Карло) с различными законами распределения.

На примере тестовой задачи проведен имитационный эксперимент [2]. Рассматривался однородный склон с известными геометрическими параметрами склона и физико-механическими свойствами грунта.

Для решения использовался простейший метод Феллениуса (1), расчет которого был перенесен в MS Excel [3] для анализа рисков по методу Монте-Карло [4] с помощью надстройки – @RISK

$$Fs = \frac{\sum(cl + tg\varphi)}{\sum W\ sin\alpha} \quad , \tag{1}$$

где c – удельное сцепление; l – длина поверхности скольжения; $tg\varphi$ – угол внутреннего трения; α – угол наклона поверхности; W – вес грунта.

Традиционно одним из признаков однородности данных считаетя коэффициент вариации (2) [4, 7]

$$V = \sigma/\bar{x}, \tag{2}$$

где σ – среднее квадратическое отклонение; $\bar{x}$ – среднее арифметическое значение (математическое ожидание).

Для проведения имитационного эксперимента рассматривались три уровня c и φ по шкале изменения их коэффициента вариации ($0 < V < 0{,}3$) при постоянных значениях средних ($c = 15{,}7$кПа, φ = 17,9°). План эксперимента представлен в таблице 1.

Таблица 1 – Комбинация условий для эксперимента типа 3^2

Факторы	A_0	A_1	A_2
B_0	00	01	02
B_1	10	11	12
B_2	20	21	22

При подгонке распределений использовалися бутстреп-метод [5, 6] (тысяча итераций для каждого распределения) и различные характеристики адекватности подгонки распределений. Результаты проведенного имитационного эксперимента в @RISK с нормальными распределениями характеристик прочности грунта и средними квадратическими отклонениями в соответствии с планом приведены в таблице 2 и на рисунке 1 только на уровне A_1B_1, что обусловлено подобием результатов. Конечные итоги на всех уровнях приведены в таблице 3. Результаты проведенного имитационного эксперимента показали, что в зависимости от сочетаний уровней среднеквадратических отклонений и характеристик оценки качества подгонки распределения лучшими являются нормальное распределение и распределение Вейбулла. Причем критерии

отличаются статистически незначимо, то есть коэффициент устойчивости может принимать значения, которые подчиняются закону распределения Вейбулла. В таблице 3 представлены приоритетные законы распределения в соответствии с критериями: усредненный логарифм правдоподобия (Av_ LogL) и χ^2.

Таблица 2 – Результаты эксперимента на уровнях A_1B_1

	A_1 B_1			
Распределение	Av_ LogL	P(Fs<1.05)	χ^2	P(Fs<1.05)
Эмпирическое		0.042		0.031
Нормальное	0.3634	0.038	23.932	0.036
Вейбулла	0.3579	0.044	33.386	0.035
Лог-логистическое	0.3566	-	31.82	-
Логистическое	0.3565	-	28.398	0.041

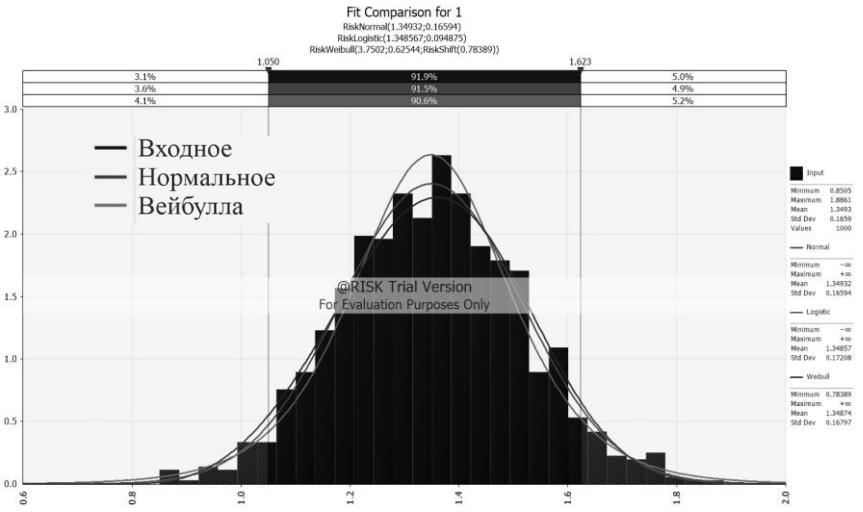


Рисунок 1 – Результаты эксперимента на уровнях A_1B_1, с критерием χ^2 (хи-квадрат)

Таблица 3 – Законы распределения для эксперимента типа 3^2

Факторы	A_0	A_1	A_2
B_0	Нормальный Вейбулла	Вейбулла Нормальный	Нормальный Лог-логорифмический
B_1	Вейбулла Нормальный	Нормальный Нормальный	Вейбулла Нормальный
B_2	Нормальный Нормальный	Нормальный Вейбулла	Нормальный Вейбулла

Таким образом, в ходе имитационного эксперимента было доказано, что в половине случаев эмпирические наблюдения лучше описываются экстремальными законами распределения [7] (Вейбулла, Лог-логарифмическое), что позволяет точнее оценить вероятность обрушения склона, учесть ее при проектировании и повысить безопасность строительства сооружений в условиях опасных геологических и инженерно-геологических процессов (оползни, осыпи, оплывины, обвалы, линейная и поверхностная эрозия склонов, сейсмические явления и т.д.).

Литература:

1. *Безуглова Е.В., Маций С.И., Подтелков В.В.* Оползневой риск транспортных природно-технических систем. – Краснодар: КубГАУ, 2015. – 239 с.

2. *Шенон Р.* Имитационное моделирование систем – искусство и наука / Р. Шенон; пер. с англ. – М.: МИР, 1978. – 420 с.

3. *Добров Э.М.* Механика грунтов. – М.: Издательский центр «Академия», 2008. – 272 с.

4. *Ивченко Г.И., Медведев Ю.И.* Введение в математическую статистику / 2-е изд., испр. и доп. – М.: Ленанд, 2017. – 608 с.

5. *Клейнен Дж.* Статистические методы в имитационном моделировании / под ред. и с предисл. Ю.П. Адлера, В.Н. Варыгина, пер. с англ. Ю.П. Адлера. – Москва: Статистика, 1978. – Вып. 1 – 222 с. Вып. 2 – 335 с.

6. *Райзер В.Д.* Вероятносные методы надежности в анализе надежности и живучести сооружений. – М.: АСВ, 2018. – 396 с.

7. *Гумбель Э.* Статистика экстремальных значений / Пер. с англ. В. Ю. Татарского, под ред. Д. М. Чибисова, с предисловием Б. В. Гнеденко. – М.: МИР, 1965. – 451 с.

DOI: 10.25728/iccss.2022.14.53.043

Чинакал В.О.

Об одном подходе к повышению производственно-технологической безопасности управления сложными промышленными объектами

Аннотация: Рассматривается подход к повышению безопасности и эффективности управления сложным распределенным промышленным объектом (СРПО) с использованием возможностей дополнительной интеллектуальной обработки оперативных и прогнозных данных о возможных изменениях ключевых технологических параметров (КТП) процессов и данных контроля состояния технологического оборудования (СТО). Предложена концепция модифицированного варианта системы усовершенствованного мониторинга AMS+ (AMS+ - Advanced Monitoring System Plus), разработаны основные требования и структура AMS+, реализующей оперативный мониторинг СРПО из класса непрерывных производств с использованием методов ситуационного анализа и предиктивной диагностики возможных изменений КТП и СТО.

Ключевые слова: безопасность управления, распределенный промышленный объект, непрерывное производство, ключевые технологические параметры, AMS

Введение

Развитие методов автоматизированного и автоматического контроля и управления в рамках концепции «Индустрия 4.0» является одним из перспективных направлений в повышении эффективности и безопасности управления сложными распределенными промышленными объектами (СРПО) в классе непрерывных производств. При управлении такими объектами необходимо обеспечивать решение ряда проблем, связанных со специфическими условиями и особенностями эксплуатации СРПО, а также высокими требованиями по производственно-

технологической, экологической, информационной и другим видам безопасности [1, 2].

Одной из таких актуальных проблем является необходимость существенного совершенствования систем оперативного мониторинга большого числа производственных процессов, ключевых технологических параметров (КТП) установок, а также постоянного контроля и диагностики состояния многочисленного технологического оборудования (СТО) и аппаратно-программных средств (АПС), используемых в системах контроля и управления в АСУТП.

В последние годы ведущие в мире фирмы в области автоматизации производства стали вкладывать значительные средства в разработку и создание новых перспективных систем усовершенствованного управления технологическими процессами – APC (Advanced Process Control) и улучшенного мониторинга – AMS (Advanced Monitoring System). При этом применяются современные информационные технологии, позволяющие создавать крупные интегрированные системы, использовать на различных платформах промышленный интернет вещей (IIoT), анализ Big Data, облачные и туманные вычисления, машинное обучение, методы и средства искусственного интеллекта, прогнозирования и другие технологии [1, 3-5].

Применение таких систем для крупномасштабных непрерывных и непрерывно-дискретных технологических производств (нефтепереработка, нефтехимия, энергетика и др.) позволяет получать значительный экономический эффект. Наибольший вклад в общий эффект достигается за счет:

– использования интегрированных систем улучшенного контроля и управления установками AMS&APC [4, 5], обеспечивающих стабилизацию и оптимизацию основных КТП (снижение излишних запасов по качеству продуктов), раннее обнаружение скрытых изменений технологических параметров КТП и СТО [5], снижение эксплуатационных затрат и др.;

– онлайн-диагностики аппаратно-программных средств АСУТП и основных параметров типового технологического оборудования (СТО) с применением различных технологий [1]. включая облачные технологии для СТО [6, 7].

В то же время следует отметить, что разработка и внедрение в промышленность таких систем все еще требует проведения достаточно объемных и затратных работ. Работы при создании систем связанны с обследованием объектов, сбором статистики, построением моделей и моделированием, проектированием, привязкой проекта к объекту, внедрением в эксплуатацию. На этапе эксплуатации систем обычно требуется выполнять дополнительные работы по адаптации моделей, структуры, интерфейса и т.д. в связи с различными обстоятельствами (сменой сырья, продукции, технологий, аппаратуры, требований и т.п.). Для проведения этих работ необходимы высококвалифицированные специалисты, которых как обычно не хватает, и эффективность применения таких систем может значительно понизиться.

Кроме того, в крупных СРПО использование и модернизация AMS и/или APC осуществляется, как правило, в составе отдельных АСУТП, что иногда может приводить к различным оценкам одних и тех же КТП в разных АСУТП. Статистика в каждой АСУТП часто пишется вся подряд, и нужно вручную выделять квазистационарные интервалы (по типам сырья, режимам, требованиям по выпуску продукции и т.д.). Также необходимо оценивать возможное влияние управления и различных нарушений на зафиксированные результаты измерений (сбои в линиях связи, ошибки лабораторного контроля или поточных измерений, частичные нарушения в работе датчиков и исполнительных и т.п.). В связи с этим программное обеспечение (ПО) AMS большинства фирм ориентировано на поддержку высококвалифицированного пользователя в режиме off-line обработки архивированных производственных данных. С учетом необходимости использования результатов мониторинга для оперативного управления, анализ и прогноз изменений КТП также должен быть on-line, чтобы иметь для управления более точные оценки КТП в реальном времени.

Для получения оценок СТО обычно используется типовые наборы сведений [6, 7], включающих паспортные данные оборудования, регламенты поверок, профилактики, капремонта, общее фактическое время работы и от последней профилактики, число ремонтов, диагностические карты, результаты онлайн-диагностики и т.п. Для выявления off-line предаварийных ситуаций, определения общего текущего уровня СТО, настройки и

планирования профилактических и ремонтных работ технологического оборудования этого вполне достаточно. Однако для оперативного анализа с помощью AMS возможных причин аномальных отклонений КТП и СТО из-за нарушений в реальном времени в работе АПС АСУТП (датчики, фильтры, исполнительные устройства, сети передачи данных и т.п.) этого недостаточно.

Необходимо дополнительно использовать методы автоматизации ситуационного анализа в реальном времени расширенной совокупности имеющихся данных [3], выяснить и устранить причины аномалий и затем определить корректирующее управление.

В данной работе рассматривается подход к разработке модифицированного варианта AMS+ с расширенными функциональными возможностями для автоматического получения в режиме «online» оценок текущих и прогнозных значений КТП и СТО, используемых при оперативном управлении СРПО.

Основная идея подхода состоит в циклическом использовании методов оперативной классификации текущих и прогнозируемых производственных ситуаций, и эволюционного выбора в различных ситуациях методов, моделей и динамической настройки параметров алгоритмов идентификации, адаптации и оперативной оценки текущих статистических характеристик КТП и СТО контролируемых и регулируемых технологических потоков. Для уточнения параметров КТП и СТО используется взвешенный прогноз значений оценок каждого параметра по различным альтернативным адаптивным моделям, известные методы и средства контроля и ранней диагностики аномальных нарушений в работе технологического оборудования [6, 7], дополненные анализом возможных скрытых изменений параметров потоков и технологических характеристик объекта [5].

Рассмотрим информационные связи AMS+, структуру и основные задачи, решаемые в системе.

Информационные связи AMS+

Основные информационные связи системы AMS+ с объектом и другими подсистемами представлены на рисунке 1.

Система AMS+ (блок 1) является внешней по отношению АСУТП (блок 2), получает исходную информацию от общей базы

данных измерений (блок 7) и передает оценки КТП и СТО в АСУТП, а также другим пользователям.

В АСУТП поступают данные от системы оперативно-диспетчерского управления (MES – блок 5) о плановых заданиях по выпуску продукции и доступным ресурсам по сырью. Эти и другие данные от АСУТП поступают в AMS+, где используются при оценке текущей и прогнозируемых ситуаций. Система противоаварийной защиты (ПАЗ - блок 3) в АСУТП обычно получает информацию по независимым каналам, а также дополнительно использует оценки КТП, СТО и оценки критических и предаварийных ситуаций из блока 1.

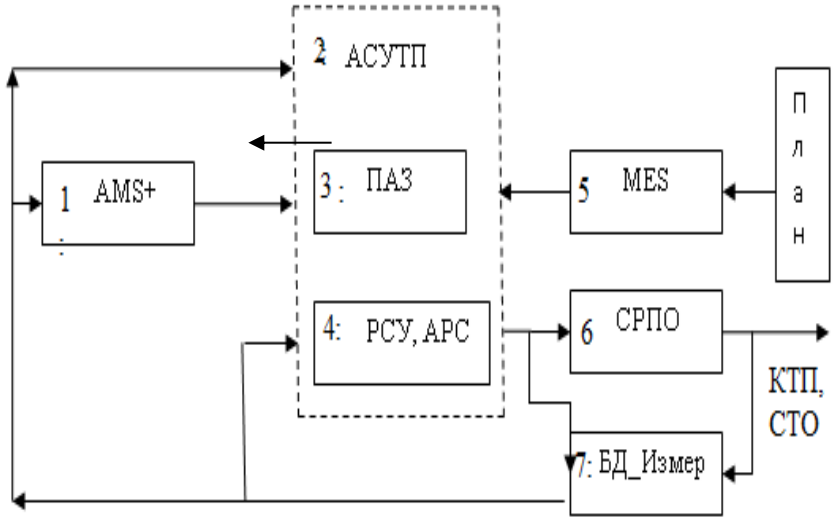


Рисунок 1 – Информационные связи AMS+ с основными подсистемами АСУТП и объекта

2. Структура и основные задачи, решаемые AMS+

Структура, основные функции и задачи, решаемые в AMS+ представлены на укрупненной структурно-функциональной схеме на рисунке 2.

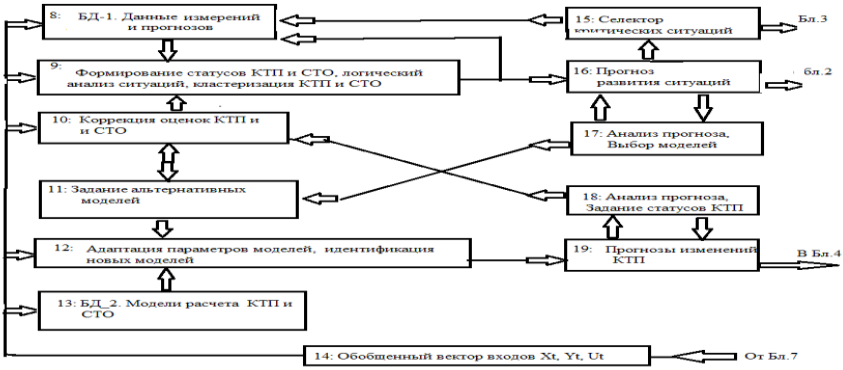


Рисунок 2 – Структурно-функциональная схема AMS+

Для удобства ссылок на информационные связи AMS+ на рисунке 1 нумерация блоков продолжена на рисунке 2 с привязкой соответствующих входов и выходов AMS+ к другим блокам.

В основе подхода к построению AMS+ лежит применение эволюционных методов, реализуемых в двух постоянно взаимодействующих автоматических подсистемах («А» и «В»). К подсистеме «А» относятся блоки: 8-10, 15-17, к подсистеме «В» - блоки: 11-13 и 18-19. В блоке 14 формируется для каждого интервала времени мониторинга **t** обобщенный вектор входов AMS+, состаящий из векторов текущего состояния объекта X_t, измеренных и вычисленных выходов объекта Y_t (качественные и количественные показатели потоков) и текущего управления U_t.

Подсистемы «А» и «В» циклически обрабатывают в реальном времени общую входную информацию из блока 14, а также информацию, накопленную в процессе функционирования AMS+ в базах данных БД-1 (блок 8) и БД-2 блок 11), данных, решая свои задачи и корректируя работу с учетом анализа результатов в каждой из подсистем.

Подсистема «А» классифицирует текущую ситуацию на объекте (блок 9), формируя статусы КТП и СТО на основе скорректированных предыдущих оценок (блок 10), выполняя логический анализ текущего и прогнозируемого развития ситуаций (блоки 16, 17) для технологического оборудования и АПС в каждом сеансе мониторинга, выделяя критические ситуации (блок 15), отправляемые в блок 3 и вырабатывает рекомендации по поиску

новых моделей для определения КТП и СТО для подсистемы «В» (блок 17).

Подсистема «В» в зависимости от ситуации (блоки 16,17) и имеющейся входной и накопленной информации (блок 13) формирует наборы из альтернативных моделей (блок 11), выполняет текущую адаптацию параметров рекомендуемых альтернативных моделей, идентифицирует новые модели (блок 12) определяет текущие и прогнозируемые значения оценок КТП и СТО (блок 19), выполняет анализ изменений КТП и СТО (блок 18), передавая их в блок 4 АСУТП и в подсистему «А» (блок 18).

Работа подсистем циклически повторяется, классифицируя и анализируя в реальном времени текущую и прогнозируемую ситуации, выполняя оперативную обработку имеющихся измерений и прогнозируемых возможных изменений КТП, СТО и АПС с учетом имеющихся ресурсов и плановых заданий. Алгоритмы реализации отдельных рассмотренных задач рассматривались ранее в [3-7].

Литература:

1. *Ицкович Э.Л.* Перспективная автоматизация агрегатов предприятий технологических отраслей. – М.: Горячая линия–Телеком, 2018. – 544 с.

2. *Чинакал В.О.* Проблемы проектирования подсистем оперативного оценивания состояния сложных промышленных объектов / Материалы 15-ой международной конференции CAD/ CAM/ PDM – 2015 «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта». – М.: ИПУ РАН, 2015. – С. 71-73.

3. *Чинакал В.О.* Применение интеллектуальных средств в системе мониторинга распределенного промышленного объекта / Материалы пятой международной конференции «Управление развитием крупномасштабных систем» MLSD’2011. – М.: ИПУ РАН, 2011. – С. 386-389.

4. *Чинакал В.О.* Создание систем усовершенствованного мониторинга и управления для повышения эффективности и безопасности управления сложными промышленными объектами / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем ПУБСС-2021 (Москва, 15 декабря 2021 г.). – М.: ИПУ РАН, 2021. – С. 493-499.

5. *Чинакал В.О.* Повышение безопасности управления сложными объектами в условиях скрытых изменений параметров технологических процессов / Материалы XXIX Международной конференции «Проблемы управления безопасностью сложных систем ПУБСС-2021 (Москва, 15 декабря 2021 г.). – М.: ИПУ РАН, 2021. – С. 390-395.

6. Онлайн-диагностика машинного оборудования. – URL: https://www.emerson.com/documents/automation/product-data-sheet-csi-6500-chassis-options-deltav-ru-ru-38896.pdf (дата обращения 30.10.2022).

7. Соколов Д.А., Соловьев С.Ю. Контроль и мониторинг промышленного оборудования с использованием платформы MindShere компании Siemens // Информатизация и системы управления в промышленности. – 2018. – №4(76). – С. 17-22.

DOI: 10.25728/iccss.2022.18.11.044

Лепешкин О.М., Остроумов М.А., Остроумов О.А., Кулаков В.В.

Подход к обеспечению выполнения функций и задач в сложной технической системе

Аннотация: Процесс функционирования сложной технической системы определяется набором задач и функций, которые она и ее элементы выполняют. При этом нарушение его выполнения может привести к тяжелым последствиям. В работе предлагается подход к обеспечению выполнения функций и задач в системе, основанный на управлении задачами и функциями, а также использовании ресурсов системы для их выполнения.

Ключевые слова: устойчивость функционирования, сложная техническая система, функции, задачи, критичность

Сложность современных технических систем определяется, в первую очередь, количеством элементов системы и связей между ними. Увеличение количества элементов и их совершенствование, как правило, приводит к появлению у системы новых возможностей,

определяющих ее способность выполнять большее количество задач и функций, либо новые задачи и функции.

Способность системы и ее элементов выполнять все необходимые задачи и функции определяет ее функциональную устойчивость [1-4], как, например, показано для сети связи общего пользования в ГОСТ 53111-2008 «Устойчивость функционирования сети связи общего пользования». Сложные системы, как правило, функционируют с целью выполнения определенного целевого предназначения в интересах другой системы (органов управления, организаций, предприятий, ведомств и т.д.). Невыполнение сложной системой целевого предназначения, функций и задач может привести к срыву в выполнении задач объектов, в интересах которых она функционирует.

Процесс функционирования системы обеспечивается ее ресурсом [5-7], распределенным в пространстве и времени, при этом, в качестве ресурса может выступать люди, техника, элементы системы, результаты их функционирования (информационный, телекоммуникационный ресурс, пропускная способность и т.д.) и т.д. Характеристика элементов системы, определение связей между ними, характеризует возможности системы, т.е. определенный набор задач и функций, которые система может выполнить в единицу времени за счет имеющегося в данный момент ресурса.

В процессе функционирования системы для выполнения задач и функций планируется ресурс, который характеризуется пространственно-временными характеристиками (рисунок 1).

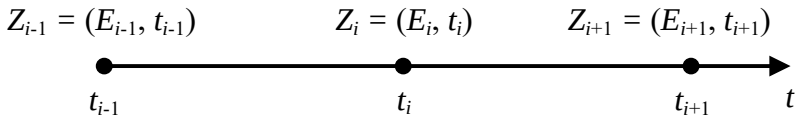


Рисунок 1 – Распределение ресурсов для выполнения задач в процессе функционирования системы

Выполнение каждой функции системы возможно при последовательном и параллельном выполнении определенного набора задач, ее характеризующих (рисунок 2) [1, 8]. При этом, при исходном планировании осуществляется закрепление для каждой задачи определенного набора ресурсов системы, позволяющих ее

выполнить. Аналогично для каждой функции формируется перечень ресурсов, обеспечивающих ее выполнение.

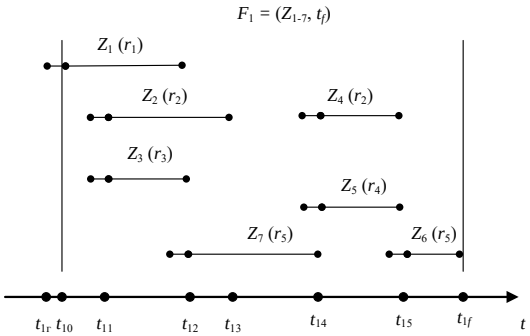


Рисунок 2 – Распределение задач для выполнения функции

В процессе планирования и закрепления ресурса необходимо согласование возможности использования ресурсов системы, характеризуемых пространственно-временными характеристиками, по задачам и по времени (рисунок 3) [1, 2, 8]. Несогласованное использование ресурсов и выполнение задач приводят к конфликтам в использовании ресурса и выполнении задач.

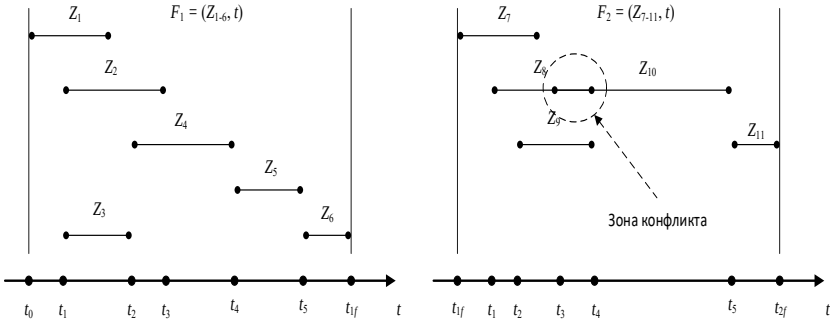


Рисунок 3 – Возникновение конфликтов в планировании выполнения задач и функций системы

Возникновение конфликтов в сложных системах обусловлено различными причинами естественного и искусственного характера, которые воздействуют на систему преднамеренно или

непреднамеренно [2, 4]. При этом, источником воздействия могут быть как внутренние, так и внешние факторы. В данном случае, интерес имеют последствия такого воздействия, которые создают предпосылки или могут привести к невыполнению (срыву в выполнении) задач и функций системы. В этом случае происходит нарушение устойчивого функционирования системы. При этом, нарушение работоспособности элементов системы, всей системы не всегда приводит к нарушению ее устойчивого функционирования. Функциональная устойчивость системы определяется выполняемыми функциями и задачами в любой момент времени функционирования системы.

Появление конфликтов в процессе функционирования системы, приводящее к нарушению ее устойчивого функционирования, требует своевременной реакции на них. При этом, правильное согласование выполнения задач, функций и использования ресурсов для их выполнения, определяют функциональную устойчивость системы на этапе построения и планирования функционирования системы.

Конфликты в системе также появляются в процессе ее функционирования (рисунок 4), что обусловлено низкой надежностью технических средств, различными воздействиями, нарушениями безопасности функционирования системы, техники безопасности эксплуатации оборудования и т.д. Конфликт приводит к нарушению или невозможности выполнения задач и функций системы. При этом, для обеспечения устойчивого функционирования системы, важным является использование предикативного контроля и мониторинга [2, 4, 9, 10] процесса функционирования системы, что позволяет прогнозировать возникновение конфликта до начала выполнения функции или задачи (рисунок 4).

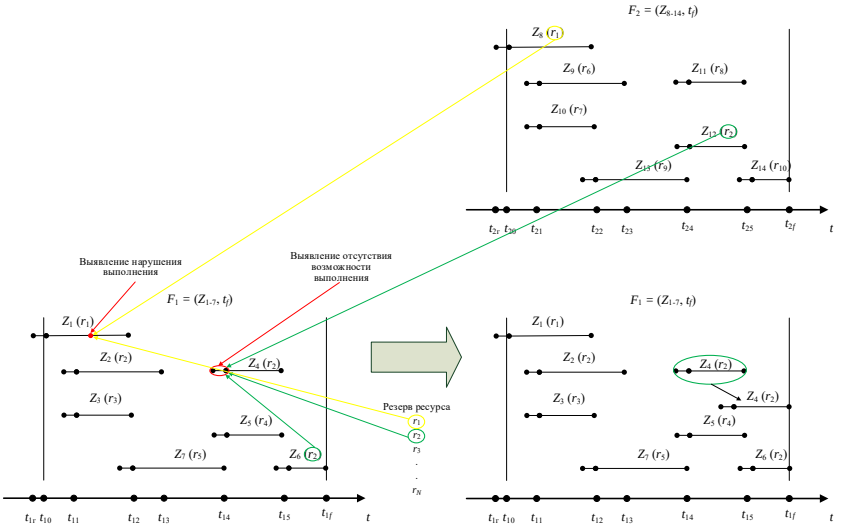


Рисунок 4 – Возникновение конфликтов в процессе функционирования сложной технической системы и их устранение

В процессе выполнения функции или задачи обнаружение конфликта требует своевременной и быстрой реакции системы (оператора, лиц, принимающих решение) для его устранения. Взаимовлияние задач и функций друг на друга, а также критичность некоторых задач и функций, определяют возможность использования ресурсов, спланированных для выполнения других задач и функций для текущих конфликтных задач и функций. Также возможно изменение времени выполнения функций и задач, которые не оказывают значительного влияния на процесс устойчивого и безопасного функционирования системы.

Вывод

Обеспечение устойчивого процесса функционирования любой системы является сложным действием. При этом традиционно устойчивость рассматривают с позиции надежности, живучести, помехоустойчивости и киберустойчивости системы и ее элементов [5-8, 10, 11]. При этом, обеспечение устойчивости системы сводится к обеспечению устойчивости отдельных элементов, без учета их

функциональной устойчивости, т.е способности выполнять функции и задачи, независимо от их состояния. Если система и ее какие-либо ее элементы неисправны, но работоспособны и способны выполнять функции и задачи системы, то она функционально устойчива.

Предлагаемый в работе подход к обеспечению функциональной устойчивости сложных технических систем строится на планировании функционирования системы, а также своевременном выявлении конфликтов в ней и управлении задачами, функциями и ресурсами для устранения возникающих конфликтов, возникновения предпосылок к конфликтам.

Литература:

1. *Остроумов О.А.* Методология обеспечения процесса устойчивого функционирования системы связи – критически важного объекта системы управления // Военная мысль. – 2022. – № 9. – С. 52-58.

2. *Остроумов О.А.* Методика обеспечения функциональной устойчивости системы связи // Вопросы радиоэлектроники. Сер. Техника телевидения. – 2022. – № 1. – С. 3-12.

3. *Lepeshkin O.M., Ostroumov O.A., Sinyk A.D.* The communication system functional stability with critical objects / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем». – Москва: ИПУ РАН, 2021. – С. 80-85.

4. *Остроумов О.А.* Модель контроля функционирования системы связи // Известия Тульского государственного университета. Технические науки. – 2022. – № 3. – С. 300-310.

5. *Дурняк Б.В., Машков О.А., Усаченко Л.М., Сабат В.И.* Методология обеспечения функциональной устойчивости иерархических организационных систем управления // Сборник научных статей: Институт проблем моделирования в энергетике, НАН Украины. –2008. – В. 48. – С. 3-21.

6. *Петренко С.А.* Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий // Труды ИСА РАН. – 2009. – Т. 41. – С. 175-193.

7. *Стародубцев Ю.И., Иванов С.А., Закалкин П.В.* Концептуальные направления решения проблем обеспечения устойчивости Единой сети электросвязи Российской Федерации в

интересах органов государственной власти и военного управления // Военная мысль. – 2021. – № 4. – С. 39-49.

8. *Burlov V.G., Lepeshkin O.M., Lepeshkin M.O., Solovev D.B.* Organization of Management of Social and Economic Systems of the Region in the Conditions of the Required Technosphere Safety / IOP Conference Series: Earth and Environmental Science, 2020. – Volume 459. Chapter 1. – 022081. DOI: 10.1088/1755-1315/459/2/022081

9. *Груздев Д.А., Закалкин П.В., Кузнецов С.И., Тесля С.П.* Мониторинг информационно-телекоммуникационных сетей // Труды учебных заведений связи. – 2016. – Т.2. №4. – С. 46-50.

10. *Коцыняк М.А., Карпов М.А., Лаута О.С., Дементьев В.Е.* Управление системой обеспечения безопасности информационно-телекоммуникационной сети на основе алгоритмов функционирования искусственной нейронной сети // Известия Тульского государственного университета. Технические науки. – 2020. – №4. – С. 3-10.

11. *Пермяков А.С., Лепешкин О.М., Митрофанов М.В.* Проблемы защищенности информационно-телекоммуникационных сетей специального назначения / Радиолокация, навигация, связь: Сборник трудов XXVI Международной научно-технической конференции. В 6-ти томах. – Воронеж: Воронежский государственный университет, 2020. – С. 44-48.

DOI: 10.25728/iccss.2022.87.98.045

Чернов К.В.

Об управлении техносферной безопасностью

Аннотация: С использованием принципа универсального эволюционизма даётся определение термину «техносферная безопасность». Проводится декомпозиция системы управления техносферной безопасностью в целях её оптимизации.

Ключевые слова: универсальный эволюционизм, антропосфера, техносферная безопасность, управление, система, декомпозиция

Принцип универсального эволюционизма (УНЭВ) сформулирован выдающимся учёным Н.Н. Моисеевым. По его словам, «… все в Природе – и неживое вещество (косная материя, по терминологии В.И. Вернадского), и мир живого, и общество – подчиняются некой общей логике, которую я однажды назвал универсальным эволюционизмом». «Универсальный эволюционизм – теория самоорганизации Универсума, объединяющая в единое целое идеи системного и эволюционного подходов» [1]. В соответствии с принципом УНЭВ и системным положением о сопринадлежности [2] часть планеты Земля при её эволюции последовательно проходит следующие стадии: абиосфера, биосфера, антропосфера, техносфера.

Абиосфера – планетарная абиогенная система с абиотическими компонентами и внешней средой, функция которой обусловлена необходимостью её устойчивого развития в целях возникновения и обеспечения существования биоты. Абиогенез представляет собой эволюцию компонентов абиосферы, в результате которой происходит возникновение биоты.

Биосфера – планетарная биогенная система с биотическими и абиотическими компонентами и внешней средой, функция которой обусловлена необходимостью её устойчивого развития в целях возникновения и обеспечения существования человека. Биогенез предстаёт эволюцией компонентов биосферы, в результате которой происходит развитие биоты и возникновение человека как носителя разума, осознающего Универсум и преобразующего его для увеличения глубины и полноты осознания.

Антропосфера – планетарная антропогенная система с биотическими, в их числе антропными и неантропными, компонентами, а также артетическими, абиотическими и иными компонентами, функция которой обусловлена необходимостью её устойчивого развития в целях гуманитарного совершенствования биосферы. Антропогенез представляет собой эволюцию компонентов антропосферы, в результате которой происходит развитие человека. Техногенез есть слагаемое антропогенеза в области эволюции артетических, прежде всего технетических, компонентов антропосферы, результатом которой становится усиление адаптационных и созидательных способностей человека, содействующих его развитию. Техносфера относится к основным

компонентам антропосферы и предстаёт планетарной техногенной системой с антропными, артетическими, в том числе технетическими, и иными компонентами, функция которой обусловлена необходимостью её устойчивого развития в целях гуманитарного совершенствования биосферы.

Техносферная безопасность как термин, – это докритическое взаимодействие человека с технетическими и другими техногенно изменёнными компонентами техносферы, эффекты которого не приводят к сокращению его продолжительности жизни, прежде всего вследствие болезней или травм. Кроме термина техносферная безопасность предстаёт областью научных теоретико-прикладных знаний, практическими знаниями при разных видах антропогенной деятельности, областью обучения, медицины и экономики, формами организационно-правового регулирования жизнедеятельности в техносфере.

Жизнедеятельность в техносфере является подвластной, т.е. управляется. Управление – это руководящая деятельность субъекта управления относительно объекта, направленной на достижение определённой цели. Субъект управления предстаёт инициатором руководящего действия. Объектом управления является то или тот, на что или на кого производится руководящее действие. Управление в соответствии с положением о сопринадлежности является иерархическим, оно может быть одноуровневым и многоуровневым. При одноуровневом управлении и на каждом уровне многоуровневого субъект и объект находятся в соподчинённом взаимодействии. При многоуровневом управлении субъекты последующих уровней могут быть объектами управления для предыдущих. Объект управления, также как и субъект, может представать отдельным работником или группой работников.

Управление техносферной безопасностью, или управление безопасностью жизнедеятельности в техносфере, – руководящая деятельность субъекта управления по прогнозированию, планированию, легитимации, мотивации, координации, надзору и контролю исполнительной деятельности объекта управления, направленная на обеспечение взаимодействия человека с другими компонентами техносферы на докритическом, безопасном, уровне, способствующем её устойчивому развитию.

Техносфера как планетарная система имеет переменный состав, определяемый принадлежностью её компонентов разным государствам. Это является причиной того, что управление техносферной безопасностью в каждом государстве осуществляется по-разному. Надгосударственная координация в области планетарной безопасности осуществляется Организацией Объединённых Наций. Надгосударственную координацию в области техносферной безопасности относительно Российской Федерации (РФ) осуществляет также Евразийский экономический союз.

Система управления техносферной безопасностью в РФ разделяется на составляющие в зависимости от следующих законодательно регулируемых областей с названием: промышленная безопасность, техническое регулирование, защита населения и территорий от чрезвычайных ситуаций (ЧС), санитарно-эпидемиологическое благополучие населения, охрана окружающей среды, охрана труда, радиационная безопасность населения, безопасность гидротехнических сооружений, транспортная безопасность. Безопасность в строительстве обеспечивается саморегулируемыми организациями в соответствии с законами РФ по указанным составляющим.

Федеральное управление применительно к областям техносферной безопасности осуществляется Правительством РФ непосредственно или по его поручению федеральным органом исполнительной власти, выполняющим функции по выработке государственной политики и нормативно-правовому регулированию в данной области, а также другими федеральными органами исполнительной власти в пределах их полномочий. Государственное управление в части выполнения контрольно-надзорных функций осуществляет федеральный орган исполнительной власти, уполномоченный на проведение федерального государственного контроля (надзора) за соблюдением законодательства и иных нормативных правовых актов, содержащих нормы права применительно к областям техносферной безопасности, и его территориальные органы.

Система управления техносферной безопасностью в области охраны окружающей среды имеет пять уровней сопринадлежности: федеральный, межрегиональный, региональный, муниципальный уровни и уровень организации. Система управления техносферной

безопасностью в области охраны окружающей среды федерального уровня сопринадлежности имеет в своём составе следующие системы, компоненты, элементы (рисунок 1):

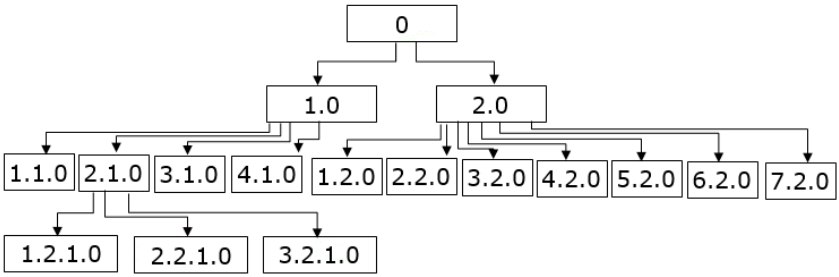


Рисунок 1 – Декомпозиция системы управления техносферной безопасностью федерального уровня в области охраны окружающей среды

Системы, компоненты и элементы, выделенные при декомпозиции, имеют следующие названия:

/0/ – система управления техносферной безопасностью федерального уровня;

/1.0/ – система управления техносферной безопасностью федерального уровня в области охраны окружающей среды;

/2.0/ – внешняя среда;

/1.1.0/ – Председатель правительства РФ и его заместитель, ответственный за государственную политику в сфере охраны окружающей среды;

/2.1.0/ – Министерство природных ресурсов и экологии РФ (Минприроды России);

/3.1.0/ – Правительственная комиссия по вопросам природопользования и охраны окружающей среды;

/4.1.0/ – Федеральные министерства, службы, агентства;

/1.2.0/ – органы президентской власти;

/2.2.0/ – органы прокуратуры;

/3.2.0/ – органы судебной власти;

/4.2.0/ – система управления техносферной безопасностью в области в области охраны окружающей среды межрегионального уровня сопринадлежности;

/5.2.0/ – система управления техносферной безопасностью в области в области охраны окружающей среды регионального уровня сопринадлежности;

/6.2.0/ – система управления техносферной безопасностью в области в области охраны окружающей среды муниципального уровня сопринадлежности;

/7.2.0/ – система управления техносферной безопасностью в области охраны окружающей среды уровня организации;

/1.2.1.0/ – руководство Минприроды России;

/2.2.1.0/ – координационные и совещательные органы Минприроды России;

/3.2.1.0/ – Федеральная служба по надзору в сфере природопользования (Росприроднадзор).

Декомпозиция позволяет раскрывать функции каждого компонента.

Подобным образом проводится декомпозиция систем последующих уровней сопринадлежности и систем относительно других составляющих техносферной безопасности. Например, системы, компоненты и элементы, выделенные при декомпозиции системы управления техносферной безопасностью в области промышленной безопасности на уровне организации, эксплуатирующей опасные производственные объекты (ОПО), имеют следующие названия:

/0/ – система управления техносферной безопасностью на уровне организации;

/1.0/ – система управления техносферной безопасностью на уровне организации в области промышленной безопасности;

/2.0/ – внешняя среда;

/1.1.0/ – компоненты системы управления промышленной безопасностью на уровне работодателя;

/2.1.0/ – компоненты системы управления промышленной безопасностью для ОПО I и II классов опасности или системы производственного контроля;

/1.2.0/ – система управления техносферной безопасностью в области промышленной безопасности федерального уровня сопринадлежности;

/2.2.0/ – система управления техносферной безопасностью в области промышленной безопасности межрегионального уровня сопринадлежности;

/3.2.0/ – система управления техносферной безопасностью в области промышленной безопасности регионального уровня сопринадлежности.

Декомпозиция и раскрытие функций компонентов дают возможность проводить анализ процессов и взаимодействий в системах.

Вывод

Результаты раскрытия термина «техносферная безопасность» и декомпозиции системы управления с последующим определением функций компонентов и анализом системных процессов и взаимодействий дают возможность для оптимизации управленческой деятельности в области техносферной безопасности.

Литература:

1. *Моисеев Н.Н.* Универсум. Информация. Общество. – М: Устойчивый мир, 2001. – 200 с.

2. *Чернов К.В.* Техногенная безопасность: научное издание. – Иваново: ГОУВПО «Ивановский государственный энергетический университет им. В.И. Ленина», 2007. – 328 с.

DOI: 10.25728/iccss.2022.37.85.046

Торгашев Р.Е.

Развитие рекреационного лесопользования как стратегический фактор устойчивого развития в экологическом туризме

Аннотация: В работе автором описан визуальный способ изучения лесов, приведена экономическая эффективность рекреационного лесопользования с учетом возрастающих антропогенных нагрузок, основные преимущества визуально-инструментальных наблюдений с борта РС МКС

за состоянием лесопользования рекреационного значения с учётом экологической и природно-антропогенной безопасности в туризме и привлекательности туристско-рекреационного потенциала регионов Российской Федерации.

Ключевые слова: эколого-экономичная оценка, рекреационное лесопользование, мониторинг, эксперимент «Дубрава», эксперимент «Экон», туризм

Рекреационный туризм связан с природными объектами. Российская Федерация обладает большим энергоресурсным и минерально-сырьевым потенциалом. Наше исследование посвящено вопросу рекреационного лесопользования, которое может способствовать устойчивому стратегическому развитию в экологическом туризме. Созданная в последние годы в Российской Федерации система лесопользования характеризуется рядом проблем, в том числе и эколого-экономического характера, которые препятствуют повышению эффективности лесохозяйственной деятельности и переходу к устойчивому развитию отрасли. Поэтому возникает необходимость совершенствования управления лесным хозяйством, экономических механизмов пользования лесом как природным богатством страны, уникальным экологическим ресурсом. Многофункциональное назначение лесов требует разработки такого механизма лесопользования, который включал бы эффективную систему организации лесохозяйственной деятельности по комплексу направлений, обеспечивая одновременно как доходность использования лесных благ, так и расширенное воспроизводство лесных ресурсов. Это особенно важно для малолесных регионов ввиду отсутствия лесопромышленного производства, являющегося экономической основой сохранения лесов, однако проблемы лесопользования на этих территориях до настоящего времени практически не рассматривались.

«Лесные ресурсы относятся к продуктам и полезностям леса, имеющим важное народнохозяйственное и социальное значение, особенно в условиях малолесистости промышленно развивающихся регионов, для России – это регионы средней (центральной) и более южной полосы» [1].

«Многофункциональная значимость лесных ресурсов, рост потребностей в древесной продукции, рекреационном лесопользовании требуют разработки новой эколого-экономической системы лесопользования, направленной на повышение доходности, эффективности использования и воспроизводства лесных ресурсов. Экологоориентированное лесопользование предполагает формирование и реализацию системы мероприятий, регулирующих воздействия на леса и направленных на организацию многоцелевого, непрерывного, неистощительного лесопользования, воспроизводство, улучшение породного состава и качества лесных ресурсов, их охрану и защиту, сохранение средообразующих и экологических функций лесных ресурсов, их биологического разнообразия» [2].

В последнее столетие в связи с бурным развитием промышленности и дальнейшей урбанизацией к началу 21 века территории все большее значение для общества приобретают рекреационные функции леса (далее – РФЛ). РФЛ – это комплекс положительного воздействия леса и лесной обстановки на состояние здоровья людей, зависящий, прежде всего, от лесорастительных условий и природных геоэколого-биологических особенностей лесного фитоценоза. Обострение интереса к эколого-экономической оценке рекреационных функций леса вызвано рядом серьезных причин. В условиях высокой плотности населения и чрезмерной урбанизации лес рассматривается как спасительный «социальный клапан», дающий человеку отдых от интенсивного труда, нервного напряжения, стрессов, смога, шума и загазованности современного города.

С эколого-экономической, психолого-социальной и медико-биологической точки зрения, сегодня практически ни у кого не вызывает сомнения необходимость целенаправленного формирования сети охраняемых природных территорий на освоенных человеком геопространствах. Однако опыт подобной работы в городских агломерациях. Вместе с тем быстрый рост урбанизации при ежегодном возрастании антропогенной нагрузки ставит неотложные задачи по сохранению элементов нетронутой или частично сохранённой природы в регионах и городских округах России. Это необходимо, прежде всего, для поддержания пригодной для жизни людей среды обитания и обеспечения полноценного

качественного отдыха и рекреации для восстановления трудоспособности в непосредственной близости от места работы и жительства.

Возникла необходимость сохранности и развитию рекреационного лесопользования средней (центральной) полосы, которая с одной стороны способствует повышению экологизации столичного мегаполиса, а с другой стороны расширить столичные функции для приобщения к культурно-туристской жизни. Но для этого необходимо отнестись с ответственным подходом: социально-ответственный туризм (далее – СОТ).

«СОТ способствует социальному и экономическому развитию местности, а также развивает уважительное отношение к культурно-историческому наследию, окружающей среде и традициям. Применим ко всем видам туризма и призывает всех туристов вносить свой посильный вклад в развитие территорий, помогать местным сообществам, проявлять активную гражданскую позицию» [3].

Среди прочих охраняемых территорий в городских округах важное место занимают сравнительно небольшие геобъекты, традиционно относящиеся к категории памятников природы. В свою очередь, ранее в процессе подготовки «Территориальной комплексной схемы охраны природы регионов России до 2035 года» встал вопрос о количестве, величине, паспортизации и выработке рекомендаций по их охране и лесопользованию принял участие ФГБУ «НИИ ЦПК имени Ю.А. Гагарина», включающий сотрудников и специалистов научного (5 управления), объединенных во временный научно-исследовательский коллектив, реализующих НИОКР и технические задания. Конкретной задачей научного коллектива было обследование территорий, связанных с элементами русел речных сетей и лесными комплексами и определение их взаимозависимости, с целью сохранения объектов природы и для дальнейшего их использования реакционного лесопользования для устойчивого развития туризма.

В последние годы встал целесообразным вопрос использовать систему целевого космического оборудования научных экспериментов, мощных камер системы наблюдения и мониторинга из космического пространства с РС МКС за отслеживанием рекреационного лесопользования с целью сохранения лесных ландшафтов в регионах России и экономии затрат на наземный

мониторинг за лесными и лесохозяйственными природными комплексами регионов России.

Исследование Земли и Космоса в рамках изучения вопроса состояния лесных ландшафтов и вопроса лесопользования в условиях повышенной антропогенной нагрузки проводится в 21 веке космический эксперимент (далее – КЭ) «Дубрава» и КЭ «Экон».

Получение экспериментальных данных спектральных измерений подстилающих поверхностей исследуемых районов с использованием научной аппаратуры ФСС (ВСС).

Результаты эксперимента: все результаты, полученные в сеансах эксперимента (фотоизображения, спектральные данные, результаты измерений, видеофайлы), записываются и хранятся на сменном возвращаемом жестком диске КЭ «Ураган».

К 2023 году КЭ «Дубрава» проходит завершение выполнения своего предназначения и приоритет отдается КЭ «Экон». В данном эксперименте, согласно ТЗ на КЭ, решаются следующие задачи: наблюдение экологической обстановки и накопление данных фото и видеосъемки по экологическому обследованию районов деятельности различных объектов на территории РФ и зарубежных государств.

Направление исследований имеет и важной целью опережающее развитие методов и средств рационального лесопользования, включая задачи охраны лесных запасов, обеспечение контроля воспроизводства леса и оптимальных региональных программ разработки ресурсов. Иными словами, на ДОС ставилась задача научиться различать и распознавать представленные спектрально-отражательные признаки, характеризующие основные параметры типового лесного массива и сопутствующие фоновые характеристики подлеска и почвенного покрова. В свою очередь, эти признаки имеют функциональные связи с породным составом в определенный сезон наблюдений, промысловым классом леса (бонитетом), состоянием здоровья леса, его физическим состоянием и сохранностью при неблагоприятных воздействиях вредных химических аэрозолей, ветра, пожаров и т.п.

Изучение лесов, их охрана и лесопользование имеют большое значение не только для народного хозяйства, но и оказывают непосредственное влияние на климат и атмосферу планеты. Лес

выполняет, кроме того, водоохранную, противоэрозионную и противооползневую роль.

Цветовые исследования в лесном хозяйстве имеют давние традиции. Еще в 1950-х гг. проводились цветовые наблюдения за изменением оптических характеристик ряда пород леса в течение сезона, а также изучение цветовых индикаторов различных заболеваний деревьев. Для этой цели использовался «лесной» атлас цвета А.С. Бондарцева.

Одна из первых задач изучения спектральных признаков леса была связана с изучением типовых цветовых контрастов лесных массивов, особенностей угловых зависимостей яркости отраженного излучения от углов визирования лесных массивов и относительных углов их освещения Солнцем.

Различными аэрокосмическими методами наблюдения возможно выявлять леса, пораженные жуками короедами-типографами, точильщиками, древоточцами, шашеля. Новые ВИН направлены и на обнаружение зон обильно населяющими клещами, представляющими опасность и для туристов.

В последнее время с борта орбитальной станций ведется наблюдение за вырубками лесов в различных частях планеты, а также за пожарами возникающих практически еженедельно.

Наличие вышеперечисленных возможностей и перспективных направлений позволит обеспечить потребление рекреационных ресурсов без ущерба для природных компонентов, то есть осуществить перевод рекреационного использования лесов и зелёных массивов на принципы современной концепции экосистемного природопользования и лесопользования, в частности, как стратегический фактор устойчивого развития в экологическом туризме [4]. Эта концепция заключается в уравновешивании существующих возможностей природы с запросами потребителей и прогнозными расчетами будущих её состояний, а также сохранении биологического разнообразия в природе региона [5].

Литература:

1. *Рысин Л.П., Рысин С.Л.* Природные и социальные аспекты рекреационного использования лесов // Лесохозяйственная информация. – 2008. – № 6-7. – С. 37-51.

2. *Сериков М.Т.* Оценка рекреационных ресурсов и рекреационного потенциала лесов при экосистемном методе лесоустройства // Лесотехнический журнал. – 2013. – № 4 (12). – С. 33-41.

3. *Горелова С.И.*, *Игнатьева Е.А.* Социально ответственный туризм как фактор устойчивого развития территорий / Актуальные проблемы развития экономики и управления в современных условиях: Материалы II Международной научно-практической конференции (Москва 28 октября 2019 года). – М.: Издательско-торговая корпорация «Дашков и К», 2019. – С. 386-389.

4. *Торгашев Р.Е.* Направления повышения эффективности использования природных ресурсов в структуре экономического потенциала государства / В книге: Современные проблемы управления и регулирования: поиск оптимальных решений. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2016. – С. 28-36.

5. *Торгашев Р.Е.* Физическая география материков и океанов: ресурсообеспечение и природопользование / Учебник для студентов вузов. – Ульяновск: Зебра, 2018. – 155 с.

VI. Методы моделирования и принятия решений при управлении безопасностью сложных систем

DOI: 10.25728/iccss.2022.80.65.047

Горелова Г.В., Мельник Э.В.

Композиция когнитивного, нейросетевого и агентного моделирования для интеллектуальных систем производственных объектов

Аннотация: В работе предложена идея композиции методов когнитивного, нейросетевого и агентного моделирования для использования в базе знаний интеллектуальных систем поддержки принятия решений производственных объектов. Дана общая постановка задачи, приведена схема взаимодействия нейросети и когнитивной карты, представлен один из разработанных алгоритмов, приведен иллюстрационный пример, поясняющий взаимосвязанную работу когнитивной и нейросетевой модели. Проведенные исследования находятся в пространстве работ «умного производства», интеллектуальных производственных систем, систем искусственного интеллекта в промышленности.

Ключевые слова: производственный объект, интеллектуальная система, имитационное когнитивное, нейросетевое, агентное моделирование, композиция

В настоящее время масштабы и содержание современного производства значительно отличаются по сравнению с началом промышленной революции. От современного производства требуется не только количество или качество, но и сохранение ресурсов, устойчивость и безопасность технологических процессов. Если традиционная производственная система работает на основе имеющихся знаний и опыта операторов, то настоящие условия

требуют от тех, кто вовлечен в производственный процесс, извлекать уроки из прошлых производственных данных и данных влияния окружающей среды, понимать и справляться с неопределенностями и сложностями в процессах, прогнозировать, находить лучшие альтернативы и стратегии устойчивого развития производства. На этом основаны интеллектуальные производственные системы (IMS), призванные объединять возможности людей, машин и процессов для достижения наилучшего возможного результата производства.

При разработке IMS необходимо учитывать множество факторов и многостадийность (многоэтапность) процессов, что представлено рисунке 1.

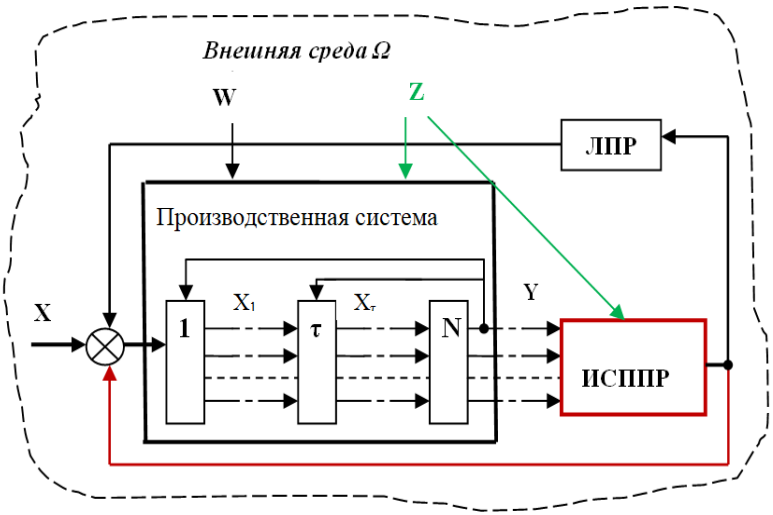


Рисунок 1 – Схема взаимодействия производственной системы, ИСППР и ЛПР

На рисунке 1:

X=$\{x_i\}$, i=1,2…k – множество входных, управляющих воздействий, автономно задаваемых СППР или ЛПР, или во взаимодействии с ЛПР; Z=$\{z_h\}$, h=1,2…H – множество контролируемых, но неуправляемых возмущающих воздействий внешней и внутренней среды; Y =$\{y_u\}$, u=1,2…U – множество оптимизируемых выходных показателей; τ=1,2,…N – стадии

производства, производственные участки, отдельные агрегаты и др. ИСППР – интеллектуальная система поддержки принятия решений.

На рисунке 2 представлена схема взаимодействия модулей когнитивного, нейросетевого, агентного моделирования для базы знаний ИСППР.

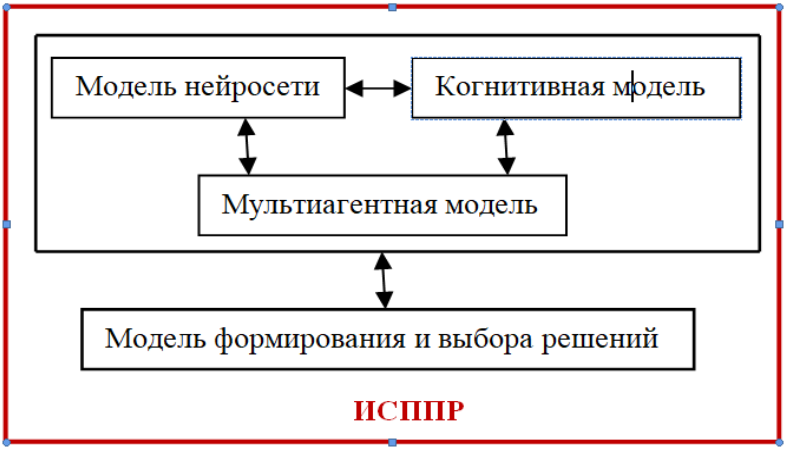


Рисунок 2 – Схема взаимодействия моделей

Разработка базовой когнитивной модели [1, 2, 6] производственной системы (структуры в виде графа) основывается на теоретических знаниях, знаниях экспертов, численных данных производства, агентном моделировании взаимодействия различных агентов (операторов, машин, и др.). Предложено использовать данные нейросетевого моделирования [3] для формирования той части базовой когнитивные модели, для которой возможно получение численных данных. При изменениях параметров внутренней и внешней среды когнитивная модель служит инструментом обучения нейросети. Эти процессы могут многократно повторяться (рисунок 3).

Рисунок 3 – Схема имитационного моделирования

На рисунке 4 изображена схема общего алгоритма имитационного моделирования.

Алгоритм №1. Когнитивное моделирование, корректировка базовой когнитивной модели $\boldsymbol{G_Б}$

1. Анализ тенденций развития ситуаций на когнитивной модели по результатам первой серии импульсного моделирования.

1.1. Введение возмущений в вершины, соответствующие сигналам изменения данных (X,Y,Z) [5].

1.2. Задание такта моделирования $t<15$, на котором происходит определение $\boldsymbol{y_j} \in [\boldsymbol{y_j}$ доп$]$

1.3. Определение вершин $\boldsymbol{Vi}$, i =1,2,…? в которых нарушается условие $\boldsymbol{y_j} \in [\boldsymbol{y_j}$ доп$]$ (рисунок 5) и в которых необходимо улучшать процесс. Ситуация отмечается как «плохая» (bad) - $\boldsymbol{Vi}_{\boldsymbol{bad}}$, i =1,2,…k.

2. Определение симплексов [1,4,5] σ^{ibad}_{p} вершин - $\boldsymbol{Vi}_{\boldsymbol{bad}}$, i =1,2,…k Из набора $\boldsymbol{G}$ = $\{G_{\text{прост}}\}$ простых структур когнитивных карт, последовательно берутся варианты $\boldsymbol{G}^{\,i}_{\text{прост}}$ = $\{V,E\}$, начиная с когнитивных карт с меньшим числом вершин, k ≤5,

$\boldsymbol{G}^{\,i}_{\text{прост}\,k} \in \boldsymbol{G}^{\,i}_{\text{прост}}$, k=1,2, …5.

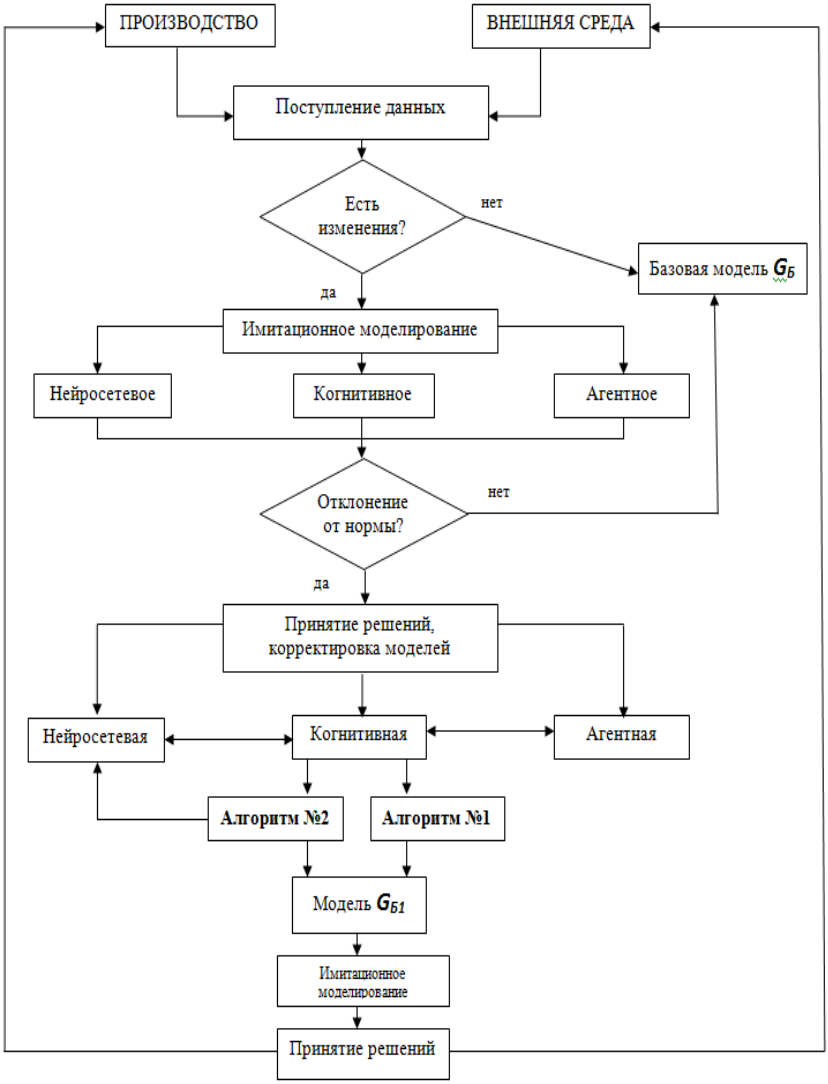


Рисунок 4 –Схема общего алгоритма

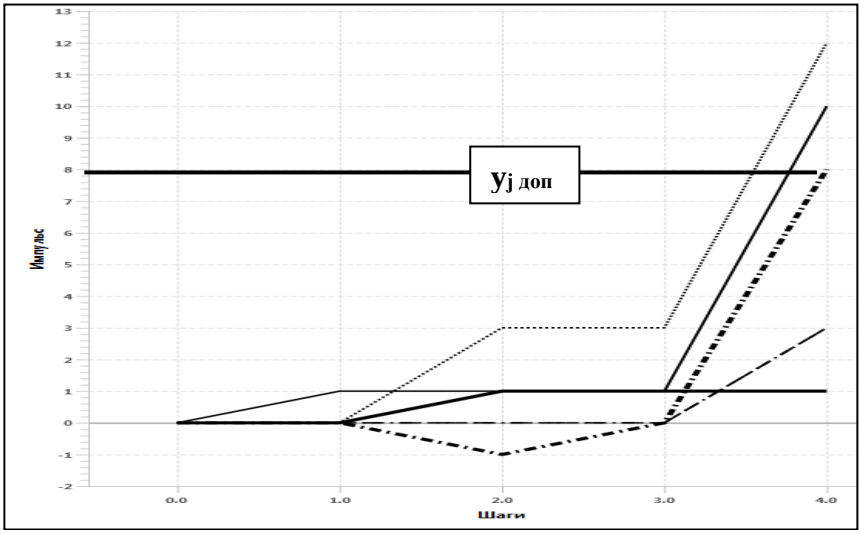


Рисунок 5 – Пример импульсных процессов на $G_Б$

3. Определяется композиция выбранной простой структуры.

3.1. $G^i_{\text{прост } k}$ с базовой когнитивной картой $G_Б$, $G_{Б1} = G_Б \circ G^i_{\text{прост } k}$

3.2. Если только одна вершина Vi_{bad} из $G^i_{\text{простk}}$ интерпретирована в терминах базовой когнитивной модели, то объединение графов происходит по одной этой вершине, остальные вершины являются «новыми».

Если несколько вершин Vi_{bad} из $G^i_{\text{прост } k}$ и отношения их (дуги) интерпретированы в терминах базовой когнитивной модели $G_Б$, то объединение графов происходит по вершинам и дугам, оставшиеся вершины и дуги являются «новыми».

4. Если появляется необходимость в «новых» вершинах и дугах, то переход к нейросетевому и агентному моделированию, разработка новой базовой когнитивной модели $G_{Б1}$.

5. Проверка структурных свойств и устойчивости новой когнитивной модели. Если свойства удовлетворяют требованиям к качеству когнитивной модели, то переход к п.7.

6. Проведение второй серии импульсного моделирования на $G_{Б1}$ в случае 4.1и 4.2; проверка условия $y_j \in [y_{j\,\text{доп}}]$.

7. Если выбранная $G^i_{\text{простk}}$ может быть полностью интерпретирована, как подграф $G_Б$, то улучшение процесса искать

путем изменения величины воздействий (начальных импульсов) или упреждением (внесение воздействий на предшествующих тактах моделирования) на проблемную вершину или на все вершины симплекса (простой структуры?)

Повтор действий для всех проблемных вершин $\boldsymbol{Vi}_{bad.}$

Алгоритм №2. Нейросетевое моделирование для корректировки базовой когнитивной модели $\boldsymbol{G_Б}$

1.Определение вершин $\boldsymbol{Vi}$, i =1,2,…? когнитивной карты, в которых нарушается условие $\boldsymbol{y_j} \in [\boldsymbol{y_j}_{\text{доп}}]$ и в которых необходимо улучшать процесс. Ситуация отмечается как «плохая» (bad) - $\boldsymbol{Vi}_{bad}$, i =1,2,…k.

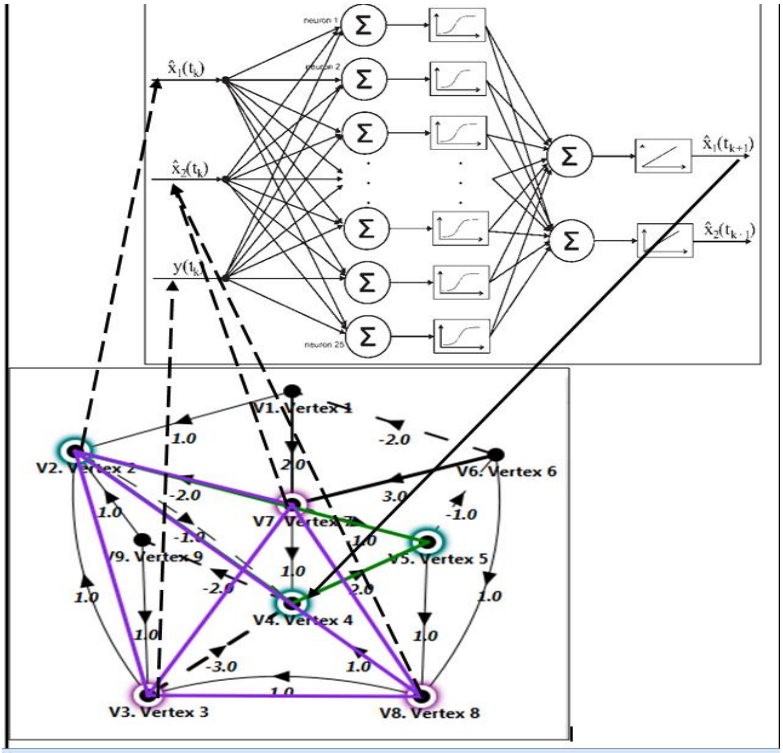


Рисунок 6 – Пример выделение симплекса вершины *V*4 и воздействие вершин симплекса на входы нейросети

2. Определение симплексов $\sigma^{ibad}{}_{p}$ вершин - $\boldsymbol{Vi}_{\boldsymbol{bad}}$, i =1,2,…k [4] (рисунок 6)

3. Выделение симплекса «плохой» выходной вершины $\boldsymbol{\sigma^{10bad}{}_{p=3}}$, определение вершин, образующих симплекс ($\boldsymbol{V_1, V_4, V_6, V_9}$).

4. Введение измененных данных (численных значений параметров X, Y,Z) в вершины графовой нейросети, соответствующие образующим симплекс вершинам, определение новых численных данных, характеризующих вершины $\boldsymbol{V_1, V_4, V_6, V_9}$ и отношения между ними для когнитивной карты $\boldsymbol{G_Б}$, получение новой когнитивной карты $\boldsymbol{G_{Б1}}$

Переход к алгоритму №1

Заключение

В статье приведены только основные моменты композиции трех методов имитационного моделирования сложных производственных систем и процессов, которые отлаживаются на примерах газонефтедобычи и переработки.

Литература:

1. *Galina V. Gorelova*. Cognitive Modeling of Complex Systems: State and Prospects / System Analysis in Engineering and Control. Lecture Notes in Networks and Systems. – Volume 442. – Springer Nature Switzerland AG 2022. – P. 212-224. DOI: 10.1007/978-3-030-98832-6_19

2. *Горелова Г.В., Мельник Э.В., Коровин Я.С.* Проектирование интеллектуальных распределенных информационно-управляющих систем / Труды Междуной научно-технической мультиконференции «Актуальные проблемы информационно-компьютерных технологий, мехатроники и робототехники. Многопроцессорные вычислительные и управляющие системы». – Таганрог: Изд. ТТИ ЮФУ, 2009. – Т. 2. – С. 28-31.

3. *Луценко Е.В.* Системная теория информации и нелокальные интерпретируемые нейронные сети прямого счета // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2003. – № 1. – С. 76-88. – URL: http://ej.kubagro.ru/2003/01/11/p11.asp (дата обращения 20.10.2022).

4. *Atkin R. H.* Combinatorial Connectivies in Social Systems. An Application of Simplicial ComplexStructures to the Study of Large Organisations. – Birkhäuser Basel, 1977. – 245 p.

5. Program for cognitive modeling and analysis of socio-economic systems at the regional level. Certificate of state registration of computer programs № 2018661506 dated 09/07/2018.

6. *Gorelova G., Melnik E., Safronenkova I*. The Problem Statement of Cognitive Modeling in Social Robotic Systems / Ronzhin A., Rigoll G., Meshcheryakov R. (eds). Interactive Collaborative Robotics. ICR 2021. Lecture Notes in Computer Science. – Vol 12998. – Springer, 2021. DOI:10.1007/978-3-030-87725-5_6

DOI: 10.25728/iccss.2022.17.54.048

Мельник Д.М.

Моделирование авиационных происшествий на основе анализа нечеткого множества данных и событий эксплуатантов воздушных судов

Аннотация: В данной работе предложен новый метод обеспечения безопасности полетов на основе риск-ориентированного подхода, что в отличие от современных методов оценки эффективности обеспечения безопасности полетов, основанных на усредненных оценках большого множества показателей, позволяет определять приемлемый уровень риска сложной производственной системы эксплуатантов воздушного транспорта. Рассматриваемый метод основан на применении теории нечетких множеств, что в условиях сложной интегрированной производственной системы дает достоверные оценки состояния безопасности полетов и позволяет смоделировать сценарий возможной катастрофы для своевременной разработки корректирующих мероприятий по предотвращению авиационных происшествий таких как катастрофа, авария, чрезвычайное происшествие.

Ключевые слова: моделирование, безопасность, уравнение, катастрофа, эксплуатант, риск

Введение

В соответствии с транспортной стратегией РФ [1] одной из форм эффективного и безопасного развития объектов транспортного комплекса государства является моделирование планирования развития транспортной и логистической инфраструктуры за счет прогнозирования на основе интеллектуального анализа большого объема данных и событий.

Следовательно, поиск эффективных методов управления сложных систем, которые используются при организации производства на предприятиях воздушного транспорта должен осуществляться одновременно с эффективным обеспечением безопасности полетов воздушных судов

1. Моделирование авиационного происшествия путем построения уравнения катастрофы

В настоящее время в гражданской авиации работа по обеспечению безопасности полетов проводится с использованием различных методик по усреднению сумм разного рода индикаторов [2]. Такой подход не явно отражает исход возможных негативных событий в сфере гражданской авиации и вносит дополнительную неопределенность при рассмотрении вопросов управления безопасностью полетов. Это объясняется тем, что у современного эксплуатанта воздушных судов существует множество показателей, связанных так или иначе с безопасностью полетов воздушных судов, мощность этих показателей велика $M_{\Sigma} \approx 100$. Поиск разного рода усредненных показателей не всегда может дать достаточную и объективную информацию по безопасности полетов воздушных судов.

В данной работе предлагается новый метод обеспечения безопасности полетов, основанный на моделировании авиационного происшествия за счет прогнозирования большого объема данных и событий. Такое моделирование предполагает анализ показателей на основе теории нечетких множеств двух групп показателей $M_{\Sigma} \Rightarrow (M_Q, M_S)$, а именно множества показателей, связанных с качеством производственных процессов M_Q и множества показателей, связанных с безопасностью полетов воздушных судов

M_S. Первые измеряются в виде выполняемости процессов, процедур, функций, вторые измеряются в виде отклонений, ошибок, нарушений, сбоев, отказов, при выполнении указанных процессов, процедур, функций. В основе моделирования авиационного происшествия легло построение уравнения катастрофы в котором выбраны данные, соответствующие неприемлемому уровню риска производственной системы эксплуатанта.

2. Составление уравнения катастрофы

Уравнение катастрофы конструируется по методу минимального сечения – в виде конъюнкций критических элементов β_i системы эксплуатанта, приводящих к отклонениям от установленных процедур либо к уязвимости системы под воздействием внешних факторов (1).

$$\hat{R} \to L_R \Rightarrow U_R = (\beta_1 \wedge \beta_2 \wedge \beta_3 \wedge .... \wedge \beta_i) = 1, \qquad (1)$$

где $\hat{R}$ – нечеткий уровень риска производственной системы, L_R – структура цепи сценария, U_R – условие катастрофы, β_i – название элемента производственной системы (порядковый номер).

Условие $U_R = 1$ означает возникновение катастрофы.

Критические элементы – это такие элементы производственной системы, цепочка из которых может привести к неблагоприятному событию. Критические элементы определяются путем вычисления комплексных показателей интегрированной системы управления качеством и безопасностью полетов, включающей в себя показатели двух видов: показатели качества I_Q и показатели безопасности полетов I_S, путем проведения типового корреляционного анализа между ними, после нормирования их в единое топологическое пространство. Единый комплексный показатель интегрированной системы получил название нечеткого многокритериального показателя эффективности $\tilde{K}_{Q,S}$, поскольку степень истинности значения этого показателя является нечетким и измеряется в

пределах: $0 \le \tilde{K}_{Q,S} \le 1$. Таким образом, критичность элемента будет зависеть от нечеткого многокритериального показателя эффективности (2).

$$\beta^* = f(\tilde{K}_{Q,S}) \quad (2)$$

Набор нечетких многокритериальных показателей эффективности интегрированной системы (НМПЭ) будет представлять собой уровень риска. Набор максимальных значений НМПЭ представляет собой общий риск производственной системы. Критичность нечеткого многокритериального показателя эффективности определяется в соответствии с матрицей оценки нечеткого уровня риска (рисунок 1). Данная матрица разрабатывается экспертным методом, применимо к условиям типового эксплуатанта воздушных судов.

Оценка нечеткого уровня риска ($\hat{R}$) возникновения опасных событий			Категория ущерба				
			A	B	C	D	E
Степень опасности		Множитель	1	0,8	0,6	0,4	0,2
	1-я	1	1	0,8	0,6	0,4	0,2
	2-я	0,8	0,8	0,64	0,48	0,32	0,16
	3-я	0,6	0,6	0,48	0,36	0,24	0,12
	4-я	0,4	0,4	0,32	0,24	0,16	0,08
	5-я	0,2	0,2	0,16	0,16	0,08	0,04

Рисунок 1 – Матрица оценки нечеткого уровня риска возникновения опасных событий

Критичность элементов определяется соотношением (3)

$$\tilde{K}^*_{Q,S} \ge 0.8. \quad (3)$$

Таким образом, осуществляется обеспечение безопасности полетов на основе риск-ориентированного подхода, при котором в интегрированной системе СУК и СУБП на эксплуатанта воздушных судов следует сначала искать множество НМПЭ ($\tilde{K}_{\Sigma}$), а затем среди них найти критические значения $\tilde{K}^{*}_{Q,S}$ (4)

$$\tilde{K}_{\Sigma} = \tilde{f}_{01}(\{I_Q\},\{I_S\}\big|\Sigma_0,\Phi_0,\Phi_1) \to \tilde{K}^{*}_{Q,S}, \qquad (4)$$

где $\{I_Q\},\{I_S\}$ – показатели качества и безопасности полетов, Φ_0 – множество факторов опасности, связанных с качеством, Φ_1 – множество факторов опасности, связанных с безопасностью полетов, Σ_0 – условия производственной системы.

3. Построение уравнение катастрофы Ту-154 Министерства обороны республики Польша 10 апреля 2010 года на аэродроме Смоленск «Северный»

10 апреля 2010 года, в 10:41 местного времени днем, в процессе выполнения захода на ВПП 26 аэродрома Смоленск «Северный» и снижения ниже установленной минимальной безопасной высоты (100 м) в метеоусловиях хуже установленного минимума аэродрома, воздушного судна и командира, потерпел катастрофу самолет Ту-154М б/н 101 государственной авиации Республики Польша (36-й специальный транспортный авиаполк ВВС Республики Польша), выполнявший нерегулярный международный рейс PLF 101 по перевозке пассажиров по маршруту Варшава (EPWA) – Смоленск «Северный» (XUBS).

Непосредственной причиной катастрофы явилось непринятие экипажем своевременного решения об уходе на запасной аэродром при неоднократно и своевременно полученной информации о фактических метеоусловиях на аэродроме посадки значительно хуже установленных для этого аэродрома минимумов.

В соответствие с окончательным отчетом об авиационном происшествии, подготовленном Межгосударственным авиационным комитетом [3], было составлено уравнение катастрофы (5)

$$\hat{R} \to L_R \Rightarrow U_R = (\beta_a \wedge \beta_b \wedge \beta_c \wedge \beta_d \wedge \beta_e \wedge \beta_f \wedge \beta_z \wedge \\ \wedge \beta_h \wedge \beta_i \wedge \beta_k \wedge \beta_l \wedge \beta_m \wedge \beta_n \wedge \beta_o \wedge \beta_p) = 1 \quad (5)$$

Описание критических элементов $\beta^*(I_Q) \subset M_Q$ и их признаков, представляющие собой подробное описание показателей безопасности полетов $I_S{}^* \subset M_S$ представлено в таблице 1.

При этом критические элементы 1-7 относятся к организационным факторам и формировались в производственной системе эксплуатанта задолго до возникновения условий катастрофы.

Таким образом, уравнение (5) можно было построить до возникновения условий катастрофы. Так, например за 1 ч. 30 минут до авиационного происшествия на аэродроме Смоленск «Северный» выполнил посадку Як-40 того же эксплуатанта (Министерство обороны республики Польша). Данная посадка была выполнена также с нарушением установленного минимума, что свидетельствует о наличии критического элемента по подготовке и выполнению полетов при минимуме погоды в производственной системе эксплуатанта.

Вывод

Рассмотренный в данной статье метод реализуется при проведении непрерывного мониторинга производственной системы, который проводится с использованием таких мероприятий как аудиты, инспекторские проверки, квалификационные проверки, анализ показателей, анализ обязательных и добровольных сообщений, анализ полетной информации, материалы расследования авиационных событий, с проведением оценки эффективности разработанных мероприятий по снижению общего риска производственной системы экспуатанта, путем проведения повторного аудита. Такой прием позволяет решить проблемы неопределенности в сложной интегрированной системе эксплуатанта и произвести оценку эффективности обеспечения безопасности полетов на основе теории нечетких множеств (Fuzzy Sets).

Таблица 1 – Критические элементы катастрофы Ту-154 10 апреля 2010 года

β^*	Название критического элемента $\beta^*(I_Q) \subset M_Q$	Признаки критических элементов в производственной системе эксплуатанта воздушных судов $I_S{}^* \subset M_S$
1	2	3
β_a	Переучивание ВС Ту-154	Штурман, второй пилот во время переучивания выполняли полеты на другом типе ВС
β_b	Тренажная подготовка	Тренажные центры по подготовке на ВС Ту-154 не использовались (тренажная подготовка не проводилась)
β_c	Подготовка к посадкам при минимуме погоды	Значительный перерыв в полетах в сложных метеоусловиях (соответствующих допуску 60х800) у КВС. В летной книжке КВС имеется необоснованная отметка о подтверждении метеоминимума при заходе на посадку в аэропорту Брюссель 11.02.2010. Проверка метеоусловий на аэродроме Брюссель 11.02.2010 показала, что фактическая погода была: облачность – 900 м, видимость более 10 км
β_d	Технология работы членов летных экипажей	У эксплуатанта отсутствовала Инструкция по взаимодействию и технология работы членов экипажа самолета Ту-154М для 4-х членного состава (далее Технология работы). По объяснениям польской стороны, полеты выполняются непосредственно с использованием РЛЭ самолета, которая была написана для 3-х членного экипажа
β_e	Формирование экипажа	К КВС имеющий малый опыт полетов в качестве КВС на Ту-154 (500 часов) назначили экипаж имеющий еще меньший опыт
β_f	Предварительная подготовка к полетам	Отсутствовал контроль за предварительной подготовкой к полетам, со стороны руководящего состава

Продолжение таблицы 1

1	2	3
β_z	Предполетная подготовка	- перед вылетом отсутствовала метеорологическая информация аэродрома Смоленск «Северный»; - использовалась не актуализированная аэронавигационная информация аэродрома Смоленск «Северный»; - был выбран запасной аэродром Витебск, который не работал 10 апреля 2010 и по нему был просроченный метеопрогноз; - превышение посадочной массы на 4.6 т.
β_h	Предпосадочная посадочная подготовка (предпосадочный брифинг)	Согласно РЛЭ Ту-154 п. 4.4.1. (11) «Действия экипажа в крейсерском полете»-экипаж по команде КВС за 10-15 мин до начала снижения приступает к предпосадочной подготовке. Предпосадочная подготовка в течение последних 7 минут 30 секунд крейсерского полета на записи звукового магнитофона не прослушивается. Из ответов на пункты контрольной карты «Перед снижением» (фактически выполнялась во время снижения) можно сделать вывод, что экипаж схему захода на посадку не рассматривал (Шт: «Процедура», КВС: «Еще не известна»).
β_i	Выполнение карт контрольных проверок	Не была выполнена карта контрольной проверки перед третьим разворотом
β_k	Навигационные процедуры	Запоздалый перевод самолета на снижение по глиссаде (с ошибкой примерно 1.5 км)
β_l	Стабилизированный заход на посадку	На предпосадочной прямой полет проходил на повышенных скоростях около 300 км/ч (при расчетной – 265 км/ч). После пролёта ДПРМ экипаж увеличил вертикальную скорость снижения до 8 м/с. Такая вертикальная скорость (8 м/с) сохранялась вплоть до момента начала действий по уходу от препятствий (Нрв=30м)
β_m	Давление на экипаж	Ожидание наказания в случае ухода на запасной аэродром формировало доминанту «сесть во что бы то ни стало» и толкало на неоправданный риск. Присутствие в кабине экипажа посторонних лиц

Продолжение таблицы 1

1	2	3
β_n	Посадка при минимуме погоды	КВС, наиболее вероятно, пошел на риск - снижаться ниже высоты принятия решения, в надежде, все – таки, установить визуальный контакт с ВПП и произвести посадку
β_o	Применение процедур РЛЭ Ту-154	Снижение на посадочной прямой выполнялось с включенным автопилотом в продольном и боковом каналах, а также с включенным автоматом тяги. Управление автопилотом в продольном канале осуществлялось от рукоятки «СПУСК-ПОДЪЁМ». Данный тип захода РЛЭ самолета не предусмотрен
β_p	Управление ресурсами членов экипажа (CRM)	Со стороны КВС не были распределены обязанности между членами экипажа и порядок ухода на второй круг. Не был определен порядок использования автопилота и минимальная высота отключения АП

Литература:

1. Распоряжение Правительства РФ от 27.11.2021 № 3363-р «О Транспортной стратегии Российской Федерации до 2030 года с прогнозом на период до 2035 года».

2. Методические рекомендации территориальным органам Росавиации по проверкам СУБП поставщиков услуг. – Федеральное агентство воздушного транспорта, 2019. – URL: https://favt.gov.ru/dejatelnost-bezopasnost-poletov-subp-proverka-postavshikov-uslug-kvp/ (дата обращения 10.10.2022).

3. Межгосударственный авиационный комитет. Окончательный отчет по расследованию авиационного происшествия самолета Ту-154 Министерства обороны республики Польша 10 апреля 2010 года на аэродроме Смоленск «Северный», 2011. – URL: https://mak-iac.org/upload/iblock/abd/finalreport_rus.pdf (дата обращения 10.10.2022).

4. Руководство по управлению безопасностью полетов (DOC 9859 ICAO). – 4-е изд. – ИКАО, 2018. – URL: https://standart.aero/ru/icao/book/документ-9859-руководство-по-управлению-безопасностью-полетов-рубп-ру-конс (дата доступа 20.10.2022).

5. *Kuklev E. et al.* Flight Safety & Aviation Risk. – Singapore:

Springer, 2019.

6. *Мельник Д.М.* Выявление критических элементов авиационного предприятия на основе анализа результатов расследования авиационных событий // Транспортная стратегия. – XXI век. – 2021. – № 47. – С. 28-31.

7. *Рухлинский В.М., Куклев Е.А., Мельник Д.М.* «Применение теории нечетких множеств при обеспечении безопасности полетов поставщиков обслуживания гражданской авиации в условиях неопределенности состояний авиационной системы». Информационный документ Межгосударственного авиационного комитета на 41 ассамблею Международной гражданской авиации (ИКАО) A41-WP/72, 2022. – URL: https://www.icao.int/Meetings/a41/Documents/WP/wp_072_ru.pdf (дата обращения 10.10.2022).

DOI: 10.25728/iccss.2022.38.11.049

Plotnikov N.I.

Risk prevention strategies of aircraft with wildlife strike

Abstract. The paper presents a set of problems of the complexity of observing strikes of aircraft with wildlife. The study was carried out on the choice of a group of birds with the most significant in terms of the number of species and strike damage. The development of a metric for observing the fuzziness of strike events is aimed at resolving the problem in interpreting data, incomplete, inaccurate information in strike reports. The set of problems consists in the extreme complexity of observing, fixing and registering the facts of strike, identifying groups and types of wildlife, which is required to develop strategies for the ecological balance of aviation and wildlife. Risk prevention strategies of aircraft with wildlife strike are developed.

Keywords: aircraft, wildlife, strike, flight safety, avian safety, risk, strategies

Introduction. This paper analyzes modern studies of strike of aircraft with objects of wild nature (Wildlife) or air-terrestrial animals: birds, bats, terrestrial mammals, reptiles (Bird/Other Wildlife Strike). The study was

carried out on the choice of a group of birds with the most significant in terms of the number of species and strike damage. The task of strike risk calculations establishes the possibility of reducing uncertainty, fuzzy event structure and creating metrics and calculations for risk management. In the subject of interaction of aviation with wildlife under study, all aircraft are considered: airplanes, helicopters, drones. The flight time starts from taxiing, takeoff run to the end of the landing run. Therefore, strike occur with air-terrestrial animals. The use of low-noise aircraft in commercial aviation is expected to reduce the ability of the wildlife to recognize a strike hazard. Aircraft at greatest risk are light, low-altitude, high-speed, single-engine aircraft. The damage from strikes differs greatly from the speed of the aircraft and the mass of the body of the wildlife [1, 2]. Airport operators use many methods to reduce the likelihood and severity of strike risks, such as fencing off take-off and landing areas, local observations for compiling eBird databases, movement monitoring, and species identification. However, these measures are not very effective in relation to the observation of migratory movements of the wildlife. Information about the location of the RBP based on expert observations and meteorological observation radars provides information on the resident and transit types of the wildlife. Radar observations provide information on the types of schooling, body weights of the wildlife, eBird data are based on the registration and reporting of previous strikes [3].

Content of the Problem. The International Civil Aviation Organization (ICAO) establishes aircraft flight safety requirements for the prevention of strike risks in the territories and near airports by fencing territories, displacement measures, scaring away and liquidations, that is, to the detriment of the safety of the airborne flight. Statistics based on the registration, recording and analysis of strikes are considered incomplete, since a significant part of the events is not recorded [4]. Real number of strikes are several times more registered. Aircraft crews and ATC services do not have volumetric information and at low altitudes. The set of problems consists in the extreme complexity of observing, fixing and registering the facts of strike, identifying groups and types of wildlife, which is required to develop strategies for the ecological balance of aviation and wildlife.

Strike Risk Prevention Strategies. At present, the aviation world community has established the following strategies and measures to prevent the risks of aircraft strike with wildlife.

Strategy 1. Increasing the strength of the aircraft. Design and construction of aircraft elements with protection against damage and destruction. Designing different characteristics of windshields and engines inlet nozzles using high-strength materials and coatings that eliminate the worst-case scenarios of accidents. Certification of the airworthiness of the aircraft and structural elements with respect to strike with the wildlife is carried out by national and international aviation administration [5, 6]. The European Aviation Safety Agency (EASA) establishes strength certification for fuselage structures, windshields and engines of wide-body commercial aircraft [7] against impact kinetic energy requirements, which is defined by (Eq. 1):

$$E_{kin} = 1/2 \cdot m \cdot (v)^2, \quad (1)$$

where (m) is mass, (v) is speed.

The kinetic energy certification criteria are set by EASA for large aircraft in the following values (table 1).

Table 1 – Certification criteria

Components	Kinetic energy criteria
Windshield	$E_{kin} = 1/2 \cdot 1{,}8\ kg \cdot \left(v_{ref}\right)^2$, v_{ref} - cruising speed at the corresponding route altitude
Hull	$E_{kin} = 1/2 \cdot 1{,}8\ kg \cdot \left(0{,}85\ v_{ref} 2438\ \text{m}\right)^2$, at the altitude 2438 м
Engine	$E_{kin} = 1/2 \cdot m_{bird} \cdot (102.9\ \text{m/s})^2$, m_{bird} – bird body mass

Strategy 2. Aircraft space freedom. Otherwise, remove the wildlife from the aircraft space. Design and organization of the aircraft movement space, minimizing strike with wildlife. This strategy is being implemented in the following areas. (1) Organization of space. Airport fencing within five miles or greater distances of habitats and land use, wetlands, dredger containment sites, municipal solid waste landfills, and nature reserves that attract wildlife. (2) Regulatory actions. Development of regulatory documentation for ornithological flight safety. Formation of a database of

strikes, statistical analysis, participation in investigations. Evaluation of the bird hazard of airfields, development and evaluation of the effectiveness of specialized means of protection against wildlife. (3) Ornithology. Organization of airport ornithological services, technical and biological means of scaring away birds in their habitats, formed by instincts over millions of years of evolution. The most productive is the content of the states of the "bird police" of hunting birds - saker falcons, golden eagles, pygmy eagles to "patrol" the sky over the airport. Creation of uncomfortable living conditions for wildlife. Extermination of insects, worms, cleaning of natural bird feeding areas near takeoff and landing areas, acoustic and bioacoustic installations, light signals, pyrotechnics, radio-controlled models of predators for scaring away, scarecrows, traps for trapping birds of prey, chemical means.

Strategy 3. Wildlife space freedom. Otherwise, remove the aircraft from the wildlife space. Preservation of the wildlife habitat outside the aircraft movement space. Visual and radar observations, notification of airports about dangerous ornithological conditions. Designing airfields and take-off and landing areas, taking into account the historical areas of bird settlement and accounting for their migration. Development of a strike risk avoidance model based on Geographic Information System (GIS), integrating data on geographical regions of habitat, migration and feeding of various bird species, the U.S. Bird Avoidance Model (BAM). The analysis of numerous studies reliably establishes that the absolute number of aircraft strikes with wildlife occurs near the earth's surface during departure and arrival up to a height of 1000 meters. The implementation of strike avoidance is based on a comparison of the trajectory of the aircraft and the wildlife, similar to the Airborne Collision Avoidance System (ACAS | TCAS), in which the space is structured into danger segments: caution, warning, strike. Unlike ACAS |TCAS, which displays the exchange of distance information between aircraft, the strike avoidance system displays information from radars of the distance between the aircraft and the wildlife to make decisions about maneuver, departure or approach delay and landing. Departure and arrival delays are related to runway and airport capacity calculations. Radars do not provide altitude information to calculate Closest Point of Approach (CPA) for comparison with Predicted Bird Position (PBP) and Actual Bird Position (ABP). The distance between PBPs when the aircraft reaches the CPA is called the CPA distance (dCPA).

Conclusion. The events of aircraft strikes with wildlife have a high frequency, extremely complex structure, and fuzzy content. These circumstances determine the complexity and costs of their observation and development of risk prevention measures. As the intensity of flights around the world increases, the total number of strikes will increase. The descriptions and structure of the subject area in this paper can be used as an approach for the development of manuals and manuals on ornithological flight safety management. The content of the work is based on the choice of a group of birds, which is recommended to be used when choosing other groups.

References:

1. *van Gasteren H., Krijgsveld K.L., Klauke N., Leshem Y., Metz I.C., Skakuj M., Sorbi S., Schekler I., & Shamoun-Baranes J.* Aeroecology meets aviation safety: Early warning systems in Europe and the Middle East prevent Strikes between birds and aircraft. – Ecography. – 2019. – Vol. 42. – P 899-911.

2. *Dolbeer R.A., & Begier M.J.* (2019) Wildlife strikes to Civil Aircraft in the United States 1990-2017. Federal Aviation Administration National Wildlife Strike Database Serial Report Number 24. 2019.

3. *Nilsson C., La Sorte F. A., Dokter A., Horton K., Van Doren B.M., Kolodzinski J.J., Shamoun-Baranes J., & Farnsworth A.* (2021). Bird strikes at commercial airports explained by citizen science and weather radar data. Journal of Applied Ecology, 2021, 00. P. 1-11.

4. *Plotnikov N.I.* Soft Computing Method in Events Risks Matrices / Proceedings of the 6th Brazilian Technology Symposium (BTSym'20). Smart Innovation, Systems and Technologies. – 2021. – Vol. 233. – P. 578-588.

5. *Dolbeer R.A.* (2011). Increasing trend of damaging bird strikes with aircraft outside the airport boundary: Implications for mitigation measures // Human-Wildlife Interactions. – 2011. – Vol. 5. – P. 235-248.

6. Federal Aviation Administration. (2020) 14 CFR 91.7 – Civil Aircraft Airworthiness; Federal Aviation Administration: Washington, DC, USA, 2020.

7. EASA. Bird Population Trends and Their Impact on Aviation Safety 1999-2008; (2009) EASA Safety Report; European Aviation Safety Agency: Cologne, Germany, 2009. Sky Library (eds).

DOI: 10.25728/iccss.2022.14.92.050

Команич Н.В., Чернов И.В.

Сценарное моделирование инновационного развития Арктической зоны РФ в условиях влияния внешних угроз

Аннотация: Работа посвящена сценарным методам оценки влияния существующих и прогнозируемых проблем и вызов развитию Арктической зоны РФ, поиску возможностей и путей управленческих воздействий в различных сферах регионального развития, а также сценарному прогнозированию последствий принимаемых решений. Актуальность работы заключается в стратегической значимости принимаемых управленческих решений, направленных на развитие Арктической зоны РФ, а также в многоаспектности проблем, влияющих на создание эффективного нефтегазового комплекса в условиях усиления внешних угроз. Результатом работы стала построенная сценарная имитационная модель и полученные сценарии её поведения при различных условиях.

Ключевые слова: сценарное моделирование, инновационное развитие, Арктическая зона, нефтегазовый комплекс, внешние угрозы, безопасность, развитие инфраструктуры

На сегодняшний день Арктика становится ключевым регионом в области экономической и национальной безопасности Российской Федерации. Направления по добыче ресурсов, развитию энергетики, социальной, транспортной, экономической и инновационной инфраструктуры Арктической зоны являются на данный момент приоритетными. Интерес ведущих стран к участию и развитию в данном регионе увеличивается по мере наращивания конкуренции на мировой арене, развития передовых технологий, открывающих доступ к разработке новых месторождений углеводородных ресурсов, созданию экологически чистых и безотходных предприятий по переработке сырья в высококачественную продукцию [1]. Также большое значение в развитии региона играет развитие транспортного и судоходного сообщения. В регионе

сосредоточено около 80 % всей арктической нефти и более 90 % процентов газа [2]. Согласно проведенным исследованиям, в Арктике находится значительная часть ещё не разведанных мировых запасов нефти.

Освоение и рациональное использование нефтегазовых ресурсов и пространств Арктической зоны Российской Федерации является одним их жизненно важных интересов нашей страны. В связи с усугублением внешней обстановки, наращиванием угроз и отставанием в научно-техническом, инновационном обеспечении и развитии региона возрастает актуальность выработки и принятия обоснованных управленческих решений, направленных на решение этих проблем [3]. На данном этапе существует ряд вызовов для России:

- усиление мировой конкуренции с ведущими добывающими и экспортирующими углеводородные ресурсы странами, применение экономических санкций против нашей страны;
- истощение потенциала российской экспортно-сырьевой и добывающей модели экономического развития России;
- усиление роли инноваций, отставание в развитие новых технологий;
- недостаточное развитие арктической инфраструктуры;
- отсутствие высококвалифицированных кадров;
- малонаселенность территории Арктической зоны России;
- сложность климатических условий Арктической зоны России;
- обеспечение экологической безопасности Арктической зоны России.

Для решения проблем глобальных вызовов освоения Арктической зоны Россия необходима реализация комплекса преобразований, направленных на:

- формирование национальной инновационной системы, научно-технологического комплекса, проведение научно-практических и полевых исследований, геологоразведовательных работ;
- развитие транспортной, энергетической и хозяйственной инфраструктуры Арктической зоны нашей страны;
- внедрение инноваций при создании комплекса по добыче и

транспортировке углеводородных и других ресурсов Арктической зоны России;

- создание специальных образовательных программ для подготовки высококвалифицированных кадров;
- стимулирование хозяйственно-экономической деятельности путём привлечения капитала и нового бизнеса в регионе для снижения оттока населения и создания эффективного механизма регулирования рынка труда, повышения интереса для освоения территории Арктической зоны России;
- создание метеорологического комплекса, механизма для оценки и прогнозирования чрезвычайных событий в регионе;
- создание безотходного и экологически безопасного нефтегазового и энергетического комплексов.

С целью обеспечения сценарно-экспертной поддержки принятия управленческих решений в рамках перечисленного комплекса мер разработана и исследована сценарная имитационная модель развития Арктической зоны РФ в условиях влияния внешних вызовов и угроз (рисунок 1). Сценарный подход является эффективным подходом к решению сложных задач в условиях ряда неопределённостей, направленным на поиск возможностей управления и прогнозирование последствий от принимаемых управленческих воздействий на основе генерирования различных сценариев развития обстановки при наличии ограничений на виды воздействий [4]. В структуре модели учтены взаимосвязи факторов, положительно и негативно влияющих на развитие рассматриваемого региона. Кроме того, учтены направления инновационного развития нефтегазового комплекса, транспортной и энергетической инфраструктур. Ряд факторов отражают проблемы арктической зоны РФ, такие как жёсткие климатические условия, низкая плотность населения и низкая квалификация кадров.

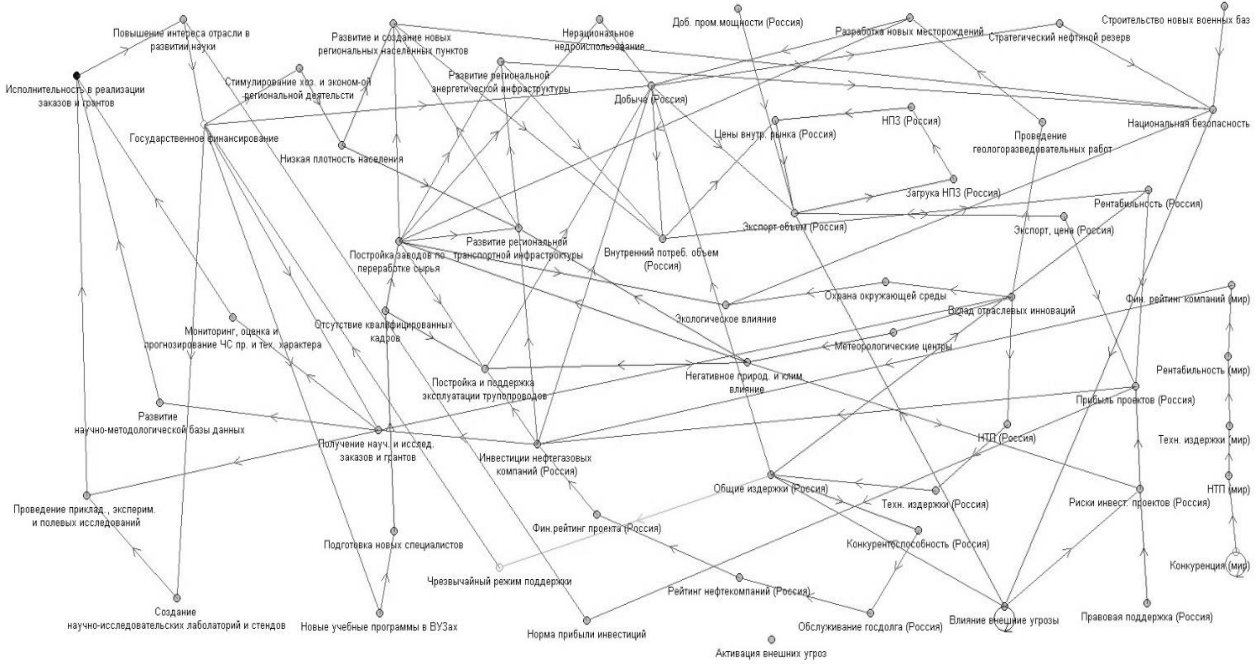


Рисунок 1 – Сценарная имитационная модель развития Арктической зоны РФ в условиях влияния внешних вызовов и угроз

При моделировании получен ряд сценариев при возникновении различных угроз и направлений управленческих воздействий. В ходе сценарного анализа было выявлено, что гибкое кооперативное управление государственным и отраслевым финансированием развития Арктической зоны РФ является эффективным аппаратом для отражения возникающих угроз. Выявлено, что в условиях активного противодействия невозможно обеспечить развитие этого региона исключительно с использованием экономических механизмов, которые очень чувствительны к нарастающим внешним угрозам и эффективны в устоявшихся условиях.

Влияние внешних угроз и проблем развития региона на отдельных этапах управления может привести к росту общих издержек, снижению вклада отраслевых инвестиций, недофинансированию инноваций и снижению рентабельности проводимых проектов в регионе. С учетом этих соображений создан механизм активации и деактивации государственного финансирования и прямого управления при усугублении влияния внешних угроз. Критерием для смены принципа управления служит поведение двух факторов: норма прибыли инвестиций и чрезвычайный режим поддержки.

Сценарное моделирование показало, что наиболее эффективным является раннее прогнозирование кризисных явлений и перехват управления и финансирования государственными структурами при снижении влияния экономических механизмов. Экономически обоснованное управление работает в стабильной обстановке при отсутствии угроз. Смещение управляющего центра и финансирование в сторону государственных структур эффективен в критических ситуациях, когда экономические критерии противоречат интересам развития региона.

В случае позднего включения государственного регулирования и финансирования лавинообразно накапливаются издержки освоения региона и финансовых вливаний требуется гораздо большего объема. Таким образом, сценарно-прогнозный подход является необходимым компонентом обеспечения эффективного управления региональным развитием и национальной безопасности страны.

Литература:

1. *Чернов С.Н.* Нефть и газ Арктики. Правовые, экологические и социальные проблемы освоения странами Арктического совета богатств Севера. – Петрозаводск: КарНЦ РАН, 2020. – 209 с.

2. *Мамахатов Т.М.* Роль Арктики в обеспечении экономической и национальной безопасности России в современных геополитических и климатических условиях // Электронное сетевое издание «Международный правовой курьер». – 2021. – №. 7. – С. 54-60.

3. Указ Президента РФ от 26 октября 2020 г. № 645 «О Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2035 года». – URL: https://base.garant.ru/74810556/ (дата обращения 13.09.2022).

4. *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.

DOI: 10.25728/iccss.2022.94.81.051

Рыженко А.А.

Организация системы подготовки сотрудников организаций в сфере противоборства механизмам социальной инженерии

Аннотация: Рассматриваются вопросы моделирования центра обучения и подготовки сотрудников организаций в сфере противоборства современным механизмам социальной инженерии.

Ключевые слова: информационная безопасность, социальная инженерия, кибербезопасность, моделирование

Вопросами противоборства методам социальной инженерии занимаются ведущие научные школы мирового уровня достаточно продолжительное время. Еще в начале двухтысячных годов ряд работ отмечал, что в ближайшем будущем, в связи с усилением контура безопасности в глобальной сети Интернет в целом, атаки злоумышленников будут все чаще перенаправляться на социально-психологические факторы социальной инженерии. Например, в

работе [1] еще в 2005 году задается достаточно молодое на тот момент времени направление исследований, которое впоследствии действительно показало свою эффективность на практике как в судебной системе, так и для подготовки технических специалистов.

Пропуская достаточно продолжительный период также стоит отметить, что количество исследований по каждому определяемому временем направлению атак на социальную среду приобретали целые научные направления, которые впоследствии переносились в учебные материалы для следователей в цифровой среде. Например, в работе [2], датированной 2016 годом, поднимаются и описываются вопросы, связанные с уже популярными методами фишинга с использованием мобильных устройств. За последние 2 года данное направление считается одним из ведущих в сфере противоборства методам социальной инженерии.

Параллельно с мировыми школами в РФ развивались свои направления исследований, тесно связанные с особенностями развития взаимодействия технической и алгоритмической составляющей атак злоумышленников с совершенствующимися с каждым годом методами противоборства. Тем не менее, сразу хочется отметить, что тенденция увеличения в процентном соотношении комплексных атак с целью кражи информации с каждым годом все больше склоняется к популярным методам социальной инженерии. Как следствие в основные фондовые программы государственного уровня по цифровой безопасности самым большим разделом является именно противоборство психологическим атакам злоумышленников. В результате с каждым годом появляется все больше информационных материалов и курсов повышения квалификации для различных слоев населения, помогающие социальной среде больше узнать о возможных методах хищения информации.

С другой стороны, ежедневно обновляемые доски объявлений в сети DarkNet, где можно купить практически любую информацию, до сих пор говорят о низкой подготовленности сотрудников многих организаций к действиям злоумышленников. Запредельное доверие мобильным устройствам, социальным сетям, мессенджерам и прочим программно-аппаратным устройствам существенно усложняет специалистам в сфере информационной безопасности профессиональную деятельность: требования не выполняются,

инструкции, лицензии и соглашения не читаются. Например, достаточно частый опрос разных групп в социальных сетях «Читали ли они пользовательское соглашение?», более 90 % опрошенных честно отрицательно отвечали, а около 40 % даже не знали, что такой документ существует.

В качестве нового инструмента возможно воздействие на социальную среду на официальном информационном ресурсе Роскомнадзора предложена модель персональной безопасности, где предлагается каждому подумать о собственном поведении в цифровой среде и разработать индивидуальный контур безопасности вполне официально. Но достаточно неэффективная рекламная кампания данного документа уже продолжительное время не показывает результаты предложенной модели.

В данных исследованиях было решено рассматривать действия злоумышленников не как независимая система воздействия на социальную среду, а как деструктивный постоянно изменяющийся элемент жизненного цикла произвольной существующей системы. В основу модели заложена концепция вируса полиморфика, предложенная еще в 2000 году одним из основателей глобальной сети Интернет. Первые результаты моделирования были представлены ранее в работах [3, 4].

Как было уже упомянуто ранее, полученные результаты переносились в учебные пособия для специалистов судебной системы цифровой среды. В результате, было предложено разработать концепцию единого центра подготовки сотрудников организаций к действиям злоумышленников методами социальной инженерии. Т.е. особенностью данного центра является синтез двух существующих направлений исследований: с одной стороны, – создание унифицированных методик противоборства в информационной среде, с другой, – формирование индивидуальных траекторий обучения, подготовки и самодиагностики для каждого профиля обучаемых. Имеющийся на тот момент опыт организации потоков информации для обучаемых [5] позволил сформировать единую модель формирования поля решений или поля индивидуальных траекторий, включающую бикубическую матрицу «атака – блокировка», иерархическое дерево сквозного проекта комплексной защиты и пирамидальное представление области знаний с фасетными уровневыми основаниями. Сразу стоит

отметить, что аналогичные исследования проводятся и на мировом уровне. Например, в работе [6] представлена аналогичная модель, позволяющая сформировать новый метод, который использует свойства обнаружения сообщества и концепции анализа социальных сетей. В статье показано, что самая высокая производительность достигается, когда функции уровня сообщества и функции социальных сетей используются в сочетании с функциями уровня класса вредоносного ПО, т.е. также строится бикубическая матрица, где связи между ячейками формируются деревом событий.

Помимо того, что в персональном клиенте для каждого обучаемого сотрудника подбираются материалы, повышающие квалификацию, система также работает в активном режиме как консультант к возможным действиям в реальном времени. Пример работы всей системы представлен далее.

В основе модели используется сетевая структура семантической сети с единым центром. Ядром системы выступает база правил, где интерпретатор строит правую часть продукционных правил на основе кратности процессов. Данный принцип достаточно подробно освещался в работах, посвященных операциям над процессами мультимножеств. Особенностью является неоднозначность решения, где после знака равно не одно конкретное решение, а множество решений. Выбор конкретного значения предоставляется агенту посреднику сети баз ассоциаций по адаптивному критерию. Например, звонок клиенту банка с известного номера технической поддержки. Агент поддержки обучаемого в виде мобильного приложения знает контрольные номера. Открывается сессия «дежурства». Так как любая речь мгновенно может быть переведена в текст, то агент сравнивает слова звонящего с внешней базой токсичного контента. Как только попадаются ключевые фразы, агент предлагает абоненту произвести проверку и сделать встречный вызов на тот же номер поддержки. Современные устройства позволяют удержать звонок и вызвать другого абонента. В то же время агент делает обращение на сервер на занятость портов обращения. В результате, даже если абонент откажется делать вызов поддержки, агент покажет достоверную информацию по открытой сессии, т.е. откуда сейчас происходит звонок. К сожалению, не удалось избежать парадоксов и коллизий. В случае одноранговых

процессов, текущая версия агента предлагает пользователю самостоятельно сделать выбор между возможными альтернативами.

Первые результаты работы полученной модели были представлены в работе [7], где изложен конкретный пример учета множественных параметров одного из направлений социальной инженерии при подготовке технических специалистов конкретной сферы профессиональной деятельности. По результатам конференции предложено более детально охватить и другие направления финансовых организаций, но в первую очередь – расширить перечень функционала для банковской сферы.

Литература:

1. *Bénichou D., Lefran S.* Introduction to Network Self-defense: technical and judicial issues // Journal in Computer Virology. – 2005. – Vol. 1. – P. 24-31. DOI: 10.1007/s11416-005-0006-5

2. *Mun H.J., Han K.H.* Blackhole attack: user identity and password seize attack using honeypot // Journal of Computer Virology and Hacking Techniques. – 2016. – Vol. 12. – P. 185-190. DOI: 10.1007/s11416-016-0270-6

3. *Рыженко А.А.* Модель деструктора-полиморфа цифровой среды / Проблемы управления безопасностью сложных систем: материалы XXVI Международной научной конференции (19 декабря 2018 г., Москва). – М.: ИПУ РАН, 2018. – С. 158-162.

4. *Рыженко А.А.* Модифицированный алгоритм вируса полиморфика как основа деструктора информационной среды / Информатика: проблемы, методология, технологии: сборник материалов XVIII международной научно-методической конференции: в 7 т. (Воронеж, Воронежский государственный университет, 14-15 февраля 2019 г.) – Воронеж: Издательство «Научно-исследовательские публикации» (ООО «Вэлборн»), 2019. – Т. 5. – С. 857-861.

5. *Рыженко А.А.* Использование пирамидального образа аналитического мышления при подготовке комплексных решений на примере системы координации ресурсов информационного поля цифровых данных / Информационно-аналитическое обеспечение профессиональной деятельности: материалы межд. научно-практической конференции от 15 мая 2018 г. – М.: МПИ ФСБ России, 2020. – С. 106-116.

6. *Reddy V., Kolli N. & Balakrishnan N.* Malware detection and

classification using community detection and social network analysis // Journal of Computer Virology and Hacking Techniques. – 2021. – Vol. 17. – P. 333-346. DOI: 10.1007/s11416-021-00387-x

7. *Рыженко А.А., Рыженко Н.Ю.* Безопасность информации цифровой экономики / Актуальные проблемы и перспективы развития экономики. Труды Юбилейной XX Всероссийской с международным участием научно-практической конференции. – Симферополь: Издательский дом КФУ, 2021. – С. 289-291.

DOI: 10.25728/iccss.2022.61.83.052

Кротова М.В.

Качественные подходы к моделированию стратегий импортозамещения на отраслевом и межотраслевом уровнях

Аннотация: Импортозамещение является одним из стратегических приоритетов развития национальной экономики РФ в сфере обеспечения собственно защищенности страны от экономических демаршей со стороны компаний и правительств недружественных государств. Это один из редких случаев, когда задачи безопасности не только сдерживают процессы экономического развития, но и непосредственно обеспечивают рост и усложнение структуры ВВП, в его части, находящейся под национальным контролем. На уровне отдельного предприятия-изготовителя стратегия импортозамещения может быть достаточно четко определена в части изменения номенклатуры выпуска. На уровне более крупных хозяйственных комплексов (различного масштаба и структуры) выработка импортозамещающей стратегии может быть представлена как оптимизационная задача с различными наборами критериев оптимизации.

Ключевые слова: экономическая безопасность, технологический суверенитет, импортозамещение, концептуальная независимость, ГИСП

Традиционными механизмами поддержки импортозамещения – во всех странах, где оно оказывалось эффективным в различные периоды новейшей истории – являются [1, 2]:

- установление «запретительных» таможенных тарифов для импорта тех видов оборудования, сырья, технологий, комплектующих и т.п., зависимость от которых собственной экономики расценивается как стратегический риск, угроза или вызов;
- нетарифное регулирование, включающее в себя:
  - текущую деятельность органов государственной власти в сфере отражения угроз экономической безопасности;
  - прямые, политически мотивированные запреты на импорт из недружественных стран либо квотирование импорта;
  - разработку законодательной базы для деятельности юридических лиц с иностранным участием, включая вопросы учредительской деятельности, лицензирования валютных операций, обеспечения отчетности и контроля со стороны органов государственной власти и т.д.;
  - национальную систему технического регулирования и стандартизации, включающая в себя требования, ограничивающие активность и номенклатуру потенциальных зарубежных поставщиков;
  - к новым методам нетарифного регулирования стоит отнести ведомственные, экспертные, общественные и образовательные кампании, способствующие формированию в промышленности устойчивого спроса на отечественные технологии (примерами последних в РФ можно считать и отраслевые выставки «Электро-2022», Weldex-2022, Mining World-2022, Securika-2022 и другие);
- государственное инвестирование и фактическое субсидирование, как в виде государственных трансфертов, так и косвенное через льготное кредитование, налоговые каникулы и иные меры финансового характера, конечный плательщик по которым – государство, плюс создание специализированных внебюджетных фондов, учреждение технопарков и т.п. точек роста;
- новое направление – создание национальных экосистем в сфере B2B – информационных платформ для проведения тендеров на закупку отечественного оборудования, банков данных

импортозамещающих технологий, структур разработки и поддержки бизнес-планов, а также алгоритмизация данных экосистем в соответствии с национальными интересами, специальные условия хранения и защиты данных в экосистемах. Это наиболее «мягкий» способ сформировать устойчивые связи между предприятиями различной формы собственности, находящимися при этом под национальным контролем, не прибегая к прямому вмешательству в экономическую деятельность предприятий.

Согласно работе [2], на рубеже 2019-2020 гг., в экономике России действовали механизмы содействия импортозамещению, относящиеся ко всем вышеназванным типам, среди которых было выделено 40 направлений содействия реализации импортозамещающих стратегий для предприятий, компаний и регионов. Был определен сам термин «импортозамещение» и сформированы соответствующие структуры, занимающиеся нетарифным регулированием. Главными из них стали Агентство по технологическому развитию (утв. Распоряжением Правительства РФ от 26.05. 2016 г. №1017-р), отвечающее не только за модернизацию, но и за переход от импорта технологий – к их экспорту.

Фонд развития промышленности был преобразован из Российского фонда технологического развития, и, как следует из его статуса фонда, опирается в своей деятельности на уполномоченные банки. Его структура носит региональный характер, позволяющий осуществить программу «70 на 30». На каждые 100 млн. руб., заложенных в областном бюджете, для фонда развития промышленности в отдельном субъекте Федерации, должно быть привлечено 233 млн. руб. федеральных средств. Кроме этого, Программа развития промышленности и ее конкурентоспособности, принятая 15.04.2014 г. Постановлением № 328 Правительства РФ, также включает в себя создание новых структур, в виде индустриальных парков с субсидируемым процессом создания инфраструктуры, т.е., по сути – государственным соинвестированием.

Федеральным законом от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» вводился механизм запретов и ограничений на поставку импортной продукции. Постановлением Правительства РФ № 719 была также

утверждена Методика определения степени локализации, механизм и условия специального инвестиционного контракта.

Эти решения действуют на отраслевом и межотраслевом уровнях, причем, как показало общение автора настоящей работы с ответственными сотрудниками предприятий, среди наиболее активно используемых, носящих сквозной характер, здесь стали региональные программы «70 на 30» и ГИСП – Государственная информационная система промышленности, запроектированная как источник данных для принятия решений и на уровне Правительства РФ, так и самих хозяйствующих субъектов промышленности. Платформа включает модуль «Мониторинг проектов импортозамещения». Одновременно с ГИСП действуют и иные источники информации об импортозамещающих технологиях – электронные каталоги и справочники, а также организации по содействию продвижения отечественных разработок на уровне субъектов Федерации (например, «Мой бизнес», г. Белгород) Поставка информации о собственных, оригинальных импортозамещающих разработках в ГИСП (и возможно, иные платформы) является обязательной для предприятий и организаций государственной формы собственности. В то же самое время, многие инновационные предприятия негосударственных форм собственности испытывают определенные сложности с доступом на тендерные платформы компаний – публичных акционерных обществ, в том числе, с контрольным пакетом у государства, но не 100 %.

В 2022 г., с началом СВО и беспрецедентным экономическим давлением, которое оказывается на Россию странами т.н. «коллективного Запада», в законодательную базу введен термин недружественное государство, который, при применении его к экономической проблематике, существенно повышает приоритетность любых импортозамещающих проектов. По состоянию на 10.10.2022 г., главными дополнительными мерами поддержки бизнеса в сложных геополитических и финансовых условиях стали:

Указ Президента РФ от 16.03.2022 №121 в связи с введением в отношении РФ и ее граждан политических, экономических и иных санкций, – предписывает властям субъектов РФ принимать исчерпывающие меры по обеспечению социально-экономической

стабильности. Очевидно, что импортозамещающие проекты, даже при недостаточной экономической эффективности, обладают высоким потенциалом к стабилизации социально-экономической обстановки, особенно в условиях градообразующих предприятий и иных экономических моноструктур.

Другие меры поддержки бизнеса носят преимущественно налоговый характер. Так, в соответствии с п.4.ст. 4 НК РФ, высшие исполнительные органы государственной власти субъектов РФ вправе в 2022 году издавать нормативные правовые акты, предусматривающие до конца 2022 г. продлевать сроков уплаты региональных и местных налогов. В соответствии с ч. 2 ст. 15 Федерального закона от 08.03. 2022 №46-ФЗ в период по 31.12. 2022 решением высшего исполнительного органа субъекта РФ, могут быть установлены иные случаи осуществления государственных закупок у единственного поставщика; определен порядок осуществления таких закупок.

В соответствии с п.4 Постановления Правительства РФ от 12.03.2022 №353, в отношении разрешительных режимов и лицензирования отдельных видов деятельности, – уполномоченные органы исполнительной власти субъектов РФ вправе принять ряд антикризисных решений, при необходимости определив порядок их реализации.

Постановлением Правительства РФ от 05.04. 2022 №590 установлены особые условия предоставления в 2022 г. субсидий и грантов из бюджетной системы РФ, в т.ч., сокращать срок приема заявок на тендеры, более гибко подходить к наличию у участников конкурса задолженностей и другие.

О фактическом положении дел в области зависимости от импорта уже в новой *геополитической реальности (нач. 2022 г.), рассказывает работа [3]: «… Проведенный аппаратом Уполномоченного при Президенте РФ по защите прав предпринимателей мониторинг текущего положения компаний – в исследовании, которое прошло в два этапа: с 14 по 18 февраля и с 3 по 7 марта – приняли участие руководители и владельцы 5995 компаний из 85 регионов – показал, что оборот 55,7 % компаний по итогам 2021 года не достиг значений конца 2019 г. … «старые» – действовавшие до 25 февраля текущего года – санкции затрагивали 26,4 % респондентов, то введенные после этой даты ограничения*

могут повлиять уже на 84,1 % компаний. Среди главных проблем, которые выделяет бизнес, … разрыв цепочек поставок (у 39,6 % опрошенных компаний)... связан прежде всего с импортными товарами, сложности возникают и с поставками российской продукции, имеющей импортные составляющие… По данным приведенного выше исследования, импортную составляющую до 10 % имеют 26,8 % компаний, от 10 до 50 % – 36,9 %, более 50 % – 26,4 %. О полной зависимости от импорта сообщили 9,9 % компаний» [3]. Здесь импортозамещение, хотя и не упоминается напрямую, но правомерно рассматривается как один из необходимых эффектов от мероприятий по государственной поддержке бизнеса. Предполагается, что государство выделяет компаниям средства либо освобождает часть прежде связанных иными расходами или обязательствами финансов предприятий – для того, чтобы освободившиеся деньги пошли на закупку отечественного оборудования, комплектующих, патентов и др., а в идеальном сценарии и на инвестиции в собственный импортозамещающий ассортимент.

Качественная, как и институционально-содержательная сторона экономического роста в промышленности и развитии новых технологий рассматривается по работе [4], и демонстрирует связь технологической политики с геополитическими факторами и безопасностью (таблица 1).

Проблема в том, что разовые решения по импортозамещению, даже при наличии комплексной поддержки, не в состоянии заменить комплексного государственного подхода к обеспечению технологического суверенитета России, создания собственных, концептуально независимых от иностранного разработчика научно-технологических школ.

Таблица 1 –Характеристики основных типов национальных стратегий по соотношению геополитических и экономических критериев

Тип стратегии	Варианты соответствующей стратегии в области технологий и научно-технической политики		Обеспечивающая техническая политика
1. Полный суверенитет, формирование собственной системы коллективной безопасности	Глобальное лидерство		Стремление к лидерству в технологиях всех категорий – оборонных, двойного назначения, гражданских, являющихся ключевыми для обеспечения мировой стратегической стабильности и высокого по мировым меркам потенциала национальной экономики
2. Стремление к обеспечению полного суверенитета в средне- и долгосрочной перспективе	Обеспечение технологической независимости при снижении значимости экономических критериев	Технологическое лидерство по отдельным технологиям или их группам	Импортозамещение или протекционизм Схемы привлечения инвестиций, маркетинга и сервиса для конвертации технологий в успешный экспортный товар Возможно копирование иностранных инноваций с большей или меньшей степенью адаптации к национальным целям и рынкам
3. Переходные стратегии, в основе которых доминирует экономический выбор	Рыночное лидерство	Догоняющее развитие	Решающей является возможность удерживать значительные объемы реализации патентованной продукции, в цене которой присутствует определенная рентная составляющая Копирование технологий
4. Ограниченный суверенитет, вхождение в другие системы коллективной безопасности	Нишевое лидерство	Длительное догоняющее развитие	Ставка на импорт технологий, с приоритетной ценностью обеспечения роста занятости либо форсированной модернизации в ущерб независимости от иностранных технологий Копирование технологий ограничено
5. Отказ от суверенитета, ситуация failed state	Деиндустриализация		Отказ от определенных видов деятельности и технологий, как правило, с целью снижения масштабов государственного сектора в военной, экономической и техносфере Отсутствие (распад) инженерных и научных школ, производственной базы

К выводам по настоящей работе следует отнести:

1. Необходимость подчинения импортозамещающих проектов единой цели – обеспечения технологического суверенитета Российской Федерации в долгосрочной перспективе, с этой же целью разработать и скорректировать меры поддержки бизнеса в условиях давления со стороны недружественных государств.

2. Потребность в разработке отраслевых и межотраслевых стратегий импортозамещения, где в качестве критерия используется достижение (поддержание) технологического суверенитета, а текущие отраслевые показатели – задают систему ограничений.

Литература:

1. Инновационная экономика: Энциклопедический словарь-справочник / Комков Н.И., Селин В.С., Цукерман В.А. Научный руководитель Ивантер В.В., Суслов В.И.; ИНП РАН. – М.: МАКС Пресс, 2012. – 544 с.

2. *Комков Н.И., Бондарева Н.Н.* Импортозамещающая стратегия РФ как фактор развития в условиях глобальных вызовов 2017-2019 гг. // МИР (Модернизация. Инновации. Развитие). – 2017. – Т. 8. № 4. – С. 640-656

3. Система «Гарант». Поддержка малого и среднего бизнеса в условиях санкций (аналитическая статья от 17 марта 2022 г. – URL: https://www.garant.ru/article/1532971/ (дата обращения 20.10.2022).

4. *Иванов В.В.* «Инновационная парадигма XXI». – М.: Наука, 2015. – 455 с.

DOI: 10.25728/iccss.2022.43.51.053

Рожнов А.В.

Совершенствование комплексных подходов и проблемные вопросы интеллектуализации технологий в сервисах медицинской диагностики

Аннотация: Рассматриваются передовые подходы развития технологий искусственного интеллекта в здравоохранении. На основе комплексного анализа зарубежного опыта обосновываются пути совершенствования методов и средств интеллектуализации. Обсуждаются основные преимущества

и проблемные вопросы технологий машинного обучения в интересах предварительного оценивания эффективности применения новых сервисов медицинской диагностики.

Ключевые слова: медицинская диагностика, машинное обучение, интеллектуализация, обработка данных, сервис

События последних лет оказали важное и бесспорное влияние на пересмотр приоритетов развития и обусловленное становление передовых подходов разработки и эффективного применения новых средств и технологий искусственного интеллекта в *здравоохранении*.

Целевой установкой комплексных исследований является адаптация приёмов *информационно-аналитического моделирования* в интересах, по сути, предварительного оценивания эффективности применения современных сервисов медицинской диагностики.

Разработка элементов таких технологий, *системная интеграция* их компонентов здесь неразрывным образом связаны с дальнейшим совершенствованием комплексных подходов и последовательным выделением проблемных вопросов интеллектуализации технологий в сервисах медицинской диагностики в ходе общего сопоставления с популярными задачами и достижениями *технической диагностики*.

Превалирующей *мотивацией* настоящей работы является стремление поиска путей компенсирования ряда складывающихся негативных тенденций и неоднозначных суждений, основанных на оценивании значимости направлений совершенствования методов и средств диагностики с позиций общей *публикационной активности*.

В работе, на основе комплексного анализа зарубежного опыта, обосновываются новые пути совершенствования методов и средств интеллектуализации *в условиях неоднородного информационного ландшафта* данной предметной области. Опорным источником предлагается аудиторский доклад «*Искусственный интеллект в здравоохранении: преимущества и проблемы технологий машинного обучения для медицинской диагностики*» [1]. При этом обсуждаются преимущества и проблемные вопросы технологий *машинного обучения* (ML) в створе интересов предварительного оценивания эффективности применения сервисов медицинской диагностики.

Итак [1], каждодневно, как учитываемые, так и скрываемые *медицинские ошибки в диагностике* сказываются на здоровье многих миллионов людей и обходятся в крупные для бюджетов различных

уровней денежные суммы. В числе прочих мер считается, что ML-технологии могут, прежде всего, выявить скрытые или сложные закономерности в *диагностических данных* для раннего выявления заболеваний и улучшения известных методов лечения в перспективе.

Но, а приоритетом возможно полагать раскрытие собственно таких технологий и наборов их компонентов, которые формируются и используются к настоящему времени, включая именно те, которые совершенствуются, повышая точность при обработке *новых данных*. Очевидно, что внедрение подобных технологий сопряжено, прежде всего, с такими трудностями, как необходимость демонстрировать реальную производительность *в различных клинических условиях*.

Так, к примеру, в США доступно несколько распространённых ML-технологий, широко используемых в процессе медицинской диагностики [1]. Полученные *преимущества* включают более раннее выявление заболеваний, отчасти более последовательный анализ медицинских данных и расширение доступа к видам медицинской помощи, особенно для малообеспеченных слоёв населения. В частности, было определено множество технологий на базе ML для пяти выбранных заболеваний, в их числе – некоторые виды рака, диабетическая ретинопатия, болезнь Альцгеймера, болезни сердца и COVID-19, – причём большинство технологий использует только данные изображений, таких как рентген или *магнитно-резонансная томография* (МРТ). Однако эти технологии ML по-прежнему, как правило, в целом всё ещё не получили широкого распространения.

Несомненно [1], и государственные, и частные инициативы во многом сориентированы на достижение и расширение возможностей медицинских диагностических технологий на базе ML. Кроме того, были выделены три более широких новых подхода ML-диагностики: *автономный*, *адаптивный* и *ориентированный на потребителя*, – которые можно применять для диагностики различных заболеваний. И не вызывает сомнения, что эти достижения позволят расширить возможности медицинских работников и улучшить качество лечения пациентов, но также имеют и определённые *ограничения*. Например, *адаптивные технологии* могут повысить точность за счёт включения дополнительных данных для самообновления, но автоматическое включение неоднородных данных низкого качества может привести к несогласованности и снижению производительности алгоритмов.

Расширение спектра адаптивных алгоритмов *интеллектуальной обработки данных* в полном объёме не разбирается в рамках данной работы и требует отдельного и более пристального рассмотрения.

Однако, прежде всего, следует отметить некоторые *проблемные вопросы*, существенно влияющие на эффективность разработки и внедрения ML для медицинской диагностики в нынешних условиях:

– приоритетное удовлетворение *клинических потребностей*, таких как разработка технологий, которые интегрируются в клинические рабочие процессы с наименьшими модификациями и издержками;

– беспристрастная демонстрация реальной *производительности* в различных клинических условиях и в скрупулёзных исследованиях;

– *опережающее в принципе* устранение множественных пробелов в действующем законодательстве, например, предоставление чётких *методических указаний* при разработке адаптивных алгоритмов.

Указанные проблемы затрагивают различные заинтересованные стороны, включая как разработчиков технологий, поставщиков медицинских услуг, так и собственно пациентов, и могут замедлить эффективные разработку и внедрение этих технологий и *сервисов*.

Следует отметить особо, что было представлено три основных варианта *технической политики*, которые могут помочь решить эти проблемы или расширить преимущества технологий диагностики на базе ML. Сформированные предложения определяют возможные действия, к примеру, законодателей, федеральных и региональных властей и органов местного самоуправления, а также акторов научно-исследовательских учреждений, отраслей промышленности.

Таким образом, данное многоаспектное исследование передовых достижений средств и технологий искусственного интеллекта в здравоохранении, под которыми подразумеваются преимущественно интеграционные компоненты интеллектуальной обработки данных, в рамках комплексных исследований востребовано при адаптации известных приёмов информационно-аналитического моделирования и в ходе приводимого предварительного оценивания эффективности применения современных сервисов медицинской ML-диагностики. В свою очередь, дальнейшее совершенствование комплексных подходов будет способствовать выявлению проблемных вопросов

интеллектуализации технологий на различных этапах формирования и применения в современных сервисах медицинской диагностики.

Кроме того [2-7], в указанном списке основных использованных источников более детально рассматриваются различные аспекты развития интеграционных компонентов искусственного интеллекта, особенности защиты интеллектуальной собственности сложных систем с достоверными признаками искусственного интеллекта, применения трансмедиа технологий обработки и представления данных медицинской информатики при реализации новых сервисов. Наряду с указанным в [5-7], может представлять интерес исследовательская активность и её анализ в сфере интеллектуальной обработки данных, которые позволяют детализироововать данную тематику с междисциплинарных позиций.

Автор считает своим приятным долгом выразить благодарность коллегам (лаборатории), принявшим непосредственное участие в предварительном обсуждении ряда частных вопросов этого доклада, касающихся специфики управления безопасностью новых сервисов.

Комплексные исследования были выполнены при частичной поддержке РФФИ, проект 19-29-09030_мк «Разработка и исследование алгоритмов выделения и распознавания объектов в видеопоследовательностях на базе специализированных мобильных устройств»

Литература:

1. GAO Issues Report on Artificial Intelligence in Health Care. JDS. Nov. 21, 2022. – URL: https://www.jdsupra.com/legalnews/gao-issues-report-on-artificial-8112443/ (дата обращения 15.10.2022).

2. *Рожнов А.В.* Конвергенция технологий управления автономными системами в контексте развития интеграционных компонентов искусственного интеллекта // Современные информационные технологии и ИТ-образование. – 2017. – Т. 13. № 3 (приложение к журналу). – С. 52-64.

3. *Рожнов А.В.* Технологический разрыв в сфере новых технологий и особенности защиты интеллектуальной собственности – систем с достоверными признаками искусственного интеллекта / Материалы 28-й Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2020. – С. 124-129.

4. *Рожнов А.В.* Применение трансмедиа технологий обработки и представления данных медицинской информатики при реализации новых сервисов / Тезисы 19-й Всероссийской научной конференции «Нейрокомпьютеры и их применение». – М.: МГППУ, 2021. – С. 149-151.

5. *Рожнов А.В.* Исследование потенциала управления траекторией полёта ЛА посредством системы, использующей сеть живых нейронов коры головного мозга / Тезисы 20-й Всероссийской научной конференции «Нейрокомпьютеры и их применение». – М.: МГППУ, 2022. – С. 159-160.

6. *Andrey V. Lychev, Aleksei V. Rozhnov & Igor A. Lobanov.* An Investigation of Research Activities in Intelligent Data Processing Using Data Envelopment Analysis // Intelligent Systems Reference Library. – 2020. – Vol. 182, Computer Vision in Control Systems – 6: Advances in Practical Applications. – P. 127-140. DOI: 10.1007/978-3-030-39177-5_10

7. *Aleksei V. Rozhnov, Andrey V. Lychev & Igor A. Lobanov.* Hybrid Optimization Modeling Framework for Research Activities in Intelligent Data Processing // Intelligent Systems Reference Library. – 2020. – Vol. 182, Computer Vision in Control Systems – 6: Advances in Practical Applications. – P. 141-152. DOI: 10.1007/978-3-030-39177-5_11

DOI: 10.25728/iccss.2022.26.47.054

Карпов С.Ю.

Прогнозирование оптимальной территории обслуживания с использованием геоинформационного моделирования

Аннотация: В работе рассматриваются вопросы, связанные с прогнозированием территории обслуживания органов правопорядка, основной деятельностью которых является расследование пожаров. Предложен алгоритм определения оптимальных границ обслуживания методом геоинформационного моделирования. Описаны основные критерии и исходные данные при определении оптимальных территорий обслуживания. Предложено использование экспериментально-аналитического метода при сборе

исходных данных, а также внедрение компьютерных технологий при определении оптимальных территорий обслуживания.

Ключевые слова: оптимальные границы обслуживания, кадровое ресурсообеспечение, пожарная безопасность, расследование пожаров, дознаватель, пожар, геоинформационные технологии, геоинформационное моделирование

В результате пожара уничтожаются (утрачивают информационную составляющую) многие следы преступления, поэтому своевременное прибытие дознавателя (следователя) на место происшествия повышает вероятность обнаружения и фиксации криминалистически значимых следов, а также сбора оперативной информации на месте. Оперативность прибытия сотрудника на место происшествия, обеспечивает сбор необходимой и достоверной информации об обстоятельствах пожара «по горячим следам», что непосредственно влияет на раскрываемость, качество и сроки производства по делу. На оперативность прибытия сотрудника влияет множество факторов, но к наиболее значимым можно отнести удаленность потенциальных объектов пожара от места дислокации подразделения органа дознания (следствия), а также особенности транспортной инфраструктуры. В этой связи возникает вопрос о необходимости установления оптимального (нормативного) времени оперативного реагирования и определения эффективных территорий обслуживания. Решение разных функциональных задач в структурах органов правопорядка и уровня их реагирования, предусматривает разработку методов и подходов по определению кадрового ресурсообеспечения с учетом различных факторов и критериев. За счет разработки и внедрения новых подходов (методов), а также компьютерных технологий можно сформировать обоснованную структурно-штатную численность подразделения с учетом территориальных особенностей. Отражение информации на карте будет являться элементом поддержки принятия управленческого решения ЛПР при формировании оптимальных территорий обслуживания и увязывания между собой сформированных межрайонных подразделений в границах субъекта Российской Федерации. Решение данной задачи позволит повысить качество

расследования и добиться снижения количества пожаров и последствий от них.

Использование метода геоинформационного моделирования давно применяется при решении различных задач, однако в деятельности связанной с обеспечением пожарной безопасности он внедряется преимущественно для служб экстренного реагирования и при моделировании ситуаций ЧС. Примененные методы научного исследования, такие как: индукция, дедукция, анализ, эксперименты, анкетирование и опросы позволили проанализировать деятельность сотрудников и разработать модель определения оптимальных территорий обслуживания. Предложенная общая структура определения границ территорий обслуживания сотрудника органа дознания при расследовании пожаров (рисунок 1), является алгоритмом разрабатываемой компьютерной программы. Данный подход можно применять и на другие службы правопорядка, осуществляющих предварительное расследование преступлений.

В рамках исследования определяются условия и факторы, при которых будет достигнут оптимальный результат (таблица 1). В ходе сбора данных для определения оптимальных границ территории обслуживания, необходимо учитывать способность сотрудника выполнять существенную нагрузку без снижения качества работы (отработка определенного количества сообщений по пожарам с учетом их типологизации по сложности (затрат времени на их выполнение) и принимаемых процессуальных решений).

Рисунок 1– Общая структура определения оптимальных границ обслуживания методом геоинформационного моделирования

Таблица 1 – Критерии и факторы при определении оптимальных границ территорий обслуживания

Критерии, факторы, влияющие на оперативность прибытия к месту пожара	Условия при формировании исходных данных
Время прибытия сотрудника на место пожара должно учитывать несколько условий: 1. оптимальным прибытием на место пожара должно быть время до убытия с места пожара пожарного подразделения. Поэтому максимальное время прибытия не должно превышать среднего времени обслуживания вызова пожарными подразделениями; 2. на основании прогнозирования плотности распределения пожаров на обслуживаемой территории, допускается предусматривать максимальную удалённость потенциальных объектов пожара с учетом 10% погрешности. То есть, при определении оптимальной территории обслуживания учитывать 10% интервал, в который могут войти некоторые объекты (пожары), расположенные вне зоны оперативного реагирования, но находящиеся в административно-территориальной юрисдикции района (районов, города, муниципального образования и т.п.); 3. в некоторых случаях, например в районах с небольшой плотностью населения и большими административными территориями (Дальний Восток, Сибирь и т.д.) границы обслуживания могут определяться с учетом 8-ми часового рабочего дня. При этом необходимо	При формировании исходных данных должны учитываться: 1. прогнозные данные количества пожаров и загораний в год на определенной административной территории; 2. достаточность материально-технической базы и транспорта (в большинстве случаев передвижение дознавателя к месту пожара происходит с использованием служебного или личного автотранспорта); 3. прогнозные данные об интенсивности и плотности пожаров в обслуживаемом районе (районах)

учитывать, что количество вызовов в удаленные локации не должны носить массовый характер, а в закреплении следов преступления на первоначальном этапе осмотра должны привлекаться сотрудники правоохранительных органов (например, участковые уполномоченные полиции с учетом иммерсивного телеприсутствия дознавателя)	

Определение оперативного времени прибытия на место происшествия - важный критерий в прогнозировании численности сотрудников и оптимальной территории обслуживания. Определение времени оперативного прибытия рассчитывается по формуле 1.

$$T_{опер.приб.} = T_{обсл.пож.} - T_{сб.} \quad (1)$$

где

$\mathbf{T_{опер.\ приб.}}$ – время оперативного прибытия сотрудника территориального подразделения к месту пожара, в часах;

$\mathbf{T_{обсл.\ пож}}$ – среднее время обслуживания пожара в зоне ответственности территориального подразделения, в часах. Прогнозируется на основании статистических данных за последние 3-5 лет.

$\mathbf{T_{сб.}}$ - среднее время на сборы и подготовительные мероприятия перед началом движения на автомобиле к месту пожара составляет: для больших городов – до 5 минут (при условии круглосуточного дежурства в подразделении), для сельской местности и небольших городов – до 15 минут.

Учитывая среднее значение времени оперативного прибытия ($\mathbf{T_{опер.\ приб}}$) на обслуживаемой территории с использованием навигационных программ (Яндекс навигатор и т.п.), можно спрогнозировать максимальное удаление сотрудника на служебном автомобиле по дорогам общего пользования. На рисунке 2представлены результаты исследования, характеризующие возможную зону (территорию) обслуживания с учетом времени

оперативного прибытия с элементами геоинформационной статистики (отображением плотности и удаленности термоточек). В некоторых случаях, где административные территории имеют большую площадь, например регионы севера, необходимо учитывать поправочные коэффициенты. Определение поправочного коэффициента k_T, характеризующего удаленность объектов пожара (при условии, что время прибытия к месту пожара более среднестатистических значений, полученных на основании экспериментально-аналитического подхода) производится по формуле 2.

Поправочный коэффициент ($\mathbf{k_т}$)определяется для каждого межрайонного подразделения индивидуально, с учетом среднестатистического времени прибытия на место пожара ($\boldsymbol{t_{v.\text{ср}}}$) (например, в городах Самара, Тольятти – городские отделы не более 33 минут (0,55 часа) и в сельской местности (межрайонные отделы) не более 36 минут (0,6 часа)). При определении поправочного коэффициента ($\mathbf{k_т}$) должно соблюдаться условие $\mathbf{t_L \leq t_{L.max}}$.

$$k_T = 1 + \frac{2(t_L + T_{\text{сб}} - t_{v.\text{ср}})}{t_{Lmax}} \qquad (2)$$

где

$\mathbf{t_L}$ – время в пути до прогнозируемых наиболее удаленных объектов пожара, в часах;

$\mathbf{T_{сб.}}$ – среднее время на сбор и подготовительные мероприятия перед началом движения на автомобиле к месту пожара, в часах;

$\mathbf{t_{L.max}}$ – максимально допустимое время в пути до объекта пожара *(не более 8 часов, с учетом 8-часового рабочего дня)*, в часах;

$\mathbf{t_{v.ср.}}$– среднее время прибытия сотрудника на место вызова (пожара), в часах.

При прогнозировании затрат времени прибытия до объекта пожара ($\mathbf{t_L}$) на подконтрольной территории, можно выделить несколько вариантов. Вариант № 1: когда границы территории обслуживания не привязаны к оперативному времени прибытия на место пожара ($\mathbf{T_{опер.\ приб.}}$). Вариант №2: когда времени оперативного реагирования достаточно, чтобы успеть доехать от места дислокации подразделения до любой удаленной локации территории обслуживания, где может произойти пожар. Поэтому, при

определении времени могут быть условия, что$\mathbf{t_L \geq T_{обсл.\ пож.}}$ *(на основе анализа плотности распределения пожаров на обслуживаемой территории (с применением геоинформационной технологий рисунка 2), а также статистических данных наиболее удаленных объектов пожара за последние 3-5 лет)*или с учетом того, что$\mathbf{t_L \leq T_{обсл.\ пож}}$ *(при условии формирования границ обслуживания территории с учетом оперативного времени прибытия к месту пожара* $\mathbf{T_{опер.\ приб.}}$).

$$t_{Lmax} = \frac{8 - T_{\text{рп}}}{2} \tag{3}$$

$$T_{\text{рп}} = \text{T}_{\text{осм}} + \text{T}_{\text{опр}} \tag{4}$$

где

$\boldsymbol{T_{\text{рп}}}$– прогнозируемое *(минимально необходимое и достаточное)* время для производства процессуальных действий по осмотру места пожара и опросу очевидцев, в часах;

$\boldsymbol{T_{\text{осм}}}$ – прогнозируемое время осмотра места пожара, в часах;

$\boldsymbol{T_{\text{опр}}}$ – прогнозируемое время опроса очевидцев, в часах.

$$\text{T}_{\text{осм}} = M_1 \times W^{\alpha} \times E^{\gamma} \tag{5}$$

где

$\boldsymbol{M_1}$ – общая факторная производительность *(среднестатистическое экспертное время, затраченное дознавателем на осмотр места пожара)*, в часах;

$\boldsymbol{\alpha}$ – коэффициент эластичности, учитывающий функциональное назначение объекта пожара;

$\boldsymbol{W}$ – фактор, учитывающий размерность объекта пожара по площади;

$\boldsymbol{\gamma}$ – коэффициент эластичности, учитывающий уровень и профиль образования;

$\boldsymbol{E}$– фактор, учитывающий стаж работы в должности.

$$\text{T}_{\text{опр}} = M_2 \times E^{\gamma} \times N^{\beta} \tag{6}$$

где

M_2 – общая факторная производительность *(среднестатистическое экспертное время, затраченное дознавателем на опрос очевидцев)*, в часах;

γ – коэффициент эластичности, учитывающий уровень и профиль образования;

E – фактор, учитывающий стаж работы в должности;

β– коэффициент эластичности, учитывающий возраст опрашиваемых;

N–коэффициент, учитывающий количество опрашиваемых *(**N**=4 при опросе не более 3-4 человек)*.

Исходя из множества факторов неопределенности при расследовании пожаров, целесообразно при определении границ территории обслуживания учитывать допустимую погрешность в 10 %. Использование геоинформационных технологий является важным инструментом в управлении структуры и штата органов оперативного реагирования, что позволяет сделать следующие выводы (на примере органа дознания МЧС России):

1. Определение оптимальных границ обслуживания при расследовании пожаров повысит качество и оперативность работы дознавателя.

2. Внедрение в деятельность органов правопорядка (на примере органа дознания МЧС России) программных продуктов, определяющих оптимальные границы межрайонных отделов (отделений) позволит сформировать эффективную структурно-штатную численность.

3. Пространственно-временная визуализация необходимых в деятельности дознавателя данных на обслуживаемой территории, позволяет оптимально решать вопросы компоновки межрайоных отделов органа дознания МЧС России и их увязке в границах субъекта Российской Федерации.

4. Применение геоинформационных технологий в определении оптимальных границ территории обслуживания при расследовании пожара, может являться инструментом в поддержке принятия управленческих решений не только для определения кадрового ресурсообеспечения, но и в других целях, например, при разработке мероприятий профилактического характера.

Литература:

1. *Тесленок К.С., Тесленок С.А.* Цифровое моделирование рельефа в предотвращении и ликвидации некоторых чрезвычайных ситуаций природного характера / Материалы второй Всероссийской научно-практической конференции «Картография и геодезия в современном мире». – Саранск: Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва, 2014. – С. 155-161.

2. *Ромашевская Я.А.* Экологический аудит, моделирование и прогнозирование экологической обстановки, принятие решений в сфере управления охраной окружающей среды посредством создания геоинформационного интернет-портала на основе интерсубъективной теории / XII Всероссийское совещание по проблемам управления ВСПУ-2014. – М.: ИПУ РАН, 2014. – С. 5666-5674.

3. *Матюшин А.В., Порошин А.А., Матюшин Ю.А., Бобринев Е.В., Кондашов А.А*. Проектированиеразмещенияподразделенийпожарной охраны в населенных пунктах с использованием геоинформационных технологий // Bezpieczenstwo i TechnikaPozarnicza. – 2013. – Т. 31. № 3. – С. 81-86.

4. *Брушлинский Н.Н., Соколов С.В., Алехин Е.М., Коломиец Ю.И., Вагнер П.* Опыт применения компьютерных имитационных систем моделирования деятельности экстренных служб // Пожаровзрывобезопасность. – 2016. – №8. – С.6-16.

5. *Карпов С.Ю.* Нормирование времени прибытия сотрудников Федерального Государственного пожарного надзора на место пожара // Техносферная безопасность. – 2020. – №4 (29). – С. 73-81.

6. *Карпов С.Ю. Прус Ю.В.* Модель прогнозирования продолжительности сбора первоначальной информации на месте пожара функцией Кобба-Дугласа // Технологии техносферной безопасности. – 2020. – №1(87) – С. 93-106.

7. *Соколов С.В.* Методологические основы разработки и использования компьютерных имитационных систем для исследования деятельности и проектирования аварийно-спасательных служб в городах: диссертация на соискание ученой степени доктора технических наук. – М., 1999. – 299 с.

DOI: 10.25728/iccss.2022.53.35.055

Скворцов О.Б., Сташенко В.И.

Высокочастотная вибрация – диагностика и усталость

Аннотация: Рассмотрена возможность мониторинга сложного оборудования в условиях воздействия широкополосной вибрации. Отмечено, что эффективная противоаварийная защита такого оборудования для безопасной эксплуатации должна включать контроль вибрационного отклика как в характеристиках перемещения (деформации), так и действия динамических нагрузок, определяемых механическим ускорением.

Ключевые слова: надежность, циклическая усталость, вибрационная прочность, фреттинг, синергия, ускорение, динамические силы, деформация, мониторинг, противоаварийная защита

Введение

Механические удары и вибрации являются одной из наиболее распространенных причин повреждения сложного технического оборудования. Ударные воздействия часто имеют малую длительность, но при большой амплитуде они могут служить причиной зарождения механических дефектов. Такие дефекты затем развиваются под влиянием вибрации оборудования. Среди механизмов разрушения под влиянием вибрации многоцикловая и сверхмногоцикловая усталость, а также фреттинг коррозия [1, 2].

Вибрация сложного оборудования, например, роторных агрегатов вызвана множеством возможных причин и, как правило характеризуется сложным спектральным составом. Исследования разрушающего действия такой вибрации [3] показывает, что присутствие высокочастотных деформаций даже малой амплитуды сильно сказывается на прочностных характеристиках конструкционных материалов. Учесть влияние сложной аддитивной вибрации на процессы повреждения возможно в этих случаях только при условии контроля вибрационного воздействия, связанного как с процессами деформации, так и учета действующих динамических сил. Процессы деформации при вибрационном воздействии

определяются перемещением участков конструкционных элементов оборудования. Такие перемещения можно контролировать проксиметрами различного типа. Действие динамических сил может контролироваться акселерометрами, установленными на конструкционных элементах оборудования. Примеры аддитивных сигналов перемещения (деформации) *d* и ускорения *a*, представлены на рисунке 1.

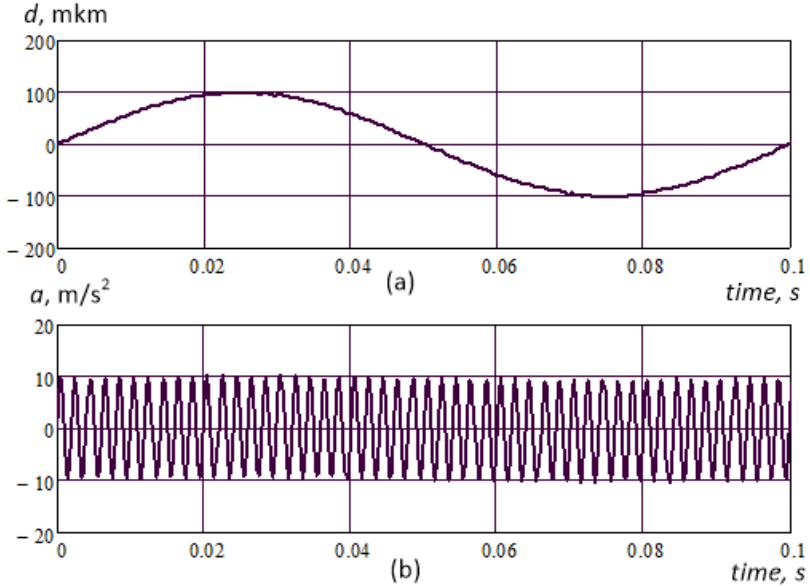


Рисунок 1 – Двухчастотная вибрация – сигналы перемещения и ускорения

Такая аддитивная смесь двух гармонических сигналов показывает, что такая вибрация в виде деформаций практически не зависит от вклада высокочастотной составляющей, а действующие динамические силы (ускорения) очень слабо реагируют на деформационные процессы низкочастотной вибрации. Такие особенности должны приниматься во внимание при создании алгоритмов работы систем вибрационного мониторинга, которыми оснащают современные сложные системы механического и электромеханического оборудования [4].

Такие особенности особенно существенны для оборудования с ограниченными усталостными прочностными характеристиками, например, электромеханического [5].

Указанные особенности относятся и к воздействию данных процессов. Пример сигнала от датчика ускорения в условиях воздействия удара и при наличии аддитивной высокочастотной вибрации приведен на рисунке 2. Особенностью ударных процессов является присущий им широкополосный ударный спектр в области повышенных частот. Сложное механическое оборудование, как правило, характеризуется наличием большого количества собственных резонансов.

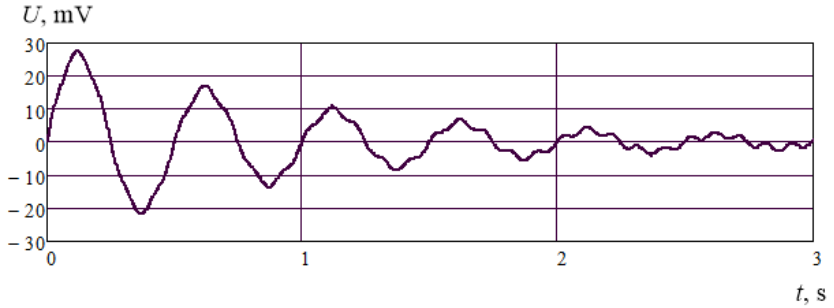


Рисунок 2 – Вибрационный сигнал с акселерометра в виде суммы оборотной вибрации и высокочастотных колебаний

Влияние резонансов может оказывать существенное влияние на снижение усталостной прочности. Это связано с тем, что широкополосный ударный вибрационный отклик возбуждает механические колебания конструкции на указанных резонансных частотах [6].

В этих условиях один и тот же вибрационный отклик по ускорению и перемещению имеет совершенно разный вид, как показано на рисунке 3. Перемещения (деформации), связанные с влиянием динамических сил, определяемых высокочастотной вибрацией, имеют малую величину по сравнению с низкочастотными деформационными процессами. При этом их вклад в снижение усталостной прочности материала может быть весьма значительным [3]. При контроле вибрационного отклика, как по перемещению, так и по ускорению получаем практически

независимые оценки, которые определяют возможности эксплуатации оборудования в условиях циклической усталости.

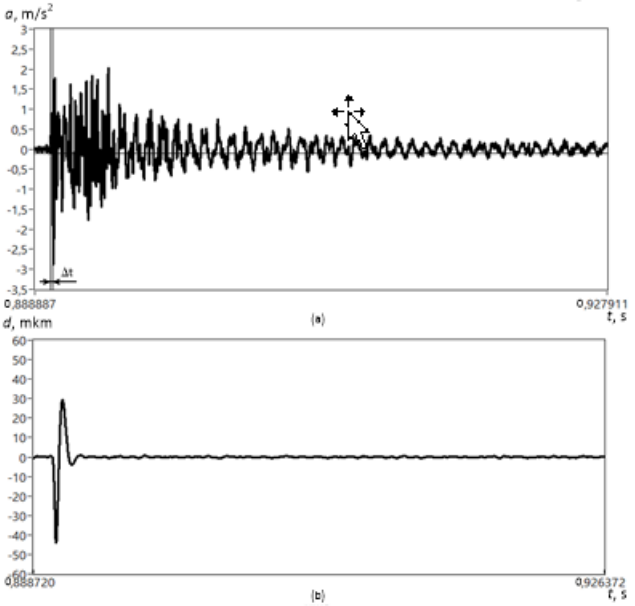


Рисунок 3 – Вибрационный отклик образца на ударное воздействие (элемент обмотки электромотора)

Влияние аддитивных составляющих при этом сказывается на получаемых оценках амплитуды и фазы механических колебаний, как показано на рисунке 4. Приведенные зависимости соответствуют влиянию затухающих резонансных процессов роторного агрегата при измерении параметров оборотной вибрации. Такие оценки важны при оценке дисбаланса практически любого роторного оборудования. На рисунке 4 показаны относительные погрешности оценок амплитуды (a), абсолютные погрешности оценок фазы (b) оборотной вибрации. Зависимости приведены для амплитуд этой составляющей при отсутствии (1) и наличии (2) аддитивных затухающих колебаний на частоте резонанса.

Рассмотренные особенности определяют требования к структурным решениям систем мониторинга вибрационного состояния сложного оборудования, которые необходимы для

обеспечения безопасности эксплуатации сложного технического оборудования. Такие особенности, к сожалению, пока не учитываются в нормативных документах, где перечислены требования к их техническим характеристикам [7].

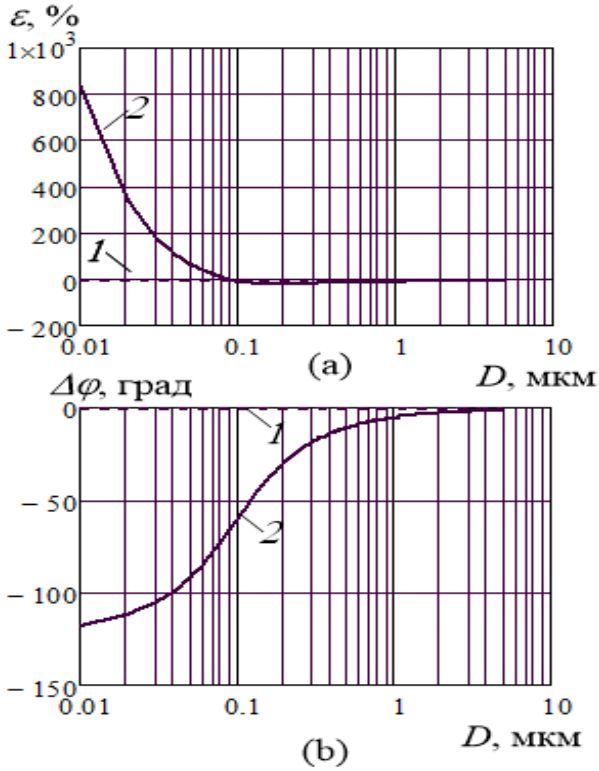


Рисунок 4 – Оценки погрешности измерения оборотной вибрации роторного оборудования

Заключение

При создании систем вибрационного мониторинга, диагностики и противоаварийной защиты сложного механического и электромеханического оборудования необходимо обеспечить параллельный синхронный контроль параметров деформационных и динамических силовых воздействий на конструкционные элементы такого оборудования, поскольку такие оценки характеризуют

различные физические изменения, влияющие на усталость материалов.

Литература:

1. *Скворцов О.Б.* Вибрационный мониторинг и прочность конструкционных элементов с учетом инерционных свойств материалов при воздействии широкополосной вибрации // Инженерный журнал: наука и инновации. – 2020. – № 6. – С. 1-17. – URL: http://engjournal.ru/articles/1986/1986.pdf (дата обращения 20.10.2022).

2. *Skvorcov O.B.* Selection of Vibration Norms and Systems Structures When Designing Means of Monitoring Units with Gear Transmissions / New Approaches to Gear Design and Production. – Springer, 2020. – P. 495-511.

3. *Махутов Н.А., Гаденин М.М., Резников Д.О., Неганов Д.А.* Анализ напряженно-деформированных и предельных состояний в экстремально нагруженных зонах машин и конструкций // Чебышевский сборник. – 2017. – Т.18. №3(63). – С. 390-412. DOI: 10.22405/2226-8383-2017-18-3-390-412

4. *Скворцов О.Б.* Вибрационный мониторинг энергетического оборудования и IIoT технологии / Четвертый междисциплинарный научный форум с международным участием «Новые материалы и перспективные технологии» (Москва, 27-30 ноября 2018 г.) Сборник материалов. Т. 1. – М: ООО «Буки Веди», 2018. – С. 804-809.

5. *Stashenko V.I, Skvorcov O.B., Troickij O.A.* Design of mechanical properties of structural materials for power plant equipment / 17th International School-Conference "New Materials: Advanced Technologies", IOP Publishing. – IOP Conf. Series: Materials Science and Engineering. – 2020. – 1005. – 012021. – P.7.

6. *Скворцов О.Б.* Влияние резонансных процессов на оценку параметров оборотной вибрации роторных узлов / Сборник докладов конференции «Инновационные технологии в электронике и приборостроении» Физико-технологического института РТУ МИРЭА. Том 1. – М.: РТУ МИРЭА, 2021. – С. 444-449.

7. *Скворцов О.Б.* Стандартизация и нормирование вибрационной усталости механизмов и машин / Проблемы управления безопасностью сложных систем. Материалы XXIX Международной научной конференции (15 декабря 2021 г., Москва). – М.: ИПУ РАН, 2021. – С. 528-533.

DOI: 10.25728/iccss.2022.58.54.056

Хабибулин Р.Ш., Кадиев Ш.К.

Поддержка управления реагированием на ЧС с учетом мнения специалистов центров управления в кризисных ситуациях

Аннотация: Показаны основные проблемы этапа реагирования на чрезвычайные ситуации в области определения необходимых ресурсов для ликвидации последствий. С помощью проведенного опроса среди сотрудников и специалистов центров управления в кризисных ситуациях обозначен для реализации комплекс информационных и программных средств, необходимый для решения задачи определения необходимого количества сил и средств для реагирования на чрезвычайную ситуацию.

Ключевые слова: опрос, чрезвычайная ситуация, корреляция, антикризисное управление, метод прецедентов, онтология, кластерный анализ

Реагирование на чрезвычайную ситуацию (далее – ЧС), как начальный этап жизненного цикла ликвидации последствий ЧС [1], должно соответствовать показателям своевременности и оперативности. От эффективности этих показателей зависит сохранность жизни и здоровья людей, а также материальных ценностей.

Таким образом, решение задачи своевременного реагирования на ЧС является актуальной проблемой в области ликвидации последствий. На сегодняшний день в Российской Федерации отсутствует единый регламент отправки сил и средств к месту чрезвычайной ситуации, поэтому, как правило, все решения по формированию необходимого состава людей и техники сводятся к старшему оперативному дежурному оперативно-дежурной смены центра управления в кризисных ситуациях (далее – ЦУКС). Проведенный ранее опрос сотрудников и специалистов [2] подтверждает ранее обозначенную проблему, вместе с тем, специалисты выделяют ранговую систему пожаров как базу для создания ранжированной системы ЧС (рисунок 1).

Рисунок 1 – Ответы специалистов на вопрос о ранжировании ЧС по примеру ранговой системы пожаров

На рисунке 1 видно, что 294 респондента считают возможным ранжирование системы ЧС, что составляет 84,5 % от общего числа опрошенных, еще около 7 % считают, что возможно, но по отдельным видам ЧС. Только 5 % опрошенных считают, что чрезвычайные ситуации невозможно ранжировать с целью определения ресурсов для реагирования из-за сложности оценки критериев ЧС в отличии от техногенного пожара. Вместе с тем 12 человек заявили, что классификация ЧС уже существует и нет необходимости в новой ранжированной системе. Тут необходимо пояснить, что действительно классификация ЧС существует и закреплена постановлением Правительства № 304 от 21. 05.2007 г. и включает в себя разделение ЧС по масштабам распространения и тяжести последствий, однако практического значения, в рамках определения необходимого количества сил и средств для реагирования, эта классификация не несет.

Таким образом, проведенный опрос подтвердил, что ранжирование ЧС является актуальной задачей в рамках совершенствования системы управления ликвидацией последствий ЧС. 297 респондентов также заявили о необходимости разработки системы поддержки принятия решений для определения сил и

средств реагирования на ЧС (рисунок 2). Вместе с тем, по результатам опроса были получены весовые коэффициенты критериев ЧС с целью поиска по методу прецедента.

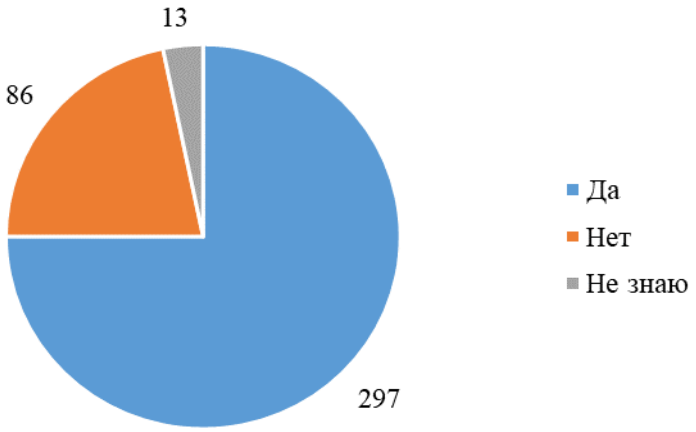


Рисунок 2 – Ответы на вопрос о необходимости поддержки принятия решений для определения сил и средств реагирования на ЧС

Подтверждается актуальность разработки комплекса программных и информационных средств поддержки должностного лица ЦУКС, отвечающего за отправку сил и средств к месту чрезвычайной ситуации с использованием методов машинного обучения (рисунок 3).

В предложенной системе при получении сообщения о ЧС лицо принимающее решение с помощью онтологических моделей получает описание типовых ситуаций при реагировании на ЧС, осуществляется поиск прецедентов реагирования с учетом весовых коэффициентов критериев ЧС, которые получены на основе результатов экспертного опроса. Определяющее значение имеет процедура кластерного анализа [3] ЧС, которая необходима для разбиения ЧС по группам на основе близости их характеристик. В результате происходит вывод решения в виде рекомендации по определению необходимого количества сил и средств для реагирования.

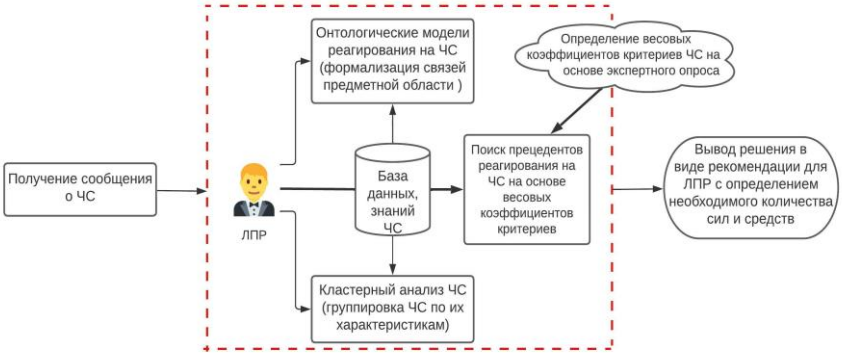


Рисунок 3 – Блок-схема поддержки решения ЛПР при получении сообщения о ЧС

Таким образом, определены проблемные вопросы существующего регламента отправки сил и средств к месту ЧС. Анализ проведенного анкетирования подтверждает проблематику предметной области и формирует направление дальнейшего исследования, сформирована блок-схема поддержки лица принимающего решения с интеграцией метода на основе онтологий, метода прецедентов и машинного обучения в виде кластерного анализа.

Литература:

1. *Кадиев Ш.К. Хабибулин Р.Ш.* Онтологический подход к выявлению проблем в области реагирования на чрезвычайные ситуации / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем». – Москва: ИПУ РАН, 2021. – С. 448-452.

2. *Кадиев Ш.К., Хабибулин Р.Ш., Рыженко Н.Ю.* Результаты анкетирования специалистов центров управления в кризисных ситуациях по вопросам реагирования на чрезвычайные ситуации // Технологии техносферной безопасности. – 2022. – Вып. 2 (96). – С. 103-122.

3. *Пранов Б.М.* Вопросы применения кластерного анализа в пожарной статистике // Технологии техносферной безопасности. – 2021. – № 4(94). – С. 117-124.

DOI: 10.25728/iccss.2022.82.10.057

Лещенко В.В.

О проблемах систем и средств спутниковой связи в России

Аннотация: Изложены результаты научно-исследовательской работы по сравнительному анализу результатов интеллектуальной деятельности в сфере систем и средств связи, в частности систем спутниковой связи, в России и за рубежом. Приведены статистические данные, характеризующие состояние проблемы развития средств связи в России. Предложено решение этой проблемы.

Ключевые слова: спутниковая связь, средства связи, 5G, патентный ландшафт, результаты интеллектуальной деятельности, сложная техническая система, Россия, мобильная связь, космический аппарат, персональная спутниковая связь

В коллективной работе [1] было отмечено, что система спутниковой связи (ССС) является сложной технической системой глобального масштаба. Соответственно она относится к большим системам, неотъемлемой частью которых является обеспечение их безопасности.

В части научно-технического отраслевого развития систем и средств связи в России показателен пример с персональной мобильной спутниковой связью.

В 2017 году в России услугой персональной спутниковой телефонной связи можно было воспользоваться только от четырех зарубежных операторов [2]:

– на геостационарных космических аппаратах (КА) – это «Инмарсат» и «Турайя»;

– на низкоорбитальных КА – «Иридиум» и «Глобалстар».

Российская низкоорбитальная система персональной спутниковой связи и передачи данных «Гонец» находилась на этапе отработки технических параметров. Развернутый сегмент этой системы имеет низкую пропускную способность (на несколько порядков меньше, чем «Иридиум») и работает в режиме электронной почты. Режим передачи голоса не поддерживается. Таким образом,

как отметил ученый секретарь ФГБУ НИИР М. М. Ступницкий, существующая группировка отечественных спутников связи, с учетом особенностей ее орбитального построения и характеристик полезных нагрузок, не отвечает требованиям перспективного развития нашей страны [2].

Основным показателем развития высокотехнологических сфер научно-технического развития, к которым относится система спутниковой связи, является результат интеллектуальной деятельности в них.

Во всем мире наблюдается рост патентной активности в сфере систем и средств связи (СиСС). За последние 20 лет различные компании, кроме российских, занимали лидирующие позиции по разработке инноваций в этой сфере. По данным Акционерного общества «Организация «Агат», являющимся головным экономическим научно-исследовательским институтом ракетно-космической промышленности России с 1973 г., текущая градация компаний по количеству поданных заявок в тематике СиСС с 2000 по 2020 г. представлена диаграммой на рисунке 1 [3], отражающей патентный ландшафт пяти ведущих в мире компаний в сфере СиСС.

Следует обратить внимание, что каждая из четырех компаний представленных диаграммой на рисунке 1, почти вдвое превосходит всю Россию по количеству заявок на выдачу патентов на изобретения и полезные модели, поданных в период с 2000 по 2020 год.

Компания SAMSUNG втрое превосходит Россию по этому показателю.

В настоящее время актуальным является патентование изобретений методов модуляции для систем связи 5G. В таблице 1 приведены данные по количеству патентов на изобретения методов модуляции для систем связи 5G по девяти странам.

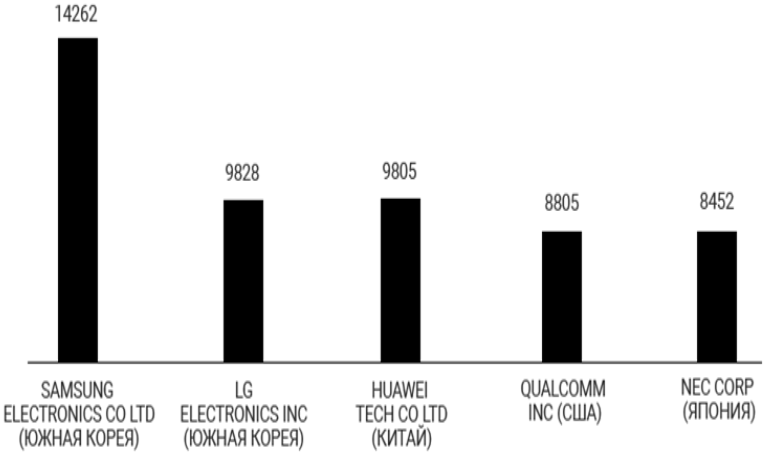


Рисунок 1 – Распределение количества поданных заявок в период с 2000 по 2020 год в сфере СиСС по компаниям

Таблица 1 – Количество патентов на изобретения методов модуляции для систем связи 5G по девяти странам

США	Китай	Корея	Европа	Япония	Австралия	Россия	Германия	Канада
19685	10784	4873	4627	2727	922	350	313	217

На рисунке 2 изображена диаграмма, отражающая патентный ландшафт методов модуляции для систем связи 5G, построенная по данным, приведенным в таблице 1.

Согласно исследованию [4], проведенному в ФГБУ НИИР, из 350 патентов на изобретения и полезные модели методов модуляции для систем связи 5G, выданных в России Роспатентом, только один патент выдан российскому заявителю.

К настоящему времени за рубежом выполнены разработки, проведены экспериментальные исследования, начато серийное производство и применение высокоскоростной космической связи.

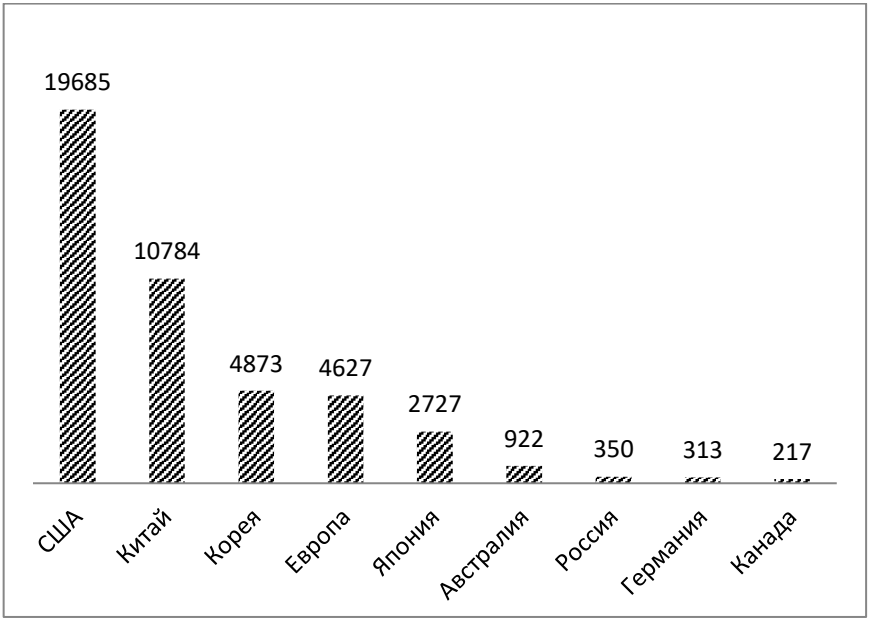


Рисунок 2 – Количество патентов на изобретения методов модуляции для систем связи 5G по девяти странам

К марту 2022 года SpaceX довела число спутников Starlink на орбите до 2000 — около 17 % от плана на 2027 год [5]. SpaceX запускает спутники на орбиту партиями по 60 штук с мая 2019 года. Каждый спутник весит 260 кг, а ступень для их запуска рассчитана на 100 миссий: каждый раз она возвращается на плавучую платформу Of Course I Still Love You.

Федеральная комиссия по связи США выдала разрешение SpaceX на запуск двух основных группировок, состоящих из 4425 и 7518 КА.

Другая спутниковая группа – OneWeb – это взаимосвязанная система спутников корпорации OneWeb, предназначенная для обеспечения широкополосного Интернета с помощью технологий мобильной спутниковой связи. OneWeb отправила на орбиту 428 аппаратов из 648 запланированных, выполнив программу по развертыванию своей системы спутниковой связи на 66 %.

На данный момент в России нет ничего подобного.

Поэтому стало очевидным, что для преодоления отсталости в сфере систем спутниковой связи России необходимо разработать и выполнить государственную программу создания сети спутниковой связи, аналогичной зарубежным [6].

Одним из основных показателей выполнения такой программы должны быть результаты интеллектуальной деятельности в сфере СиСС, и, в частности, систем спутниковой связи.

Опыт военных действий в последние два десятилетия показал всё возрастающее значение спутниковых систем связи для стратегического обеспечения национальной безопасности страны в современном мире.

Литература:

1. *Бакулин М. Г., Пантелеймонов И. Н., Мырова Л. О., Яхин И. Х., Лещенко В. В., Тодуркин М. В.* Основные перспективные направления системного проектирования сетей и систем спутниковой связи // Электросвязь. – 2022. – № 8. – С. 3.

2. *Ступницкий М. М.* Спутниковая связь в эпоху перехода к цифровой экономике // Спутниковые технологии, Connect WIT. – 2017. – № 11-12. – URL: https://www.connect-wit.ru/sputnikovaya-svyaz-v-epohu-perehoda-k-tsifrovoj-ekonomike.html/ (дата обращения 06.10.2022).

3. Дайджест патентной информации. Системы и средства связи. Август 2021. – URL: https://agat-roscosmos.ru/digests/sistemy-i-sredstva-svyazi-9/(дата обращения 05.10.2022).

4. *Девяткин Е. Е., Иванкович М. В., Бочечка Г. С., Кузнецов И. В.* Повышение эффективности сетей мобильной связи 5G – мировая гонка исследований // Электросвязь. – 2021.– № 6. – С. 58-59.

5. Starlink: как сверхскоростной интернет покоряет космос. – URL: https://trends.rbc.ru/trends/industry/5f72f4e39a7947caaf0f5bf1 (дата обращения 06.10.2022).

6. *Лещенко В.В.* Динамическое регулирование реализации государственной программы // Фундаментальные и прикладные исследования в современном мире «Стратегия будущего». – 2015. – № 12-2. – С. 51-55.

DOI: 10.25728/iccss.2022.79.52.058

Сташенко В.И., Скворцов О.Б.

Надежность электромеханического оборудования и импульсные ударные процессы

Аннотация: Рассмотрены вопросы обеспечения эксплуатационного контроля вибрации современного электромеханического оборудования. Действие механических динамических сил в условиях электроимпульсных воздействий связано с проявлением электропластического и вибропластического эффектов. Такое влияние необходимо учитывать в условиях длительной эксплуатации электромеханического оборудования и развития усталостных повреждений.

Ключевые слова: надежность, циклическая усталость, усталость, фреттинг, электрогенератор, импульсный инвертор, электрический импульс, вибрация, электропластический эффект, вибропластический эффект

Введение

Обеспечение надежной непрерывной работы мощного энергетического оборудования является важнейшей задачей создания критической инфраструктуры. Прочностные характеристики большей части электропроводящих элементов такого оборудования обычно существенно ниже, чем прочность несущих механических конструкций и определяется выбором материала по его электрическим и теплофизическим параметрам. С другой стороны, электропроводящие элементы обычно эксплуатируются в условиях как обычных механических динамических нагрузок [1], так и специфических динамических воздействий [2, 3], которые определяются динамическим электроимпульсным воздействием. Последние особенности особенно сильно проявляются в условиях воздействия электрических импульсов большой мощности [4]. Такие воздействия типичны для современного энергетического оборудования, работа которого связана с использованием импульсных преобразователей

энергии. Пример структуры с таким преобразованием представлен на рисунке 1.

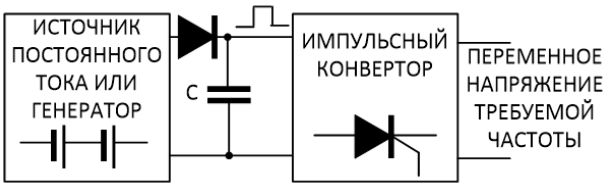


Рисунок 1 – Типовая структура преобразователя электрической энергии от источника постоянного тока (аккумулятора) или генератора переменного тока переменной частоты с использованием импульсного ключевого преобразователя

Механическое действие электрических импульсов в условиях нагружения электропроводящего материала получило название электропластического эффекта. Такой эффект нашел применение, например, при механической обработке металлов давлением с одновременным воздействием электрических импульсов, как показано на рисунке 2.

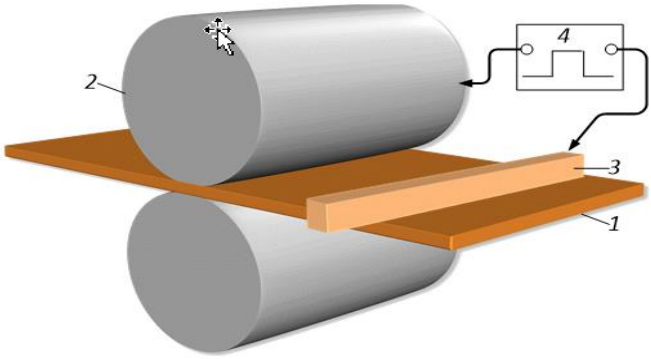


Рисунок 2 – Обработка металлической заготовки 1 давлением инструмента 2 с применением электропластического эффекта. На шину 3 и инструмент 2 поступают электрические импульсы от генератора 4

Простая технология обработки с использованием электропластического эффекта ограничивается необходимостью учета большого количества внешних влияющих факторов, определяющих результаты ее применения на практике. Некоторые из таких дополнительных факторов показаны на рисунке 3.

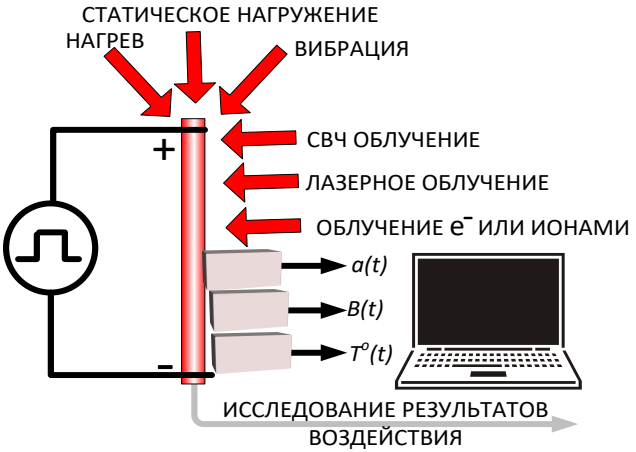


Рисунок 3 – Наличие внешних дополнительных факторов, оказывающих влияние на электропроводящую шину, используемую для передачи силовых электрических импульсов

В публикациях [2, 3, 5-7] было предложено несколько механизмов проявления электропластического эффекта, но общепризнаной теории на настоящее время нет. Сходные с электропластическим эффектом явления изменения пластических свойств материалов наблюдаются и при вибропластическом эффекте. При электроимпульсном воздействии в материале проводника наблюдаются значительные по амплитуде вибрационные колебания. Изучение таких вибрационных откликов может быть полезным при изучении механизмов электропластического эффекта и его применения для решения практических задач.

Изменение таких параметров электрического импульса как длительность и период позволяет изменять вибрационный отклик. При этом зависимость размаха вибрационных колебаний нелинейно

зависит от этих параметров. На рисунке 4 приведен пример такой зависимости от длительности электрического импульса *Т*и.

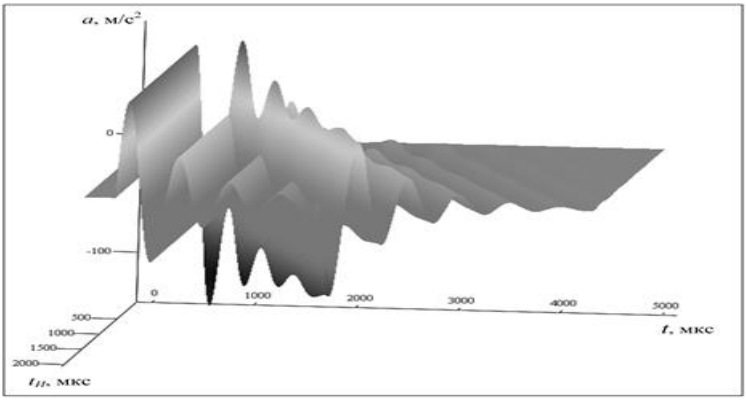


Рисунок 4 – Зависимости результата сложения вибрационных сигналов, формируемых под действием переднего и заднего фронтов импульса тока от длительности импульс

Действие электрических импульсов обеспечивает сравнительно малые деформации материала проводника, но такое воздействие может оказывать значительное влияние на зависимость процесса разрушения проводника от величины статического разрушения. Это можно. Это иллюстрируется зависимость напряжения от деформации, которая получена для испытаний проводящего образца на статической машине нагружения с дополнительным электроимпульсным воздействием, как показано на рисунке 5.

Статическое или низкочастотное деформирование проводниковых элементов оборудования в условиях электроимпульсного высокочастотного воздействия сопровождается сложными вибрационными процессами, которые влияют на усталость электропроводящих элементов. Эти эффекты необходимо учитывать при построении систем вибрационной противоаварийной защиты. Структура организации многоуровневой системы противоаварийной защиты (рисунок 6) с коррекцией уровней срабатывания по данным о наличие дефектов (из системы диагностики) и об износе (из системы прогнозирования).

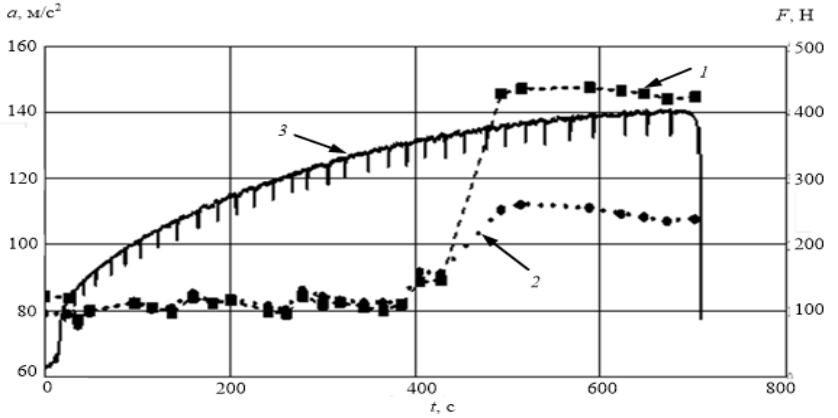


Рисунок 5 – Зависимость от деформации (времени) для максимального осевого ускорения кривая–*1*, перпендикулярного ускорения кривая –*2*, а также величины приложенной статической силы *F* кривая –*3* (шкала справа)

Рисунок 6 – Структура системы вибрационной противоаварийной защиты электромеханического оборудования

Литература:

1. *Скворцов О.Б.* Вибрационный мониторинг и прочность конструкционных элементов с учетом инерционных свойств материалов при воздействии широкополосной вибрации // Инженерный журнал: наука и инновации. – 2020. – № 6. – С. 1-17. – URL: http://engjournal.ru/articles/1986/1986.pdf (дата обращения 20.10.2022).

2. *Троицкий О.А., Сташенко В.И., Савенко В.С., Скворцов О.Б., Самуйлов С.Д., Правоторова Е.А., Терещук В.С*. Воздействия импульсами тока и СВЧ-изучением на конструкционные материалы. Электродинамические и электрохимические эффекты в проводниках. – М.: Издательство «Ким Л.А.», 2019. – 278 с.

3. *Троицкий О.А., Сташенко В.И., Скворцов О.Б., Савенко В.С., Самуйлов С.Д., Терещук В.С., Зайцев С.В., Иванов А.М*. Интенсивная пластическая деформация металла при токовых и СВЧ-воздействиях. Новые данные и закономерности. – М.: Издательство «Ким Л.А.», 2020. – 342 с.

4. *Сташенко В.И., Скворцов О.Б., Троицкий О.А.* Электродинамические процессы в проводниках при воздействии электрическими импульсами // Проблемы машиностроения и автоматизации. – 2021. – №1. – С. 39-47.

5. *Guan L., Tang G., Chu P.K.* Recent advances and challenges in electroplastic manufacturing processing of metals // Journal of Materials Research. – 2010. – Vol. 25. №. 7. – P. 1216-1224.

6. *Скворцов О.Б., Сташенко В.И., Троицкий О.А.* Влияние термического нагрева на вибрационный отклик проводников от электрического импульса / Материалы VI Международной научно-технической конференции «Современные методы и средства исследований теплофизических свойств веществ» (27-28 мая 2021 г.). – СПб.: Университет ИТМО, 2021. – С. 76-77.

7. *Скворцов О.Б., Сташенко В.И., Троицкий О.А.* Динамические эффекты в проводниках при воздействии импульсных токов // Вестник Сибирского государственного индустриального университета. – 2020. – № 1 (31). – С. 27-34.

VII. Автоматизированные системы и средства обеспечения безопасности сложных систем

DOI: 10.25728/iccss.2022.74.34.059

Сиротюк В.О., Богатырева Л.В.

Построение эффективной системы управления качеством и информационной безопасностью цифровых фондов интеллектуальной собственности

Аннотация: В работе рассмотрены цели, задачи и методы построения системы управления качеством и информационной безопасностью (СУКИБ) цифровых информационных фондов интеллектуальной собственности (ЦИФИС). Приведены характеристики информационных фондов и особенности построения баз данных (БД) ЦИФИС, требования к качеству и защищенности патентной и научно-технической информации ЦИФИС. Сформулированы критерии и показатели качества и информационной безопасности БД ЦИФИС. Рассмотрена формализованная методология построения эффективной СУКИБ, включающая решение задач выбора и оценки показателей качества и безопасности БД ЦИФИС, формирования базы метаданных репозитория ЦИФИС, выбора методов и средств повышения качества и защищенности данных, формирования ролевой структуры комплексной СУКИБ. Предложенные методы и средства использовались при разработке СУКИБ ЦИФИС региональной международной патентной организации.

Ключевые слова: система управления интеллектуальной собственностью, цифровой информационный фонд интеллектуальной собственности, база данных патентной информации, база данных научно-технической информации,

показатели качества данных, показатели защищенности данных, система управления качеством и информационной безопасностью

Введение

Цифровая трансформация системы управления интеллектуальной собственностью (ИС) позволяет повысить эффективность и качество работы патентных, научных и образовательных организаций и оказываемых ими услуг, перейти на новые бизнес-модели и методы управления и тем самым повысить их конкурентоспособность [1].

Эффективность построения и функционирования цифровых систем управления ИС во многом зависит от эффективности используемых методов и средств их проектирования, создания и сопровождения патентных (ПБД) и баз данных научно-технической информации (БД НТИ) цифрового информационного фонда интеллектуальной собственностью (ЦИФИС), обеспечения полноты, достоверности, доступности и защиты содержащейся в них информации [2, 3].

В работе рассмотрены характеристики информационных фондов ИС и особенности создания и сопровождения БД ЦИФИС, критерии и показатели качества и защищенности данных ПБД и БД НТИ, рассмотрены цели, задачи и методы построения эффективной комплексной системы управления качеством и информационной безопасностью (СУКИБ) ЦИФИС.

Характеристики фондов интеллектуальной собственности и особенности создания ПБД и БД НТИ ЦИФИС

Необходимым условием трансформации традиционной системы управления ИС и перехода к цифровому органу ИС является наличие и доступность информационных фондов патентной и научно-технической документации в цифровом виде.

Ответственность за полноту фондов патентной и научно-технической информации, достоверность, надежность, неизменность, актуальность и безопасность данных ЦИФИС несут его создатели – патентные организации, ведомства, издательства и редакции (публикующие организации), библиотеки, а также провайдеры патентно-информационных продуктов, поисковых и

сервисных услуг. Современный ЦИФИС имеет распределенную структуру и содержит фонд патентной документации, фонд научно-технической литературы и документации, фонд законодательной, нормативно-правовой и справочной информации в области интеллектуальной собственности [2].

Формирование, хранение и развитие фондов патентной, научно-технической и справочной информации ИС включает операции, связанные с получением документов, комплектованием и организацией хранения документов информационных фондов, переводом их в цифровую форму и загрузкой в соответствующие БД патентной информации (ПБД) и БД научно-технической информации (БД НТИ) ЦИФИС.

ПБД и БД НТИ содержат уникальную информацию по различным аспектам научно-технических, экономических, социальных, культурных и других видов знаний, которая используется при выполнении НИР и ОКР, проведении экспертизы работ, принятии решений по приоритетным направлениям научно-технологического развития и в других областях человеческой деятельности. Они относятся к типу документальных мультимедийных баз данных. Требования, предъявляемые к их составу и структуре более высокие, чем к традиционным документальным, библиографическим или фактографическим БД. Сложность их создания и эксплуатации увеличиваются в связи с тем, что в них загружаются и хранятся очень большие объемы информации. Эти особенности обусловливают повышенные требования к качеству и безопасности информации ПБД и БД НТИ.

Рассмотрим характеристики ПБД и БД НТИ.

ПБД хранят информацию о патентных документах конкретных стран, в которых подавались заявки на изобретения и выдавались патенты. ПБД относятся к типу документальных политематических баз данных. Каждая ПБД формируется патентной организацией путём обработки данных определённого источника патентной информации. Они должны проектироваться с учетом информационных и функциональных требований пользователей ЦИФИС и транзакций, а также требований и рекомендаций ВОИС и цифровых библиотек интеллектуальной собственности.

В БД НТИ хранится информация о статьях и публикациях из журналов, периодических изданий, книгах, нормативно-

методических документах, законодательных актах, справочной литературы и других информационных материалах. БД НТИ относятся к типу документальных мультимедийных баз данных категории больших данных (Big Data). Информация БД НТИ содержит, как правило, реферативно-библиографическое описание документа, аннотацию и полный текст документа.

Построение эффективных структур БД ЦИФИС должно осуществляться с учетом как общесистемных требований предметной области системы управления ИС, так и требований эффективного обслуживания множества запросов пользователей.

Для проектирования ПБД и БД НТИ могут использоваться как структурные, так и объектно-ориентированные методы, рассмотренные в [4]. При этом объектно-ориентированные модели и методы наиболее полно, естественно и адекватно отражают технологию формирования, представления и использования информации об объектах и субъектах системы управления ИС, хранимой в соответствующих ПБД и БД НТИ ЦИФИС.

Критерии и показатели качества и защищенности БД ЦИФИС

Общим критерием качества и безопасности патентной и научно-технической информации является степень ее соответствия целям использования, например, проведения патентной экспертизы, выполнения НИР и ОКР, реализации патентно-информационных поисков, коммерциализации результатов интеллектуальной деятельности и т.п.[5].

Частными критериями качества данных и информационной безопасности ЦИФИС являются полнота, достоверность, корректность, согласованность, актуальность и своевременность данных ПБД и БД НТИ, обеспечение заданного уровня конфиденциальности, неизменности и доступности данных.

Основными показателями качества БД ЦИФИС являются: полнота, достоверность, актуальность, доступность и своевременность данных. Формальные методы оценки показателей качества данных БД ЦИФИС рассмотрены в [2, 6].

Требуемое качество данных достигается путем решения следующих задач: выбор системы критериев и показателей оценки качества данных, расчет показателей качества данных в бизнес-

процессах и задачах управления, обеспечение непрерывного контроля качества данных на основе выявления, идентификации и классификации ошибок в данных, разработка мероприятий по повышению качества данных.

Высокий уровень информационной безопасности ПБД и БД НТИ достигается разработкой и внедрением формализованных моделей и методов анализа и синтеза оптимальных механизмов защиты структур БД на различных уровнях их представления (концептуальном, логическом, физическом) и построением системы защиты ЦИФИС от несанкционированного доступа [3].

Комплексное решение задач повышения качества и защищенности данных ЦИФИС может осуществляться в рамках построения как отдельных систем управления качеством данных (СУКД) и информационной безопасностью (СУИБ), так и комплексной системы управления качеством и информационной безопасностью (СУКИБ) ЦИФИС с назначенными ролями и функциональными обязанностями служащих организации.

Разработка комплексной системы управления качеством и информационной безопасностью ЦИФИС

Система управления качеством и информационной безопасностью (СУКИБ) ЦИФИС является неотъемлемой составляющей (подсистемой) общей административной системы управления ИС со встроенными в нее функциями, обязанностями и ролями служащих по обеспечению надлежащего уровня качества и информационной безопасности патентной и научно-технической информации.

Целью создания СУКИБ ЦИФИС является обеспечение заданного уровня качества, эффективности и защищенности научно-технической, патентной и справочной информации.

Область действия СУКИБ ЦИФИС охватывает восемь основных бизнес-процессов, связанных с производственной деятельностью субъектов системы управления ИС:

– обработка входящей информации по объектам ИС (результатам интеллектуальной деятельности);
– формирование и обслуживание ПБД и БД НТИ ЦИФИС;
– проведение патентно-информационных поисков;
– проведение экспертизы по заявкам на объекты ИС;

– выполнение НИР и ОКР;

– выдача охранных документов на объекты ИС;

– публикация и сопровождение информации по объектам ИС;

– сопровождение опубликованных материалов (патентов, авторских свидетельств, произведений науки, искусства, литературы), регистрация изменений правового статуса объектов ИС.

Основными задачами построения и функционирования СУКИБ являются:

– формирование и ведение базы метаданных (БмД) репозитория ЦИФИС, содержащей, формализованные описания предметной области системы управления ИС, требований пользователей ЦИФИС, бизнес-процессов системы управления ИС, структур БД и др. сведения;

– оценка качества данных и защищенности информационных активов ЦИФИС в соответствии с выбранными критериями и показателями оценки;

– анализ результатов оценки с целью выявления проблем, вызывающих снижение качества и эффективности данных и уровня их безопасности;

– формирование сценариев (шаблонов) действий по исправлению неточностей и ошибок в данных в зависимости от причин их возникновения, а также механизмов защиты информационных активов БД ЦИФИС, основанных на анализе рисков информационной безопасности. Хранение сценариев и механизмов защиты в БмД репозитория;

– разработка методов и мероприятий для решения проблем с качеством данных при обнаружении несоответствий и их применение в соответствии с заданными сценариями (шаблонами) БмД репозитория;

– разработка мер и мероприятий по обеспечению заданного уровня конфиденциальности, неизменности и доступности данных ЦИФИС, защиты информационных активов БД НТИ и ПБД от несанкционированного доступа с использованием механизмов защиты БД и БмД репозитория ЦИФИС;

– обеспечение непрерывного контроля качества патентной и научно-технической информации, выполнения требований к уровню

информационной безопасности и усовершенствование данных;

– обеспечение соответствия правовым и нормативным требованиям законодательства и нормативно-правовых документов в области качества данных и защиты информации;

– обеспечение осведомленности служащих организации в вопросах качества данных и информационной безопасности.

Комплексное управление качеством и информационной безопасностью данных ЦИФИС опирается на три элемента: 1) организационная структура СУКИБ, 2) процессы управления качеством и ИБ и 3) методы и инструментальные средства управления качеством и ИБ.

В СУКИБ используется ролевая организационная структура, которая представляет собой иерархию ролей по обеспечению качества и защищенности научной, технической и патентной информации в соответствии с основными процессами управления качеством данными и информационной безопасности.

В рамках СУКИБ ЦИФИС организации можно выделить следующие основные роли:

– представитель руководства организации;

– председатель рабочей группы (подразделения)по контролю качества данных и ИБ;

– управляющий (менеджер) данными;

– администратор данных;

– специалист по обработке данных;

– специалист по управлению ИБ;

– специалист по управлению информационными технологиями;

– владелец информационного актива;

– владелец технологического бизнес-процесса;

– внутренний аудитор СУКИБ.

Процессы управления качеством и ИБ ЦИФИС включают 3 основных процесса: процесс выполнения операций над данными; процесс непрерывного анализа и контроля качества и защищенности данных и процесс повышения качества и уровня ИБ ЦИФИС. Роли и процессы управления качеством и ИБ СУКИБ взаимосвязаны и взаимодействуют в рамках установленной (действующей) оргструктуры системы управления ИС.

Методами управления качеством и ИБ являются предложенные в работах [2-4] формализованные модели и методы оптимизации структур БД ЦИФИС, управления качеством данных и обеспечения информационной безопасности и защиты БД. Их использование обеспечивает построение эффективных структур данных и механизмов защиты БД от несанкционированного доступа, а также позволяет производить оценку основных показателей качества данных (полноты, актуальности, достоверности и доступности) и защищенности информации БД ЦИФИС (рисков и угроз ИБ).

Инструментальные средства управления качеством и ИБ данных представлены на рынке ИТ системами и программными продуктами класса Data Quality, системами управления Master DB и базами метаданных, другими специализированными средствами для решения задач повышения эффективности, качества и уровня информационной безопасности данных [3].

Заключение

В работе рассмотрены характеристики информационных фондов ИС и особенности проектирования и эксплуатации БД ЦИФИС, требования к качеству и защищенности данных ПБД и БД НТИ, сформулированы критерии качества и защищенности ПБД и БД НТИ ЦИФИС, определена область действия СУКИБ ЦИФИС. Предложена формализованная методология и рассмотрены задачи и методы построения эффективной СУКИБ ЦИФИС. Полученные результаты использовались при построении системы управления качеством и информационной безопасностью Евразийского патентного ведомства – международной региональной патентной организации [7].

Литература:

1. Программа «Цифровая экономика Российской Федерации». Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. – URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 20.09.2022).

2. *Кульба В.В., Сиротюк В.О.* Формализованная методология повышения эффективности и качества патентных информационных фондов и опыт ее использования при формировании и развитии

евразийского патентно-информационного пространства. – М.: ИПУ РАН, 2019. – 236 с.

3. *Кульба В.В., Сиротюк В.О., Косяченко С.А.* Информационная безопасность патентных ведомств: теория и практика. – М.: ИПУ РАН, 2017. – 166 с.

4. *Кульба В.В., Ковалевский С.С., Косяченко С.А., Сиротюк В.О.* Теоретические основы проектирования оптимальных структур распределенных баз данных. Серия «Информатизации России на пороге XXI века». – М.: СИНТЕГ, 1999. – 660 с.

5. *Сиротюк В.О.* Цели, задачи и принципы обеспечения безопасности цифровых систем управления интеллектуальной собственностью / Материалы 29-й Международной научной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС'2021, Москва). – М.: ИПУ РАН, 2021. – С. 182-188.

6. *Сиротюк В.О.* Методы анализа и оценки показателей качества патентных данных, используемых при формировании и развитии распределенных патентных информационных фондов / Труды 14-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD-2021). – М.: ИПУ РАН, 2021. – С. 1467-1478.

7. Материалы веб-портала Евразийской патентной организации [Электронный ресурс]. – URL: http://www.eapo.org (дата обращения 12.03.2022).

DOI: 10.25728/iccss.2022.41.63.060

Сидоренко В.Г.

Математические модели и методы управления безопасностью транспортных систем

Аннотация: Работа посвящена анализу возможностей применения различных типов математического аппарата к решению задач управления безопасностью транспортных систем и полученных результатов.

Ключевые слова: безопасность движения, машинное обучение, прогнозирование, транспортная система, теория графов

В [1] определены вызовы безопасности городских транспортных систем, основой для решения которых является комплексный подход к решению задач управления ресурсами разных типов с использованием единого математического аппарата, который базируется на разностороннем анализе статистических данных, использовании методов системного анализа, машинного обучения, генетических алгоритмов, теории управления, оптимизации, графов, экстраполяции.

Получение синергетического эффекта определяется уровнем развития интеллектуальной системы управления производственными ресурсами городской рельсовой транспортной системой (ИСУ ПР ГРТС), синтез структуры которой проведен на базе основных положений теории систем и теории графов [2, 3].

Разработанная архитектура позволяет решать в рамках единого информационного пространства задачи планирования перевозочного процесса, управления движением на разных уровнях, оценки качества движения, управления персоналом, связанного с управлением движением, диагностики исправной работы объектов ГРТС, связанных с управлением движением, и информационного обмена. ИСУ ПР ГРТС включает в себя следующие системы, автоматизирующие процессы, связанные с ресурсами разных типов.

Отличительной чертой ИСУ ПР ГРТС является необходимость собирать и обрабатывать большие объемы гетерогенной информации (данные, речь, видео, результаты телеизмерений и телесигнализации, команды удаленного управления, в том числе ответственные, данные систем контроля доступа на инфраструктуру и др.) с неподвижных и подвижных объектов с соблюдением высоких стандартов защиты от несанкционированного доступа к этой информации. В основе построения маршрутизации лежит использование полносвязной сети. Это позволяет значительно увеличить пропускную способность сети и выполнить требования по защите информации, так как информационные потоки формируются на базе однотипных протоколов с использованием шифрованных меток информационных потоков, что препятствует образованию скрытых каналов передачи.

Взаимодействие элементов ИСУ ПР ГРТС должно быть организовано на основе комбинации подходов, используемых в

области *BigData*, сочетания методологии интернета вещей (*IoT*) и микросервисной архитектуры [3].

Теория графов также находит применение при решении задач централизованного управления совокупностью транспортных средств, анализе топологии транспортной системы и надежности элементов ее инфраструктуры, планировании работы сотрудников ГРТС, разработке графических моделей процессов, автоматизируемых в ИСУ ПР ГРТС [4, 5].

Анализ результатов применения разработанного алгоритма поиска рационального графика работы основных машинистов для Замоскворецкой и Таганско-Краснопресненской линий Московского метрополитена показал возможность экономии трудовых ресурсов машинистов в случае применения автоматизированного планирования их труда на 10-25 %, а также труда сотрудников, составляющих этих графики в случае его автоматизации на основе разработанных алгоритмов [3].

Разработка эвристических алгоритмов централизованного управления движения транспортными средствами ГРТС при компенсируемых возмущениях базируется на учете зависимости ограничений от состояния системы и прогноза случайных возмущений, приводящих к увеличению длительности стоянки с использованием экстраполяторов на базе многочленов Чебышева, работающих в реальном времени [3].

Комплексное решение задач энергооптимального беспилотного управления совокупностью транспортных средств ГРТС позволит обеспечить необходимый уровень качества предоставления транспортных услуг, развитие «зеленой» экономики и бережливого производства на основе использования ранее не доступной в режиме реального времени информации о ходе предоставления транспортных услуг имеет большое значение в современных условиях.

Экстраполяторы также нашли свое применение при обработке информации в реальном времени для оценки состояния транспортных средств при решении задач предиктивной диагностики [3].

Использование положений теории вероятности позволяет решать задачи повышения точности систем технического зрения, используемых для предотвращения столкновения движущегося

поезда с препятствием на пути и обеспечить вероятность опасного отказа, в данном случае – вероятность наезда на препятствие, не более 10 в степени (-8) при доверительной вероятности 0,95 по SIL-4 (ГОСТ-Р61508) путем использования алгоритмов многократных измерений до препятствия [6].

Применение различных метод проверки статистических гипотез, например, о равенстве выборочного среднего у двух наборов данных, отличающихся наличием или отсутствием какого-либо аномального состояния, позволили выявить признаки, которые являются значимыми для определения состояния тяговых электродвигателей (ТЭД) транспортных средств или уровня надежности машинистов транспортных средств [3].

Генетические алгоритмы показали свою эффективность при решении широкого круга задач, связанных с планированием использования человеческих и технических ресурсов при составлении планового графика движения транспортных средств, графика оборота подвижного состава, графика работы коллективов работников, обладающих различными компетенциями для выполнения разного вида работ в рамках одного множества [3].

Применение генетических алгоритмов дало положительный эффект, заключающийся в уменьшении времени решения поставленных задач, генерации большого числа допустимых вариантов решения задачи, возможности учета различных ограничений.

Желаемый баланс показателей комфорта при перевозке пассажиров, эффективности работы персонала, поддержания в исправном состоянии транспортных средств на протяжении длительного периода времени, а также затрат энергетических ресурсов во многом обеспечивается за счёт соблюдения принципов равномерности при решении задач планирования [4].

Методы машинного обучения применены для решения задач предиктивной диагностики состояния транспортных средств ГРТС, в частности, разработан алгоритм расчёта вероятности выхода из строя тягового электродвигателя и синтезирована архитектура автокодировщика, решающего эту задачу. Данный алгоритм позволит определять ТЭД с аномальным состоянием [3].

Создание и апробация новых моделей оценки влияния квалификации сотрудников ГРТС и графика их работы на

безопасность движения и показатели эффективности функционирования ГРТС, а также методики снижения этого влияния, речевых технологий и сценарного подхода включало в себя несколько направлений работы.

Комплексный анализ работы машиниста и влияния его квалификации на безопасность движения и показатели эффективности функционирования ГРТС включает в себя следующие направления, решаемые на базе использования технологий искусственного интеллекта и *BigData*:

– расчёт вероятности совершения нарушения машинистом в предстоящей поездке и расчёт уровня надежности машиниста;

– определение рейтинга машиниста;

– математическая модель прогнозирования типа будущих нарушений в зависимости от ранее совершаемых нарушений.

На основе объединения результатов работы алгоритмов происходит разбиение машинистов на группы надежности, автоматизированное формирование списка мероприятий по повышению уровня безопасности движения, контроль проверки их выполнения и анализ достигнутых результатов.

Внедрение подсистемы распознавания речи существенно облегчит процесс взаимодействия сотрудников ГРТС [7].

В качестве основного требования к подсистеме распознавания речи в рамках средств электронного обучения и повышения квалификации персонала, в частности, поездных диспетчеров, выступает точность и надежность модуля преобразования аудиофайла в текст, а также точность разбиения текста на реплики диспетчера и других работников. Система включает модули классификации текста по типу команды, поиска команд в тексте, поиска субъектов и станций в тексте.

Для достижения поставленной цели был разработан классификатор текста по типу сообщения в нем.

В результате обучения нейронной сети классификации предложений на протяжении 100 итераций обучения была достигнута точность прогноза порядка 94-96 % на тестовой выборке.

Сформирован классификатор управляющих команд.

Команды можно классифицировать по объекту управления (команды управления маршрутами, команды управления стрелками

и сигналами) и типу действий (запрет на движение, разрешение на движение и др.).

Разработан алгоритм классификации команд диспетчера на основе обработки текста.

В результате проведенных исследований получены следующие показатели качества распознавания слитной речи: 98,3 % правильно распознанных команд, 0,5 % ошибочно распознанных команд, 1,2 % нераспознанных команд.

Совместно с иностранными студентами исследования проводились не только для русского, но и для китайского и узбекского языков.

Таким образом, в ходе выполнения исследований создана теоретическая база для комплексного решения задач управления безопасностью производственных ресурсов транспортных систем.

Благодарности. Исследование выполнено при финансовой поддержке РФФИ, НТУ «Сириус», ОАО «РЖД» и Образовательного Фонда «Талант и успех» в рамках научного проекта № 20-37-51001.

Acknowledgments. The reported study was funded by RFBR, Sirius University of Science and Technology, JSC Russian Railways and Educational Fund "Talent and success", project number 20-37-51001.

Литература:

1. *Сидоренко В.Г.* Современные вызовы безопасности городских транспортных систем / Материалы XXVIII Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2020. – С. 434-439. DOI: 10.25728/iccss.2020.35.36.079

2. *Кульба В.В., Ковалевский С.С., Косяченко С.А., Кузнецов Н. А.* Методы анализа и синтеза модульных информационно-управляющих систем. − М.: Физматлит, 2002. − 800 с.

3. *Баранов Л.А., Сидоренко В. Г., Балакина Е. П., Логинова Л.Н., Сафронов А.И.* Комплексное решение задач планирования и управления движением городских рельсовых транспортных средств / Сборник трудов международной научно-практической конференции, посвященной 125-летию Университета «Академик Владимир Николаевич Образцов – основоположник

транспортной науки». – М.: РУТ(МИИТ), 2021. – С. 56-64. DOI: 10.47581/2022/Obrazcov.09

4. *Сафронов А.И.* Доступность рельсовых транспортных систем города Москвы / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем». – Москва: ИПУ РАН, 2021. – С. 336-342.

5. *Баранов Л.А., Ермолин Ю.А.* Надежность транспортирующих систем водоотведения крупных городов // Надежность. – 2022. – №2. – С. 3-9.

6. *Баранов Л.А., Бестемьянов П.Ф., Балакина Е.П., Охотников А. Л.* Методология обоснования требований безопасности при использовании систем технического зрения в интеллектуальных системах управления движением поездов / Материалы Международной научно-практической конференции «Интеллектуальные транспортные системы». – М.: РУТ (МИИТ), 2022. – С. 54-58.

7. *Балакина Е.П., Кулагин М.А., Логинова Л.Н., Сидоренко В.Г.* Обеспечение безопасности применения речевых технологий в работе оперативного персонала городских рельсовых транспортных систем / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2021. – С. 355-361.

DOI: 10.25728/iccss.2022.16.56.061

Чернов И.В., Шелков А.Б.

Сценарный анализ проблем развития строительной отрасли в современных условиях

Аннотация: Рассмотрен комплекс проблем повышения эффективности управления развитием строительного комплекса в новых условиях. Представлены результаты сценарного анализа влияния административных барьеров и экономических последствий внешнего санкционного давления на предприятия отрасли.

Ключевые слова: управление, сценарный анализ, строительная отрасль, административные барьеры, санкции

Введение

Капитальное строительство является одной из ведущих отраслей национальной экономики России, выступающей по сути «локомотивом» развития многих смежных отраслей, а также играющей во многом определяющую роль в социально-экономическом развитии России. Современный строительный комплекс представляет собой крайне сложную в управлении (в силу множественности и многогранности экономических, организационных и производственных связей) и материалоемкую (характеризующуюся большими объемами и значительным многообразием номенклатуры используемых материалов, конструкций, оборудования и т.д.) отрасль.

Одновременно с этим строительная отрасль характеризуется значительной зависимостью от целого ряда внешних факторов (общих для страны экономических проблем, устойчивости кредитно-финансовой сферы, организационно-технических проблем во взаимодействии подрядных, снабжающих, транспортных и контролирующих организаций и предприятий и т.д.).

1. Сценарный анализ влияния административных барьеров на развитие строительной отрасли

Отдельную и крайне серьезную проблему представляет характерное для отрасли большое количество разнообразных избыточных административных барьеров, преодолевать которые строительным организациям приходится в течение всего цикла работ – от подготовки земельного участка до государственной регистрации прав собственности на построенные объекты [1].

В настоящее время административные барьеры представляют собой одно из наиболее серьезных «окон» уязвимости отечественного строительного комплекса, способствующих постоянному самовоспроизводству свойственных рассматриваемой отрасли проблем, в том числе и выходящих далеко за рамки простых бюрократических проволочек (коррупция, монополизация рынка, падение инвестиционной привлекательности, снижение объемов строительного производства и т.д.) [2].

Во многом негативное влияние на рассматриваемую отрасль и сложность преодоления данных барьеров определяется целым рядом недостатков действующей системы нормативно-правового

регулирования строительного комплекса [3]. Большое количество сопровождающих капитальное строительство административных процедур, длительные сроки и высокая стоимость их прохождения существенно снижают эффективность инвестиционно-строительного сектора экономики. Они также приводят к значительным прямым и косвенным потерям, способствующим обострению существующих и появлению новых социально-экономических проблем государственного и регионального развития.

С использованием разработанной сценарной модели проведен анализ влияния административных барьеров на эффективность развития строительного комплекса (структура базовой модели представлена на рисунке 1). В рамках моделируемой ситуации рассмотрены проблемы реализации комплекса мер по снижению количества, затрат времени на реализацию (документальное оформление) и стоимости административно-бюрократических процедур в строительной отрасли, а также повышения их прозрачности в том числе на базе современных цифровых технологий.

Как показали результаты исследования разработанной модели, сокращение избыточных требований и количества необходимых для реализации строительства документов и согласований, а также цифровизация и обеспечение прозрачности контрольно-надзорных процедур являются крайне важным направлением совершенствования системы нормативно-правового регулирования рассматриваемой отрасли, поскольку напрямую способствуют наращиванию объемов капитального строительства и снижению издержек инвестиционно-строительного цикла.

Одновременно с этим избыточные административные барьеры и бюрократические процедуры являются существенной, но далеко не единственной проблемой, препятствующей эффективному развитию отрасли в условиях внешнего санкционного давления.

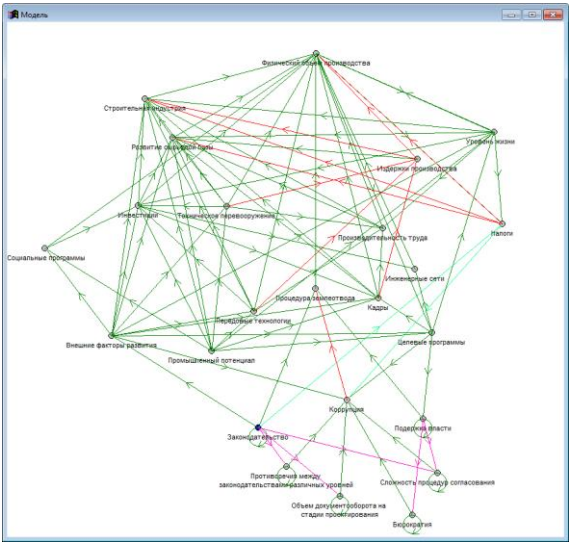


Рисунок 1 – Модель влияния административных барьеров

2. Анализ и моделирование проблем строительных организаций и холдингов

В настоящее время у многих строительных организаций возникает целый ряд принципиально новых проблем, являющихся следствием санкционной политики консолидированного Запада, а также попыток изоляции России от внешних рынков.

С одной стороны, как показывает анализ, санкционное давление на отечественную строительную отрасль носит все же в большей степени секторальный характер, поскольку, например, по имеющимся оценкам доля используемых в строительстве российских материалов за исключением элитного сегмента капитальных строений составляет порядка 95 % [4]. С другой стороны, сегодня достаточно существенна доля импортного инженерного оборудования, строительной техники и т.д., что вызывает целый ряд проблем. Определенные трудности вызывает и рост стоимости некоторых стройматериалов, в том числе как следствие зависимости производящей их промышленности от зарубежных поставок сырья, оборудования и комплектующих. Одновременно с этим некоторые позиции импортных отделочных

материалов, (которые не производятся отечественными предприятиями) кратно выросли в цене [5]. Аналогичная ситуация и с лифтовым и другим инженерно-техническим оборудованием. Нельзя не отметить и определенные проблемы с приемлемостью условий финансирования и кредитования предприятий отрасли. В сложившейся ситуации рост себестоимости строительства приходится покрывать за счет снижения маржинальности по проектам и частично перекладывать на конечного потребителя.

Проведенный сценарный анализ проблем развития строительного комплекса в условиях внешних экономических санкций показал, что наибольшие трудности в связи с описанными выше негативными процессами возникают малых и средних предприятий отрасли (структура модифицированной сценарной модели предсталена на рисунке 2).

Анализ полученных в ходе исследования модели сценариев показал, что крупные строительные организации (финансово-, инвестиционно- и промышленно-строительные холдинги и корпорации) более успешно справляются с возникающими пробемами (включая и рассмотренные выше административные барьеры). Но даже они в кратковременном переходном периоде трансформации рынка и логистики могут испытывать трудности от возникновения рассматриваемых проблем (графики 1-3 на рисунке 3).

Одновременно с этим холдинги в конечном итоге выходят из подобных «шоковых ситуаций» на успешный сценарий развития за счет объединения производственных возможностей нескольких входящих в их состав хозяйствующих субъектов, высокого уровня их кооперированности и возможности маневрирования имеющимися ресурсами. Для отдельных и относительно небольших организаций положение прямо противоположное, что иллюстрируется графиком 4 на рисунке 3.

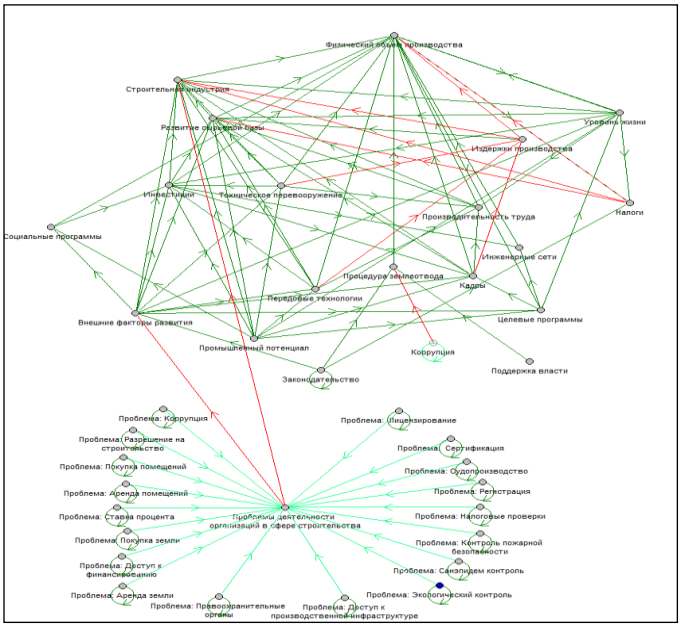


Рисунок 2 – Модель анализа проблем развития строительного комплекса

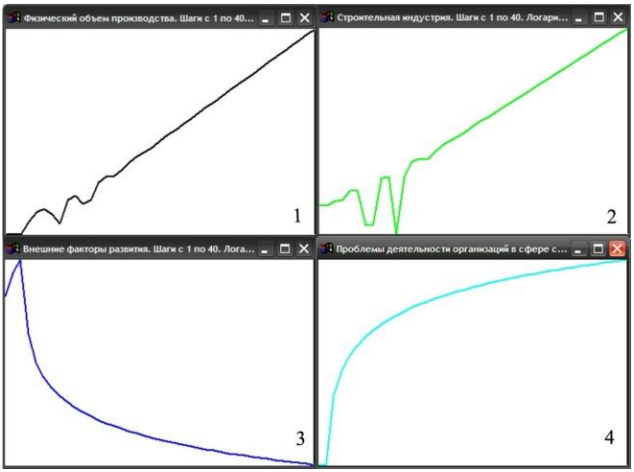


Рисунок 3 – Результаты моделирования (фрагмент)

Заключение

Стратегическую роль строительной отрасли в развитии национальной экономики в условиях внешнего санкционного давления трудно переоценить, в силу этого строительный комплекс нуждается в целенаправленной, систематической, комплексной и долгосрочной государственной поддержке на различных уровнях.

Одновременно с этим в реалиях сегодняшнего дня процессы подготовки решений в рассматриваемой предметной области должны опираться на многофакторный сценарный прогноз поведения как самого объекта управления, так и его окружения (внешней среды), позволяющий выделять совокупность ключевых факторов риска и диагностировать «окна» уязвимости на различных временных горизонтах.

В настоящее время накоплен значительный опыт использования методологии сценарного анализа для решения прикладных и практических задач организационного управления, который может быть использован в качестве методологической базы для дальнейшего развития мультидисциплинарных исследований в рассматриваемой предметной области.

Литература:

1. *Полиди Т.Д.* Жилищное строительство в России: инвестиционный климат и административные барьеры // Имущественные отношения в РФ. – 2014. – № 2 (149). – С. 89-99.

2. *Скупов Б.А.* Призрак дебюрократизации появляется в сфере отечественного строительства // Информационный портал «Строительный эксперт». 27 марта 2021. – URL: https://ardexpert.ru/article/20340?ysclid=l96thbx26q207300259 (дата обращения 12.10.2022).

3. *Терентьев В.А.* Административные барьеры в строительстве и пути их преодоления // Строительная орбита. – 2018. – № 10. – С. 230-232.

4. Как санкции влияют на рынок строительства и недвижимости. – URL: https://www.spsss.ru/news/2022/ (дата обращения 12.10.2022).

5. *Данилов А.А.* Как меняется строительный рынок в эпоху санкций. – URL: https://www.novostroy.ru/articles/expert/kak-menyaetsya-stroitelnyy-rynok-v-epokhu-sanktsiy/ (дата обращения 10.10.2022).

DOI: 10.25728/iccss.2022.46.38.062

Сидоренко И.А., Силюнцев С.В., Кураков В.А.

Оценка временных показателей решения задач радиомониторинга перспективной пространственно-распределенной системой

Аннотация: Приведены результаты экспресс-оценки требуемых показателей заблаговременного решения задач радиомониторинга пространственно-распределенной системой радио- и радиотехнического контроля в условиях конфликтного взаимодействия с системой технической разведки.

Ключевые слова: информационный конфликт, средства радио- и радиотехнического контроля, технические средства разведки

Стремительное развитие и повсеместное применение современных радиоэлектронных систем, применяемых для решения широкого спектра задач разведки, связи, навигации, радиоэлектронной борьбы и других не менее важных задач, значительно увеличивает нагрузку на радиочастотный спектр, усложняя задачу ведения радио- и радиотехнического контроля (РРТК). Учитывая количество, мощности и диапазон рабочих частот современных радиоэлектронных систем, можно сделать вывод, что усовершенствование радиоприемных устройств проходит не так оперативно, а вследствие чего становится невозможным одновременный охват всех объектов РРТК. Кроме того, сейчас наблюдается интенсивный рост возможностей радио- и радиотехнической разведки, как основного источника получения разведывательной информации. Поэтому в настоящее время перед специалистами комплексного технического контроля (КТК) и разработчиками перспективной техники КТК стоит задача оптимально подобрать время контроля типовых объектов РРТК (диапазона частот), в целях упреждающего выполнения задач информационного конфликта технических средств разведки (ТСР) и средств радио- и радиотехнического контроля (РРТК) мер противодействия (ПД) ТСР. Выполнение этой задачи сводится к

необходимости заблаговременному выявлению нарушений мер ПД ТСР на объектах контроля, что является ключевым условием достижения требуемого уровня защиты информации.

Оценка текущего уровня готовности средств РРТК к заблаговременному решению информационных задач, в условиях постоянно нарастающего конфликта средств РРТК и ТСР, является актуальной задачей, важнейшей целю которой, является заблаговременное выявление нарушений мер по ПД ТСР, для оперативного принятия мер к их устранению (ослаблению) и снижению эффективности применения ТСР.

Для успешного решения указанной задачи проведено структурное представление процесса рассматриваемого конфликта, представленное на рисунке 1. Такое представление существенно облегчает понимание конфликта между сложными системами. Схема отражает основные этапы ведения РРТК, выявление каналов утечки информации и принятия мер к их закрытию (ослаблению). При анализе состояний объекта контроля, вероятностей переходных процессов из состояния в состояние, а также динамику информационного конфликта, каждая из вероятностей перехода объекта из одного состояния в другое будет зависеть только от времени и текущего состояния. Таким образом, система интегро-дифференциальных уравнений, описывающих данный конфликт, имеет следующий вид

$$\begin{gathered}
\tilde{P}_1(t) = P_{1\text{н}} \cdot \delta(t) + P_{81} \int_0^t \varphi_{81}(t-\tau) \cdot \tilde{P}_8(\tau) d\tau, \\
\dots \\
\tilde{P}_8(t) = P_{8\text{н}} \cdot \delta(t) + P_{68} \int_0^t \varphi_{68}(t-\tau) \cdot \tilde{P}_6(\tau) d\tau, \\
\tilde{P}_9(t) = P_{9\text{н}} \cdot \delta(t) + P_{79} \int_0^t \varphi_{79}(t-\tau) \cdot \tilde{P}_7(\tau) d\tau \\
+ P_{69} \int_0^t \varphi_{69}(t-\tau) \cdot \tilde{P}_6(\tau) d\tau,
\end{gathered} \tag{1}$$

где $\tilde{P}_i(t)$ – вероятность того, что объект контроля в течение бесконечно малого интервала времени $(\mathrm{t}, \mathrm{t}+\mathrm{dt})$ перейдет в состояние C_i; P_{ij} и $\varphi_{ij}(t)$ – соответственно вероятность и функция

плотности вероятности перехода объекта из состояния C_i в состояние C_j; $P_{i\text{н}}$ – вероятность нахождения объекта в состоянии C_i в момент времени $\mathrm{t} = 0$; $\sum_{i=1}^{4} P_{i\text{н}} = 1$; $\delta(t)$ – дельта-функция Дирака.

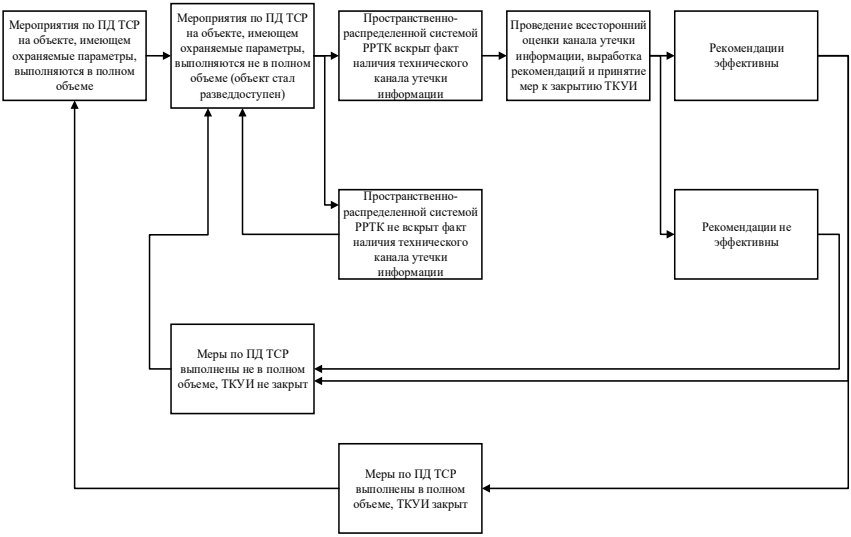


Рисунок 1 – Структурное представление процесса информационного конфликта средств РРТК и сигнальных технических разведок

Для перехода упрощения формулы вероятности обозначим через $H_j^+(t)$ и $H_j^-(t)$ среднее число переходов рассматриваемого процесса в интервале $(0, \mathrm{t})$, после каждого из которых процесс попадает в состояние C_i и покидает состояние C_j. Учитывая то, что дифференциалы функций восстановления $dH_j^+(t)$ и $\mathrm{d}H_j^-(t)$ интерпретируются как вероятности того, что в интервале времени $(\mathrm{t}, \mathrm{t} + \mathrm{dt})$ произойдут соответствующие переходы, то для данного случая указанные дифференциалы функции восстановления примут следующий вид

$$dH_i^+(t) = P_i, \text{ где } i=1\ldots9,$$
$$dH_1^-(t) = P_{12}\int_0^t \varphi_{12}(t-\tau)\cdot\tilde{P}_1(\tau)d\tau,$$
$$dH_2^-(t) = P_{23}\int_0^t \varphi_{23}(t-\tau)\cdot\tilde{P}_2(\tau)d\tau$$
$$+P_{24}\int_0^t \varphi_{24}(t-\tau)\cdot\tilde{P}_2(\tau)d\tau, \qquad (2)$$
$$\ldots$$
$$dH_9^-(t) = P_{91}\int_0^t \varphi_{91}(t-\tau)\cdot\tilde{P}_9(\tau)d\tau.$$

Таким образом, полученные функции восстановления позволяют построить математическую модель рассматриваемого информационного конфликта, представленную на рисунке 2.

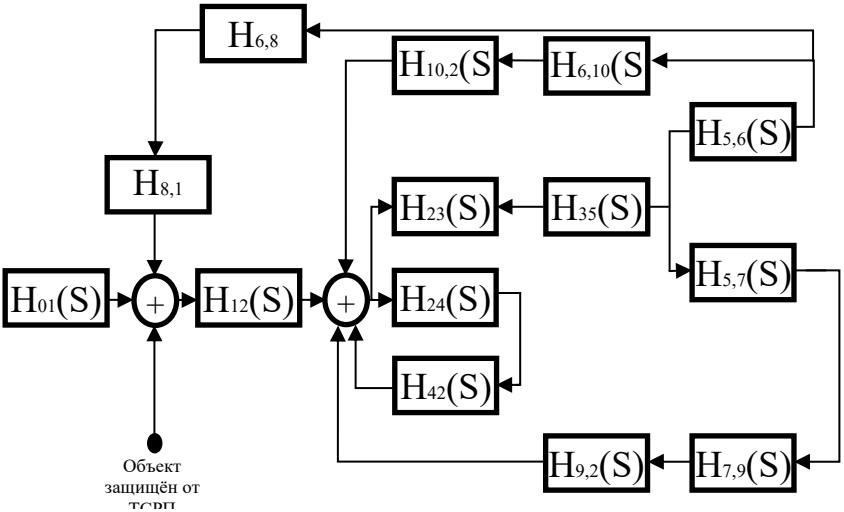


Рисунок 2 – Математическая модель информационного конфликта средств РРТК и ТСР

Вероятности нахождения объекта контроля в системе можно представить следующим образом

$$P_1(t) = \int_0^t \{dH_1^+(u) - dH_1^-(u)\}du =$$
$$= P_{1н} + P_{81} \cdot \int_0^t \int_0^u \varphi_{81}(u-\tau) \cdot \tilde{P}_8(\tau)dtdu - P_{12}$$
$$\cdot \int_0^t \int_0^u \varphi_{12}(u-\tau) \cdot \tilde{P}_1(\tau)dtdu,$$
$$\dots$$
$$P_9(t) = \int_0^t \{dH_9^+(u) - dH_9^-(u)\}du = \quad (3)$$
$$= P_{9н} + P_{69} \cdot \int_0^t \int_0^u \varphi_{69}(u-\tau) \cdot \tilde{P}_6(\tau)dtdu + P_{79}$$
$$\cdot \int_0^t \int_0^u \varphi_{79}(u-\tau) \cdot \tilde{P}_7(\tau)dtdu - P_{92}$$
$$\cdot \int_0^t \int_0^u \varphi_{92}(u-\tau) \cdot \tilde{P}_9(\tau)dtdu,$$

Применив преобразование Лапласа, данную систему уравнений можно преобразовать к виду

$$L\{P_1(t)\} = P_1(s) = \frac{1}{s} \cdot \begin{bmatrix} P_{1н} + P_{81} \cdot \varphi_{81}(s) \cdot \tilde{P}_8(s) \\ -P_{81} \cdot \varphi_{81}(s) \cdot \tilde{P}_8(s) \end{bmatrix},$$
$$\dots \quad (4)$$
$$L\{P_9(t)\} = P_9(s) = \frac{1}{s} \cdot \begin{bmatrix} P_{9н} - P_{92} \cdot \varphi_{92}(s) \cdot \tilde{P}_9(s) \\ +P_{69} \cdot \varphi_{69}(s) \cdot \tilde{P}_6(s) \\ +P_{79} \cdot \varphi_{79}(s) \cdot \tilde{P}_7(s) \end{bmatrix},$$

где $\tilde{P}_i(s)$ и $\varphi_{ij}(s)$ – соответственно, преобразования Лапласа от $\tilde{P}_i(t)$ и $\varphi_{ij}(t)$.

Для определения оптимального времени упреждающего выполнения информационных задач перспективной пространственно-распределенной системой радио- и радиотехнического контроля обозначим случайные моменты времени, в которых объект контроля разведдоступен и неразведдоступен, то есть τ_{C_1} – мероприятия по ПД ТСР

выполняются в полном объеме, τ_{C_2} – мероприятия по ПД ТСР выполняются не в полном объеме. Функция плотности вероятности разницы сравниваемых моментов времени есть не что иное, как свертка плотностей вероятностей случайных величин τ_{C_1} и τ_{C_2}

$$W_{C_1}(\tau_{C_1} - \tau_{C_2}) = \int_0^{\infty} \varphi_{C_1}(t) \cdot \varphi_{C_2}(t - \tau_{C_1} + \tau_{C_2})dt. \quad (5)$$

Отсюда вероятность нахождения объекта в состоянии C_1 не менее t единиц времени будет определяться интегралом от выражения (5)

$$P_{C_1}(t > t_c) = \int_{t_c}^{\infty} W_{C_1}(\tau_{C_1} - \tau_{C_2})d\tau. \quad (6)$$

Аналогично (6) может быть найдена вероятность нахождения объекта РРТК в состоянии C_2, а полученные значения могут быть применены для расчета времени упреждающего выполнения информационных задач.

Таким образом, основываясь на полученных результатах, не трудно определить конкретные значения требуемого времени выполнения задач по ведению РРТК, которые должны находиться в пределах от единиц миллисекунд до единиц секунд. Полученные результаты могут быть успешно применены как при проектировании перспективных комплексов РРТК, так и при оценке, распределении и постановки задач имеющимся силам и средствам комплексного технического контроля. Учитывая предельно малый диапазон времени, отводимые на решение информационных задач, значительно усложняют задачу мгновенного выявления существующих каналов утечки информации, с целью упреждающего принятия мер к его закрытию, до его вскрытия СТР, и свидетельствует о необходимости повышения оперативности решения задач КТК, автоматизации процесса ведения РРТК, анализа выявленных каналов утечки информации и принятии мер к их закрытию.

Литература:

1. *Козирацкий Ю.Л.* Модели информационного конфликта средств поиска и обнаружения. Монография. – М.: Радиотехника, 2013. – 232 с.

2. *Леньшин А.В., Кравцов Е.В., Славнов К.В.* Методика оценки эффективности защиты информации на объектах комплексного технического контроля // Радиотехника. – 2021. – №1. – С. 20-27.

3. *Кравцов Е.В.* Методический подход к комплексной оперативной оценке возможностей выявления сведений об объектах защиты // Телекоммуникации. – 2020. – № 9. – С. 33-41.

DOI: 10.25728/iccss.2022.22.51.063

Еронин Д. А., Мелихов А.А.

Разработка автоматизированного средства, предназначенного для выявления потенциально опасных конфигураций ИС малого предприятия

Аннотация: В работе рассматривается проблематика использования средств обнаружения уязвимостей в конфигурации ИС малого предприятия и предложено решение позволяющие автоматически проводить регулярный аудит и выявлять уязвимости.

Ключевые слова: обнаружение уязвимостей, сканер безопасности, аудит безопасности, управление уязвимостями

Введение

Поддержание надёжного функционирования бизнес-процессов и обеспечение конфиденциальности данных сегодня актуально для любого типа предприятия - как большого, так и малого. Однако возможностей для построения системы обеспечения безопасности у малого предприятия значительно меньше. Это вызвано как бюджетными ограничениями, так и отсутствием финансовой возможности найма отдельных специалистов, занимающихся непосредственно обеспечением информационной безопасности. В итоге, задача обеспечения информационной безопасности предприятия ложится на системного администратора, для которого

она имеет гораздо меньший приоритет, чем обеспечение физической работоспособности вверенной системы, что в свою очередь непосредственно влияет на качество и оперативность принимаемых решений [1].

Отдельную проблему представляет собой инструментарий. Полномасштабные автоматизированные системы контроля защищённности дороги и сложны в эксплуатации, у малого предприятия просто не будет средств на их закупку. Альтернатива – применение бесплатных инструментов с открытым исходным кодом, однако их условная бесплатность на практике требует существенно больших временных затрат на адаптацию инструментов к условиям конкретной информационной среды предприятия. Такой подход позволяет покрыть базовые задачи, возникающие в рамках процесса управления уязвимостями, однако требует использования разнородных компонент фактически в ручном режиме, что существенно снижает общую производительность сотрудника, замедляя реакцию на возникающие угрозы. Помимо этого, обработка данных, полученных из различных источников, требует их детального анализа и консолидации с учётом особенностей режимов работы применяемых инструментов [2].

Таким образом, возникает задача объединения результатов работа различных сканеров в единый внутренне непротиворечивый отчёт, на основе которого квалифицированный системный администратор сможет оперативно и обоснованно принимать решения, направленные на повышение защищённости вверенной системы.

В рамках настоящей публикации предложено решение данной задачи, позволяющее автоматизировать процесс выявления опасных конфигураций информационных систем малого предприятия и отслеживать их устранение. Данное решение было представлено и защищено в качестве бакалаврской выпускной квалификационной работы на кафедре информатики и вычислительных сетей ИНБИКСТ МФТИ.

Требования к системе

Основная идея разрабатываемого решения – взять доступные утилиты, используемые для ручного анализа защищённости и объединить их в единую автоматизированную систему, требующую

от оператора только задания необходимого диапазона сканирования. В рамках процесса управления уязвимостями подразумевается определять подверженность сканируемой инфраструктуры к следующим видам атак: эксплуатации уязвимостей ПО, подбору учётных записей и атакам на незащищённые протоколы.

Разрабатываемая система должна быть реализована на основе модульной архитектуры, где каждый модуль отвечает за свой вид проверок, покрывающих обнаружение одной из указанных выше уязвимостей, или другие задачи, как например составление отчёта. Это позволяет использовать лишь необходимые проверки, а в случае необходимости, изменять имеющиеся или добавлять новые модули без изменения остальных.

Выбор интегрируемых компонентов должен быть обоснован функциональными возможностями. Поскольку разрабатываемое средство относится к классу средств защиты, необходимо контролировать прозрачность получения исходных кодов, определять и устранять найденные в них уязвимости, а также обеспечить независимое хранение на базе локального репозитория [3].

Техническая реализация

Для унификации данных о сканируемой системе используется единый JSON-объект, создаваемый при запуске сканирования и впоследствии пополняемый модулями проверок. Требуемые параметры сканирования хранятся в конфигурационном файле, где указываются IP-адреса сканируемых хостов, требуемые модули и их конфигурация.

Система включает в себя модули сетевого сканирования, проверки по базе данных известных уязвимостей, определения разрешённых/запрещённых сервисов, подбора учётных записей и составления отчёта.

В основе модуля сетевого сканирования лежит утилита Nmap – сетевой сканер с открытым исходным кодом, со скриптовым движком NSE, позволяющим значительно расширить функционал. Так, проверка на наличие известных уязвимостей ПО реализована в виде NSE-скрипта, где в качестве базы данных уязвимостей используется Vulners, которая представляет из себя агрегатор популярных баз уязвимостей, баг-репортов поставщиков ПО и

общедоступных эксплоитов. Это облегчает задачу, поскольку получаемы данные имеют единый вид, а за счёт большого количества источников, снижается вероятность не обнаружить имеющуюся уязвимость. Результаты сетевого сканирования и проверке по базе уязвимостей сохраняются в XML-формате, после чего преобразуются в JSON-объект.

Затем выполняется проверка обнаруженных сервисов, запущенных на сканируемом хосте, по спискам разрешённых/запрещённых, указанным в конфигурационном файле.

Подбор учётных записей производится утилитой Patator. Данная утилита способна работать с большим количеством протоколов и позволяет самостоятельно настраивать фильтрацию получаемых от серверов ответов, что позволяет исключить ложные срабатывания. В конфигурационном файле указывается, какие из возможных сервисов требуется сканировать. Учётные данные успешных подключений добавляются в CSV-файл, откуда парсятся и добавляются в список всех обнаруженных уязвимостей.

После всех проверок, создаётся HTML-отчёт. Выполняется сравнение, результаты текущего сканирования сравниваются с предыдущими, указываются новые хосты и порты. Для каждого хоста указывается его операционная система, время работы с последней перезагрузки, открытые порты, сервисы, запущенные на этих портах и их версии. Для каждого порта указываются названия модулей проверок и список обнаруженных ими уязвимостей. Если какие-либо уязвимости не были закрыты с предыдущего сканирования, это также указывается. Цветом обозначается уровень уязвимости соответствующего порта: зелёный – уязвимостей не обнаружено, жёлтый – низкий уровень опасности, оранжевый – средний, красный – высокий. Уровень опасности соответствует наибольшему CVSS среди обнаруженных для него уязвимостей. Полученный HTML-отчёт сохраняется. Помимо этого, в JSON-формате сохраняется вся информация о просканированной системе с названием, соответствующим текущей дате и времени на момент завершения сканирования.

Тестирование программного средства

Для подтверждения соответствия разработанного решения поставленной задаче, проводилось два вида тестирования: первый –

для подтверждения корректности обнаружения уязвимостей и полноты покрытия модели реализации внешних угроз, возникающих на этапе преодоления периметра; второй — с целью убедиться в корректности подтверждения закрытия ранее обнаруженных уязвимостей. В первом случае тестирование производилось на платформе Metasploitable2 – машине под управлением операционной системы Ubuntu, содержащей множество уязвимостей. Во втором случае – на машине с неактуальной версией ОС Ubuntu и с устаревшими версиями ssh-сервера OpenSHH и http-сервера Apache2, после чего было проведено обновление до актуальных версий. Таким образом, было подтверждено, что система способна определять, насколько уязвима сканируемая инфраструктура к таким техникам атак как: эксплуатация уязвимостей ПО, подбор учётных записей и атака на незащищённые протоколы, а также для мониторинга процесса устранения уязвимостей.

Заключение

В настоящей работе была рассмотрена проблема защиты информационных систем малого предприятия, а именно обнаружение уязвимостей в рамках процесса управления уязвимостями. Разработано программное средство, позволяющее проводить сканирование инфраструктуры предприятия на подверженность к распространённым техникам реализации угроз информационной безопасности со стороны внешнего нарушителя. Данное средство прошло апробацию и подтвердило свою эффективность.

Литература:

1. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В*. Анализ фактора неопределённости в процессе подготовки управленческих решений / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2021. – С. 40-46.

2. *Козлов А.Д., Нога Н.Л.* Достоверность информации как элемент обеспечения информационной безопасности и оценка её уровня / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2021. – С. 195-200.

3. *Мелихов А.А.* Обеспечение непрерывной разработки программных продуктов, сертифицируемых по требованиям безопасности / Материалы XXIX Международной научной конференции «Проблемы управления безопасностью сложных систем». – М.: ИПУ РАН, 2021. – С. 189-195.

DOI: 10.25728/iccss.2022.65.81.064

Ковач Е.В., Ткаченко В.А.

Анализ как инструмент улучшения системы управления промышленной безопасностью и охраной труда

Аннотация: Рассмотрены и прокомментированы требования к процедуре проведения анализа функционирования системы управления промышленной безопасностью и охраной труда, предъявляемые со стороны международного стандарта ISO 45001:2018. Приведены рекомендации по проведению такого анализа в части рассмотрения необходимых сведений, формированию полученных результатов. Сделан вывод о том, что досконально проведённый анализ – инструмент улучшения системы управления.

Ключевые слова: анализ, управление, промышленная безопасность и охрана труда

Вопросы обеспечения безопасности производства не теряют своей актуальности. Череда событий с крайне негативными, резонансными последствиями, которая произошла в конце 2021 года, к сожалению, в очередной раз подтвердила остроту этой проблемы. Безусловно, максимум озабоченности был достигнут в результате аварии на шахте «Листвяжная». Ситуация вынудила обратить самое пристальное внимание на решение этой проблемы всю вертикаль управления в Российской Федерации, включая её самые верхние уровни. Стоит отметить тот факт, что работа по повышению результативности существующих мер управления рисками в области промышленной безопасности, охраны труда и других смежных областей, может протекать на самых разных уровнях управления, начиная уровнем соответствующих федеральных органов

исполнительной власти и заканчивая уровнем эксплуатирующих организаций.

К последнему, безусловно, можно отнести и деятельность по совершенствованию систем управления промышленной безопасностью и охраной труда (далее СУПБиОТ), как их зачастую называют в российских организациях, разработанных в соответствии с требованиями международного стандарта ISO 45001:2018 «Системы менеджмента профессионального здоровья и безопасности – Требования и руководство по применению», осуществляемую в эксплуатирующих организациях.

Одним из важнейших элементов управления в любой сложной системе, к числу которых бесспорно можно отнести и СУПБиОТ, является регулярный анализ функционирования системы. С позиций классических представлений, лежащих в основе теории управления [1], в том числе, и организационными системами, к которым относятся СУПБиОТ [2], важнейшим моментом является наличие обратной связи, которая позволяет поддерживать объект управления в заданных условиях и достигать намеченных целей. И именно анализ функционирования системы управления со стороны высшего руководства можно рассматривать в качестве такой обратной связи.

Напомним, что в международном стандарте ISO 45001:2018 этому элементу управления посвящён отдельный пункт 9.3 «Анализ руководством», входящий в раздел 9 «Оценка результатов». То есть, если возвращаться к широко известному циклу Деминга-Шухарта, циклу PDCA, речь идёт об этапе C – «control/проверка», этапе, который позволяет получить информацию о текущей ситуации и стать основой для разработки дальнейших действий по повышению результативности системы управления и достижению поставленных перед системой целей.

Итак, напомним и прокомментируем основные требования пункта 9.3 международного стандарта ISO 45001:2018.

«Высшее руководство должно анализировать систему менеджмента OH&S организации через запланированные интервалы времени, чтобы обеспечивать ее постоянную пригодность, адекватность и результативность» (здесь и далее выделение курсивом – цитата ISO 45001:2018).

Очень важно подчеркнуть тезис о том, что анализ должен проводиться через запланированные интервалы времени. Таким

образом, речь идёт о том, что Организация сама определяет, в какой именно момент, применительно к какому этапу, например, годового цикла существования Организации стоит приурочить момент проведения такого анализа.

Теперь о том, что же должно быть проанализировано в качестве входных данных в соответствии с требованиями международного стандарта ISO 45001:2018.

«*Анализ руководством должен включать рассмотрение следующих вопросов:*

a) статус действий по результатам предыдущих анализов руководством;

b) изменение внешних и внутренних факторов, относящихся к системе менеджмента OH&S, включая:

1) потребности и ожидания заинтересованных сторон;

2) законодательные требования и иные требования;

3) риски и возможности;

c) степень достижения политики в области OH&S и целей в области OH&S;

d) информация о результатах в области OH&S, включая тенденции в отношении следующего:

1) инциденты, несоответствия, корректирующие действия и постоянное улучшение;

2) результаты мониторинга и измерений;

3) результаты оценки соответствия законодательным требованиям и иным требованиям;

4) результаты аудитов;

5) консультации и участие работников;

6) риски и возможности;

e) адекватность ресурсов для поддержания результативной системы менеджмента OH&S;

f) соответствующие коммуникации с заинтересованными сторонами;

g) возможности для постоянного улучшения».

Остановимся на ключевых типах входных данных, которые должны быть рассмотрены в ходе анализа со стороны высшего руководства. Начнём с необходимости рассмотрения действий по результатам предыдущих анализов руководством. Чрезвычайно важно сохранять преемственность принимаемых решений,

отталкивающихся от результатов оценки степени выполнения ранее принятых решений и запланированных мероприятий.

При проведении анализа функционирования системы управления акцент также сделан и на происходящих изменениях. В настоящее время настолько часты и существенны любые изменения, затрагивающие вопросы обеспечения безопасности, что без их учёта тяжело представить функционирование любой системы. Изменения системных рисков и возможностей также могут оказать существенное влияние на функционирование системы управления и способность достигать поставленных целей, что, в свою очередь, должно подвергаться анализу со стороны руководства.

Степень достижения политики в области промышленной безопасности и охраны труда и целей в этой сфере должна отслеживаться и анализироваться для своевременного внесения корректировок в управленческие механизмы внутри системы управления в случае отклонения от траектории их достижения.

Чрезвычайно важен анализ тенденций, будь то тенденции негативные, инциденты и несоответствия, или же позитивные, постоянное улучшение. И в том, и в другом случаях настоятельно рекомендуется при анализе, по возможности, использовать фоновые показатели и отраслевые сведения для проведения сравнения и определения позиций в области обеспечения безопасности производства, на которых в текущий момент находится Организация. При этом, при проведении анализа произошедших негативных событий необходимо учитывать весь их спектр. Таким образом, следует рассматривать не только характерные обстоятельства и причины зарегистрированных несчастных случаев или аварий, но и всех случаев микротравм и событий, которые могли бы привести к нанесению ущерба здоровью сотрудников Организации, что в очередной раз должно подчеркнуть проактивную нацеленность системы управления в целом, а аналитической деятельности, осуществляемой в её рамках, в частности.

Не менее важны и тенденции, фиксируемые по результатам осуществления различных контрольных действий внутри системы управления. Необходимо вовремя уловить начало тенденций, демонстрирующих начало роста выявляемых отклонений, проанализировать порождающие их причины и своевременно предпринять соответствующие управленческие действия.

Среди входных данных для анализа функционирования системы со стороны высшего руководства находятся и возможности для постоянного улучшения. Очень важно, что они являются именно входными данными, то есть уже на этапе начала проведения анализа, а не только в его заключительной фазе, должны быть рассмотрены такие возможности, и что не менее важно, это должно происходить в контексте рассмотрения всех остальных входных данных, то бишь в рамках комплексного анализа.

Теперь перейдём к результатам анализа функционирования системы управления со стороны высшего руководства. Вот, что требует международный стандарт ISO 45001:2018.

«Результаты анализа руководством должны включать решения, относящиеся к следующему:

– сохраняющаяся пригодность, адекватность и результативность системы менеджмента OH&S в достижении намеченных результатов;

– возможности для постоянного улучшения;

– любая необходимость в изменениях системы менеджмента OH&S;

– необходимые ресурсы;

– действия, если необходимы;

– возможности для улучшения интеграции системы менеджмента OH&S с другими бизнес-процессами;

– любые последствия для стратегического направления развития организации».

Логично, что результатом проведённого анализа функционирования системы управления является пакет решений. Авторы уже упоминали о том, что возможности для постоянного улучшения являются частью входных данных при проведении анализа, но, помимо этого, что вполне логично, являются и частью принимаемых решений, то есть частью выхода по результатам анализа. Собственно, по всем канонам теории управления, интегральным, синергетическим результатом анализа должны стать решения, направленные на развитие системы.

Безусловно, деятельность по обеспечению безопасности производственных процессов не является самоцелью Организации. Основная цель существования любой производственной Организации – получение прибыли, всё остальное – содействие в

достижении этой главной цели. Посему деятельность по обеспечению безопасности трудового процесса должна быть плавно интегрирована в совокупность бизнес-процессов Организации, всячески содействовать им.

Существование любой Организации невозможно без стратегического планирования, а стратегическое планирование в целом невозможно без учёта вопросов обеспечения безопасности производственной деятельности, без которой ни о каком позитивном развитии речи идти не может, а все ресурсы будут направлены на возмещение ущерба от происходящих негативных событий.

Отметим заключительные требования международного стандарта ISO 45001:2018, регламентирующие процедуру проведения анализа.

«Высшее руководство должно информировать о соответствующих результатах анализа своих работников и, где имеются, их представителей.

Организация должна сохранять документированную информацию в качестве свидетельств результатов анализа руководством».

Чрезвычайно важно, что результаты анализа со стороны высшего руководства должны быть прозрачными, не являться тайной за семью печатями. Каковы бы иногда не были нерадужными результаты такого анализа, они должны доводиться до сведения сотрудников Организации, они должны видеть, что определённые шаги со стороны руководства предпринимаются, что ситуация не является бесконтрольной, что прикладываются усилия для постоянного улучшения в этой сфере.

Повторим, полноценный, скрупулёзный, всеобъемлющий анализ функционирования СУПБиОТ – безусловно, возможность улучшения положения дел в области обеспечения безопасности производства. Вовремя уловленные признаки зарождения негативных тенденций, оперативно предпринятая управленческая реакция, своевременно перераспределённые и перенаправленные ресурсы, планомерное выполнение различных мероприятий – важный шаг в поддержании проактивного характера деятельности Организации в сфере обеспечения безопасности.

Литература:

1. *Новиков Д.А.* Теория управления организационными системами. – М.: МПСИ, 2005. – 584 с.

2. *Ткаченко В.А.* Система управления промышленной безопасностью с позиций теории систем / Труды XII международной конференции «Проблемы управления безопасностью сложных систем». – М.: РГГУ, 2004. – С. 432-437.

DOI: 10.25728/iccss.2022.26.90.065

Plotnikov N.I.

Estimation of accident hazard and magnitude of aircraft with wildlife strike damage in aviation safety vs avian safety

Abstract: This paper analyzes modern studies of strike of aircraft with objects of wildlife or air-terrestrial animals: birds, bats, terrestrial mammals, reptiles (Bird/Other Wildlife Strike). The probabilities of actual damages and risks are calculated. The solution to the problem of calculating strike risks is carried out in the development of a relational matrix that contains data by parameters, indicators in selected scales. The results of the work are presented as algorithms for optimizing the mutual protection of the aircraft and the wildlife.

Keywords: aircraft, wildlife, strike, hazard, magnitude, estimation

Introduction. The International Civil Aviation Organization (ICAO) establishes aircraft flight safety requirements for the prevention of strike risks in the territories and near airports by fencing territories, displacement measures, scaring away and liquidations, that is, to the detriment of the safety of the airborne flight. Statistics based on the registration, recording and analysis of strikes are considered incomplete, since a significant part of the events is not recorded. Real number of strikes are several times more registered. According to the US Federal Aviation Administration (FAA) estimates from 1991-1997 to the present, about 20% of strike that actually occur are recorded. Full statistics of strike observations is not maintained for various reasons: a) most of the strike are not critical, in the absence of damage to the aircraft, they may not be detected; b) lower priority of

expenditures invested in security for this factor; c) a representative statistical sample of observations is preferred to complete statistics; d) insufficient formation and requirements for voluntary registration and accounting of the legal framework. In this paper estimation of accident hazard and magnitude of aircraft with wildlife strike damage in aviation safety vs avian safety of civil aviation (CA) has been completed. Methods of resource modeling of organizational objects are used [1].

Estimation of Strike Damage. Critical parameters are determined with the highest values of the "number of strikes" indicators, as well as the data "number of strikes with damage", established by expert and experimental means. In studies, it was statistically established that the highest frequency of strikes occurs with birds of 0.5-2 kg. It has been experimentally determined that the most striking mass of a bird is determined to be 2.7 kg. In the identified 33 bird species, a correlation (R2 = 0.82) was established between the average body weight and the probability of aircraft injuries: for every 100 grams of weight, the probability of injury increases by 1.22% [2]. It was revealed that the main danger is in the event of a strikes of the wildlife in the windshield and in the aircraft engines. A large bird breaks the windshield at speeds of over 500 km/h and this can have fatal consequences for the life of the pilot and catastrophic destruction of the aircraft. The impact force of a bird weighing 400 grams at an aircraft speed of 700 km/h reaches 20 tons. The risk of a pilot's death increases sharply at a speed of 400 km/h. Getting into the engine can lead to failure and disaster. The peculiarity of the consequences of strikes is that they can be either immediate or delayed. If destruction does not occur immediately, then destruction is possible during climb under the action of intra-cabin pressure and continued destruction of mechanical damage from high-speed air pressure in flight. An assessment has been made: the critical values of the indicators in the above matrix are highlighted in bold.

Aviation Safety vs Avian Safety. The solution of the problem of flight safety of aviation safety vs avian safety is similar to the solution of the problem of avoiding aircraft strikes in air traffic control. However, there is an important difference: in the strike avoidance problem, the motion of the aircraft is considered to be deterministic, which is possible for a formalized description, while in the problem of strikes between the aircraft and the wildlife, the motion of the wildlife is stochastic, the description of

which is formally impossible. Observation parameters aircraft and wildlife are general and specific for each object.

Damages assessment. The following data are used to estimate and calculate the environmental damage caused by the wildlife in strikes with aircraft, the conditions and assumptions are accepted. Under the damages of the wildlife is meant the death of objects, since there is no statistical record of injuries. Wildlife data with aircraft damage is used as evidence of the damage and death of the wildlife. The calculations use statistical data on the ratios (coefficients) of strikes on the number of aircraft flights [3]. For certified commercial aviation airports for the years 2000-2020, the number of recorded strikes (hence, dead wildlife) per 100,000 flights is 21.29, including strikes with aircraft damage 1.25. According to the data of [4], the number of strikes that have occurred is five times more than the number taken into account, that is, 106.45 dead objects per 100,000 flights. In the behavior of the flocking parameter of birds, an indicator of 10-100 individuals is taken as statistically the most verifiable. For the sake of calculation, let's assume that 10 individuals from the flock die in each strike. For further calculations, the data of [3] are extrapolated to the global scale.

Currently, about 40 million commercial aviation flights take place in the world every year [5]. Calculations:

Damage to the wildlife: (40000000 flights) / (100000 flights) x (21.29 counted (106,45) strikes) x (10 birds) = 85160 (425800) counted (occurred) dead birds annually.

Aircraft damage vs wildlife damage: (1.25 / 100000 flights) = 0.0000125 vs (21.29 (106.45) / 100,000 flights) = 0.0002129 (0.0010645). Ratio: 0.0000125 / 0.0002129 (0.0010645) = 17032 (85.16).

Otherwise, the damages of wildlife exceed the damages of aircraft by 17 (85) times.

Human victims vs death of birds. Between 1988 and 2020, more than 293 people died in strikes around the world [3], on average, 9 people per year. Calculation: 85160 (425800) counted (occurred) dead birds / dead people (9) = 9 462 (47 311).

Otherwise, the victims of the wildlife exceed 9462 (47311) times the human victims. Almost 50000 birds die yearly in strikes between aircraft and wildlife per one human fatality. Let's summarize the calculations by comparing the annual number of casualties and damage to aircraft per 100000 flights with the estimated number of human fatalities (table 1).

Table 1 – Strike damage

	Damages	Number	1 / 2	1 / 3	Probability
1	Wildlife	85 160 (425 800)		9 462 (47 311)	P = 10-5 (10-4)
2	Aircraft	21,29 (106,45)	17 (85)		P = 10-8
3	Human fatalities	9			P = 10-8

The performed calculations can be performed in more detail. First, separately perform calculations for groups, types of wildlife, for geographical scales. Calculations should take into account the CA data. For 100 000 CA flights, the number of strikes is 1.52, including 0.28 strikes with aircraft damage. Strikes with damage account for about 6-7 percent in commercial aviation, and 18 percent in CA of the total number of recorded strikes. The total number of birds in the world is estimated at about 100 billion individuals. From here, it is possible to structure and calculate the size of environmental damage.

Conclusion. Calculations show that damage indicators do not depend on the number of species in groups. Due to their weight, damage from strikes with terrestrial mammals is five times greater than from strikes with birds. The development of a metric for observing the fuzziness of events makes it possible to calculate the probabilities of actual damages and strike risks. In the statistics of all accident causes, the events of strikes with the wildlife in this work are calculated by the probability of casualties for every 10-8 flights. Yearly almost 50000 birds die in strikes between aircraft and wildlife per one human fatality. A matrix and algorithms for observing and calculating strikes have been developed. Experimental studies have been carried out, which confirm the main results of statistical studies. It satisfies the need of airlines and airports to actively manage measures to protect flights from strike events and reduce the risks of accidents. Consumers are flight departments of airlines, ornithological services of airports, emergency rescue services.

References:

1. *Plotnikov N.I.* (2021) Methods of resource modeling of organizational objects. Lecture Notes in Intelligent Transportation and Infrastructure. Advances in Air Traffic Engineering Selected Papers from 6th International Scientific Conference on Air Traffic Engineering, ATE 2020, October 2020. – Warsaw, Poland, Springer Nature Switzerland AG. – P. 116-130

2. Federal Aviation Administration. (2020) 14 CFR 91.7 – Civil Aircraft Airworthiness; Federal Aviation Administration**:** Washington, DC, USA, 2020.

3. *Dolbeer R.A., Begier M.J., Miller P.R., Weller J.R., Anderson A.L.* (2021) Wildlife Strikes to Civil Aircraft in the US, 1990-2020, FAA Report 27. – p. 141.

4. *Allan J.R., Bell J.C., Jackson V.S.* "An Assessment Of The World-wide Risk To Aircraft From Large flocking Birds" (1999). 1999 Bird Strike Committee-USA/Canada, First Joint Annual Meeting, Vancouver, BC. Retrieved from [https://digitalcommons.unl.edu/birdstrike1999/4]

5. Retrieved from [https://www.un.org/en/observances/civil-aviation-day].

DOI: 10.25728/iccss.2022.33.65.066

Чинакал В.О.

Применение встраиваемых интеллектуальных компонентов в системах улучшенного мониторинга сложными промышленными объектами

Аннотация: Рассматриваются вопросы разработки и применения встраиваемых интеллектуальных компонентов (ВИК) в систему усовершенствованного мониторинга AMS+ (AMS+ - Advanced Monitoring System Plus) сложного промышленного объекта. ВИКи обеспечивают автоматизацию решения задач ситуационного анализа обработки данных об изменениях ключевых технологических параметров (КТП) непрерывных производств и состояния технологического оборудования (СТО). Разработана структура распределенной системы ВИК с использованием продукционных моделей

представления знаний и методов ускоренного вывода на базе матричных вычислений.

Ключевые слова: безопасность управления, сложный промышленный объект, непрерывное производство, встраиваемый интеллектуальный компонент, матричный вывод, ключевые технологические параметры, усовершенствованный мониторинг

Введение

Для успешной реализации современных повышенных требований к обеспечению эффективной и безопасной эксплуатации сложных распределенных промышленных объектов (СРПО) необходимо существенно улучшить качество проектных решений по созданию усовершенствованных систем мониторинга AMS (AMS - Advanced Monitoring System) такими объектами. Отличительной чертой систем AMS является использование современных интеллектуальных методов [1] при решении сложных задач контроля и управления СРПО [2].

В [3] рассматривались возможности применения различных интеллектуальных средств в системах мониторинга СРПО, в [4] рассмотрены возможности эффективного использования встраиваемых интеллектуальных компонентов (ВИК) в современных системах управления сложными подвижными объектами.

В данной работе рассматриваются вопросы разработки и применения ВИК в составе системы усовершенствованного мониторинга (AMS+ - Advanced Monitoring System Plus). В частности, в AMS+ предлагается использование распределенной интеллектуальной системы поддержки мониторинга (ИСПМ) для автоматического решения ряда сложных задач. ВИКи в ИСПМ обеспечивают автоматизацию решения задач ситуационного анализа обработки данных об изменениях ключевых технологических параметров (КТП) непрерывных производств и состояния технологического оборудования (СТО). Локальные ВИКи, взаимодействуют между собой, базами данных и программным обеспечением (ПО) подсистем АСУТП СРПО.

1. Основные требования к проектированию ИСПМ

Выделим следующие основные общие требования к созданию и работе ИСПМ и ВИК:

– удобство описания и изменения локальных моделей представления знаний (МПЗ) на проблематику конкретных задач AMS+;

– возможность простой индивидуальной настройки, изменения и дополнения локальных баз данных (БД) и баз знаний (БЗ);

– формирование БД и БЗ ВИК в соответствии с классом решаемых задач с помощью единого подхода;

– существенное сокращение общей размерности МПЗ и БЗ локальных ВИК;

– повышение динамических характеристик работы отдельных ВИК и ИСПМ для обеспечения поддержки работы AMS+ в жестком реальном времени;

– построение МПЗ на базе продукционных правил с использованием матричных вычислений, уровневой структуризации МПЗ и применения «к» значных логик [5];

– модульное построение ПО ВИК на основе типового микроядра и локальных наборов БД и БЗ;

– возможность использования встроенных систем имитационного моделирования (СИМ), сконфигурированных на решение конкретных задач в реальном и ускоренном масштабе времени (прогноз состояния).

Разработка ВИК ориентирована на поддержку решения как традиционных задач контроля и управления в, так и на автоматизацию решения ряда специальных задач. К таким задачам относятся:

– автоматическая настройка работы МПЗ на актуальные источники данных от аппаратно-программных средств подсистем АСУТП СРПО с учетом возможных отказов технических средств контроля и управления (ТСУ);

– прогноз расходуемых ресурсов ТСУ и выбор ТСУ с достаточным запасом ресурсов;

– формирование оценок текущих ситуаций и прогноза их возможного развития;

– формирование вариантов выбора альтернативных моделей для определения КТП и СТО в зависимости от ситуации [6];

– выявление возможных причин возникновения отклонений и нарушений в работе источников данных и ТСУ;

– обнаружение предпосылок возникновения нештатных ситуаций для класса задач мониторинга в AMS+.

Рассмотрим общую структуру ИСПМ, разработанную на основе анализа основных требований к построению ИСПМ и решаемым задачам мониторинга в СРПО.

2. Разработка структуры ИСПМ

На рисунке 1 представлена общая структура ИСПМ, включающая локальные ВИК, объединенные в подсистемы, и представлены ее основные связи со штатной АСУТП. Условно к основным подсистемам ИСПМ можно отнести группы ВИК, реализующие следующие задачи:

– оценки ситуаций (контроль изменений КТП и СТО, состояния ТСУ и анализ доступных ресурсов ТСУ;

– выбора альтернативных моделей для оценки КТП и СТО в AMS+ СРПО и анализ данных прогноза;

– управления адаптацией параметров моделей и настройкой алгоритмов;

– управления кластеризацией ситуаций, выделение критических ситуаций, генерация целей и подцелей (ГЦ) и выбор сценария.

Монитор ИСПМ обеспечивает координацию работы ИСПМ и локальных ВИК, а также взаимодействие ВИК с сервером приложений и подсистемами штатной АСУТП СРПО с помощью локальных сетей (рисунок 2).

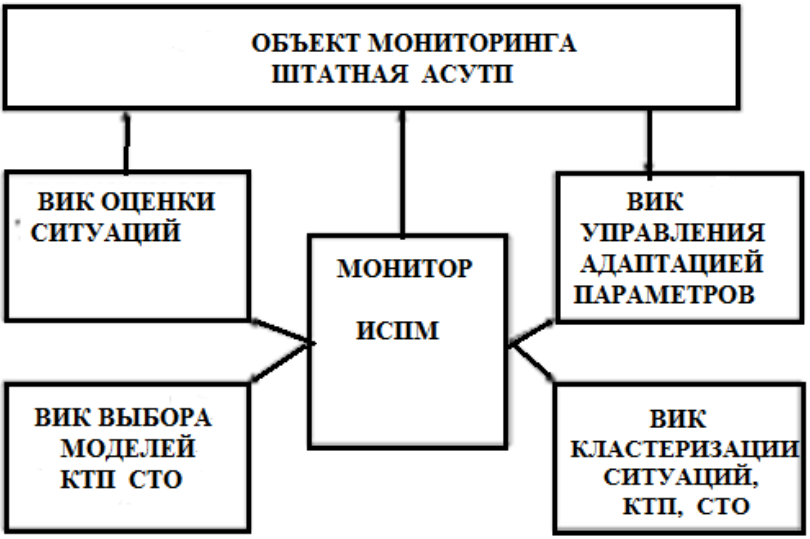


Рисунок 1 – Общая структура ИСПМ

На рисунке 2 представлена укрупненная функциональная блок-схема ИСПМ. На схеме показаны:

– локальные ВИК с соответствующими БД и БЗ (левый столбец схемы);

– основные функции ПО ИСПМ, выполняемые с использованием ВИК (средний и правый столбец схемы);

– основные блоки подсистемы имитационного моделирования (СИМ) (в нижней части схемы).

С помощью СИМ обеспечивается моделирование в реальном и ускоренном времени различных ситуаций, определение оценок КТП и СТО для AMS+ и АСУТП СРПО. В состав СИМ входят модели сырья, технологических процессов и установок, модели ТСУ, модели динамики объекта, модели датчиков, систем измерения и систем управления СРПО, а также БД СИМ, содержащая вспомогательные данные о параметрах моделей и конфигурировании задач, решаемых на СИМ. Монитор встроенной подсистемы имитационного моделирования (Монитор СИМ) координирует работу соответствующих блоков СИМ в реальном и ускоренном времени, обеспечивая прогноз и получение необходимых оценок применения

различных вариантов моделей и методов для определения ситуаций, КТП и СТО.

При построении ИСПМ использован событийный подход, модульное построение подсистем, использование вложенных, динамически выбираемых сценариев работы ИСПМ (стратегические, тактические, рабочие сценарии), мониторный принцип управления основными этапами работы ИСПМ. Центральный монитор ИСПМ координирует работу всех блоков ИСПМ, обеспечивая их бесконфликтное взаимодействие, получение, хранение и обработку входной, экспертной и выходной информации, исполнение сценариев работы, сформированных с использованием ВИК.

Группы ВИК, используемые в ИСПМ, ориентированы на поддержку решения следующих задач: ВИК1 – автоматическая настройка работы МПЗ (Б31) на актуальные источники данных от аппаратно-программных средств АСУТП; ВИК2 – анализ условий, событий, штатных и аварийных ситуаций, генерация и проверка динамических рабочих сценариев ИСПМ; ВИК3 – анализ состояния СРПО, ТСУ, генерация, проверка и отбор гипотез о состоянии объекта, ТСУ и сырья; ВИК4 – генерация, оценка и отбор альтернативных вариантов моделей в зависимости от текущих и прогнозируемых ситуаций; ВИК5 – комплексный анализ данных о параметрах КТП и СПО СРПО, построение границ предупредительных и критических отклонений параметров

Для обеспечения эффективного и безопасного управления СРПО необходима оперативная автоматическая оценка ситуации, путем проверки ряда гипотез в ускоренном времени на основе соответствующих продукционных правил и сформированного расширенного вектора текущих (и прогнозируемых) событий. Аналогично формируются и проверяются гипотезы о выборе различных сценариев действий на основе соответствующих продукционных правил и вектора возможных текущих и прогнозируемых ситуаций. В соответствии с результатами текущих оценок ситуаций и выбора сценария действий формируются соответствующие альтернативные варианты моделей и параметров настройки алгоритмов обработки данных.

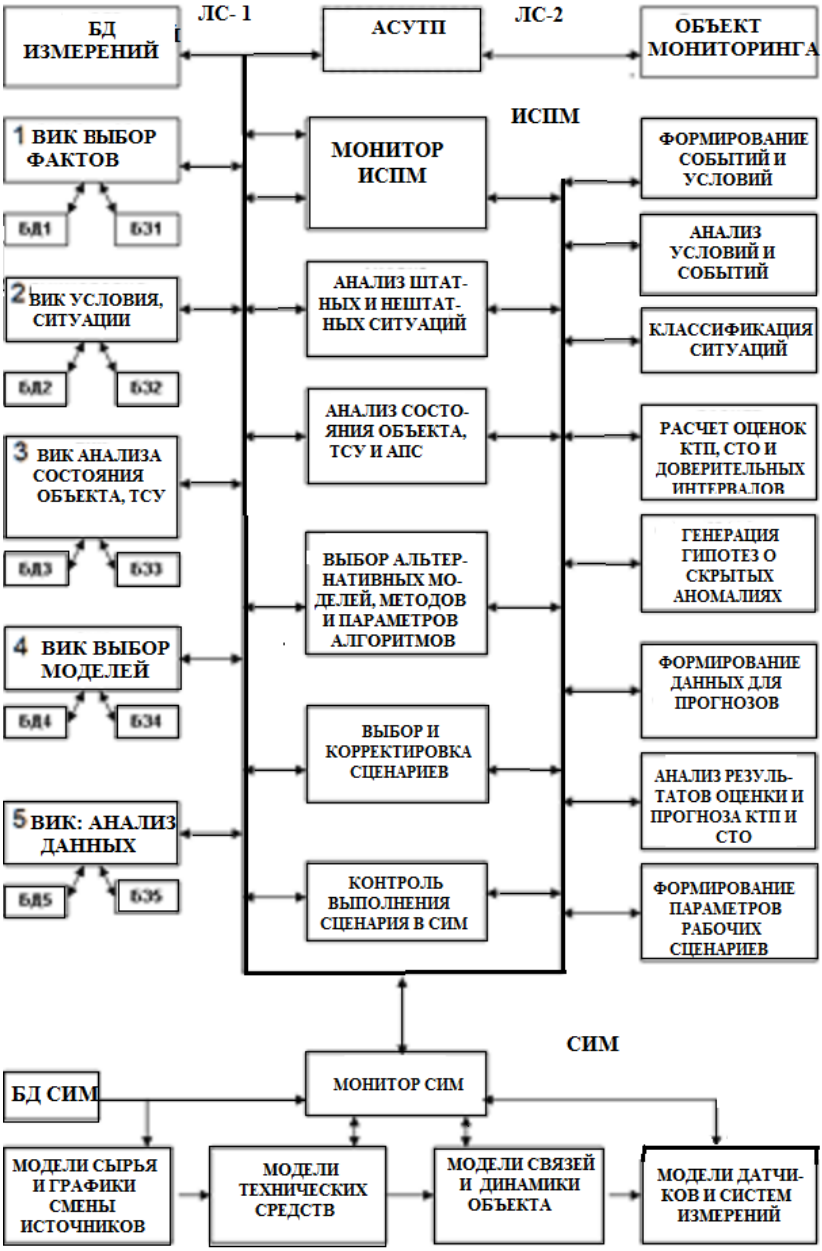


Рисунок 2 – Функциональная блок-схема ИСПМ

Литература:

1. *Рассел С., Норвиг П.* Искусственный интеллект: современный подход, 2-ое изд. – М.: Изд. дом «Вильямс», 2007. – 1408 с.

2. *Чинакал В.О.* Создание систем усовершенствованного мониторинга и управления для повышения эффективности и безопасности управления сложными промышленными объектами / Материалы XXIX Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС-2021). Москва, 15 декабря 2021 г. – М.: ИПУ РАН, 2021. – С. 493-499.

3. *Чинакал В.О.* Применение интеллектуальных средств в системе мониторинга распределенного промышленного объекта / Материалы пятой международной конференции «Управление развитием крупномасштабных систем» (MLSD'2011). – М.: ИПУ РАН, 2011. – С. 386-389.

4. *Чинакал В.О.* Проектирование систем управления подвижными объектами с использованием встраиваемых интеллектуальных компонентов / Труды 14-й Международной конференции «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта» (CAD/CAM/PDM-2014, Москва). – М.: ООО «Аналитик», 2014. Т.1. – С. 141-145.

5. *Чинакал В.О.* Разработка и применение встраиваемых интеллектуальных компонентов, построенных с использованием матричных методов. Труды 8-й Международной научно-практической конференции «Инженерные системы-2015». – М.: Издательство РУДН, 2015. Т.1 – С. 145-150.

6. *Чинакал В.О.* Проектирование виртуальных анализаторов с использованием альтернативных моделей / Труды 17 международной научно-практической конференции «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта (CAD/CAM/PDM – 2017, Москва)». – М.: ИПУ РАН, 2017. – С. 364-357.

DOI: 10.25728/iccss.2022.38.82.067

Черняев М.Д.

Итеративные подходы к анализу риска и система EBIOS

Аннотация: Цель работы заключается в рассмотрении особенностей итеративного подхода к анализу риска на примере французской системы EBIOS. В ходе работы представлен пример использования данной системы и описан ее инструментарий. Это позволяет сделать выводы об удобности и области применения системы EBIOS, а также о рациональности применения итеративного подхода в целом. При анализе использовались ресурсы, находящиеся в открытом доступе. С помощью данных ресурсов был создан типовой пример, призванный продемонстрировать эффективность метода.

Ключевые слова: риск, анализ, безопасность, итеративный, сценарии, кибератака, экосистема

Введение

В данной работе проводится исследование и тестирование системы анализа риска EBIOS. В настоящее время качественная оценка риска необходима для надежного функционирования любой информационной системы. Существует значительное количество методик, призванных упростить и систематизировать процесс оценки рисков, однако в данной работе предлагается ознакомиться конкретно с принципами работы системы EBIOS.

В результате проведенного исследования будет продемонстрирована работа пяти этапов EBIOS и доказана эффективность данной системы.

Объект исследования – организация, нуждающаяся в защите.

Предмет исследования – система анализа риска EBIOS.

Данная система очень мало изучена в современных исследованиях из-за ее относительной новизны и достаточно локального использования на территории франкоговорящих стран.

Обзор метода

EBIOS Risk Manager (EBIOS RM) – это метод оценки и обработки цифровых рисков, опубликованный национальным агентством кибербезопасности Франции (ANSSI) при поддержке Club EBIOS. Он обеспечивает набор инструментов, который можно адаптировать, использование которого варьируется в зависимости от цели проекта и который совместим с действующими эталонными стандартами с точки зрения управления рисками, а также с точки зрения кибербезопасности.

EBIOS RM позволяет оценивать цифровые риски и определить меры безопасности, которые необходимо предпринять для их контроля. Это также позволяет подтвердить приемлемый уровень риска и в долгосрочной перспективе придерживаться подхода непрерывного улучшения. Наконец, этот метод позволяет использовать ресурсы и аргументы, полезные для общения и принятия решений внутри организации и в отношении ее партнеров.

Метод EBIOS RM можно использовать для нескольких целей:

- создание или укрепление процесса управления цифровыми рисками в организации;
- оценка и обработка рисков, связанные с цифровым проектом, в частности, с целью аккредитации безопасности;
- определение уровня безопасности, который должен быть достигнут для продукта или услуги, в соответствии с его вариантами использования и рисками, которым необходимо противодействовать, как то, с точки зрения сертификации или аккредитации.

Это применимо как к государственным, так и к частным организациям, независимо от их размера, сферы деятельности и того, разрабатываются ли их информационные системы или уже существуют.

Также стоит отметить, что инструментарий EBIOS находится в открытом доступе и распространяется бесплатно, что делает систему доступнее. Минусом является то, что на данный момент EBIOS поддерживает только французский язык, однако разработчики недавно упоминали, что планируют перевод на английский.

Подход пяти шагов

Метод EBIOS Risk Manager использует подход к управлению цифровыми рисками, начиная с самого высокого уровня (основные

задачи изучаемого объекта) и постепенно доходя до бизнес- и технических функций путем изучения возможных сценариев риска. Он направлен на вырабатывание синтеза между «соблюдением требований» и «сценариями», размещая эти два взаимодополняющих подхода так, чтобы максимизировать их эффективность.

Подход на основе соответствия используется для определения базовых требований безопасности, на которых основан подход для разработки узконаправленных или комплексных сценариев риска. Это предполагает, что случайные риски и риски окружающей среды априори обрабатываются с помощью подхода, основанного на соблюдении базовых требований безопасности. Исходя из этого, оценка рисков с помощью сценариев, описанных методом EBIOS, фокусируется на преднамеренных угрозах.

EBIOS – это метод, который можно адаптировать. Он представляет собой удобный набор инструментов, из которого выполняемые действия, их уровень детализации и их последовательность легко адаптировать под желаемый метод использования. Способ применения метода различается в зависимости от изучаемого предмета, ожидаемых результатов, степени изученности периметра исследования или сектора, к которому он применяется. Итеративность метода выражается в том, что некоторые его этапы подразумевают постоянное обновление путем повторного анализа и дополнения данных.

Шаг 1: Область действия и базовые требования безопасности

Первый шаг направлен на определение изучаемого объекта, участников семинаров и временных рамок. В течение этого шага перечисляются миссии, бизнес-активы и вспомогательные активы, связанные с изучаемым объектом.

Определяются опасные события, связанные с бизнес-активами, и оценивается серьезность их последствий. Также определяются базовые требования безопасности и дифференциал.

Шаг 1 позволяет следовать подходу «соблюдение требований», соответствующему первым двум этапам пирамиды управления цифровыми рисками, и рассматривать исследование с точки зрения «защиты».

Шаг 2: Источники рисков

На втором шаге определяются и характеризуются источники риска (ИР) и их цели высокого уровня, называемые целевыми задачами (ЦЗ). В конце этого семинара выбираются наиболее подходящие пары ИР/ЦЗ. Результаты формализуются в составлении карты источников риска.

Шаг 3: Стратегические сценарии

На шаге 3 получается четкое представление об экосистеме и налаживается картографирование цифровой угрозы последней по отношению к изучаемому объекту.

Это позволяет создавать высокоуровневые сценарии, называемые стратегическими сценариями.

Они представляют собой пути атаки, которые источник риска может использовать для достижения своей цели. Эти сценарии разрабатываются в масштабе экосистемы и бизнес-активов изучаемого объекта. Их оценивают по степени тяжести.

В конце этого шага вы уже можете определить меры безопасности в экосистеме.

Шаг 4: Сценарии операций

Целью шага 4 является создание технических сценариев, включающих методы атаки, которые, вероятно, будут использоваться источниками риска, для реализации стратегических сценариев. На этом шаге используется подход, аналогичный подходу предыдущей секции, но основное внимание уделяется критически важным вспомогательным активам. Затем оценивается уровень вероятности воплощения в жизнь полученных операционных сценариев.

Примечания: Данные шагов 3 и 4 естественным образом пополняются во время последовательных итераций.

Шаги 2, 3 и 4 позволяют оценить риски, что составляет последний этап пирамиды управления цифровыми рисками. Они используют базовые требования безопасности в соответствии с различными путями атак, которые напрямую исходят из рассматриваемых угроз и число которых ограничено для облегчения анализа.

Шаг 5: Обработка рисков

Последний шаг заключается в составлении сводки всех изученных рисков для определения стратегии обработки рисков. Последняя затем разбивается на конкретные меры безопасности, записанные в план непрерывного усовершенствования. В ходе этого шага составляется сводка остаточных рисков и определяется основа для мониторинга рисков.

Заключение

В результате проведения анализа рисков с помощью EBIOS RM была создана картина рисков и предложены сценарии их контроля и предотвращения.

В данной работе было проведено исследование и тестирование системы анализа риска EBIOS.

В результате проведенного исследования была продемонстрирована работа пяти этапов EBIOS и доказана эффективность данной системы.

Благодаря находящемуся в открытом доступе инструментарию и интуитивно понятной навигации, система управления риском EBIOS является удобным инструментом для поддерживания безопасности информационной системы.

Литература:

1. Wissam Abbass, Amine Baina, Mostafa Bellafkih. Using EBIOS for risk management in critical information infrastructure – 5th World Congress on Information and Communication Technologies (WICT) Year: 2015 Conference Paper Publisher: IEEE. – URL: https://ieeexplore.ieee.org/document/7489654 (дата обращения 9.10.2022).

2. Application of EBIOS for the risk assessment of ICT use in electrical distribution sub-stations John Mcdonald; Nouha Oualha; Armaud Puccetti; Artur Hecker; Frederic Planchon 2013 IEEE Grenoble Conference Year: 2013 Conference Paper Publisher: IEEE. – URL: https://ieeexplore.ieee.org/document/6652221 (дата обращения 11.10.2022).

3. Berrehili Fatima Zahra, Belmekki Abdelhamid Risk analysis in Internet of Things using EBIOS 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC). – URL: (дата обращения 12.10.2022).

4. Hicham Elachgar; Boubker. Information security, new approach Regragui Second International Conference on the Innovative Computing Technology (INTECH 2012) Year: 2012 Conference Paper Publisher: IEEE Cited by: Papers (2). – URL: https://ieeexplore.ieee.org/document/6457815 (дата обращения 13.10.2022).

5. Omar EL IDRISSI; Abdellatif MEZRIOUI; Abdelhamid BELMEKKI. A lightweight risk analysis of a critical infrastructure based ICSs 2019 1st International Conference on Smart Systems and Data Science (ICSSD) Year: 2019 Conference Paper Publisher: IEEE. – URL: https://ieeexplore.ieee.org/document/9002902 (дата обращения 14.10.2022).

DOI: 10.25728/iccss.2022.65.55.068

Кафидов В.В.

Стратегия и тактика управления для безопасности народного хозяйства

Аннотация: В работе предлагается механизм создания системы управления экономикой на переходный период.

Ключевые слова: двойная структура управления, рынок, план, прибыль как средство, оценка эффективности

В результате поиска в интернете заголовки статей звучат как плановая и рыночная экономика, более того, объясняют, почему рыночная экономика лучше, чем плановая. На самом деле говорить как о рыночной экономике, так и о плановой экономике в чистом виде, госплане в существующих условиях бессмысленно, тем более без идеологических посылов.

Нужно понимать существующие и изменяющиеся потребности народного хозяйства и возможности их удовлетворения. Учитывая санкции и потребности в импортозамещении, потребности проведения специальной военной операции нужно удовлетворять существующий спрос и думать о развитии. Необходимо сочетать стратегические и тактические цели. Для этого могут быть сформированы две ветви управления не только экономическим развитием, но и развитием культуры, образования, здравоохранения,

всего, что мы раньше называли народным хозяйством: восстановить дефицит, существующий сегодня и делать задел на завтра (по мнению П.Друкера, это значит, что нужно сделать сегодня, чтобы получить результат в будущем).

В сложившейся ситуации потребность в перестройке системы управления экономикой становится очевидным. Оказалось, что рынок не может быть эффективным инструментом не только экономически, но и социально без участия государства. Рынок должен только расширять возможности государственного управления по привлечению организаций и отдельных предпринимателей к решению насущных и перспективных проблем народнохозяйственного развития. А государственное управление должно отойти от своей традиционной громоздкой структуры и стать скорее аналитическим центром, организатором и координатором деятельности в параллельных направлениях устранения дефицита и стратегического развития. Этим обеспечивается социально-экономическая безопасность.

Под безопасностью понимается состояние защищенности объекта защиты от опасностей среды. Безопасность народного хозяйства как социально-экономической системы зависит от стратегии развития, от состояния динамического равновесия системы со средой. При этом учитываются опасности внешней и внутренней среды системы. Учитывая резкие изменения внешней среды, приходится регулировать развитие внутренней среды. Саморегуляции уже недостаточно и приходится прибегать к регулированию.

Современная позиция государства в создании условия для развития бизнеса и поддержки стартапов не дает желаемого результата.

Мало кто в нашей стране был заинтересован что-либо производить самостоятельно. Разработали, а в Китае или Гонконге пусть производят. Трудно конкурировать с иностранными производителями, поэтому никто не берется за решение крайне важных задач для отечественной экономики, когда можно купить за рубежом. Эта ситуация не изменилась. Цветы до сих пор везут из Голландии и Боливии, а не из подмосковного совхоза.

И раньше мы сталкивались с такой ситуацией, когда бизнесу выгоднее продавать нефтепродукты за рубеж, в то время, когда на

внутреннем рынке дефицит. В ситуации эпидемии мы столкнулись с тем, что бизнесу выгоднее продавать медицинские маски и оборудование в другие страны, когда в своей стране даже врачи на начальном этапе не были ими обеспечены. Фармацевтические компании заявляли, что им не выгодно производить дешевые жизненно важные лекарства, когда закупить их в других странах нет возможности – в условиях бедствия все оказались сами за себя.

В рыночных условиях «Бизнесмены, которые вкладываются в стартапы, очень рискуют, но, в то же время, имеют существенный стимул – вложившись в успешный проект, они получают прибыль гораздо более существенную, чем могли бы получить, вложившись в другие финансовые инструменты» [1]. Рыночная модель ставит на первое место прибыль, а это не всегда соответствует интересам государства и общества.

Соединить преимущества плановой и рыночной моделей экономики или предложить новую модель должны современные правительства сегодняшнего и завтрашнего дня. Должна измениться и система оценки деятельности этих правительств. Для «сегодняшнего» это уровень удовлетворения существующих потребностей граждан и организаций. Для «завтрашнего» – образ будущего и риски его достижения.

Методология показателей KPI получила широкое распространение, стала модной и потеряла смысл. А смысл нужно найти и задуматься, ведь еще Т. Питерс и Р. Уотермен писали, что финансовые показатели оказываются лучше у тех компаний, которые ставят перед собой качественные, а не количественные задачи. Необходимо при разработке критериев KPI иметь в виду образ, модель. При этом отдельные показатели могут изменяться в зависимости от текущих и стратегических задач.

Это оказалось трудным для понимания нашим амбициозным выпускникам, ориентированным на Запад, обученным по западным учебникам и верящим в безраздельные возможности математики и IT-технологий.

Возникает парадокс. Казалось бы, изучение математики должно развивать логику и абстрактное мышление у студентов. На деле же наших аналитиков и разработчиков методик оценки всего и всех во время обучения так напичкают математикой, что они перестают самостоятельно мыслить и не могут решить элементарные

логические задачки. Не все так просто и с IT. Крупнейшие специалисты в менеджменте и информатике сходятся во мнении о переносе внимания с T на I. Нужны смыслы.

Нужно сказать, что и те, кто учит, уже не пытаются вникнуть в смысл того, чему учат. Достаточно часто так называемые бизнес-тренеры дают задание своим слушателям разработать структуру своего предприятия. В качестве примера приводится структура, где главному инженеру подчинен отдел главного механика (самого главного механика нет), отдел главного энергетика (самого главного энергетика нет), директор сталелитейного комплекса (самого комплекса нет) и т.д. При этом нет понятия о том, чем на самом деле должен заниматься главный инженер и из каких подразделений состоит предприятие. И вот такой пример выдается как образец.

В представленных к защите научных работах очень часто приходится сталкиваться с утверждением, что в работе применен системный подход. Когда спрашиваешь автора, в чем смысл примененного системного подхода, чаще всего, разумного ответа не получается. А вместе с тем, системный подход – это не единственный, но достаточно эффективный инструмент для анализа структуры и системы управления организации. Непонимание элементарных принципов и методов управления, непонимание сущности системного подхода приводит к принятию ошибочных решений в социальной сфере и экономике страны. Одной из главных причин такого положения – современное образование, ориентированное не на знания и понимание, а на умение использовать существующие (главным образом западные) модели и алгоритмы. Современная подготовка специалистов (а теперь многие из них даже формально специалистами не считаются) и их ориентация на глобализм и либеральные ценности не ориентируют на решение оперативных и стратегических задач отечественной экономики. Ориентация только на прибыль, здесь и сейчас, «свежее решение», приводит к индивидуализму. Решаются проблемы, которые быстро принесут прибыль и не важно в какой стране, для какого народа.

Нужна новая идеология управления экономикой. Прибыль – результат, а не цель производства. Заграница нам не поможет, теперь это уже ясно. Нужно направленно создавать новые и использовать имеющиеся предприятия. Для этого нужно системно думать и

системно действовать, менять ориентацию системы образования, производства и всех сфер жизнедеятельности на отечественную идеологию.

Появилась робкая заявка на создание более совершенного механизма, пока в локальных масштабах, объединения рыночной и плановой моделей экономики.

Частная компания, Денис Ковалевич, взяли на себя такую роль. Но это риск и учёт интересов этой компании. Почему бы этот опыт, а скорее идею, модель, адаптированную к масштабам страны не принять государству. В чем смысл такой идеи.

Господин Денис Ковалевич говорит о конвейере предпринимателей. «Нам нужны не гении бизнеса, а обычные люди, готовые заниматься предпринимательским трудом… Каждый год мы создаем полтора десятка новых компаний и открываем несколько десятков предпринимательских позиций… для тех людей, которые способны к упорному труду, но не держат себя за прирожденных гениев бизнеса» [2].

Примеров создания творческих коллективов внутри организации можно привести большое количество. Хорошо известен опыт фирмы IBM, по созданию таких групп, которые они называли «дикие утки» и «независимые хозяйственные единицы»: «Люди, управляющие этими независимыми хозяйственными единицами, приходят сюда из самых разных отделов IBM, а во главе подразделений стоят ведущие руководители и административные работники. Они должны разрабатывать новые изделия и находить для них рынки сбыта. Желательно при этом, чтобы они брались за освоение самых сложных рынков сбыта, требующих максимального внимания и труда. В перспективе, по достижении этими подразделениями зрелости, они должны вливаться в общую организационную структуру компании» [3].

Правительство, его аналитический центр должен определить задачи, на решение которых создаются коллективы. Если это может делать частная компания, то почему не стимулировать создание десятка «Ковалевичей». Метод своей работы он описывает так: «Мы строим компании в дюжине новых индустрий и поэтому тратим совокупно сотни тысяч часов в год на анализ рынков и технологий. Мы регулярно покупаем и переносим в Россию глобальные технологии. Даже несмотря на санкции» [4].

Получается такой конвейер: правительство – «Ковалевичи» – Созданные ими компании – нанятые предприниматели – менеджеры. Создатели бизнеса и руководители производства не становятся собственниками, а возможно совладельцами или на каких-то еще условиях договора. Этот тезис звучит и в IBM и в Техноспарке. Целями создания таких предприятий может быть успешное и необходимое импортозамещение, производство жизненно важной продукции и обеспечение безопасности страны (кроме вооружения). В этом случае оценки дает не рынок, а потребности государства и общества.

В отличие от обычной работы со стартапами, в данном случае должны быть использованы новые подходы к оценке реализации проектов. В настоящее время отмечается, что «9 из 10 стартапов не достигают успеха. В 42 % случаев как раз потому, что не нужны рынку, поскольку не решают реальные проблемы пользователей» [5]. С точки зрения успешности бизнеса скорее всего это так. Но «не нужен рынку» и «не решают реальные проблемы пользователей» – это не очевидно с позиций государственного регулирования рынка. Возвращаясь к началу этой работы, следует еще раз подчеркнуть, что для решения рассмотренных проблем вполне возможно потребуется сформировать две ветви управления не только экономическим развитием, но и развитием культуры, образования, здравоохранения, всего народного хозяйства: восстановить дефицит, существующий сегодня и делать задел на завтра. Нужно сказать, что в теории и практике стратегического управления известна рекомендация использовать варианты так называемой двойной структуры, когда внедрение стратегии отделяется от оперативной деятельности. Нужна и новая идеология постановки целей и оценки эффективности их достижения.

Литература:

1. Как на самом деле инвесторы оценивают стартапы. – URL: https://www.medium.com/ стартап-джедай/как-на-самом-деле-инвесторы-оценивают-стартапы (дата обращения 01.06.2022).

2. Не стоит превращать предпринимателей в наемных менеджеров. – URL: https://iz.ru/news/650480 (дата обращения 01.06.2022).

3. *Роджерс Ф. Дж.* ИБМ. Взгляд изнутри: Человек – фирма –

маркетинг; Пер. с англ. / При участии Р.Л. Шука. – М.: Прогресс, 1990. – 280 с.

4. *Денис Ковалевич*. «Техноспарк»: «Нам нужны не гении бизнеса, а обычные люди, готовые заниматься предпринимательским трудом». – URL: https://incrussia.ru/understand/denis-kovalevich-tehnospark-nam-nuzhny-ne-genii-biznesa-a-obychnyelyudi-gotovye-zanimatsya-predprinimatelskim-trudom/ (дата обращения 01.06.2022).

5. The Top 20 Reasons Startups Fail. – URL: https://www.cbinsights.com/research/startupfailure-reasons-top (дата обращения 01.06.2022).

DOI: 10.25728/iccss.2022.79.40.069

Панасенко А.В., Васильев М.А.

Анализ физико-химических свойств аэрозолей, предназначенных для тестирования пожарных извещателей

Аннотация: В работе рассмотрены и проанализированы физико-химические свойства аэрозолей, предназначенных для проверки дымовых пожарных извещателей. Анализ выявил, что в составе каждого образца присутствуют различные вещества, воздействующие на людей. Итогом исследования является сводная таблица с основными характеристиками рассматриваемых аэрозолей.

Ключевые слова: безопасность, извещатель пожарный, дымовые аэрозоли, состав, физико-химические свойства, дым

По статистическим данным Государственного доклада [1], индивидуальный риск гибели при пожарах за последние годы вырос. Дабы не допускать этого, существует необходимость усовершенствования систем пожарной автоматики.

Согласно данным доклада [2] доктора технических наук Евгения Мешалкина, 86 % смертей при возникновении пожара, происходят до прибытия пожарных подразделений и только 5% в ходе его ликвидации. В данном случае важную роль играет быстрое и правильное срабатывание пожарных извещателей. К примеру, дымовой пожарный извещатель реагирует на появление в воздухе

продуктов горения и определяет наличие возгорания. Данный извещатель сообщает людям о пожаре. Именно поэтому очень важно системы пожарной сигнализации содержать в надлежащем состоянии.

Для мониторинга работоспособности таких приборов применяют различные подходы. С начала осени 2021 года в силу вступил ГОСТ Р 59638-2021. В этом документе предлагается для проверки дымовых пожарных извещателей использовать аэрозоли, имитирующие дым [3]. При внедрении такого нового подхода к проверке, возникает вопрос о безопасности применения подобных аэрозолей. Данный вопрос является актуальным в наши дни. Поэтому цель исследования – анализ физико-химических свойств аэрозольных составов. В ходе исследования были поставлены следующие задачи.

1. Изучить актуальные предложения на рынке.
2. Выделить сегмент наиболее востребованных аэрозолей.
3. Провести анализ паспортов безопасности.
4. Сделать вывод о безопасности использования аэрозолей.

Для решения поставленных задач был применен ряд методов научного исследования: постановка проблемы; поиск и сбор необходимой информации путем изучения литературы, НПА, статей ученых; анализ физико-химического состава тестовых аэрозолей; синтез полученных данных; формулирование выводов.

При изучении рынка продажи тестовых аэрозолей, был выделен перечень наиболее популярных марок среди потребителей: SOLO, SmokeSabre, CHEKKIT.

Первым был изучен аэрозоль Chekkit Smoke. В январе 2018 г. его сняли с производства [4]. Однако остатки со склада все еще можно встретить в продаже. В таблице 1 представлен внешний вид этикетки в разрезе и её перевод на русский язык.

Таблица 1 –Этикетка «Chekkit Smoke»

		
«CHEKKIT SMOKE» Тестер для извещателя Для функциональных испытаний дымовых извещателей Оборудование пожарной сигнализации Аэрозольный дым для тестирования извещателя Продукция, отвечающая требованиям UL*. *Underwriter Laboratories – наиболее авторитетное учреждение, занимающееся тестированием и оценкой безопасности в США. Не горюч Без CFCs (фреонов) Без силикона Без сложных эфиров Фталата Минимальное содержание: 150 мл – эффективный объем.	ВНИМАНИЕ – Ознакомьтесь с указаниями на этикете и с соответствующей литературой перед использованием данного продукта – Емкость под давлением: защищать от солнечного света и не подвергать воздействию температуры, превышающей 50^0C – Не горюч – Однако содержимое может сгореть в необычных/экстремальных условиях пожара – Не более 15% по массе содержимого считаются легковоспламеняющимися – Не прокалывать и не сжигать, даже после использования – Не распылять на открытый огонь или раскаленный материал – Хранить емкость в прохладных хорошо вентилируемых местах – Не пускать детей (держите детей вне досягаемости) – Избегайть контакта с кожей и глазами	РУКОВОДСТВО ПО ПРИМЕНЕНИЮ – Хорошо встряхнуть перед применением – Удерживая вертикально, распылять на извещатель на расстоянии не менее 30 см (12 дюймов) и не более 1 м (40 дюймов) – Выпускать аэрозоль только 0,5-1 с, повторять каждые 10 с при необходимости – Если извещатель не реагирует, он может быть неисправен ИСПОЛЬЗОВАТЬ ТОЛЬКО В СООТВЕТСТВИИ С РУКОВОДСТВОМ Также доступно Полный спектр технических средств для испытания извещателей дыма, тепла и CO (моно оксид углерода), и средства технического

	– Использовать только в прохладных, хорошо вентилируемых зонах – Не следует преднамеренно вдыхать пары – Никакая ответственность не может быть признана за неправильное использование	обслуживания для полного соответствия функциональным требованиям и требованиям чувствительности

Однако, при анализе паспорта безопасности [5] становится ясно, что основными компонентами аэрозоля являются изопропанол и 1,1,1,2 тетрафторэтан. Первый компонент – это прозрачная, легко воспламеняющаяся жидкость с резким характерным запахом, её пары могут образовывать с воздухом взрывоопасные смеси, является опасной при вдыхании, пары вызывают раздражение слизистых оболочек и кожи. Второй компонент – газ под давлением, емкости которого могут взорваться при нагревании. Данные особенности необходимо знать сотрудникам, проверяющим работоспособность пожарных извещателей.

Одними из известных являются аэрозоли марки SOLO. Их существует большое разнообразие, в данном исследовании был изучен SOLO C3 (для проверки газовых ИП). Согласно данным дистрибьютора [5] этот аэрозоль не горюч. При изучении паспорта было выяснено, основной компонент аэрозоля – CO. Все опасности в паспорте зашифрованы в цифробуквенные обозначения. Их расшифровка гласит, что данный аэрозоль имеет следующие характеристики: воспламеняющийся газ под давлением; емкости могут взрываться при нагревании; острая токсичность при вдыхании; может нанести вред ребенку в утробе матери; вызывает повреждение органов в результате длительного или неоднократного воздействия. Из этого следует, что прежде, чем приступить к проведению тестирования, работник должен быть подготовлен и заранее должен знать и понимать все необходимые меры безопасности (таблица 2) [5].

Следующим тестируемым образцом явился аэрозоль марки SmokeSabre 01-001. Анализ паспорта безопасности [5] выявил, что основными компонентами являются бутан, пропан и этанол. Первые два – воспламеняющиеся газы под давлением, ёмкости которых

могут взрываться при нагревании выше 50 ^{0}C, при этом будет формироваться газовоздушное облако, как и у пропан-бутановых газовых баллонов. Третий элемент аэрозоля легковоспламеняющаяся жидкость – этиловый спирт. Таким образом, при смеси с кислородом воздуха все три компонента образуют взрывопожароопасную смесь. В данном случае при проведении тестирования персоналу необходимо применить все меры по предотвращению образования искр в проверяемых пожарных извещателях и в непосредственной близости от них.

На основе анализа паспортов безопасности исследуемых аэрозолей и научной литературы по опасности различных газовых составов были получены данные, представленные в таблице 2.

Таблица 2 – Основные физико-химические свойства тестовых аэрозолей

Наименование	CHEKKIT SMOKE	SOLO C3-001	SmokeSabre-01-001
Внешний вид			
Стоимость	1.802 руб.	2.624 руб.	2.645 руб.
Условия эксплуатации	держать вдали от источников тепла; не курить; обеспечить наличие подходящей вентиляции (не применять в плохо проветриваемых помещениях)	держать вдали от источников тепла, не курить; обеспечить наличие подходящей вентиляции; в условиях недостаточной вентиляции работать в респираторе.	не курить; обеспечить наличие подходящей вентиляции; не нагревать выше 50 ^{0}C; не применять для систем не обеспечивающих искробезопасность.
Негативное воздействие на персонал	опасен при вдыхании; ядовит при приеме внутрь; пары вызывают	взрывоопасен при нагревании; токсичен при вдыхании	при проверке извещателей образуется взрывопожарное

	раздражение слизистых оболочек и кожи; при контакте с раскаленными предметами образует высокотоксичные компоненты		газовоздушное облако
Физико-химические свойства	без цвета; с характерным запахом; аэрозоль, содержит в своем составе изопропилен и хладон 134а.	без цвета; без запаха; аэрозоль, содержащий в своем составе моно оксид углерода (угарный газ)	без цвета; с характерным запахом; аэрозоль, содержит в своем составе пропан-бутановую смесь с добавлением этанола

Проверка пожарных извещателей не считается проверяющими опасной процедурой, тем не менее, очевидно, что составы могут содержать высокотоксичные составляющие (моно оксид углерода), взрывопожароопасные или ядовитые компонента. Следует отметить, что все изделия данного иностранного производства и точный химический состав достоверно неизвестен.

Необходимо подготовить рекомендации по безопасному применению данного типа продукции, а в перспективе разработать национальный стандарт, регламентирующий требования безопасности к аэрозольным баллонам, применяемым при проверке пожарных извещателей различного типа.

Таким образом, тестирование пожарных извещателей – обязательная процедура в области пожарной безопасности, но при этом нельзя забывать и о других областях безопасности, а именно об охране труда и об экологии. Вот почему состав тестового аэрозоля должен быть безопасным. Полученные сведения могут быть полезны для дальнейшего, более детального изучения каждого состава. В качестве направления последующих исследований можно задаться целью разработки более безопасного состава по программе импортозамещения.

Литература:

1. Государственный доклад «О состоянии защиты населения и территорий Российской Федерации от чрезвычайных ситуаций

природного и техногенного характера». – URL: https://www.mchs.gov.ru/deyatelnost/itogi-deyatelnosti-mchs-rossii/2021-god (дата обращения 29.09.2022).

2. «На выставке Securika/MIPS обсудили пожарную безопасность в условиях надзорных реформ». Информационно-аналитический журнал «РУБЕЖ». – URL: https://ru-bezh.ru/news/2017/03/24/na-vyistavke-securika/mips-obsudili-pozharnuyu-bezopasnost-v-usl (дата обращения 02.10.2022).

3. ГОСТ Р 59638-2021. Национальный стандарт Российской Федерации. Системы пожарной сигнализации. Руководство по проектированию, монтажу, техническому обслуживанию и ремонту. Методы испытаний на работоспособность. – URL: https://docs.cntd.ru/document/1200180685 (дата обращения 02.10.2022).

4. CHEKKIT – спрей для проверки датчиков. Новости от detectortesters. – URL: https://www.nordtech.ru/noclimb.htm (дата обращения 03.10.2022).

5. Каталог тестового оборудования от DETECTORTESTERS. Аэрозоли, капсулы. – URL: https://www.detectortesters.ru/catalog/aerozoli_kapsuly/ (дата обращения 04.10.2022).

DOI: 10.25728/iccss.2022.80.92.070

Мусаев В.К.

Вычислительный эксперимент в задаче о моделировании взрывных воздействий в подвале десятиэтажного здания с упругой полуплоскостью

Аннотация: Приводится информация о математическом (компьютерном) моделировании нестационарных взрывных волн в подвале десятиэтажного здания с основанием в виде упругой полуплоскости. Разработана методика и алгоритм. Создан комплекс программ. При разработке комплекса программ использовался алгоритмический язык Фортран-90. Решена задача о компьютерном (цифровом) моделировании нестационарных взрывных волн в подвале

десятиэтажного здания с упругим основанием в виде полуплоскости.

Ключевые слова: волновая теория взрывной безопасности; вычислительный эксперимент, комплекс программ Мусаева В.К., взрывное воздействие, треугольный импульс, контурные напряжения, подвал, десятиэтажное здание

Приведенные исследования в рассматриваемой научной работе являются продолжением ранее полученных результатов. Такой подход к исследованию новых задач, которые опираются и продолжают предыдущие результаты, можно выполнять, если изначально была принята постановка и реализация задач с использований методов фундаментальной науки. Этот выбор можно было сделать благодаря применению методов вычислительной механики деформируемых тел (вычислительная механика) с возможностями языков программирования и вычислительным машин.

Составлен комплекс программ для решения нестационарной динамической задачи теории упругости для областей разной (сложной) формы. В работе приводится компьютерное (цифровое) решение задачи о моделировании нестационарных взрывных волн в подвале десятиэтажного здания с упругой полуплоскостью. Применяется методика неотражающих граничных условий.

Некоторые вопросы в области моделирования нестационарных динамических задач рассмотрены в следующих работах [1-6].

В работах [2-3, 5-6] приведена информация о верификации моделирования нестационарных волн напряжений в деформируемых телах с помощью рассматриваемого численного метода, алгоритма и комплекса программ.

Приближенное значение уравнения движения в теории упругости приведено в следующих работах [2-6]. В работах приведена информация о явной двухслойной схеме [2-6]. Шаг по времени для устойчивости явной двухслойной схемы для внутренних и граничных узловых точек на квазирегулярных сетках приведен в следующих работах [2-6].

Рассматриваемая задача впервые решена Мусаевым В.К. с помощью разработанной методики, алгоритма и комплекса программ [2-6].

Расчеты проводились при следующих единицах измерения: килограмм-сила (кгс); сантиметр (см); секунда (с).

Рассматривается задача о воздействии взрывной волны в виде треугольного импульса (дельта функция) в подвале десятиэтажного здания с упругим основанием (рисунки 1, 2). Начальные условия приняты нулевыми.

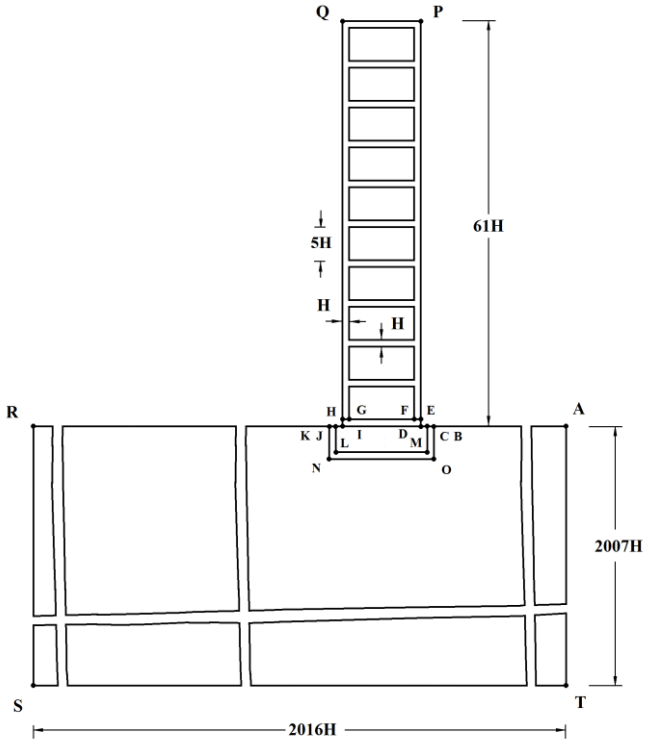


Рисунок 1 – Постановка задачи для десятиэтажного здания с подвалом и упругим основанием в виде полуплоскости. Схема В.К. Мусаева

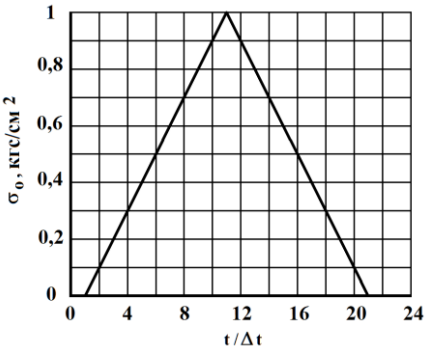


Рисунок 2 – Воздействие в виде треугольного импульса.
График В.К. Мусаева

Начальные условия приняты нулевыми. По нормали к контуру DJLM приложено нормальное напряжение σ_n (рисунок 3), которое при $1 \le n \le 11$ ($n = t/\Delta t$) изменяется линейно от 0 до P, а при $11 \le n \le 21$ от P до 0 ($P = \sigma_0$).

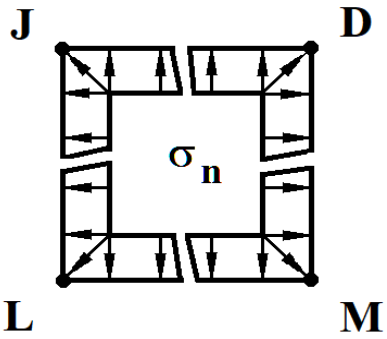


Рисунок 3 – Взрывное воздействие по контуру подвального этажа.
Схема В.К. Мусаева

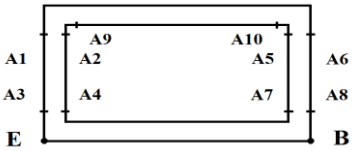


Рисунок 4 – Точки, в которых получены упругие напряжения во времени. Схема В.К. Мусаева

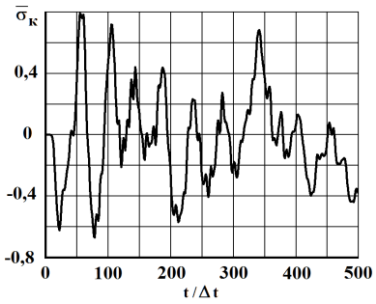


Рисунок 5 – Изменение упругого контурного напряжения $\overline{\sigma}_k$ в точке А1 на контуре десятиэтажного здания во времени $t / \Delta t$. График В.К. Мусаева

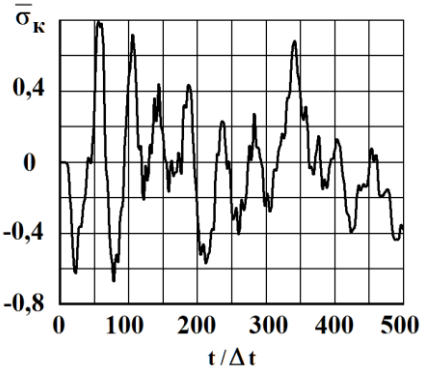


Рисунок 6 – Изменение упругого контурного напряжения $\overline{\sigma}_k$ в точке А6 на контуре десятиэтажного здания во времени $t / \Delta t$. График В.К. Мусаева

На контуре JD приложено нормальное напряжение σ_y ($\sigma_y = \sigma_0$, $\sigma_0 = 0{,}1$ МПа (1 кгс/см^2)). На контуре LM приложено нормальное напряжение σ_y ($\sigma_y = \sigma_0$, $\sigma_0 = -0{,}1$ МПа (- 1 кгс/см^2)). На контуре DM приложено нормальное напряжение σ_x ($\sigma_x = \sigma_0$, $\sigma_0 = 0{,}1$ МПа (1 кгс/см^2)). На контуре JL приложено нормальное напряжение σ_x ($\sigma_x = \sigma_0$, $\sigma_0 = -0{,}1$ МПа (- 1 кгс/см^2)). Граничные условия для контура *RSTA* при $t > 0$ $u = v = \dot{u} = \dot{v} = 0$. Отраженные волны от контура *RSTA* не доходят до исследуемых точек при $0 \le n \le 500$.

При расчетах приняты следующие исходные данные: $H = \Delta x = \Delta y$; $\Delta t = 2{,}788 \cdot 10^{-6}$ с; $E = 3{,}15 \cdot 10^4$ МПа ($3{,}15 \cdot 10^5$ кгс/см^2); $\nu = 0{,}2$; $\rho = 0{,}255 \cdot 10^4$ кг/м^3 ($0{,}255 \cdot 10^{-5}$ кгс с^2/см^4); $C_p = 3587$ м/с; $C_s = 2269$ м/с.

Решается система уравнений из 16202276 неизвестных.

Контурное напряжение $\overline{\sigma}_k$ получено в точках *A*1-*A*10 (рисунок 4). В точках *A*1 и *A*6 (рисунки 5, 6) показано изменение контурного напряжения $\overline{\sigma}_k$ в десятиэтажном здании с основанием в виде упругой полуплоскости во времени $t / \Delta t$.

Выводы

1. На основе метода конечных элементов (компьютерное моделирование) разработан комплекс программ для решения линейных волновых задач.

2. Линейная динамическая задача с начальными и граничными условиями в виде дифференциальных уравнений в частных производных, для решения задач при волновых воздействиях, с помощью метода конечных элементов приведена к системе линейных обыкновенных дифференциальных уравнений с начальными условиями, которая решается по явной двухслойной схеме.

3. Десятиэтажное здание моделируется с упругим основанием в виде упругой полуплоскости. Взрывное воздействие моделируется в виде функции треугольного импульса (дельта функция). Решается система уравнений из 16202276 неизвестных.

4. Получены контурные напряжения в характерных точках исследуемого объекта (десятиэтажное здание с подвалом).

5. Профили контурных напряжений соответствуют симметрии конструкции и нагрузки при решении задачи переходного процесса при моделировании взрывных волн в подвале десятиэтажного здания с упругим основанием.

Литература:

1. *Ионов В.И., Огибалов П.М.* Напряжения в телах при импульсивном нагружении. – М.: Высшая школа, 1975. – 464 с.

2. *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.

3. *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.

4. *Мусаев В.К.* Математическое моделирование нестационарных упругих волн напряжений (переходной процесс) при воздействии (вертикальное сосредоточенное в виде треугольного импульса) на поверхность полуплоскости (задача Лэмба) // Геология и геофизика Юга России. – 2020. – № 4. – С. 164-174.

5. *Мусаев В.К.* Математическое моделирование нестационарных волн напряжений в деформируемых телах при ударных, взрывных и сейсмических воздействиях. – М.: Российский университет транспорта, 2021. – 629 с.

6. *Мусаев В.К.* Защита нарушенного авторского права (плагиат) в Пушкинском городском, Московском областном и Верховном Судах Российской Федерации. – М.: Российский университет транспорта, 2021. – 874 с.

DOI: 10.25728/iccss.2022.57.12.071

Шихалев Д.В.

Мониторинг противопожарного состояния объекта в режиме реального времени

Аннотация: Работа посвящена развитию области противопожарного мониторинга объекта защиты в режиме реального времени. Приводится критерий осуществления мониторинга поддержки принятия решений на основе критерия безопасной эвакуации. Представлены результаты оценки данного критерия в ходе компьютерного моделирования.

Ключевые слова: мониторинг, пожарная безопасность, поддержка принятия решений, эвакуация, режим реального времени

Обеспечение безопасности людей в здании является одной из составляющих системы обеспечения безопасности объекта. Несмотря на относительно небольшое снижение количества пожаров и погибших при пожарах в зданиях с торговых центров, числовые значения все еще высоки. Как показано в работе [1], руководитель организации (в том числе торгового центра) не в состоянии собственными силами, без привлечения профильных специалистов, оценить состояние безопасности его организации (объекта). В тоже время, существующий арсенал методов заблаговременного оценивания состояния уровня безопасности [2-6] трудно применим к решению поставленной задачи без предварительной подготовки.

Одним из способов решения данной задачи является оценка состояния пожарной безопасности объекта на основе мониторинга уровня безопасности людей, концептуально изложенная в работе [7].

Базовым параметром мониторинга является критерий безопасной эвакуации (1), который определяется следующим выражением

$$P_{\text{э}} = \begin{cases} 0{,}999, \text{если } t_{\text{р}} + t_{\text{нэ}} \le 0{,}8 \cdot t_{\text{бл}} \text{ или } t_{\text{ск}} \le 6 \text{ мин} \\ 0, \text{если } t_{\text{р}} \ge 0{,}8 \cdot t_{\text{бл}} \text{ или } t_{\text{ск}} > 6 \text{ мин} \end{cases} \quad (1)$$

где $t_{нэ}$ – время начала эвакуации (сек.), $t_р$ – расчетное время эвакуации (сек.), $t_{бл}$ – время блокирования пути эвакуации (сек.), $t_{ск}$ – время существенного скопления людей (сек.).

Данный критерий мониторинга позволяют оценивать в динамическом режиме развитие пожара и эвакуации, учитывать количество людей и их распределение на объекте в рассматриваемый момент времени, ближайшие расстояние до эвакуационных выходов, ширину проходов, работу систем сигнализации и пожаротушения. Более подробное описание структурной схемы системы мониторинга приведено в работе [7]. На рисунке 1 показан алгоритм работы системы мониторинга противопожарного состояния объекта в режиме реального времени.

Предложенный алгоритм позволяет оценить необходимость тех или иных решений в зависимости от результата расчета критерия безопасной эвакуации. Безусловно, в текущей постановке он требует развития так как осуществляет поиск решений методом полного перебора. Однако так как область допустимых решений не так велика (не более 20), а ресурсы на вычисление занимают мало времени (не более 5 сек на один расчет), считаем это приемлемым.

Предложенный критерий и алгоритм оценены в ходе компьютерного моделирования, которое проведено на примере одного из этажей учебного корпуса Академии ГПС МЧС России. Здание оборудовано пожарной сигнализацией, системой оповещения и системой дымоудаления. В тоже время необходимо отметить важный аспект. Для здания посчитан пожарный риск, когда оно вводилось в эксплуатацию. Результаты расчета подтвердили, что здание безопасно в соответствии с действующим пожарным законодательством.

Оценка проведена путем сравнения значения критерия эффективной эвакуации при помощи предлагаемого подхода и без него. Сравнение проводилось при одинаковых начальных условиях. Принимаем допущение, что лицо принимающее решение строго следует указаниям информационной системы.

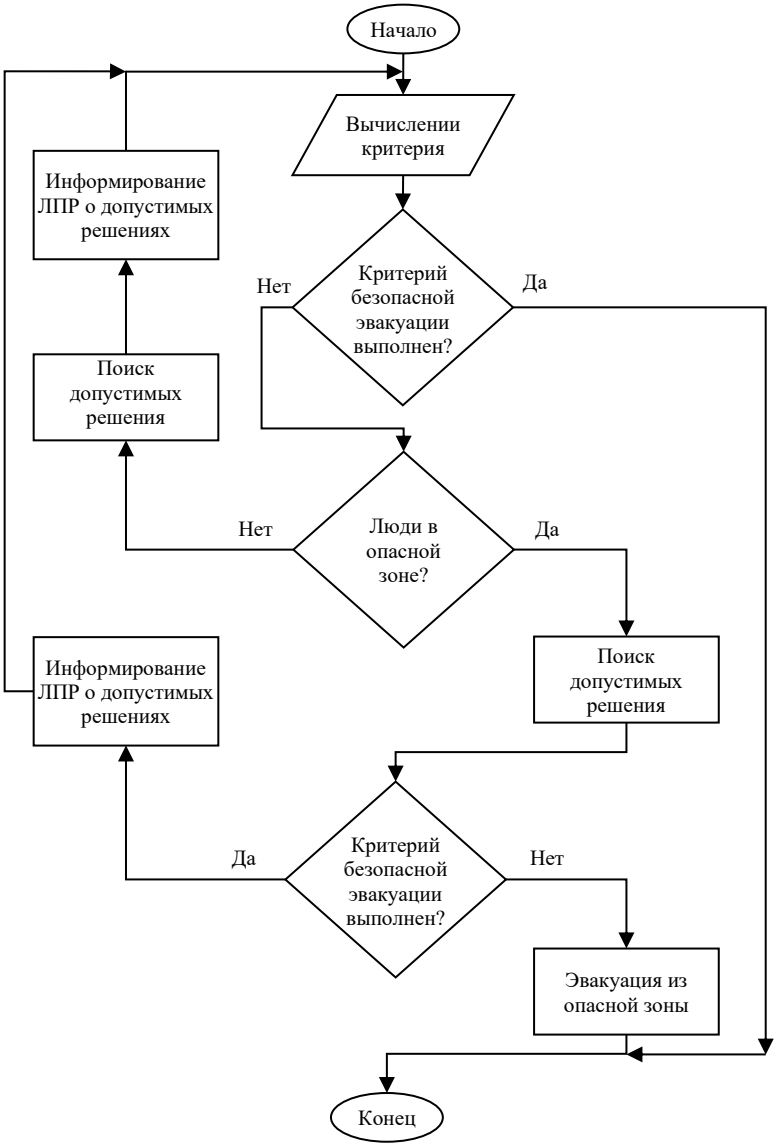


Рисунок 1 – Алгоритм работы системы мониторинга противопожарного состояния объекта

В рамках компьютерного моделирования рассматривался следующий сценарий – отказ датчика пожарной сигнализации. В одном из помещений произошел отказ датчика пожарной сигнализации.

Результаты без учета предлагаемого решения

Моделирование установило, что критерий безопасной эвакуации равен 0. При принятых условиях безопасность людей не обеспечивается. Это связано с поздним оповещением о пожаре из-за неработающего датчика пожарной сигнализации. Суммарное время эвакуации составило 129,6 сек.

Результаты с учетом предлагаемого решения

Повторное моделирование проведено с учетом предложенного подхода. Результаты моделирования показывают, что критерий безопасной эвакуации соответствуют значению 0,999 т.е. выполняются условия безопасной эвакуации. В качестве управленческого решения принято направление сотрудников охраны в помещение отказа датчика пожарной сигнализации. Благодаря этому при возникновении пожара время начала эвакуации равнялось 0, и эвакуация началась незамедлительно (без учета предлагаемого подхода составляла 90 сек.). Суммарное время эвакуации составило 39 сек. Таким образом, предложенный подход позволил обеспечить безопасную эвакуацию при возникновении пожара.

Целью настоящей работы являлось развитие области противопожарного мониторинга объекта защиты в режиме реального времени. Ряд научных исследований и статистические данные показывают, что пожары и гибель людей на них связана в основном с наличием проблем в области управления системой пожарной безопасности объекта. Анализ методов оценки пожарной безопасности показал, что имеются хорошо развитые способы оценки, однако они не применимы для руководителя объекта и не позволяют оценить пожарную опасность в режиме реального времени. В связи с этим предложен критерий мониторинга противопожарного состояния и алгоритм поддержки принятия решений на основе данного критерия. В ходе компьютерного моделирования подтверждена возможность не только оценивать пожарную безопасность в режиме реального времени, но и подбирать решения по повышению уровня безопасности.

Таким образом, предложенные решения показали свою применимость к рассматриваемой задаче и возможность поиска обоснованных управленческих решений по повышению безопасности в режиме реального времени. Все сомнений, данный подход требует развития в отношении модуля поддержки принятия решений, что и будет являться направлением дальнейших исследований.

Литература:

1. *Шихалев* Д. В. Проблемы управления системой обеспечения пожарной безопасности объекта. Ч.1. методы оценки // Проблемы управления. – 2022. – № 1. – С. 3-18.

2. *Кульба* В.В., *Шульц* В.Л., *Шелков* А.Б, *Чернов* И.В. Методы и механизмы планирования и управления в условиях чрезвычайных ситуаций // Тренды и управление. – 2013. – № 2. – С. 134-155.

3. *Шульц* В.Л., *Кульба* В.В., *Шелков* А.Б, *Чернов* И.В. Методы планирования и управления техногенной безопасностью на основе сценарного подхода // Национальная безопасность. – 2013. – № 2. – С. 198-216.

4. *Кульба* В.В., *Чернов* И.В. О методологических подходах к сценарному анализу сложных систем / Материалы международной конференции «Управление развитием крупномасштабных систем MLSD'2012». – М.: ИПУ РАН, 2012. – С. 82-87.

5. *Капашин* В.П., *Толстых* А.В., *Бурков* В.Н., *Назаров* А.В. Промышленная безопасность особо опасных химических объектов. – М.: ИПУ РАН, 2009. – 238 с.

6. *Титаренко* Б.П., *Бурков* В.Н. Оценка эффективности механизмов управления риском чрезвычайных ситуаций // Вестник МГСУ. – 2017. – № 5. – С. 581-585.

7. *Шихалев* Д. В. Оценка состояния пожарной безопасности объекта на основе мониторинга уровня безопасности людей // Проблемы техносферной безопасности: материалы международной научно-практической конференции молодых учёных и специалистов. – 2022. – № 11. – С. 217-221.

DOI: 10.25728/iccss.2022.68.87.072

Шихалев Д.В.

Метод управления системой обеспечения пожарной безопасности объекта

Аннотация: Работа посвящена развитию метода управления системой обеспечения пожарной безопасности объекта. Представлены основные этапы метода и проведено их описание по существу. Сформулирован подход к организации процесса управления системой обеспечения пожарной безопасности.

Ключевые слова: пожар, управление, организационная система, система обеспечения пожарной безопасности, метод

В работе [1] показано, что в ходе эксплуатации объекта, система обеспечения пожарной безопасности объекта (СОПБ) может переходить из одного состояния в другое, в зависимости от складывающейся обстановки. Результаты рассмотрения процессов принятия решений [2-3], возникающих в ходе управления СОПБ, установлено, что большинство из них нуждается в существенной модернизации. Исходя из проведенного анализа и рассмотрения процессов, определен рациональный порядок их исполнения. В соответствии с теорией управления [4-7], рассматриваем организацию как процесс, т.е. определяем как именно и в какой последовательности должно осуществляться управление системой обеспечения пожарной безопасности в организации.

Метод управления системой обеспечения пожарной безопасности объекта представляет собой последовательную реализацию лицом, принимающим решения (ЛПР) взаимосвязанных (по времени и логике) этапов, направленных на организацию (процесс) [4] управления системой пожарной безопасности в организации (организационная система). Компоненты метода показаны на рисунке 1. Рассмотрим представленный метод по существу.

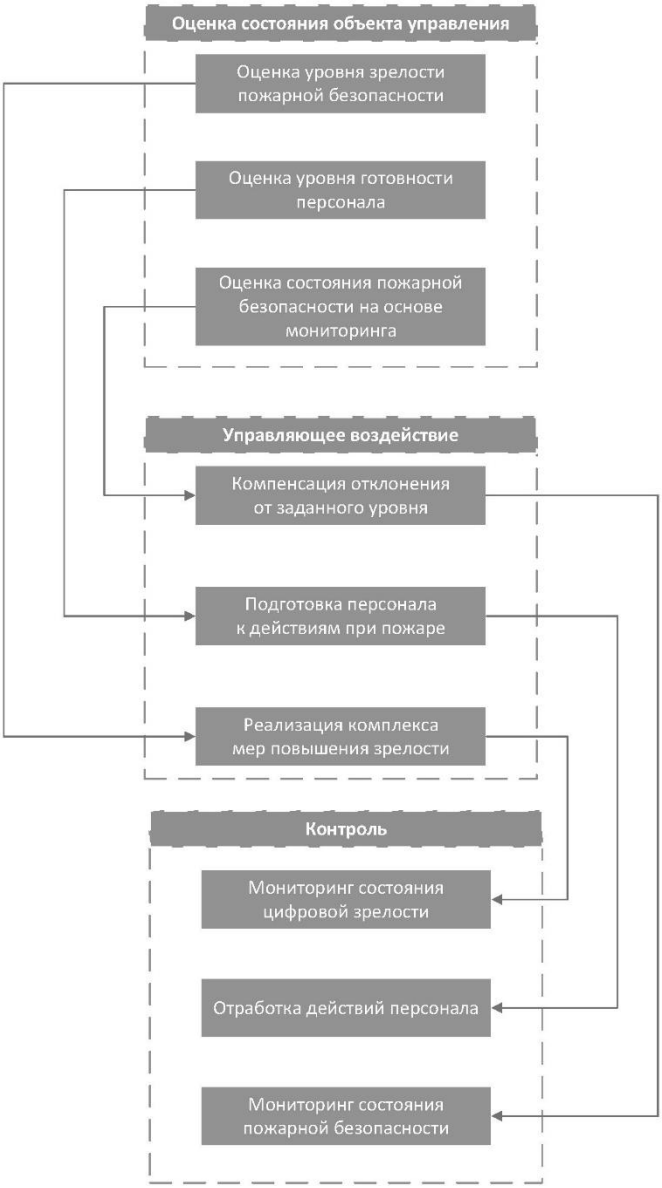


Рисунок 1 – Компоненты метода управления системой обеспечения пожарной безопасности объекта

Необходимо отметить, что данный метод отражает подход к организации управления на уровне функционирования «Нормальный режим». Однако шаги, реализуемые в данной методе, напрямую влияют на другие уровни функционирования (угроза пожара, управление эвакуацией, спасение на пожаре), а от их (шагов) реализации зависит эффективность функционирования системы обеспечении пожарной безопасности на соответствующем этапе.

С учетом представленных компонентов метода и его шагов, организация процесса управления системой обеспечения пожарной безопасности формулируется следующим образом.

1. Общая часть

Шаг 1. Определение уровня зрелости пожарной безопасности в организации.

На данном шаге на основании моделей и алгоритмов определяется уровень зрелости организации в области пожарной безопасности. Каждому уровню зрелости соответствует квалификационные признаки и комплекс мер для перехода на новый уровень зрелости. Комплекс мер содержит заранее подготовленные мероприятия, принятие и реализация которых позволит организации перейти на следующий уровень. Кроме того, предусматриваются качественные и количественные параметры для проведения соответствующего контроля.

Шаг 2. Оценка уровня готовности персонала объекта к действиям при пожаре.

На данном шаге на основании модели и алгоритма оценивается готовность персонала к действиям при пожаре. Действия персонала рассматриваются в контексте разных этапов функционирования СОПБ, в том числе для задач при: угрозе возникновения пожара; при организации и управлении эвакуацией; при взаимодействии с пожарно-спасательными подразделениями. Результатом данного шага является выявленный уровень готовности и комплекс мероприятия, направленных на совершенствование подготовки персонала.

Шаг 3. Мониторинга противопожарного состояния объекта с помощью специального программно-аппаратного комплекса.

На данном шаге с помощью метода, моделей и алгоритмов осуществляется мониторинга противопожарного состояния объекта

в режиме реального времени. Для ЛПР становится доступна количественная характеристика состояния пожарной безопасности здания (технических параметров, условий безопасной эвакуации, организационных мер), которая постоянно сравнивается с установленным (требуемым) значением. При отклонении состояния, предлагаются мероприятия по приведению текущего состояния к нормативному, путем реализации обоснованных (путем компьютерного моделирования) управленческих решений.

Шаг 4. Принятия управленческих решений.

Данный шаг реализуется по результатам каждого из *Шагов 1-3*, в рамках которых производится их подбор. В случае, если предлагаемое мероприятие не применимо для организации (доступно только для *Шага 3*), ЛПР может его изменить и выбрать иное, эффективность которого будет подтверждена путем компьютерного моделирования.

Шаг 5. Контроль реализации управленческих решений.

Данный шаг реализуется по результатам принятия решений в каждом из *Шагов 1-3*. Контроль мероприятий осуществляется с помощью автоматизированной информационной системы, ведущей специальный учет и реализацию *Шага 3*.

2. Специализированная часть

Специализированная часть шагов разработана на случай угрозы или возникновении пожара.

Все из вышеприведенных шагов является обязательным и выступают в качестве исходных (дополнительных) для специализированных шагов в случае угрозы или возникновения пожара.

Шаг 2.1. Действия персонала при угрозе возникновения пожара.

Данный шаг реализуется при срабатывании автоматической пожарной сигнализации. В этом случае, персонал объекта занимает позиции в здании и реализует определенную роль (алгоритм) в зависимости от начальных условий (определяемых автоматически по *Шагу 3*) и предварительно отрабатываемые в планах подготовки (определяемых по *Шагу 2*) в рамках тренировок по эвакуации.

Шаг 2.2. Управление эвакуацией людей при пожаре.

Данный шаг реализуется при подтверждении возникновения пожара в рамках по *Шагу 2.1*. В таком случае, с помощью модели и

алгоритмов поиска безопасных маршрутов движения во время эвакуации при пожаре, входящих в состав системы мониторинга (*Шаг 3*) определяются доступные эвакуационные маршруты движения на основе складывающейся ситуации, которые сообщаются персоналу и непосредственно реализуется им.

Шаг 2.3. Информационное обеспечение спасения людей на пожаре.

Данный шаг реализуется в случае, если в здании оказались заблокированы люди. В таком случае, с помощью модели и алгоритмов, входящих в состав системы мониторинга (*Шаг 3*) производится поиск безопасных маршрутов движения пожарно-спасательных подразделений. И, к моменту прибытия пожарно-спасательных подразделений, персонал объекта (определяемый по *Шагу 2*) информирует руководителя тушения пожара о рациональных маршрутах движения внутри здания к месту, где оказались заблокированы люди, о месте очага пожара, о ходе развития пожара и его особенностях.

Представленный метод управления системой обеспечения пожарной безопасности объекта позволяет подходить к решению задач организации процесса управления такой системой на более качественном уровне.

В ходе дальнейших исследований планируется детализация каждого из выше приведенных шагов метода, в частности, разработка моделей и алгоритмов для оценки зрелости организации в области пожарной безопасности и оценки готовности персонала к действиям при пожаре.

Литература:

1. *Шихалев Д.В*. Информационное обеспечение управления в системе обеспечения пожарной безопасности объекта защиты // Безопасность в техносфере: сборник статей. Выпуск 15. – Ижевск: Удмуртский университет, 2022. – С. 46-52.

2. *Шихалев Д.В.* Проблемы управления системой обеспечения пожарной безопасности объекта. Ч.1. методы оценки // Проблемы управления. – 2022. – № 1. – С. 3-18.

3. *Шихалев Д.В*. Проблемы управления системой обеспечения пожарной безопасности объекта. Ч.2. методы мониторинга // Проблемы управления. – 2022. – № 2. – С. 3-11.

4. *Новиков Д.А.* Методология управления. – М.: Либроком, 2011. – 128 с.

5. *Новиков Д.А*. Теория управления организационными системами. – М.: Ленанд, 2022. – 500 с.

6. Теория управления (дополнительные главы) / Под ред. Д.А. Новикова. – М.: Ленанд, 2019. – 552 с.

7. *Новиков Д.А.* Исследовательские принципы теории управления организационно-техническими системами / Труды 13 Международной конференции «Управление развитием крупномасштабных систем» MLSD'2020 (Москва, 28-30 сентября 2020 года). – Москва: ИПУ РАН, 2020. – С. 79-83.

DOI: 10.25728/iccss.2022.37.22.073

Фуругян М.Г.

Распределение памяти в многопроцессорной системе реального времени с нефиксированными параметрами

Аннотация: Рассматривается задача планирования вычислений в многопроцессорной системе реального времени для случая, когда длительности выполнения прикладных модулей линейно зависят от выделенной им дополнительной памяти. Определяется минимальный объем дополнительной памяти, при котором для заданного директивного срока существует допустимое расписание, а также минимальный директивный срок, для которого существует допустимое расписание при заданном объеме дополнительной памяти. Получены аналитические формулы для указанных величин.

Ключевые слова: многопроцессорная система реального времени, оптимальное расписание, нефиксированные параметры

Вычислительные системы реального времени находят применение в тех случаях, когда за короткий промежуток времени требуется выполнить определенные расчеты, иногда достаточно большого объемы. Такие задачи возникают при проектировании, испытаниях и функционировании сложных технических объектов,

как например, самолетов и ракет, электростанций, транспортных систем, конвейерных производств, во многих других областях. Вычислительные системы реального времени позволяют производить нужные расчеты к заданным срокам, что позволяет повысить безопасность работы указанных объектов.

Одна из основных задач вычислительных систем реального времени заключается в построении расписаний выполнения прикладных модулей, при котором каждый модуль успевает завершиться к установленному заранее директивному сроку. В работах [1-3] исследованы различные постановки таких задач и предложены методы их решения. В [4-6] задача планирования вычислений для многоядерной вычислительной системы реального времени решается с использованием обобщенных конечных автоматов и построенной на их основе имитационной модели. С помощью этой модели строится временная диаграмма, описывающая функционирование системы и позволяющая осуществить непосредственную проверку того, что каждая работа выполняется в заданном директивном интервале.

В настоящей работе рассматривается задача планирования вычислений в многопроцессорной системе реального времени для случая, когда длительности выполнения прикладных модулей линейно зависят от выделенной им дополнительной памяти. Кроме того, определяется минимальный объем дополнительной памяти, при котором для заданного директивного срока существует допустимое расписание, а также минимальный директивный срок, для которого существует допустимое расписание при заданном объеме дополнительной памяти. Получены аналитические формулы для указанных величин.

Постановка задачи. Требуется выполнить n программных модулей $W = \{1, 2, \ldots, n\}$ на m идентичных процессорах во временном интервале $[0; T]$. Все модули $i \in W$ допускают при их выполнении прерывания и переключения с одного процессора на другой. При этом временными издержками на прерывания и переключения можно пренебречь. Помимо процессоров каждому модулю $i \in W$ может быть выделена дополнительная память объемом v_i, которая закрепляется за этим модулем и другими модулями использоваться не может. Суммарный объем

дополнительной памяти равен V. При этом должны выполняться следующие ограничения

$$v_i \in [0; v_i^0], i = \overline{1, n}, \tag{1}$$

$$\sum_{i \in W} v_i \le V. \tag{2}$$

Длительность выполнения модуля i оставляет

$$t_i = t_i^0 - a_i v_i, \tag{3}$$

т.е. линейно зависит от объема выделенной этому модулю дополнительной памяти. Здесь v_i^0, t_i^0 и a_i – заданные положительные величины; v_i^0 – это максимальный объем памяти, который может быть выделен модулю i, t_i^0 – это длительность выполнения модуля i в случае, когда дополнительная память ему не выделяется. Предполагается, что $t_i^0 - a_i v_i^0 > 0$, $t_i^0 \le T$, $v_i^0 \le V$ при всех $i \in W$.

Требуется определить распределение дополнительной памяти, удовлетворяющее соотношениям (1), (2), и найти расписание, при котором каждый модуль $i \in W$ успевает полностью выполниться в директивном интервале $[0; T]$ (такое расписание будем называть допустимым), либо показать, что такого расписания не существует. Кроме того, необходимо найти а) минимальный объем дополнительной памяти $V_{\min}$, обеспечивающий для заданного директивного срока T существование допустимого расписания; б) минимальную величину директивного срока $T_{\min}$, при котором для заданного объема дополнительной памяти V допустимое расписание существует.

Решение задачи. В [1] доказано, что в рассматриваемом случае необходимым и достаточным условием существования допустимого расписания является выполнение неравенства

$$\sum_{i \in W} t_i \le mT. \tag{4}$$

В [1] также представлен алгоритм построения допустимого расписания для данного случая (алгоритм упаковки), имеющий линейную вычислительную сложность. Из (3), (4) следует, что в рассматриваемой постановке для существования допустимого расписания необходимо и достаточно существования распределения памяти v_i, $i \in W$, удовлетворяющего соотношениям (1), (2) и неравенству

$$\sum_{i \in W} (t_i^0 - a_i v_i) \le mT. \tag{5}$$

Перепишем (5) в следующем виде

$$\sum_{i \in W} a_i v_i \ge \sum_{i \in W} t_i^0 - mT. \tag{6}$$

Из неравенства (6) видно, что в первую очередь нужно выделять максимально возможный объем памяти модулям $i \in W$ с наибольшими значениями коэффициентов a_i с тем, чтобы минимизировать длительности их выполнения. Упорядочим работы W по не возрастанию величин a_i, $i \in W$, и пусть $a_1 \ge a_2 \ge \ldots \ge a_n$. Распределим память между модулями W по следующему простому алгоритму.

Алгоритм 1 (распределение памяти).

1) Инициализация: $i = 0$.

2) Вычислить: $i = i + 1$, $v_i = \min(v_i^0, V)$, $V = V - v_i$.

3) Если выполнены неравенства $V > 0$ и $i < n$, то перейти на шаг 2.

4) Если $V = 0$ или $i = n$, алгоритм завершает работу.

В результате работы этого алгоритма будут определены объемы памяти v_i и длительности t_i всех модулей $i \in W$, вычисленные согласно (3). В случае выполнения неравенства (6) допустимое расписание существует и строится с помощью алгоритма упаковки [1]. Если неравенство (6) нарушено, то это означает, что при данных входных параметрах допустимого расписания не существует. Предложенный алгоритм распределения

невозобновляемого ресурса, а также алгоритма упаковки имеют вычислительную сложность $O(n)$.

Для определения минимального объема памяти $V_{\min}$, при котором для заданного директивного интервала $[0;T]$ допустимое расписание существует, предлагается следующий алгоритм (алгоритм 2).

Алгоритм 2.

1) Если в случае, когда при $v_i = v_i^0$, $i = \overline{1,n}$, неравенство (6) не выполнено, то допустимого расписания не существует ни при каком значении V.

2) Если при $v_i = v_i^0$, $i = \overline{1,n}$, неравенство (6) выполнено, то обозначим через i_0 минимальный номер, при котором $\sum_{i=1}^{i_0-1} a_i v_i^0 < A$, $\sum_{i=1}^{i_0} a_i v_i^0 \geq A$, где $A = \sum_{i \in W} t_i^0 - mT$

3) Если $\sum_{i=1}^{i_0} a_i v_i^0 = A$ то $V_{\min} = \sum_{i=1}^{i_0} v_i^0$.

4) Если $\sum_{i=1}^{i_0} a_i v_i^0 > A$, то $V_{\min} = \sum_{i=1}^{i_0-1} v_i^0 + \frac{A - \sum_{i=1}^{i_0-1} a_i v_i^0}{a_{i_0}}$.

Определим теперь минимальный директивный срок $T_{\min}$, для которого при заданном значении R существует допустимое расписание. Из (6) следует, что

$$T_{\min} = \frac{1}{m} \min_{r_1,\ldots,r_n} \left(\sum_{i \in W} t_i^0 - \sum_{i \in W} a_i v_i \right) = \frac{1}{m} \left(\sum_{i \in W} t_i^0 - \max_{r_1,\ldots,r_n} \sum_{i \in W} a_i v_i \right) \qquad (7)$$

при выполнении соотношений (1), (2). Как было показано выше, максимум в (7) достигается при значениях $v_1, \ldots, v_n$, вычисляемых с помощью алгоритма 1. Отметим, что в [7] рассмотренные в данном разделе задачи были сведены к задачам линейного программирования с $\theta(n)$ переменными и $\theta(n)$ ограничениями.

Алгоритмы решения подобных задач являются более трудоемкими, чем предложенные в настоящей работе.

Литература:

1. *Танаев В.С., Гордон В.С., Шафранский Я.М.* Теория расписаний. Одностадийные системы. – М.: Наука, 1984. – 384 с.

2. *Brucker P.* Scheduling Algorithms. – Heidelberg, Springer, 2007 – 371 p.

3. *Лазарев А.А.* Теория расписаний. Оценка абсолютной погрешности и схема приближенного решения задач теории расписаний. – М.: МФТИ, 2008. – 222 с.

4. *Глонина А.Б., Балашов В.В.* О корректности моделирования модульных вычислительных систем реального времени с помощью сетей временных автоматов // Моделирование и анализ информационных систем. – 2018. – Т. 25. № 2. – С. 174-192.

5. *Глонина А.Б.* Обобщенная модель функционирования модульных вычислительных систем реального времени для проверки допустимости конфигураций таких систем // Вестник ЮУрГУ. Сер. Вычисл. математика и информатика. – 2017. – Т.6. № 4. – С. 43-59.

6. *Глонина А.Б.* Инструментальная система проверки выполнения ограничений реального времени для конфигураций модульных вычислительных систем // Вестник МГУ. Сер. 15. Вычисл. математика и кибернетика. – 2020. – № 3. – С. 16-29.

7. *Косоруков Е.О., Фуругян М.Г.* Некоторые алгоритмы распределения ресурсов в многопроцессорных системах. // Вестник МГУ. Сер. 15. Вычисл. математика и кибернетика. – 2009. – № 4. – С. 34-37.

Авторы

Plotnikov N.I.	SRPCAI “AviaManager”
Абдулова Е.А.	ИПУ РАН
Авдеева З.К.	ИПУ РАН
Асратян Р.Э.	ИПУ РАН
Ахромеева Т.С.	ИПМ им. М.В. Келдыша РАН
Байрамов О. Б.о.	ФИЦ ИУ РАН
Балакина Е.П.	РУТ (МИИТ)
Баранов Л.А.	РУТ (МИИТ)
Бестемьянов П.Ф	РУТ (МИИТ)
Богатырева Л.В	ИПУ РАН
Васильев М.А.	ФГАОУ ВО СПбПУ
Волгина О.А.	ИПУ РАН
Горелова Г.В.,	ИУС ЮФУ
Дашков Р.Ю.	ИНП РАН
Еременко В.А.	ИЗМИРАН
Еронин Д. А.	МФТИ
Жарко Е.Ф.	ИПУ РАН
Жубанов М.С.	РГУ НГ (НИУ) им. И.М. Губкина
Зорин В.А.	ИПУ РАН
Исхаков А.Ю.	ИПУ РАН
Исхакова А.О.	ИПУ РАН
Кадиев Ш.К.	АГПС МЧС России
Карпов С.Ю.	ФГБУ ВНИИПО МЧС РОССИИ
Кафидов В.В.	РАНХиГС при Президенте РФ
Кацко А.И.	КубГАУ
Кацко Д.И.	КубГАУ
Кловач Е.В.	ЗАО НТЦ ПБ
Коврига С.В.	ИПУ РАН
Козлов А.Д.	ИПУ РАН
Команич Н.В.	ИПУ РАН
Комков Н.И.	ИНП РАН
Кононов Д.А.	ИПУ РАН
Королев А.Д.	РУТ (МИИТ)
Краснов А.Е.	РГСУ
Кротова М.В.	ИНП РАН

Кулаков В.В.	Военная орденов Жукова и Ленина краснознаменная академия связи им. Маршала Советского Союза С.М. Буденного
Кульба В.В.	ИПУ РАН
Курако Е.А.	ИПУ РАН
Кураков В.А.	ВУНЦ ВВС «ВВА»
Лазарев А.А.	ИНП РАН
Лантер Н.Н.	ИНП РАН
Лепешкин О.М.	Инженерно-строительный институт Санкт-Петербургского Политехнического университета Петра Великого
Лещенко В.В.	ФГБУ НИИР
Лобанов И.А.	АГПС МЧС России
Логинова Л.Н.	РУТ (МИИТ)
Малинецкий Г.Г.	ИПМ им. М.В. Келдыша РАН
Манаенкова Н.И.	ИЗМИРАН
Меденников В.И.	ФИЦ ИУ РАН
Мелихов А.А.	ЗАО «Безант»
Мельник Д.М.	Акционерное общество Авиакомпания «РусДжет»
Мельник Э.В.	ЮНЦ РАН
Мистров Л.Е.	Центральный филиал ФГБОУ ВО «РГУП»
Мусаев В.К.	НИУ МГСУ
Ненашева Ю.А.	НИУ МИЭТ
Нога Н.Л.	ИПУ РАН
Орлов В.Л.	ИПУ РАН
Остроумов М.А.	Военная орденов Жукова и Ленина краснознаменная академия связи им. Маршала Советского Союза С.М. Буденного
Остроумов О.А.	Военная орденов Жукова и Ленина краснознаменная академия связи им. Маршала Советского Союза С.М. Буденного
Панасенко А.В.	ФГАОУ ВО СПбПУ

Промыслов В.Г.	ИПУ РАН
Прус М.Ю., ,	РАНХиГС
Прус Ю.В.	ВНИИ ГОЧС МЧС России
Пудовиков О.Е.	РУТ (МИИТ)
Рожнов А.В.	ИПУ РАН
Рыженко А.А.	Финансовый университет при Правительстве РФ
Саломатин А.А.	ИПУ РАН
Семенков К.В.	ИПУ РАН
Сидоренко В.Г.	РУТ (МИИТ)
Сидоренко И.А.	ВУНЦ ВВС «ВВА»
Силюнцев С.В.	ВУНЦ ВВС «ВВА»
Синюк А.Д.	ВАС им. С.М.Буденного
Сиротюк В.О.,.	ИПУ РАН
Скворцов О.Б.,	ИМАШ РАН
Сомов С.К.	ИПУ РАН
Сташенко В.И.	ИМАШ РАН
Степанцов М.Е.	ИПМ им. М.В. Келдыша РАН
Сутягин В.В.	ИНП РАН
Тарасов А.А.	ВАС им. С.М.Буденного
Тимиршаяхова Ю.В.	ИПУ РАН
Тимошенко А.А.	УП РФ
Ткаченко В.А.	ЗАО НТЦ ПБ
Торгашев Р.Е.	РГГУ
Торопыгина С.А.	ИПМ им. М.В. Келдыша РАН
Усманова Т.Х.	ИНП РАН
Фейзов В.Р.	ИПУ РАН
Фомичев А.Н.	РАНХиГС
Фуругян М.Г.	ФИЦ ИУ РАН
Хабибулин Р.Ш.	АГПС МЧС России
Ходнев Н.Д.	РГСУ
Цыганов В.В.	ИПУ РАН
Чеканов И.Р.	РГСУ
Чернов И.В.	ИПУ РАН
Чернов К.В.	ИГЭУ
Черняев М.Д.	ИПУ РАН
Чинакал В.О.	ИПУ РАН
Шагин Н.А.	МФТИ

Шелков А.Б.	ИПУ РАН
Шихалев Д.В.	АГПС МЧС России
Шульц В.Л.	ЦИПБ РАН

Сокращения

SRPCAI «AviaManager»	Scientific Research Project Civil Aviation Institute “AviaManager”
АГПС МЧС России	ФГБОУ ВО Академия Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий
ВАС им. С.М.Буденного	ФГКУВОУ ВПО «Военная академия связи им. Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации
ВНИИ ГОЧС МЧС России	Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России, федеральный центр науки и высоких технологий
ВНИИПО МЧС РОССИИ	ФГБУ «Всероссийский ордена «Знак Почета» научно-исследовательский институт противопожарной обороны» МЧС России
ВУНЦ ВВС «ВВА»	Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина»
ЗАО НТЦ ПБ	Закрытое акционерное общество «Научно-технический центр исследований проблем промышленной безопасности»
ИГЭУ	ФБГОУ ВО Ивановский государственный энергетический университет имени В.И. Ленина

ИЗМИРАН	ФГБУН Институт земного магнетизма, ионосферы и распространения радиоволн им. Н.В.Пушкова РАН
ИМАШ РАН	Институт машиноведения им. А.А. Благонравова РАН
ИНП РАН	Институт народнохозяйственного прогнозирования РАН
ИПМ им. М.В. Келдыша РАН	Институт прикладной математики им. М.В. Келдыша РАН
ИПУ РАН	ФГБУН Институт проблем управления им. В.А. Трапезникова РАН
ИУС ЮФУ	Институт управления в экономических, социальных и экологических системах Южного федерального университета
КубГАУ	ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина»
МФТИ	ФГАОУ ВО «Московский физико-технический институт (национальный исследовательский университет)»
НИУ МГСУ	Научно-исследовательский университет Московский государственный строительный университет
НИУ МИЭТ	ФГАОУ ВО «Национальный исследовательский университет «Московский институт электронной техники» (МИЭТ)
РАНХиГС при Президенте РФ	ФГБОУ Российская академия народного хозяйства и государственной службы при Президенте РФ

РГГУ	ФГБОУ ВО «Российский государственный гуманитарный университет»
РГСУ	ФГБОУ ВО «Российский Государственный Социальный Университет»
РГУ НГ (НИУ) им. И. М. Губкина	Российский государственный университет нефти и газа НИУ имени И.М. Губкина
РУТ (МИИТ)	ФГАОУ ВО «Российский университет транспорта»
УП РФ	ФГКОУ ВО Университет прокуратуры Российской Федерации
ФГАОУ ВО СПбПУ	ФГАОУ ВО Санкт-петербургский политехнический университет Петра Великого
ФГБУ НИИР	ФГБУ «Ордена Трудового Красного Знамени Российский научно-исследовательский институт радио им. М.И. Кривошеева»
ФИЦ ИУ РАН	Федеральный исследовательский центр «Информатика и управление» РАН
Центральный филиал ФГБОУ ВО «РГУП»	Центральный филиал ФГБОУ ВО «Российский государственный университет правосудия»
ЦИПБ РАН	ФГБУН Центр исследования проблем безопасности РАН
ЮНЦ РАН	Южный научный центр РАН

Научное электронное издание

ПРОБЛЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ

Материалы
XXX Международной научной конференции
(14 декабря 2022 г., Москва)

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

Локальное электронное издание
ꞁ tsdʒ tɕ ɕtsfʧ ɕɖfʧsʧ·ɥɖɖ ɘ ꞁ ʊʌ "ʀ ʣ tsʨʒʨ ɕɖfʧsʧ" 0322204178

Мин. системные требования:
Pentium 4; 1,3 ГГц и выше; Windows XP/7/8, Acrobat reader 4.0 и выше
Дата подписания к использованию 28.11.2022
1 электронно-оптический диск (CD-R), 10,0 Мб, Тираж 100 экз.

Федеральное государственное бюджетное учреждение науки
Институт проблем управления им. В. А. Трапезникова
Российской академии наук
117997, Москва,
ул. Профсоюзная, д. 65
http://www.ipu.ru